Click here to view PowerPoint presentation; Press Esc to exit

# Detection of Terrorist Preparations by an Artificial Intelligence Expert System Employing Fuzzy Signal Detection Theory

**Mark E. Koltko-Rivera, Ph.D.**
Director of Research
Professional Services Group, Inc.
P.O. Box 4914
Winter Park, Florida 32793-4914 USA

E-mail: mark@professionalservicesgroup.net

## *SUMMARY*

*Terrorist actions are often preceded by preparatory activities that are at least slightly anomalous compared to the activities of the general population (such as unusual purchasing patterns). Analysis of patterns of such anomalies will detect potential preparations for terrorist activity. However, each such anomaly is what is known technically as a "fuzzy signal": each anomaly taken individually might indicate terrorist preparations, but usually does not. This paper describes the hypothetical computer system FUSEDOT (FUzzy Signal Expert system for the Detection Of Terrorism preparations). As the name suggests, FUSEDOT applies artificial intelligence expert system technology to the fuzzy signals presented by certain anomalous data, such as interpersonal relationships, financial relationships, travel patterns, purchasing patterns, patterns of Internet usage, and personal background. The components of the system—data acquisition, data processing, report generation, and feedback and further system development—are described in outline. System limitations are described. FUSEDOT is compared with other systems for the analysis of massive amounts of data to detect terrorism, specifically the Novel Intelligence from Massive Data program, and the Terrorist Information Awareness program. In comparison with these programs, FUSEDOT will implement some superior technology, will be easier to develop, and poses fewer privacy concerns. NATO member nations would do well to consider the development of FUSEDOT, which can be a valuable asset in the defence against terrorism.*

## 1.0 INTRODUCTION

I should like to begin with a somewhat controversial proposition: Sometimes, a battle against terrorism can be won at the supermarket checkout counter. No doubt an explanation is in order.

It is well-known that the individual states comprising the United States of America have very different attitudes and policies concerning tobacco. Some of the states of the American Southeast—typically states that produce a good deal of tobacco—charge little tax for the sale of cigarettes. Other states may charge a fairly hefty sales or excise tax on cigarettes. Thus, recently, the State of Kentucky charged an excise tax of 3 U.S. cents per pack of cigarettes, while the State of New York charged an excise tax of US$1.50 per pack, or fifty times the rate charged in Kentucky [1].

This disparity has not gone unnoticed by organized crime rings, which have been known to purchase cigarettes in low-tax states and sell them in high-tax states, pocketing most of the tax differential as profit. Consequently, some of the low-tax states have instituted systems where special paperwork must be filed by individuals purchasing a number of cartons of cigarettes over some predetermined limit.

*Paper presented at the RTO SCI Symposium on "Systems, Concepts and Integration (SCI) Methods and Technologies for Defence Against Terrorism," held in London, United Kingdom, 25-27 October 2004, and published in RTO-MP-SCI-158.*

# Report Documentation Page

*Form Approved*
*OMB No. 0704-0188*

Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

| 1. REPORT DATE | 2. REPORT TYPE | 3. DATES COVERED |
|---|---|---|
| **25 OCT 2004** | **N/A** | **-** |

| 4. TITLE AND SUBTITLE | 5a. CONTRACT NUMBER |
|---|---|
| **Detection of Terrorist Preparations by an Artificial Intelligence Expert System Employing Fuzzy Signal Detection Theory** | 5b. GRANT NUMBER |
| | 5c. PROGRAM ELEMENT NUMBER |
| 6. AUTHOR(S) | 5d. PROJECT NUMBER |
| | 5e. TASK NUMBER |
| | 5f. WORK UNIT NUMBER |
| 7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Professional Services Group, Inc. P.O. Box 4914 Winter Park, Florida 32793-4914 USA** | 8. PERFORMING ORGANIZATION REPORT NUMBER |
| 9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) | 10. SPONSOR/MONITOR'S ACRONYM(S) |
| | 11. SPONSOR/MONITOR'S REPORT NUMBER(S) |

12. DISTRIBUTION/AVAILABILITY STATEMENT
**Approved for public release, distribution unlimited**

13. SUPPLEMENTARY NOTES
**See also ADM201977, Systems, Concepts and Integration Methods and Technologies for Defence against Terrorism (Systemes, concepts, methodes d'integration et technologies pour la luttre contre le terrorisme)., The original document contains color images.**

14. ABSTRACT

15. SUBJECT TERMS

| 16. SECURITY CLASSIFICATION OF: | | | 17. LIMITATION OF ABSTRACT | 18. NUMBER OF PAGES | 19a. NAME OF RESPONSIBLE PERSON |
|---|---|---|---|---|---|
| a. REPORT | b. ABSTRACT | c. THIS PAGE | | | |
| **unclassified** | **unclassified** | **unclassified** | **UU** | **46** | |

Not long ago in one low-tax state, North Carolina, the daily limit (at or above which special notice was taken of the purchaser) was a purchase of 300 or more cartons of cigarettes. At one large retailer in this state, a guard happened to notice that several individuals in one group each were consistently purchasing 299 cartons per visit. The guard notified law enforcement authorities, who conducted an investigation, and found that these individuals were purchasing cigarettes in North Carolina and selling them illegally in the high-tax state of Michigan—and then using the profits to fund the activities of a terrorist cell in Charlotte, North Carolina, affiliated with Hezbollah [2].

The point to note here is that the discovery of this terrorist cell began with someone noticing an anomaly, in this case, the purchase of an unusually large amount of an everyday commodity. There was nothing illegal about this anomaly in and of itself, but it raised an eyebrow. That eyebrow, in turn, prompted an investigation that uncovered preparations for terrorist activity.

In many cases, preparations for terrorist activities are attended by such anomalies, by which I mean activities that, although not illegal in and of themselves, are at least very slightly out of the ordinary. Here are a few examples:

- In preparation for the first World Trade Center bombing, in 1993, Mohammed Salameh rented a van in which to deliver the explosives to the targeted site. Nidal Ayyad acquired chemicals for the explosive. Both were affiliated with a house of worship dominated by an extremist cleric, the so-called "Blind Sheikh," who preached violence against the United States ([3], p. 72). To a greater or lesser extent, these activities were anomalies: purchasing chemicals, affiliating with an extremist house of worship, even renting a van. None of them are or should be illegal or prohibited in a democracy. However, were it possible to connect the dots presented here—van rental, plus chemicals, plus extremist preacher—then surely this conjunction of events could reasonably be termed a noteworthy occurrence.

- In preparation for the Oklahoma City bombing, in 1995, Timothy McVeigh and Terry Nichols rented a truck in which to deliver the explosives to the targeted site. They also purchased a total of over 5000 pounds (over 2200 kg) of ammonium nitrate fertilizer to process into explosive. Of this total, about 4000 pounds (over 1800 kg) were obtained in eight purchases spaced over several weeks. (Although McVeigh and Nichols split the purchases between themselves, they stayed in touch using a calling card that later would be traced back to McVeigh; [4], pp. 195-196, 247, 249). Here again, neither of these two sets of activities—renting a truck or purchasing large amounts of fertilizer—was or should be illegal. However, were it possible to connect these activities—truck rental, plus multiple purchases of fertilizer—this conjunction too could reasonably be termed a noteworthy occurrence.

- In preparation for the 9/11 attacks, several of the hijackers, such as Waleed Alsherhri, obtained training as commercial pilots ([5], p. 186; [3], pp. 168, 242). At least one of the hijackers, Mohamed Atta, had attended the International Officer's School at Maxwell/Gunter Air Force Base in Montgomery, Alabama ([5], p. 186). The hijackers engaged in a great deal of domestic and international travel, despite not having legitimate business or family reasons to do so. Although the funds used in the attack were relatively modest, in the US$400K-$500K range, some of this money was supplied by wire transfer, with at least one case involving an amount over US$10K; significant funds in foreign accounts were accessed by the hijackers in the United States ([3], pp. 169, 172, 497 note 110). In addition, in the days just before the attack, the hijackers returned leftover funds to al Qaeda by wire transfer, amounting to about US$26K ([3], p. 252). Here again, none of these anomalies was illegal. However, were it possible to connect these activities, this conjunction would of course be a noteworthy occurrence.

There are several points that should be made in regard to what I have termed anomalies in these examples:

1. It bears repeating that all of the anomalies I have selected are legal activities in and of themselves. I have deliberately avoided, to this point, mentioning the illegal preparations that terrorists make. (For example, McVeigh stole electric blasting caps and other supplies from a quarry; [4], p. 194.)

2. All of the anomalies I have selected are in some way or another directly relevant to the terrorist activities of the individuals involved.

3. The individual anomalies I have mentioned are, in many cases, only slightly out of the ordinary. It is the *pattern of conjunction* of several such anomalies that is noteworthy.

4. All or almost all of the anomalies I have selected occurred within the country where the terrorist act occurred. Hence, in principle, cooperation between a NATO-member nation and a non-member nation would not have been required to obtain information concerning these anomalies.

5. No one anomaly is either necessary or sufficient for terrorist preparations, even when different groups of terrorists are sponsored by the same organization. (For example, although the terrorists in the 1993 World Trade Center bombing were affiliated with an extremist mosque, most of the terrorists in the 2001 attacks were instructed to stay away from mosques; [3], p. 215.)

6. I have avoided selecting anomalies that involve profiling by racial, ethnic, or religious group.

7. I have avoided selecting anomalies that involve knowledge of the *content* of individual telephone or Internet communications; it is only *patterns* of connection that I have emphasized.

The lesson to be learned here is simple in principle, and concerns a worthwhile goal:

> ***If* it were possible (1) to sort through terrorism-relevant information about large numbers of individuals, (2) to connect information about terrorism-relevant anomalies to the appropriate individuals, and (3) to connect relevant individuals with one another, *then* we should be able to identify those relatively few individuals and groups who present some significant risk of being involved in preparation for terrorist activities.**

This might seem to be a pie-in-the-sky idea that is beyond the reach of the members of NATO. It is not. To meet this goal, we must be able to do the following:

- gain access to and sort through vast amounts of information about massive numbers of individuals;
- connect disparate pieces of information about massive numbers of individuals;
- connect individuals to other individuals who are in their social or professional circles;
- process this data so as to identify potential terrorist activity.

Although this is a challenging set of requirements, it is possible to meet them. The vehicle for meeting this goal is an artificial intelligence expert system, applying fuzzy signal detection theory. In the remainder of this presentation, I describe this hypothetical system in conceptual terms. Such a system would not merely connect the dots, but would fuse them into a meaningful gestalt. Hence, in this presentation I shall call this system **FUSEDOT**: FUzzy Signal Expert system for the Detection Of Terrorist preparations. Although FUSEDOT would be best implemented on a NATO-wide basis, it would be useful even if implemented on a single-nation basis. I shall proceed by explaining what a "fuzzy signal" and fuzzy signal detection theory are. Briefly, I shall describe the use of expert systems. I shall then outline the general functions of FUSEDOT.

## 2.0 FUZZY SIGNALS

Classical signal detection involves the detection of a signal against a background of noise [6]. There is uncertainty in the situation because of the noise; hence, the basic signal detection question is, "Is there a signal present, or not?" Classical signal detection has a long history of application in fields such as communications, medical diagnosis, and weather forecasting [7].

At first glance, it might seem as if classical signal detection theory were a good framework for anti- and counter-terrorism work, but this is not the case. The various anomalies mentioned earlier are *not* signals in the classical sense. A classical signal may be obscured by noise, but the signal is always essentially different in nature from that noise. (For example, a radio signal is the result of deliberate modulation of the amplitude or frequency of a radio transmission. Radio noise, or static, typically occurs as a result of random processes in the atmosphere, or characteristics of terrestrial geography. Thus, the signal and the noise are essentially different in nature.) In addition, a classical signal is either present or not; if the signal is present, a message is being sent; if the signal is not present, no message is being sent. In contrast, the anomalies mentioned earlier are ambiguous. Sometimes an anomaly is a signal of terrorist preparation, but usually that very same anomaly is not such a signal at all. For example, usually a person purchasing a large amount of agricultural fertilizer simply has a large farm; very rarely, such a person is using the fertilizer to produce powerful explosives for terrorist activity. The purchase of large quantities of fertilizer, then, is not a straightforward signal of terrorist activity. Rather, such a purchase is what is technically referred to as a "fuzzy signal": sometimes the signal denotes terrorism, but most often it does not.

Although classical signal detection theory breaks down here, there is an alternative that does apply to this kind of situation: fuzzy signal detection theory (FSDT) [8, 9]. FSDT derives from fuzzy set theory in mathematics, where sometimes an item is only probabilistically a member of a set [10].

Thus, we may conceive of what I have called here "anomalies" as fuzzy signals: sometimes these anomalies are signs of terrorist preparations, even though often they are nothing of the sort. An early step in developing our system would involve composing a list of potential relevant fuzzy signals. These might involve certain patterns of travel, purchases, communications, Internet usage, or electronic funds transfer, as I describe later. One particular challenge in this area involves the specification of fuzzy signals that are potentially characteristic of preparations for radiological or nuclear attack; certainly the threat of nuclear terrorism has been noted, specifically in relation to al Qaeda [11-13]. In addition, it would be worthwhile to specify fuzzy signals that are suggestive of preparations for agroterrorism, that is, disruption of agriculture and the food supply [14], as well as bioterrorism [15, 16].

In passing, it should be noted that the identification of anomalies is nothing new in intelligence work. Over 30 years ago, the noted American intelligence analyst Cynthia Grabo taught of the importance of attending to lists of "indicators" in intelligence analysis:

> In about 1948, the intelligence agencies began developing lists of actions or possible actions which might be undertaken by an adversary … prior to the initiation of hostilities. From this beginning, the intelligence services of the U.S. (and its Allies) have gradually developed a series of indicator lists….
>
> The philosophy behind indicator lists is that any nation in preparation for war (either general or localized) will or may undertake certain measures (military, political and possibly economic), and that it is useful for analysts and collectors to determine in advance what these are or might be, and to identify them as specifically as possible. ([17], p. 25)

Much more could be quoted with profit from Grabo's account. What Grabo wrote concerning the "indicators" generated by potentially hostile nations applies to the "anomalies" generated by potential terrorists. In brief: hostile entities (whether nations or individuals) prepare for hostility, and those preparations comprise information that should be noted. What the present work introduces to this discussion is the matter of "fuzziness" in this information, and the use of higher technology in ferreting it out.

## 3.0 ARTIFICIAL INTELLIGENCE (AI) AND EXPERT SYSTEMS

Analysis of the data needed by FUSEDOT cannot be accomplished by human intelligence analysts alone. There is simply far too much data than can be analyzed by even an army of human beings, in a timely fashion. However, the type of data we anticipate capturing is eminently appropriate for automated data processing with off-the-shelf technology. The data types at issue here are simple and straightforward. We are dealing with types and amounts of purchases, telephone numbers called, amounts of money transferred, and so forth; we are not considering voice recognition, visual pattern recognition, or decryption. (The most sophisticated type of data would involve the analysis of Internet usage, described later.) In particular, the data analysis that needs to be accomplished is suitable for an artificial intelligence expert system.

The topic of expert systems has amassed an enormous literature, perhaps because expert systems have a history as the most successful aspect of artificial intelligence, in terms of the development of practical applications ([18], p. v). Expressed technically, "expert systems attempt to capture human knowledge and reasoning processes in a well-defined domain through a set of rules" ([19], p. 68). Briefly put, expert systems apply rules defined by human experts to make decisions based on available data. In this instance, the type of rules that we wish to incorporate into our expert system involve the assignment of risk scores to individuals, based on the presence of certain fuzzy signals: the higher the score, the higher the risk that the individual may be involved in preparations for terrorism. Expert systems have been developed to process fuzzy data [20]. Fuzzy-logic enabled expert systems have been shown to have good discriminative power in such difficult tasks as determining the provenance of the travertine stones used in the construction of ancient buildings [21].

## 4.0 A FUZZY SIGNAL EXPERT SYSTEM TO DETECT TERRORISM: FUSEDOT

We shall pass over the activities that would involved in the development of FUSEDOT, in favor of discussing its components. These components include data acquisition, data processing, report generation, and feedback and further system development.

## 4.1 Data Acquisition

Data for FUSEDOT is to be acquired through data mining [22]; for our purposes, a hybrid framework for data mining is appropriate [23]. One particular challenge with FUSEDOT will be the acquisition of data from multiple sources, for which some procedures have been described [24].

The types of data to be acquired for FUSEDOT fall into several categories, not unlike some of the categories of data used by such intelligence-related systems as the Novel Intelligence from Massive Data program [25] and the Terrorist Information Awareness program [26]:

- Interpersonal relationships
- Financial relationships
- Travel patterns
- Purchasing patterns
- Patterns of Internet usage
- Personal background

The following subsections describe each type of data to be acquired.

### 4.1.1 Interpersonal relationships

Social network analysis is important for identifying and understanding many terrorist groups, which may have very fuzzy boundaries, and which may stay in contact through newer communication technology and the Internet [27]. Interpersonal relationship data can be obtained in various ways. Telephone calling data and e-mail are particularly important in this respect; these data are available in real time from telephone and Internet service providers. Attendance at events sponsored by extremist institutions is available through conventional intelligence gathering, typically some time after the event; individuals who attend such an event simultaneously may know one another.

### 4.1.2 Financial relationships

Electronic funds transfers to or from an individual are matters of record. Patterns of accounts held by individuals are also recorded by banks. The funding of terrorist operations is a complex matter that has been described in several open sources [28, 29].

### 4.1.3 Travel patterns

Travel by air, and increasingly by train and bus, is recorded electronically by the transportation companies involved. These data are particularly useful when compared to occupational data (see “Personal Background,” below); it is one thing for an international business consultant to travel across the country or across national borders with some frequency; it is something else again for the manager of a grocery store to do so.

### 4.1.4 Purchasing patterns

Purchase data are often captured by point-of-sale terminals (i.e., Universal Product Code scanners and the like). Two types of purchases are particularly of interest here. One involves purchases of materials or substances that either form or can be processed into components of explosives or other weapons of mass destruction (e.g., certain agricultural fertilizers). For example, with post-9/11 restrictions on the obtaining of blasting caps, some terrorists may resort to home-made varieties constructed from potassium perchlorate and pyro-grade aluminum powder, as initiators for ammonium nitrate explosives derived from agricultural fertilizers [30]; thus, purchases of these substances are of interest.

Another type of purchase involves legal substances that can be used to generate illicit profits, potentially generating assets to finance terrorist activities. As mentioned in the opening example, unusually large quantities of tobacco would be one such substance. Some over-the-counter medications, purchased in large quantities, can be processed into illicit methamphetamine; unusually large purchases of such medications (perhaps in aggregate, over a period of time) are thus of interest.

### 4.1.5 Patterns of Internet usage

It is well-established that the ideology of some terrorist groups is available on numerous websites and bulletin boards [31, 32]. Internet usage is traceable. In passing, it should be noted that a "gingerbread house" technique can be utilized by anti-terrorism authorities; in this technique, known historical texts relevant to terrorism [33-35] are made available on the Internet, and subsequent viewing is tracked. (The term "gingerbread house," of course, refers to the fairy tale of Hansel and Gretel, lured into a witch's grasp by her gingerbread house.)

### 4.1.6 Personal background

Occupational data can be obtained from a variety of sources. Military training (e.g., demolition, ordnance) is a matter of government record. Academic majors (e.g., chemistry) are often available in open sources. Enrollment in private vocational schools (e.g., aviation) also generates records.

## 4.2 Data Processing

After post-acquisition data cleaning [36] and pre-processing [37, 38], the data acquired for FUSEDOT will be stored in a vast relational database involving a massive number of individuals. At the heart of the FUSEDOT system, an inferential engine will apply an algorithm to assign risk scores to individuals, based on the fuzzy signals that they have generated. Although the precise nature of the algorithm that we have developed at Professional Services Group, Inc., is proprietary, it can be discussed in generalities here. On the basis of Bayesian reasoning [39], a rather high risk score might be assigned, for example, to an individual who showed the following characteristics:

- Is affiliated with an extremist group advocating violence
- Recipient of multiple wire transfers of money, each involving a small amount, but totalling in aggregate US$20K over the course of 18 months
- A licensed electrician, this individual has made cross-country travel by air, train, and bus monthly for the last 18 months
- Has purchased substantial amounts of ammonium nitrate fertilizer and pyro-grade aluminum powder, in multiple purchases over the last 6 months

- Has just rented a pickup truck
- Frequently visits Internet sites devoted to political and religious violence
- Currently majoring in chemistry at an undergraduate institution
- History of military training in demolition

One important aspect of the data analysis involves the linking of individuals. As noted earlier, the conspirators in the first World Trade Center bombing each had a different part in the plan; one purchased chemicals for the bomb, another rented the car, and so on. The Oklahoma City bombers split the purchase of the ammonium nitrate fertilizer between two individuals. The 9/11 hijackers had wire transfers of cash made to other individuals, on their behalves. Although this makes the task of data analysis substantially more complex, this is one reason to involve an expert system. Using records of telephone numbers called, e-mail addresses accessed, and other affiliation data, the expert system will devise risk scores, not only for individuals, but for groups of individuals that are defined by a history of interaction. This will allow highlighting of a pattern of terrorist-preparation-consistent behavior by a group, rather than just by its constituent individuals.

## 4.3 Report Generation: Terrorism Risk Ratings

There are several ways in which FUSEDOT can issue reports. One way would be for the system to assemble a distribution of risk scores, and designate the individuals and groups scoring in the top .0003% of the distribution as indicating an unusually high potential terrorism risk. (This would amount to 3 individuals in every 1 million people in the population.) Using this arbitrary guideline, and based on year 2000 population estimates, the number of people within the designated NATO member nations whom FUSEDOT would designate as indicating an unusually high potential terrorism risk is given in Table 1.

Based on FUSEDOT's report, the national authorities responsible for the defence against terrorism would then have the option of, for example, passively observing those designated as posing an unusually high risk for potential terrorism. (It is my sense of the situation that the internal security resources of NATO member nations would not be unduly strained by launching passive observations focused on the number of individuals indicated in Table 1.) Such an investigation might reveal that the individuals involved actually pose no risk for terrorism, in which case no further action need be taken. On the other hand, such an investigation might reveal that the individuals involved are actually engaged in suspicious behavior, in which case more active investigations may be initiated.

| NATO Member Nation | # Citizens Identified as Risky |
|---|---|
| Belgium | 31 |
| Bulgaria | 24 |
| Canada | 94 |
| Czech Republic | 31 |
| Denmark | 16 |
| Estonia | 4 |
| France | 178 |
| Germany | 249 |
| Greece | 32 |
| Hungary | 30 |
| Iceland | 1 |
| Italy | 173 |
| Latvia | 7 |
| Lithuania | 11 |
| Luxembourg | 1 |
| Netherlands | 48 |
| Norway | 14 |
| Poland | 116 |
| Portugal | 30 |
| Romania | 67 |
| United Kingdom | 179 |
| United States | 827 |
| Slovakia | 16 |
| Slovenia | 6 |
| Spain | 120 |
| Turkey | 197 |

**Table 1: Number of people in NATO member nations whom FUSEDOT would indicate as posing an unusually high risk for potential terrorism (using the 3:1,000,000 ratio)**

### 4.5 Feedback and Further System Development

Evaluation of the system will be an important aspect of FUSEDOT, particularly in terms of adjustments for false positives and true hit rates [40]. Feedback from security authorities using FUSEDOT would allow developers to enhance the system. One such enhancement would be the inclusion of knowledge discovery algorithms. That is, based on the feedback data, we could enhance the system to allow for the recognition of structural data patterns indicating preparations for terrorist activity. Approaches to such a type of knowledge discovery capacity have already been described in the artificial intelligence literature [41]. On the basis of feedback, it also may be appropriate to enhance the system so as to exploit functional dependencies [42] and hidden Markov processes in the data [43].

After a sufficient number of true positive cases of terrorist preparation have been identified, it may be possible to restructure the risk score equations by applying structural equation modeling [44, 45]. This powerful statistical technique has been used for risk identification programs in different domains than the present project (e.g., the identification of HIV risk in vulnerable youth [46]).

### 4.4 System Limitations

Could terrorists evade FUSEDOT? No system is perfect. Terrorists who were highly adept at fabricating multiple false identities for each group member would be very hard to detect by any system. Other terrorists could evade detection by FUSEDOT if they always paid for crucial purchases with cash, transported themselves exclusively by foot or personal automobile, avoided all contact with suspect groups and individuals, never used the Internet, and communicated with each other and transferred funds solely by postal mail. However, my sense of the situation is that not every terrorist cell is this fastidious. Although FUSEDOT will not highlight every possible terrorist preparation, it will highlight many, in potential, and that is reason enough to give the development of FUSEDOT very serious consideration.

## 5.0 COMPARISON TO OTHER APPROACHES

The approach I have advocated here is not utterly unique. Two approaches currently under development, each with some similarities to FUSEDOT, are the Novel Intelligence from Massive Data program, and the Terrorist Information Awareness program, each of which is described and compared to FUSEDOT, below.

### 5.1 Novel Intelligence from Massive Data (NIMD)

In the United States, the Novel Intelligence from Massive Data (NIMD) Program, sponsored by the Advanced Research and Development Activity (ARDA), is devoted to helping human intelligence analysts search through massive databases [25, 47]. One noteworthy aspect of the NIMD program is the use of (artificially) intelligent agents to assist human intelligence analysts; the development of these AI agents is called Knowledge Associates for Novel Intelligence (KAMI) [48]. With these projects in place, what use will FUSEDOT be?

NIMD and KAMI seem to involve the relating of data to individuals who already have been identified as terrorists or terrorist abetters. There is an obvious need for such systems. However, FUSEDOT does not depend on input regarding known terrorists or their associates. FUSEDOT specifically involves identifying terrorist preparations, whether or not the individual or individuals involved have previously been identified as terrorists. Surely there is an obvious need for this type of system, as well.

In what could be read as a critique of the NIMD approach, intelligence scholar John Bodnar has written:

> Data-mining is easy for tracking known entities with known interactions, but virtually impossible for identifying new kinds of interactions with unknown entities…. Data-mining is easy for known "bad guys" but not very good for identifying new ones—without a source somehow saying "this new guy is suspicious, and you should examine him." This is the true challenge that "massive" data presents—"How can we data-mine an existing dataset for new relationships between unknown entities?" ([49], p. 50)

FUSEDOT's inclusion of an artificial intelligence expert system that uses fuzzy signal detection theory will make it possible for data mining techniques to accomplish precisely the task that Bodnar has declared "virtually impossible."

### 5.2 Terrorist Information Awareness (TIA)

In the U.S. Department of Defense, the Defense Advanced Research Projects Agency (DARPA) is said to be currently developing the Terrorist Information Awareness (TIA) program [26]. In many ways, TIA resembles FUSEDOT, both in terms of the types of data gathered, and the use of artificial intelligence in analyzing data [50]. However, there also seem to be several crucial differences. Many details concerning the current DARPA TIA program seem to be classified, so it is difficult to identify differences with certainty. However, if it is legitimate to assume that the current TIA program includes some components of a predecessor, the now-defunct Total Information Awareness program, then several points of comparison between TIA and FUSEDOT come into focus:

- Although absence of evidence is not conclusive evidence of absence, it is noteworthy that no mention is made in any TIA-related documents concerning the use of fuzzy signal detection theory, which is a crucial aspect of FUSEDOT.

- FUSEDOT does not require facial recognition, or video surveillance of public areas, both of which are apparently a component of TIA ([26], pp. 10-12; [51]).

- FUSEDOT does not involve the monitoring of the content of voice communications, nor translation thereof, both of which are apparently an aspect of TIA [52].

These differences would seem to give FUSEDOT several advantages in a direct comparison with TIA. First, FUSEDOT would employ fuzzy signal detection, which TIA does not. Second, FUSEDOT would be easier to develop, because it does not require the development of facial recognition or language translation software. Third, for the same reasons, FUSEDOT poses fewer privacy concerns.

## 6.0 CONCLUSION AND OUTLOOK

I have outlined here the broad specifications of FUSEDOT, an artificial intelligence expert system that can be used to detect potential preparation for terrorist activity. Relative to other systems that analyze massive amounts of data about the general public for terrorist detection, FUSEDOT would implement some superior technology (fuzzy signal detection), would be much simpler to develop, and would pose far fewer privacy concerns. NATO member nations would do well to consider developing a system such as FUSEDOT, which would be a valuable asset for the defence against terrorism.

## 7.0 REFERENCES

[1] "Panel to seek increase in Nevada cigarette tax." RenoGazette Journal, June 26, 2002, retrieved from http://www.rgj.com/news/stories/html/2002/06/26/17795.php on September 17, 2004.

[2] M. Crowley, "Blood money," Reader's Digest, February 2004, pp. 190-193, 195-200, 202-209.

[3] The 9/11 Commission Report: Final report of the National Commission on Terrorist Attacks upon the United States, Authorized Edition, New York: Norton, 2004.

[4] L. Michel, D. Herbeck, American terrorist: Timothy McVeigh and the tragedy at Oklahoma City (paperback ed.), New York: Avon/HarperCollins, 2002.

[5] P. Thompson, The terror timeline, New York: HarperCollins, 2004.

[6] T.D. Wickens, Elementary signal detection theory, Oxford, UK: Oxford University Press, 2002.

[7] D.M. Green, J.A. Swets, Signal detection theory and psychophysics (rev. ed.), Los Altos, CA: Peninsula Publishing, 1988.

[8] P.A. Hancock, A.J. Masalonis, R. Parasuraman, "On the theory of fuzzy signal detection: Theoretical and practical considerations," Theoretical Issues in Ergonomic Science, vol. 1, 2000, pp. 207-230.

[9] R. Parasuraman, A.J. Masalonis, P.A. Hancock, "Fuzzy signal detection theory: Basic postulates and formulas for analyzing human and machine performance," Human Factors, vol. 42, 2000, pp. 636-659.

[10] G.J. Klir, U.H. St. Clair, B. Yuan, Fuzzy set theory: Foundations and applications, Upper Saddle River, NJ: Prentice Hall PTR, 1997.

[11] G. Allison, Nuclear terrorism: The ultimate preventable catastrophe, New York: Times Books, 2004.

[12] Anonymous, Imperial hubris, Washington, DC: Brassey's, 2004.

[13] P.L. Williams, Osama's revenge, Amherst, NY: Prometheus Books, 2004.

[14] O.S. Cupp, D.E. Walker II, J. Hillison, "Agroterrorism in the U.S.: Key security challenge for the 21st century," Biosecurity and Bioterrorism, vol. 2, 2004, pp. 97-105.

[15] G. Kwik, J. Fitzgerald, T.V. Inglesby, T. O'Toole, "Biosecurity: Responsible stewardship of bioscience in an age of catastrophic terror," Biosecurity and Bioterrorism, vol. 1, 2003, pp. 27-35.

[16] B. Sundelius, J. Grönvall, "Dilemmas of biosecurity in the European Union," Biosecurity and Bioterrorism, vol. 2, 2004, pp. 17-23.

[17] C.M. Grabo, Anticipating surprise: Analysis for strategic warning [unclassified ed.], The Joint Military Intelligence College's Center for Strategic Intelligence Research [NTIS No. PB2003-103279], 2002

[18] A.J. Gonzalez, D.D. Dankel, The engineering of knowledge-based systems: Theory and practice, Upper Saddle River, NJ: Prentice Hall, 1993.

[19] K.C. Desouza, Managing knowledge through artificial intelligence: An introduction with guidelines for nonspecialists, Westport, CT: Quorum Books, 2002.

[20] A.B. Badiru, J.Y. Cheung. Fuzzy engineering expert systems with neural network applications, New York: Wiley, 2002.

[21] M. Petrelli, D. Perugini, B. Moroni, G. Poli, "Determination of travertine provenance from ancient buildings using self-organizing maps and fuzzy logic," Applied Artificial Intelligence, vol. 17, 2003, pp. 885-900.

[22] N. Ye (Ed.), The handbook of data mining, Mahwah, NJ: Erlbaum, 2003.

[23] Z. Zhang, C. Zhang, S. Zhang, "An agent-based hybrid framework for database mining," Applied Artificial Intelligence, vol. 17, 2003, pp. 383-398.

[24] B.-H. Park, H. Kargupta, "Distributed data mining," N. Ye (Ed.), The handbook of data mining, Mahwah, NJ: Erlbaum, 2003, pp. 341-362.

[25] E. Whitaker, R. Simpson, L. Burkhart, R. MacTavish, C. Lobb, "Reusing intelligence analysts' search plans," Proceedings of the Human Factors and Ergonomics Society 48th annual meeting (New Orleans, Louisiana), Santa Monica, CA: Human Factors and Ergonomics Society, 2004, pp. 367-370.

[26] Report to Congress regarding the Terrorism Information Awareness Program, Defense Advanced Research Projects Agency, May 20, 2003, retrieved from http://www.epic.org/privacy/profiling/tia /may03_report.pdf on September 27, 2004.

[27] M. Sageman, Understanding terror networks, Philadelphia: University of Pennsylvania Press, 2004.

[28] L. Napoleoni, Modern jihad: Tracing the dollars behind the terror networks, London: Pluto Press, 2003.

[29] N. Raphaeli, "Financing of terrorism: Sources, methods, and channels," Terrorism and Political Violence, vol. 15, no. 4, 2003, pp. 59-82.

[30] Anonymous U.S. government employee, personal communication, September 20, 2004.

[31] E. Lipton, E. Lichtblau, "Online and even near home, new front in the terror fight," The New York Times, vol. 154, no. 52981 [national edition], September 23, 2004, pp. A1, A6.

[32] L. Wright, "The terror web," The New Yorker, August 2, 2004, pp. 40-47, 49-53.

[33] R. Israeli, "A manual of Islamic fundamentalist terrorism," Terrorism and Political Violence, vol. 14, no. 4, 2002, pp. 23-40.

[34] W. Laqueur (Ed.), Voices of terror: Manifestos, writings and manuals of al Qaeda, Hamas and other terrorists from around the world and throughout the ages, New York: Reed Press, 2004.

[35] A. Macdonald, The Turner diaries (2nd ed.), New York: Barricade Books, 1996.

[36] S. Zhang, C. Zhang, Q. Yang, "Data preparation for data mining," Applied Artificial Intelligence, vol. 17, 2003, pp. 375-381.

[37] D. Pyle, "Data collection, preparation, quality, and visualization," N. Ye (Ed.), The handbook of data mining, Mahwah, NJ: Erlbaum, 2003, pp. 365-391.

[38] X. Yan, C. Zhang, S. Zhang, "Toward databases mining: Pre-processing collected data," Applied Artificial Intelligence, vol. 17, 2003, pp. 545-561.

[39] D. Madigan, G. Ridgeway, "Bayesian data analysis," N. Ye (Ed.), The handbook of data mining, Mahwah, NJ: Erlbaum, 2003, pp. 103-131.

[40] S.M. Weiss, T. Zhang, "Performance analysis and evaluation," N. Ye (Ed.), The handbook of data mining, Mahwah, NJ: Erlbaum, 2003, pp. 425-440.

[41] N.N.B. Abdullah, M. Liquière, S.A. Cerri, "GAsRULE for knowledge discovery," Applied Artificial Intelligence, Vol. 17, 2003, 399-417.

[42] R.S. King, J.J. Legendre, "Discovery of functional and approximate functional dependencies in relational databases," Journal of Applied Mathematical and Decision Sciences, vol. 7, 2003, pp. 49-59.

[43] S.L. Scott, "Hidden Markov processes and sequential pattern mining," N. Ye (Ed.), The handbook of data mining, Mahwah, NJ: Erlbaum, 2003, pp. 133-157.

[44] L. Klem, "Structural equation modeling," L.G. Grimm, P.R. Yarnold (Eds.), Reading and understanding more multivariate statistics, Washington, DC: American Psychological Association, 2000, pp. 227-259.

[45] R.B. Kline, Principles and practices of structural equation modeling (2nd ed.), New York: Guilford, 2004.

[46] G.J. Huba, A.T. Panter, L.A. Melchior, L. Trevithick, E. Wright, et al., "Modeling HIV risk in highly vulnerable youth," Structural Equation Modeling, vol. 10, 2003, pp. 583-608.

[47] "Novel Intelligence from Massive Data," no date, retrieved from NIMD home page on ARDA website, http://www.ic-arda.org/Novel_Intelligence/ on September 27, 2004.

[48] A.R. Chappell, A.J. Cowell, D.A. Thurman, J.R. Thomson, "Supporting mutual understanding in a visual dialogue between analyst and computer," Proceedings of the Human Factors and Ergonomics Society 48th annual meeting (New Orleans, Louisiana), Santa Monica, CA: Human Factors and Ergonomics Society, 2004, pp. 376-380.

[49] J.W. Bodnar, Warning analysis for the information age: Rethinking the intelligence process, Washington, DC: The Joint Military Intelligence College's Center for Strategic Intelligence Research [NTIS No. PB2004-104379], 2003.

[50] J.B. Sharkey, "Total information awareness," presentation at DARPATech Symposium (Denver, Colorado), June 1999, slides retrieved from http://www.darpa.mil/darpatech99/Presentations/isopdf/isotia.pdf, speaking text retrieved from http://www.darpa.mil/darpatech99/Presentations/Scripts/ISO/ISO_TIA_Sharkey_Script.txt, on September 27, 2004.

[51] J. Poindexter, "DARPA's initiative on asymmetric threat: Total Information Awareness," presentation made at DARPATech 2002, slides retrieved from http://www.darpa.mil/darpatech2002/presentations/

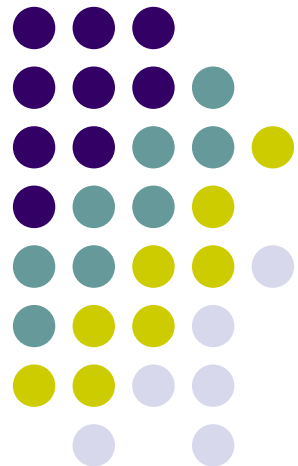
iao_pdf/slides/poindexteriao.pdf, text retrieved from retrieved from http://www.darpa.mil/darpatech2002/presentations/iao_pdf/speeches/poindext.pdf on September 27, 2004.

[52] C.L. Wayne, "Human language technology: TIDES, EAR, Babylon," 2002, retrieved from http://www.darpa.mil/darpatech2002/presentations/iao_pdf/z_hlt%20for%20darpatech_wayne.pdf on September 27, 2004.

# Detecting Preparations for Terrorism by AI Expert System Employing FSDT

Mark E. Koltko-Rivera, Ph.D.

NATO RTO-MP-SCI-158



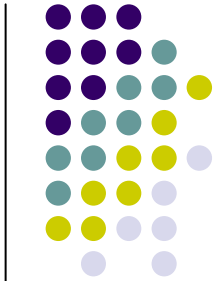
# Outline

- Anomalies
- Fuzzy Signals
- Artificial Intelligence (AI) Expert Systems
- FUSEDOT
- Comparisons to Other Approaches
- Conclusion and Outlook

# Outline

- Anomalies
- Fuzzy Signals
- Artificial Intelligence (AI) Expert Systems
- FUSEDOT
- Comparisons to Other Approaches
- Conclusion and Outlook

# “Anomaly”



- An activity that, although legal, is at least very slightly out of the ordinary.

# Anomaly:
# North Carolina supermarket (ca. 2002)

- Abnormally large tobacco purchases.

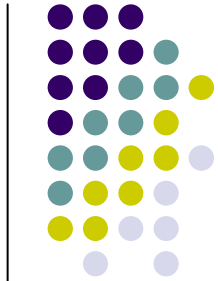
# Anomalies:
# World Trade Center bombing 1 (1993)

- Rental of van
- Purchase of chemicals
- Affiliation with extremist cleric

# Anomalies:
# Oklahoma City bombing (1995)

- Rental of a truck
- Purchase of large quantities of fertilizer

# Anomalies:
# The 9/11 Attacks (2001)



- Pilot training
- Military training
- Large amounts of travel
- International wire transfers of large amounts of money

# Characteristics of Anomalies

- Legal
- Directly relevant to terrorist activity
- Only slightly out of the ordinary
- The *pattern* is what matters
- Occurred “in country”
- None necessary or sufficient
- None involve ethnic/religious profiling
- None involve monitoring of content

# The Goal

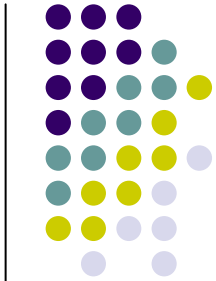
**If** we can:

- sort through terrorism-relevant anomalies;
- connect information about anomalies to individuals;
- connect relevant individuals;

**Then** we can:

- identify those who present significant terrorism risk

# Abilities We Need to Meet the Goal



- Access and sort vast information about massive numbers of individuals
- Connect disparate pieces of information
- Connect individuals
- Process data ➔ potential terrorism

# FUSEDOT

Fuzzy Signal Expert System for the Detection of Terrorist Preparations

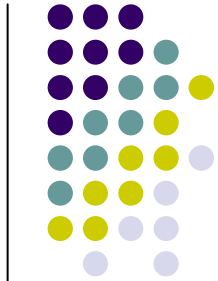
# Outline

- Anomalies
- Fuzzy Signals
- Artificial Intelligence (AI) Expert Systems
- FUSEDOT
- Comparisons to Other Approaches
- Conclusion and Outlook

# Classical Signal Detection Theory

- Involves the detection of a signal against a background of noise.
- The basic question: “Is a signal present, or not?”
- The signal and noise are fundamentally different.
- Signal is either present or not.

# Terrorist Preparation's Anomalies



- Sometimes an anomaly is a signal—but sometimes is not a signal at all.
- Example: Purchase of agricultural fertilizer.
- Anomaly ➔ Fuzzy signal

# Outline

- Anomalies
- Fuzzy Signals
- Artificial Intelligence (AI) Expert Systems
- FUSEDOT
- Comparisons to Other Approaches
- Conclusion and Outlook

# Expert System

- Automated artificial intelligence construct
- Applies rules defined by human experts to make decisions based on available data.
- Assigns risk scores based on anomalies/ fuzzy signals.

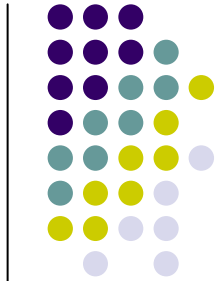
# Outline

- Anomalies
- Fuzzy Signals
- Artificial Intelligence (AI) Expert Systems
- FUSEDOT
- Comparisons to Other Approaches
- Conclusion and Outlook

# FUSEDOT Components

- Data Acquisition
- Data Processing
- Report Generation
- Feedback
- System Refinement

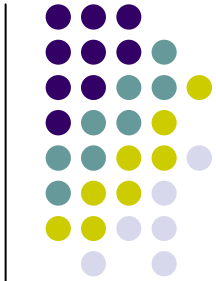
# FUSEDOT Components



Data Acquisition

- Personal relationships
- Financial relationships
- Travel patterns
- Purchase patterns
- Internet usage patterns
- Personal background

# FUSEDOT Components



Data Processing

- Inferential engine
- Algorithm: Bayesian reasoning
- Example of a high risk individual
- Importance of linking individuals

# FUSEDOT Components

Report Generation

- Terrorism risk ratings
- One approach: top 3 in 1 000 000
- Actions to take

# FUSEDOT Components

Feedback

- Adjustments for false positives and true hit rates.

# FUSEDOT Components

System Refinement

- Knowledge discovery algorithms
- Structural equation modeling

# Outline

- Anomalies
- Fuzzy Signals
- Artificial Intelligence (AI) Expert Systems
- FUSEDOT
- Comparisons to Other Approaches
- Conclusion and Outlook

# Comparisons to Other Approaches: NIMD/KAMI

Novel Intelligence from Massive Data program (NIMD)

Knowledge Associates for Novel Intelligence (KAMI)

- Relates data to individuals already identified with terrorism.

# Comparisons to Other Approaches: TIA

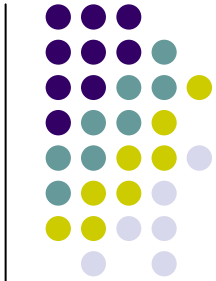
Terrorist Information Awareness (TIA)

- Apparently does not use fuzzy signal detection.
- Involves facial recognition and video surveillance of public areas.
- Involves monitoring the content of voice communications.

# Outline

- Anomalies
- Fuzzy Signals
- Artificial Intelligence (AI) Expert Systems
- FUSEDOT
- Comparisons to Other Approaches
- Conclusion and Outlook

# Conclusion



FUSEDOT:

- Implements superior technology (FSD)
- Simpler to develop
- Fewer privacy concerns

# Thank you for your kind attention.


- Mark E. Koltko-Rivera, Ph.D.
  Director of Research
  Professional Services Group, Inc.
  Winter Park, Florida, USA
  <mark@professionalservicesgroup.net>