Calhoun: The NPS Institutional Archive

DSpace Repository

Faculty and Researchers | Faculty and Researchers Collection

Tracking and disrupting dark networks: challenges of data collection and analysis

Roberts, Nancy C.

N.C. Roberts, "Tracking and disrupting dark networks: Challenges of data collection and analysis," Information Systems Frontiers (2011) v.13, pp.5-19
http://hdl.handle.net/10945/53069

Downloaded from NPS Archive: Calhoun

Calhoun is a project of the Dudley Knox Library at NPS, furthering the precepts and goals of open government and government transparency. All information contained herein has been approved for release by the NPS Public Affairs Officer.

Dudley Knox Library / Naval Postgraduate School
411 Dyer Road / 1 University Circle
Monterey, California USA 93943

http://www.nps.edu/library

Inf Syst Front (2011) 13:5–19
DOI 10.1007/s10796-010-9271-z

Tracking and disrupting dark networks: Challenges of data collection and analysis

Nancy C. Roberts

Published online: 12 October 2010
© Springer Science+Business Media, LLC (outside the USA) 2010

Abstract The attack on September 11, 2001 set off numerous efforts to counter terrorism and insurgencies. Central to these efforts has been the drive to improve data collection and analysis. Section 1 summarizes some of the more notable improvements among U.S. government agencies as they strive to develop their capabilities. Although progress has been made, daunting challenges remain. Section 2 reviews the basic challenges to data collection and analysis focusing in some depth on the difficulties of data integration. Three general approaches to data integration are identified—*discipline-centric, placed-centric and virtual.* A summary of the major challenges in data integration confronting field operators in Iraq and Afghanistan illustrates the work that lies ahead. Section 3 shifts gears to focus on the future and introduces the discipline of Visual Analytics—an emerging field dedicated to improving data collection and analysis through the use of computer-mediated visualization techniques and tools. The purpose of Visual Analytics is to maximize human capability to perceive, understand, reason, make judgments and work collaboratively with multidimensional, conflicting, and dynamic data. The paper concludes with two excellent examples of analytic software platforms that have been developed for the intelligence community—Palantir and ORA. They signal the progress made in the field of Visual Analytics to date and illustrate the opportunities that await other IS researchers interested in applying their knowledge and skills to the tracking and disrupting of dark networks.

N. C. Roberts (✉)
Department of Defense Analysis, School of Operational and Information Sciences, Naval Postgraduate School,
Root Hall 103H,
Monterey, CA 93943, USA
e-mail: nroberts@nps.edu

Keywords Dark networks · Visual analytics · Data collection · Analysis and fusion

The attack on September 11, 2001 set off numerous efforts to counter terrorism and insurgencies ranging from military interventions to the development of new technologies and tools. Central to many has been the drive to improve data collection and data analytic capabilities (Larson et al. 2008; Treverton 2009; Treverton and Gabbard 2008; Treverton et al. 2006).

Data collection, defined as the process of gathering raw data and information from many different sources, both open and secret, employs a range of technologies and methods. Six categories typically describe the major data or intelligence[1] sources: Signals Intelligence (SIGNIT), Imagery Intelligence (IMINT), Measurement and Signature Intelligence, (MASINT), Human-source Intelligence (HUMINT), Open Source Intelligence (OSINT), and Geospatial Intelligence (GEOINT).

SIGNIT data are obtained from various types of signals. It is subdivided into three categories: Communication Intelligence (COMINT), Electronic Intelligence (ELINT), and Foreign Instrumentation Intelligence (FISNT). COMINT is the interception of signals between people. ELINT is the interception of signals between machines and people or mixtures between COMINT and ELINT. And FISINT is the interception of signals from foreign instrumentation.

IMINT comes from visual photography, radar sensors, infrared sensors, lasers, and electro-optics that are reproduced electronically or by optical means on film electronic

[1] The Department of Defense defines intelligence as "information and knowledge obtained through observation, investigation, analysis, or understanding" (Department of Defense, *Joint Publication 1-02, DOD Dictionary of Military and Associated Terms*, 12 April 2001, as amended 15 Oct 2001, p. 214.

display devices, or other media. MASINT is technically derived data other than imagery and signal intelligence. These data are gathered from technically measurable aspects of a target such as its vibrations or hyper-spectral emissions (e.g. radar signatures and acoustic and seismic signals). HUMINT is derived from people through photography, documents, debriefings, and official contacts with foreign governments. OSINT is publicly available information appearing in print and electronic form (e.g. radio, television, newspapers, journals, the Internet, commercial databases, videos, graphics, and drawings). GEOINT is the analysis and visual representation of security related activities on the earth. It is produced through an integration of imagery, imagery intelligence, and geospatial information (Best 2006).[2]

Data analysis is the ability to make sense of the collected information by processing, converting, integrating, evaluating, and analyzing the available data. It begins with analysts processing the collected data and converting them into usable forms through decryption, language translations, and data reduction. Analysts then piece together disparate data, re-represent them as needed, and probe for connections and patterns. Ultimately, the purpose in counterterrorism and counterinsurgency is to develop insights and judgments to explain what is happening and when, who is involved, and where it is occurring. Data analysis is thus a challenging integration effort that pulls together information into a coherent whole, puts it into context, and quickly creates a consolidated situational assessment. Assessments then inform the decision process and enable decision makers to take timely and appropriate action (Treverton and Gabbard 2008).

Work is underway throughout the U.S. intelligence community to improve data collection and data analytic capabilities. Section 1 of the paper summarizes some of the more notable efforts among U.S. government agencies. Their extensive plans and contributions, many launched after 9–11, are impressive in such a short period of time. However, daunting challenges remain.

Section 2 reviews some of the basic challenges to data collection in general and to the collection of terrorism and insurgency data in particular. It also describes in some depth the analytical challenge of data analysis focusing on data integration or synthesis. I identify three general approaches to integration: *disciplined-based; placed-based; and virtual.* Section 2 concludes with a summary of the major challenges confronting field operators in Iraq and Afghanistan in the collection and analysis of data.

Section 3 shifts gears to focus on the future. I briefly describe the discipline of Visual Analytics—an emerging field dedicated to improving data collection and analysis through the use of computer-mediated visualization techniques and tools. The purpose of Visual Analytics is to maximize human capability to perceive, understand, reason, make judgments and work collaboratively with multidimensional, conflicting, and dynamic data, such as terrorism and counterinsurgency data. The paper concludes with two excellent examples of analytic software platforms that have been developed for the intelligence community—Palantir and ORA. They signal the progress made in the field of Visual Analytics to date and illustrate the opportunities that await other IS researchers interested in applying their knowledge and skills to the tracking and disrupting of dark networks.

1 Intelligence community's improvements in data collection and data analysis

The United States Intelligence Community (IC) is a federation of 16 separate U.S. government agencies that work together to conduct intelligence activities. As we see in Table 1, member organizations of the IC include intelligence agencies, and military intelligence and civilian intelligence analysis offices within Cabinet departments (Best 2006).[3]

The IC is led by the Director of National Intelligence (DNI), the US Government official responsible for advising the President, the National Security Council, and the Homeland Security Council about intelligence matters related to national security. The Director also serves as head of the sixteen-member Intelligence Community, and in this capacity, manages the intelligence cycle (Tenet 1999; Waltz 2003).

The Office of National Intelligence (ONI) houses centers important to counterterrorism and counterinsurgency, two of which are pertinent for data collection and data analysis: the National Counterterrorism Center (NCTC) and the Center for Information Sharing Environment (ISE). The NCTC is the primary organization for integration and analysis of all intelligence pertaining to terrorism and counterterrorism. It also conducts strategic operational planning by integrating all instruments of national power. The ISE promotes an information sharing culture among ISE partners and facilitates the sharing of timely, validated, protected, and actionable terrorism information. Its integrated approach supports the establishment of an Integrated Network of Fusion Centers. Since 2001, the U.S. Federal Government has provided significant grant funding to support the establishment of fusion centers owned and operated by States and major urban areas.

Improvements in data collection and analysis are being made within the U.S. intelligence community. For example,

[2] See also "An Overview of the United States Intelligence Community 2007". (http://www.dni.gov/what_collection.htm).

[3] See also "An Overview of the United States Intelligence Community 2007" (http://www.dni.gov/overview.pdf).

Table 1 Sixteen-member intelligence community agencies and organizations

Central Intelligence Agency (CIA) (https://www.cia.gov/)
United States Department of Defense (DOD) (http://www.defenselink.mil/)
Air Force Intelligence, Surveillance and Reconnaissance Agency (AF ISR or AIA) (http://www.afisr.af.mil/)
Army Military Intelligence (MI) (http://www.us-army-info.com/pages/mos/intelligence/intelligence.html)
Defense Intelligence Agency (DIA) (http://www.dia.mil/)
Marine Corps Intelligence Activity (MCIA) (http://www.quantico.usmc.mil/activities/?Section=MCIA)
National Geospatial-Intelligence Agency (NGA) (http://www.nga.mil/portal/site/nga01/)
National Reconnaissance Office (NRO) (http://www.nro.gov/)
National Security Agency (NSA) (http://www.nsa.gov/)
Office of Naval Intelligence (ONI) (http://www.nmic.navy.mil/)
United States Department of Energy (http://www.energy.gov/)
Office of Intelligence and Counterintelligence (OICI) (http://www.doe.gov/nationalsecurity/intelligence_counterterrorism.htm)
United States Department of Homeland Security (http://www.dhs.gov/index.shtm)
Office of Intelligence Analysis (OIA) (http://www.dhs.gov/xabout/structure/#1)
Coast Guard Intelligence (CGI) (http://www.uscg.mil/history/faqs/CGI.asp)
United States Department of Justice (http://www.usdoj.gov/)
Federal Bureau of Investigation (FBI) (http://www.fbi.gov/)
Drug Enforcement Administration (DEA) (http://www.usdoj.gov/dea/index.htm)
United States Department of State (http://www.state.gov/)
Bureau of Intelligence and Research (INR) (http://www.state.gov/s/inr/)
United States Department of Treasury (http://www.ustreas.gov/)
Office of Terrorism and Financial Intelligence (TFI) (http://www.ustreas.gov/offices/enforcement/)

In October 2005, the National Clandestine Service was established at CIA to undertake HUMINT operations and coordinate HUMINT efforts by other intelligence agencies. The CIA also houses the Technology Innovation Center (ITIC) and In-Q-Tel and its in-house CIA counterpart, the In-Q-Tel Interface Center (QIC). Through these entities, the CIA is linking its requirements with new technologies. The CIA has also developed the Trident workstation that segregates the data and software layer that can undergo constant changes with new modifications, versions, and products. It is also experimenting with other products such as Inspire that maps key messages or key words where there is similarity to enable analysts to get a quick picture of the message traffic. Other features of its systems include quick machine translations, a video library with translations, a mapping function, data visualization extraction, intelligent agents, link and relationship analysis, and search and retrieval to sort people, places and things (Treverton and Gabbard 2008, pp. 25–26). Despite the changes in the Intelligence Reform Act, the CIA continues to be the keystone of the Intelligence Community with its all-source analytical capabilities that cover the whole world outside U.S. borders.

The National Geospatial-Intelligence Agency (NGA), a primary producer of geospatial intelligence (e.g. maps and imagery), is attempting to digitize all geospatial intelligence to aid in the processing and dissemination of the gathered intelligence, as well as the fusing of it with other intelligence resources.[4] It also plans to deploy a Future Imagery Architecture which consists of a large number of small imagery satellites to provide more persistent and better coverage of areas of interest than today's satellite architecture. An effort to make geo-location information for precision strikes in every location the services continues.[5]

The Assistant Secretary of Defense for Command, Control, Communications and Intelligence (ASD/C3I) is focusing on interoperability and networking to ensure that collected data are available to all entities working in the same theater. Central to this effort is ASD/C3I's coordination of the Distributed Common Ground System (DCGS). It is a single, integrated architecture that is tailored to receive and process different types of data which come in different forms and often in different networks, to support analysis of the data, and to distribute intelligence to their users both on the battlefield and higher headquarters.[6]

Joint Forces Command (JFCOM), established in 1999 to improve interoperability among the services, is pulling together Joint Interface Control teams comprised of specialists in communication, hardware and software in order to

[4] (http://erg.usgs.gov/nimamaps)
[5] (http://www.globalsecurity.org/intell/systems/fia.htm).
[6] (http://www.globalsecurity.org/intell/systems/dcgs.htm).

improve communications among intelligence sources in Afghanistan (Carter 2008). JFCOM is also testing a new analytical capability known as Operational Net Assessment—a system of databases, analytical tools, and networks that aim to fuse intelligence and other data in an interagency environment (Best 2003; Chizek 2003).

The Defense Intelligence Agency (DIA) has been the military's source of human intelligence and strategic analysis since 9–11.[7] It also runs several military-wide programs that support strategic analysis. For example, its Joint Intelligence Virtual Architecture, a collaborative intelligence network, has made major headway in establishing standardized access to data and analysts throughout the military intelligence community. The architecture has incorporated many analytical tools including the Army's Pathfinder (see below) as well as a single integrated data base which seeks to improve analysts' ability to fuse all sources of intelligence.[8]

The military services have been moving toward improved data collection and analysis as well. The Army, reliant on national agencies and other services for its data collection, has focused its current research and development efforts on analytical tools, especially data fusion and validation. It has had some success with the Pathfinder text analysis software, used by the Army's National Ground Intelligence Center and now being incorporated into analysis systems throughout the military. This software system is reported to be able to sort through 500,000 documents in just a few minutes in order to find patterns and trends.[9] At the tactical level, the Army has formed Reconnaissance, Surveillance, Targeting and Acquisition (RSTA) squadrons to provide focused analysis for the brigade commander, in contrast to previous programs that relied on data collection and analysis at the division and the corps levels. RSTA squadrons employ the latest technologies for data collection and analysis and personnel, trained in data collection and analysis, are expected to operate directly with tactical patrol units. Ultimately, every soldier, regardless of occupational specialty, is expected to contribute his/her observations to the intelligence network.[10]

The Air Force is creating multiple platforms which together can watch a battlefield regardless of the terrain, time of day or weather conditions, and communicate observations to identify a target, and if necessary, destroy it within 10 min of the initial observations (Goodman 2003).[11] The Air Force also has moved some intelligence analysis from the IC community directly into operations as it did in the Air Force's Checkmate analysis cell that participated in the planning of air operations for Dessert Storm (Best 2003; Chizek 2003, p. 26).

The Navy and Marine Corps are focusing on network centric warfare that links sensors and weapon systems in local and wide-area networks such as the Cooperative Engagement Capability (CEC).[12] The Navy is also developing the Naval Fires Network, the primary program supporting the Navy's entire process of identifying targets and striking them (Nagle 2002).[13] The Marine Corps is expanding its Intelligence Analysis System to bring various sources of intelligence together for analysis by intelligence personnel.[14] The Coast Guard, having foreseen the need for shore-based fusion and analysis centers to handle the increased quantity of intelligence, is coordinating with the Navy to establish a 24-h operation center on each US coast. (Best 2003; Chizek 2003).

Special Operation Force (SOF), composed of elite, specialized military units that can be inserted into enemy territory, is pursuing the goal of receiving the highest-quality intelligence at the lowest tactical level. Although its philosophy is that "humans are more important than hardware," it too is acquiring high-quality technical systems such as the Joint Threat Warning System that provides a downlink for intelligence broadcasts and a signal receiver for immediate warning. This system has been designed in body-ware and maritime-based physical configurations to support different SOF operations throughout the world. SOFs also have upgraded and modified the "humvee," known as the SOF Intelligence Vehicle, with communications links and analysis terminals to support analysis for field personnel. During Operational Enduring Freedom in Afghanistan, SOFs demonstrated the ability to identify and communicate potential targets for aircraft to strike. It was the first time in combat that GPS and Predator videos were melded with the observations of SOF personnel (Best 2003).

U.S. Special Operations Command (USSOCOM) is also actively participating in the intelligence community's efforts to develop an adaptable information architecture that provides timely, relevant, and precise information to enable them to collaboratively work with other commands and agencies to support its Global War on Terror (GWOT) mission. For example, the Joint Deployable Intelligence Support System SOCOM Research, Analysis, and Threat

[7] (http://www.dia.mil/thisisdia/intro/index.htm).
[8] (http://www.globalsecurity.org/intell/systems/jiva.htm).
[9] (http://www.tdwi.org/Education/display.aspx?ID=7591).
[10] (http://en.wikipedia.org/wiki/RSTA).
[11] (http://www.defensenews.com/promos/conferences/isr1103/2399864.html).
[12] (http://www.globalsecurity.org/military/systems/ship/systems/cec.htm).
[13] (http://www.globalsecurity.org/military/library/news/2002/05/mil-020518-usn01.htm).
[14] (http://www.fas.org/irp/program/core/ias.htm).

Evaluation System (JDISS-SOCRATES) is an umbrella program with the following capabilities: "access to national, theater, and SOF-specific databases; news service and message traffic; softcopy imagery processing; imagery product archiving and dissemination; analyst-to-analyst electronic mail and chat communications; Intelink and Intelink-S web servers; and secure voice and facsimile" (Wurster 2004, p. 9). The Tactical Local Area Network (TACLAN), an extension of JDISS-SOCRATES, also "provides a deployable command and control system capable of sharing operations, intelligence, and administrative information throughout USSOCOM, the Service components, supported Geographic Combatant Commands, TSOCs, and deployed task forces in all security domains" (Wurster 2004, p. 9). The intent is to provide a "nearly seamless transition of intelligence system connectivity from home station to combat operations" (Wurster 2004, p. 9). The Special Operations Joint Interagency Collaboration Center (SOJICC) also uses "advanced computing capabilities and nodal analysis to rapidly collate, process, display, and disseminate relevant information for timely decision support. The SOJICC information technology is scalable in design and corresponds to current industry standards in data mining, data retrieval, data warehousing, knowledge management, pattern recognition, speech recognition, machine learning/neural networking, audio and video capture, parallel/distributive computing, visualization and search optimization" (Wurster 2004).

The military's overall progress in data collection and analysis can best be illustrated with the movement of data from the reconnaissance platform to the weapon system for action—the so-called "sensor to shooter" sequence. This sequence generally required at least a full day in Operation Desert Storm. First, imagery collected from a satellite or reconnaissance aircraft had to be analyzed. Then targets had to be identified. Descriptions of locations had to be turned into hard-copy and intensively studied by the aircrew before a weapon could be dropped accurately. In contrast, it took only 20 min during Operation Enduring Freedom for Special Operations Forces personnel on the ground to identify a Taliban troop concentration, call the target back to the Combined Air Operations Center in Saudi Arabia, receive permission to call in an air strike, determine the exact coordinates of the enemy using Global Positioning System (GPS), and pass those coordinates to a loitering B-52 bomber using GPS to guide bombs onto the target (Best 2003). Similarly, within minutes of original target identification, Predator UAVs are able to transmit live video pictures to waiting AC-130 gunships which then are able to attack moving targets while the Predator monitors for effectiveness (Best 2003). These examples highlight the recent gains in linking intelligence and operations as well as interoperability among weapon systems and among the services. In terms of analysis, the growth of an intelligence-community-wide secure intranet known as INTELINK has significantly increased the ability of intelligence personnel to access to data, reports of all types, and other analysts, worldwide (Best 2003).

2 Challenges to data collection, processing and analysis

Plans and efforts to counter terrorism, many launched after 9-11, have been impressive in such a short period of time. However, despite the massive efforts, daunting challenges remain. This section reviews some of the major challenges to data collection and analysis in general and to terrorism and insurgency data collection and analysis in particular.

2.1 Challenges of scalability[15]

Scalability is a problem that cuts across all phases of data collection and analysis. It first surfaces in data collection, sometimes referred to as data acquisition, when we understand the massive amount of information being collected. The National Visualization and Analytics Center (NVAC) warns that the "the scale of data is staggering" (Thomas and Cook 2005, p. 2). In 2002 alone, it is estimated that the world produced 5 exabytes (5×10^{18} bytes) of new stored information in the form of paper, film, and electronic media and another 18 exabytes of streaming information. Growth of new storage is estimated to be more than 30% per year (Lyman and Varian (2003) cited in Thomas and Cook 2005, p. 24). Although no estimates are available for the amount and growth of terror-related data, these data are likely to be growing at a comparable rate.

It is true that advances in computer technology performance in terms of processor speed and memory density (which according to Moore's Law tends to double every 18 months while graphics technology tends to double every 12 months), there are limits to what humans can do with the collected data. Although it is a matter of time (some experts say 10 years or more) before the fundamental limitations of physics are encountered in computer and graphics technology, we are asymptotically approaching the limits of human capability to process data that are collected (Thomas and Cook 2005, p. 26). In popular parlance, analysts are suffering from an *information glut* and it is expected to get worse. The problem is *human scalability.* Human abilities and skills are relatively fixed; *they do not scale*

[15] Scalability refers to a system's ability to accommodate a change in load either through contraction or expansion. It can also refer to the ease with which a system component can be modified to accommodate changes in load.

(p. 27). Furthermore, although the number of people involved in counterterrorism and counterinsurgency data collection and analysis does scale (at least theoretically), we do not as yet have the techniques and technology to "'gracefully scale' from a single user to a collaborative (multi-user) environment" (p. 27), especially when working with geographically dispersed teams speaking different languages, using different terminology within the same language, and operating at different levels of expertise in different organizations and institutions.

In addition, we face problems of *information scalability*—the ability to extract relevant information from massive data streams, filter and reduce the amount of data, represent the data in a multi-resolution manner, abstract data sets, handle dynamic data that changes over time, adapt data to different target audiences, and change between and among scales (Thomas and Cook 2005, p. 26).

Analysts also confront *visual scalability* problems—the ability to visually represent massive data sets in terms of the number of individual data elements (Eick and Karr 2002 in Thomas and Cook 2005, p. 26). Currently, only a few techniques in the area of visual representation can handle hundreds of thousands up to one million elements in the data. Yet some counter-terror data requires the processing of tens of millions of new documents per day, with a total database size of tens of billions of documents. At least one existing data base is reported to have 120 billion documents (Thomas and Cook 2005, p. 26–27). Given the pace of data acquisition, it seems very likely that these database sizes will increase dramatically over time.

Display scalability is a related challenge. Currently, visualization techniques do not scale. Most techniques are designed for one size displays—generally a desktop display (1280×1024 pixels). Techniques need to include displays that range from wall-sized displays in fusion centers to PDAs used by field operators.

Software scalability, or the capability of a software system to permit analysts to interactively manipulate large data sets, is also a problem. New algorithms are needed that scale to larger datasets. Software also needs to enable the transfer data across software systems instead of getting data locked into non-interacting systems. Other issues are related to privacy and security, especially when scaling to multi-user environments. Software must protect data from inappropriate access down to the item and individual user level.

2.2 Challenges of data collection

Data are multi-dimensional and vary by source and type which makes the data collection process very complex. As noted above, data or intelligence sources range from *SIGNIT, IMINT* (which also includes *COMINT, ELINT, and FISINT*), *MASINT, HUMINT, OSINT, and GEOINT* Typically these data are collected by different organizations. The CIA and the Defense Intelligence Agency (DIA) produce HUMINT and MASINT; the National Security Agency (NSA) produces most SIGINT; and the National Imagery and Mapping Agency (NIMA), produces most IMINT. Thus, the data are usually collected in separate streams and are have different distribution channels.

Data also vary in types that range from *textual data and databases* to *image sensor, and video data. Textual data* come from documents, news, e-mails and web pages, etc. Current targets aim to support "the rate of one billion new structured messages or transactions per hour, and one million new unstructured messages or documents per hour" (Thomas and Cook 2005, p. 24). *Databases*, constructed to house the data, are diverse and distributed, many of which are localized and difficult to integrate with larger databases. *Image data* is collected by satellites, surveillance cameras, and other visual instruments and its exploding volume is testing data storing and processing limits. *Sensor data,* such as data collected about light, temperature, radiation, location etc., produce very large streaming data. Sensors not only collect and analyze data, but they can communicate among themselves. Unfortunately, the sensor systems collect more data than can be combined and warehoused in a centralized system. *Video data* also produce streaming data that has a temporal dimension that is not easy to integrate with other data types (Thomas and Cook 2005, pp. 24–25). Data types can be refined further by distinguishing whether they are numeric, non-numeric, or both, and how they are formatted in the data collection process. Data formats can range from completely structured, such as categorical data, to semi-structured, such as e-mail, to completely unstructured such as a narrative description. Data can have geospatial characteristics when they are associated with a particular location or region and temporal associations that are discrete or continuous or static and unchanging over time (Thomas and Cook 2005, pp. 108).

Data about dark networks are difficult to collect. Terrorists survive to the extent their actions are hidden from scrutiny. The more successful they are, the more incomplete the data about them will be. Moreover, terrorists have an incentive to obscure and plant deceptive data in order to mislead those who attempt to track them. Thus, most data about terrorists and their operations are likely to have different levels of uncertainty attached to them. These uncertainties will become magnified as data are transformed in the analysis process (see below). In addition, although terror data usually requires input from all the various intelligence disciplines, most people believe that terror data are especially dependent upon HUMINT sources, especially the kind of HUMINT that is far removed from embassy interactions and business functions. Terrorists speak and

write in many different languages and come from many different cultures. Translating and interpreting data about them often requires specialized language ability and cultural sensitivity. These skill sets are in short supply, and given the voluminous data on dark networks, backlogs on translations and data interpretations are a major handicap, especially as the volume of data increases. Furthermore, terrorists' use of new information technology makes it more challenging to collect data about them. Fiber-optic cables make eavesdropping difficult and cell phones, pagers and the internet make it very tedious and taxing to shift through massive amounts of data to find communications of interest.

Data on terrorists are dynamic, not static. Terrorists travel to conduct operations and change venues in order to avoid discovery. They seek out protected enclaves with civilians and neutral parties making their detection and identification difficult. Not only are they a moving target, but a great deal of data collected on their activities are streaming data—data that are continuously being received and updated at such a steady high-speed rate, that in some cases, the data may never be stored. Even if data are stored, they require some combination of bandwidth sufficiency and, for real-time perception of the data, the ability to make sure that enough data is being continuously received without any noticeable time lag (Best 2003). In addition, special databases have to be designed to support the unique requirements of terrorist data. Imagery requires different software, hardware, and bandwidth compared to human intelligence data and each data source typically fills a completely different type of field in a database (Best 2003), making the integration of these data difficult.

2.3 Challenges of data analysis

Data analysis is the preparation, examination and summarization of data for the purpose of extracting salient features, including commonalities and anomalies, discovering new features, developing conclusions, and in the case of confirmatory data analysis, confirming or falsifying existing hypotheses. Unfortunately the explosive rate at which data are accumulating, "our ability to collect data is increasing at a faster rate than our ability to analyze it" (Thomas and Cook 2005, p. 2).

Analysts have the daunting task of gathering the massive amounts of information, sorting through it to find the strands that are relevant to the questions or issues being addressed, becoming familiar with the essential information, and integrating it with the knowledge already gained. Analysts then must generate multiple explanations, sometimes in the form of hypotheses, evaluate the explanations in light of evidence and assumptions, and then make judgments about the most likely explanations or outcomes. At the completion of the analysis, analysts are required to generate reports or other products that summarize their judgments (Tenet 1999: Waltz 2003; Treverton 2001, 2009; Treverton and Gabbard 2008; Treverton et al. 2006). In essence, the analyst's charge is "the application of human judgment to reach conclusion from a combination of evidence and assumptions" (Thomas and Cook 2005, p. 6). These efforts require collaboration with teams of people who typically operate under considerable time pressure often without adequate training, resources, appropriate technology and methods.

Complicating the data processing and analysis are the multiple *levels of analysis* within the Intelligence Community. In the case of DIA, the focus tends to be at the strategic level of analysis level while in the Marine Corps the focus tends to be at the tactical level. For example, the CORP's Intelligence Analysis System brings all data collected by the front-line troops into one location for comparison, analysis, and dissemination. This division of analytic capabilities into different levels of analysis has been a serious problem, particularly for combat troops. An oft-repeated complaint is that data are collected and sent "up the chain" to be analyzed, but never returned to the tactical level in a timely manner in order to inform operations. The charge is that those who need data to conduct day-to-day combat operations are not those for whom the data collection and analysis efforts are designed to support.

Data integration Central to the challenges of data analysis is *data integration*—piecing together relevant information from "divergent multi-source, multi-dimensional, time-varying information streams" (Thomas and Cook 2005, p. 94).[16] Details buried in immigration records, travel documentation, telephone calls, names and locations of suspected terrorists, updates about terrorist financing and facilities and streaming data from sensors have to be synthesized, analyzed, and represented in concert in order to gain insights about what is happening. However, the synthesis is more than integration based on data type. Data come in different levels of abstraction and do not include information at the same meaning level. They need to be integrated in such a way so as to create one consolidated picture of the threat environment. Only then can analysts concentrate on the meaning of the data rather than on the form in which the data are initially packaged (Thomas and Cook 2005, p. 10). Creating this common operational picture is especially difficult when combating very adaptive terrorists and insurgent groups that are constantly changing their tactics and strategies to pursue their aims. There is

[16] See also Best (2003, 2006) and Rollins (2008).

almost no guidance on what data need to be integrated, in what sequence, and with what level of detail.

I have identified three general approaches to data integration in the literature: *discipline-centric; place-centric*; and *virtual. Discipline-centric data integration* evolved from different methodological approaches to data analysis. Figure 1 illustrates a very early example that combines troop strength and movement, geography, time and temperature. The map, based on Minard's 1869 chart, graphically illustrates Napoleon's ill-fated 1812 expedition into Czarist Russia. The size of the grey-colored bar shows the relative strength of the French army as it marched toward Moscow. The black bar reveals how the troop levels declined over time as the temperature dropped and the French retreated into Poland. Only 10,000 troops remained from a force of 422,000.

Other examples of discipline-based data integration are the studies of relationships among terror networks using Social Network Analysis (SNA). Often used by sociologists, this methodology can combine or "stack" information about different relations such as kinship, friendship, finance, education, and religion etc. to form a composite view of the all relationships (Hanneman and Riddle 2005). In Fig. 2, we see how NETDRAW, a SNA software visualization tool, shows three different relations among the terrorists in Noordin's Network of Southeast Asia. Although I am unable to demonstrate the relational ties in greyscale, a representation in colour would identify c*ommunication relations* in red, *meeting* connections in blue, and a *composite of business, friendship and training relations in black*. Green lines would show multiplex or overlapping relations among all those in the terror network.

Place-centric data integration, as the name implies, occurs in one location. Treverton and Gabbard's recent study (2008) found some of the "most interesting" experiments in "multi-INT," as he refers to data integration, depend on small and experimental efforts where analysts have the "license to operate 'within the security fence,' sharing information in ways that the originating agencies probably would not have permitted on a larger scale" (Treverton and Gabbard 2008, p. 41). Typically these "fusion" centers involve groups of people, each with specialized expertise and experience, each drawing on different data sources, and each coming from different agencies or organizations. All share their data and attempt to coordinate their operations. In this instance, *data integration means people integration*—people talking together about their data, deriving some collective interpretation of what they mean, and developing some plan of action.

One variant of place-centric data integration is what has been referred to, in all seriousness, as "wheeled fusion" (Treverton and Gabbard 2008, p. 41). In this instance, one analyst sits on a chair with wheels on it. He then rolls himself back and forth between two rows of long tables, each having a handful of computer screens representing different kinds of data. Data integration under these conditions occurs when the analyst's is able to understand, integrate, and make sense of all the data in his own head.

Recent reports from Iraq indicate that military-led teams coordinated by the Joint Task Force, composed of Special Operations Troops and backed by specialists in intelligence, forensics, mapping, politics and computer specialists piloting unmanned aircraft, have been having some success in counter terror missions. According to a recent interview with Joint Chiefs of Staff Chairman Admiral Mullen, theses fusions cells in Iraq are netting 10 to 20 captures a night (Warrick and Wright 2008).

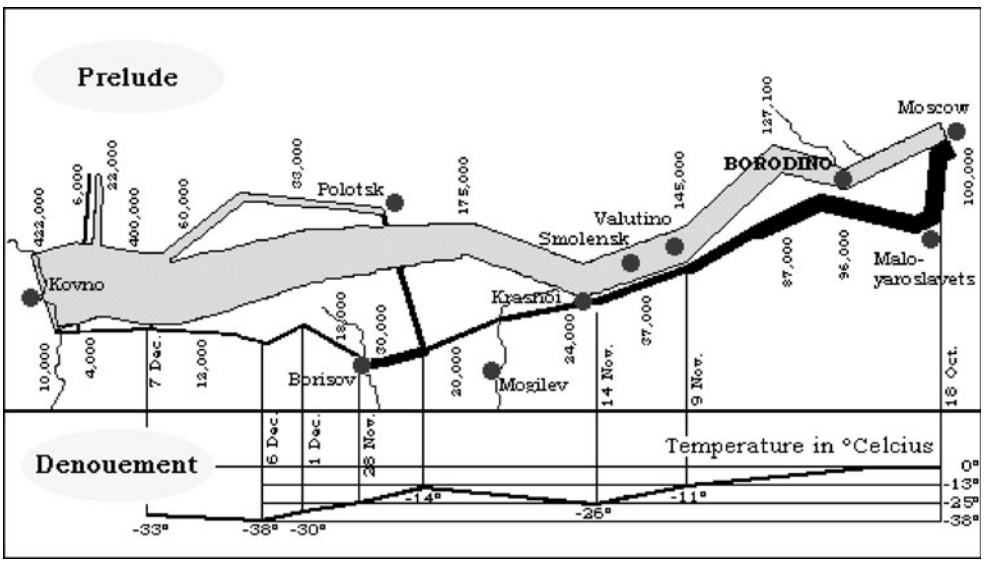

Fig. 1 Napoleon's invasion of Russia, 1812 ((http://uts.cc.utexas.edu/~jrubarth/gslis/lis385t.16/Napoleon/).)

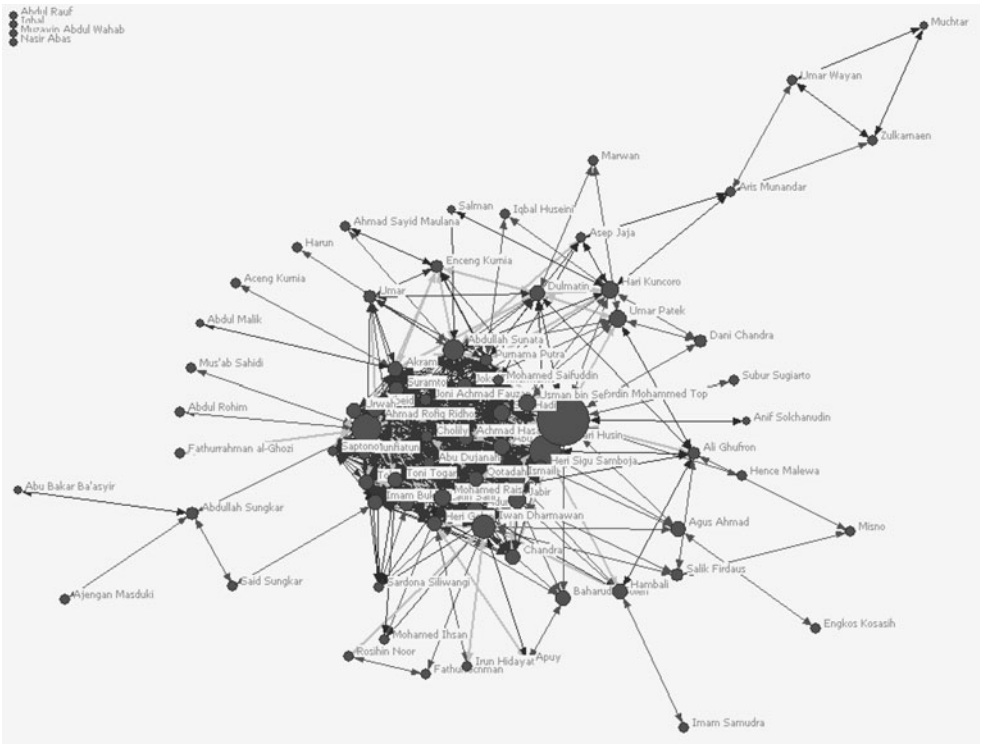

Fig. 2 Data layering using NETDRAW (My thanks to Trond Gimmingsrud of Norway for this representation of Noordin's Networks.)

Many US placed-based data integration such as those in Iraq began with the Department of Homeland Security's strategic plan. The first objective of the plan was "to gather and *fuse*[17] all terrorism-related data and to analyze and coordinate access to it in order to alert people to potential terrorist or other threats" (U.S. Department of Homeland Security, Strategic Plan, 2004, p. 10). In support of this initiative, many state and major urban areas, funded by the federal government, established "fusion centers" for all entities involved in public safety and national security (Rollins 2006). As of February 2009, there were 58 fusion centers around the country[18] in addition to the Coast Guard's two centers located on each coast. Despite the proliferation of these fusion cells, numerous issues concerning their functions and operations await Congressional attention: the clarity concerning the federal government's relationship with fusion centers and the potential for drafting of a formal national fusion center strategy to outline the federal government's clear expectations of fusion centers; the federal government's position on sustained funding; the agreement on metrics to assess fusion center performance; and a definition of what constitutes a "mature" fusion center (Rollins 2006).

Virtual data integration Given the limitations of people's memory and ability to process information,[19] and given the difficulties of assembling experts from various agencies together in one locale, virtual data integration relies on advanced computer and software systems to support virtual data sharing among analysts from many different organizations. A good example of virtual data integration is "A-Space," an on-line collaborative environment that will link all 16 intelligence agencies.[20] A-Space analysts will have access to shared and personal workspaces, wikis, blogs, widgets, RSS feeds and other tools. They also will have a search function that enables them to look for content on other classification domains, including those that allied countries share. Most importantly, they will be able to access data from six data sources from different agencies, including the National Security Agency, State Department and Defense Intelligence Agency and more datasets are expected to be added in the future. Ultimately, the purpose of A-Space is to create an interactive workspace for problem solving around which a community of interest can form to share information, lower barriers to collaboration, standardize analytic processes, and ultimately make information technology invisible to the analyst.

[17] I will use the word 'fusion' in a more precise way as we will see below. In general, practitioners use the word fusion to refer to 'one-stop shops' where coordination across all sectors and levels of government occurs.

[18] http://www.dhs.gov/xinfoshare/programs/gc_1156877184684.shtm.

[19] See George A. Miller. "The Magical Number of Seven, Plus or Minus Two." *The Psychological Review*, 1956, vol. 63, Issue 2, pp. 81–97

[20] http://en.wikipedia.org/wiki/US_intelligence_community_A-Space.

A-Space went live on the government's classified Joint Worldwide Intelligence Communications System September 22, 2008. Sponsored by the Office of the Director of National Intelligence overseen by the Defense Intelligence Agency, it is based on the standards the Army and the Defense Department are using for the Army and Defense Knowledge Online portals. Initial tests of A-Space are limited to top-secret information, but secret and unclassified information is expected to become available as the portal develops.

Data layering and data fusion There are at least two versions of technical data integration that I have been able to identify: *data layering and data fusion.*[21] *Data layering* refers to the overlay of data on a pictorial image. In the case of data layering, data are assigned to a general area of the map rather than geo-coded to a specific location. For example, Fig. 3 illustrates data layering by indicating the variation in sigacts (significant activity) based on incident levels in each Iraqi district. The darkest districts represent the highest levels of sigacts and the lightest districts represent the lowest levels. Figure 4 illustrates data fusion, where each data point is geo-coded and overlaid on a specific location on the map.

Data layering while useful, does not lend itself to further data analysis since no data underlie the actual images. The images are only suggestive not definitive and require additional analysis with other analytic tools. Data fusion, in contrast to data layering, co-registers information on a map display to a precise geographic grid (Treverton and Gabbard 2008, p. 9). In other words, different data types, not just pictorial images of the data, are overlaid on *the same geospatial coordinates*. This type of fusion is enabled by software such as ARC-GIS which integrates information about the human and the geographic terrain. So for example, the map of Sudan in Fig. 5 illustrates fused data that identifies the precise location of villages that have been completely or partially destroyed, along with locations of the roads, IDP camps, population centers, international and administrative boundaries, refugee sites and camps, cities, and airports. Each piece of information is overlaid on specific geospatial coordinates to create this comprehensive overview. Fused data can then be subjected to further analysis to explore the relationships among the data coordinates as a whole.

Data integration at the fusion level is much more difficult to achieve than at the level of data layering. Getting good data to fuse, especially for those working with open sources, is the most fundamental issue, but there are other considerations as well. Not all data can be geospatially fused. Terror relationships are not usually anchored to specific geospatial coordinates. And relational data, like all non-spatial information, must be synthesized at *the meaning level* before it can be integrated with spatial data. How this integration occurs, in what sequence and with what software capability is beyond the scope of this paper.[22] Suffice it to say at this point, data fusion as it is defined in this section of the paper is a goal but not as yet a well-supported practice.

2.4 Challenges and their consequences in field settings

The problems of scale and the challenges of data collection and data analysis outlined above have produced serious consequences in operational environments like Iraq and Afghanistan. In a recent study entitled *Analytic Support to Intelligence in Counterinsurgencies,* Perry and Gordon (2008) identify the limitations that currently exist despite the advances made in data collection and analysis. Section 2 closes with what they have identified as some of the more serious lapses in our most recent counter-terror and counterinsurgency efforts. They serve as a reminder of the work that still remains:

- Although other sources of data about enemy activity in Iraq are available, the Multinational Command Iraq's (MNC-I) major source of information on enemy activities in Iraq is the significant activities (SIGACTS) report.[23]
- Most data collection supports operations and not analysis. Consequently, data "vary in terms of quality, accuracy, timeliness, completeness, consistency" (p. 25). Convincing commanders to collect additional data or to collect data in formats more amenable for analysis has been difficult.
- Reporting is uneven. Data are "coded" differently by different units. What is considered a "significant incident" varies with the reporting unit's experience. Units early in their tours record most incidents even minor ones while those later in their tours report less frequently.

[21] The use of the terms data fusion in this section has a very specific meaning. It refers to information that is co-registered to a precise geographic grid (Treverton 2008, p. 9).

[22] Readers are advised to consult the book edited by James J. Thomas and Kristin A. Cook entitled *Illuminating the Path: The Research and Development Agenda for Visual Analytics* for some of the more technical issues involved in data integration.

[23] SIGACTS (significant activities) are recorded online at the brigade level using an online system called the Combined Information Data Network Exchange (CIDNE). A significant activity is defined as any incident deemed important enough to record. For example, attacks on convoys or locating a weapons cache are considered significant activities.

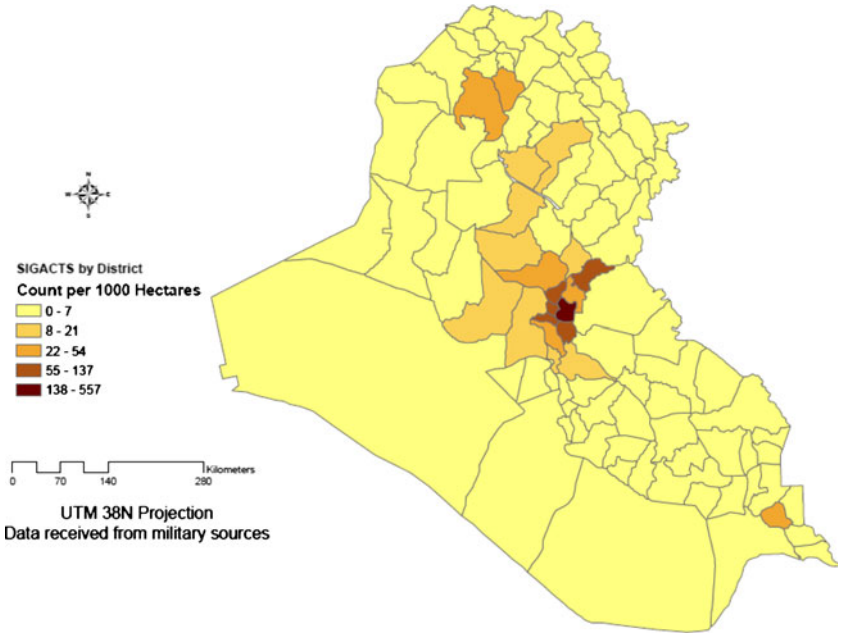

Fig. 3 SIGACTS in Iraq 2005–2008

- Multiple databases exist and are not linked or cross-referenced in Iraq, and to some degree in Afghanistan, such as the SIGACTS database and CEXC database which contains forensic data. Many databases are stored locally and are not easily accessible.
- A standard lexicon is lacking. Database terms are not consistent and only recently have standard definitions been applied to data entries in Iraq.
- Most data in Iraq and Afghanistan are collected on enemy activities, but data on "friendly operations" are generally not collected. In an insurgency, it is important to know what friendly units are doing not just what the insurgents are doing.
- The sharing of data, much of it time-sensitive, is often inhibited or prohibited by bureaucratic procedures among organizations that dealing with insurgencies

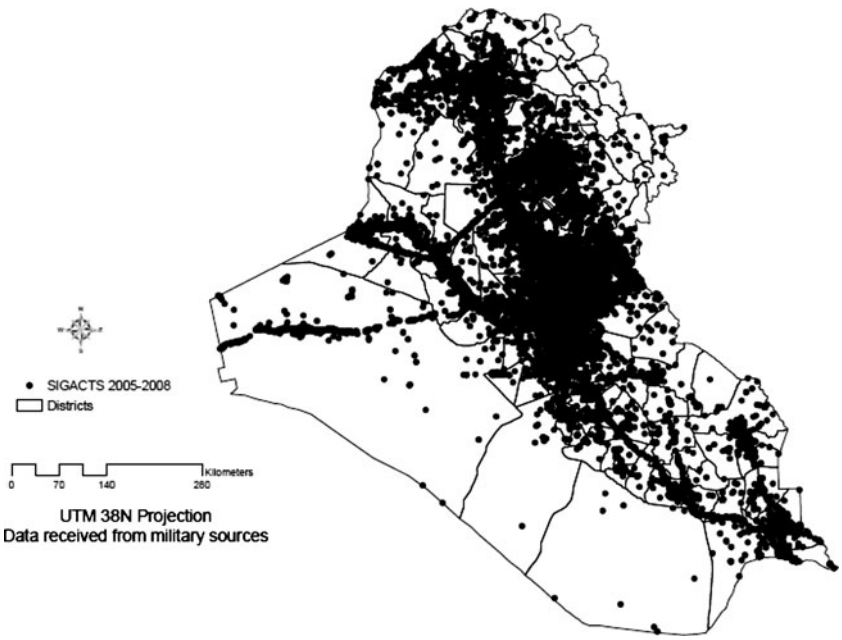

Fig. 4 SIGACTS in Iraq 2005–2008

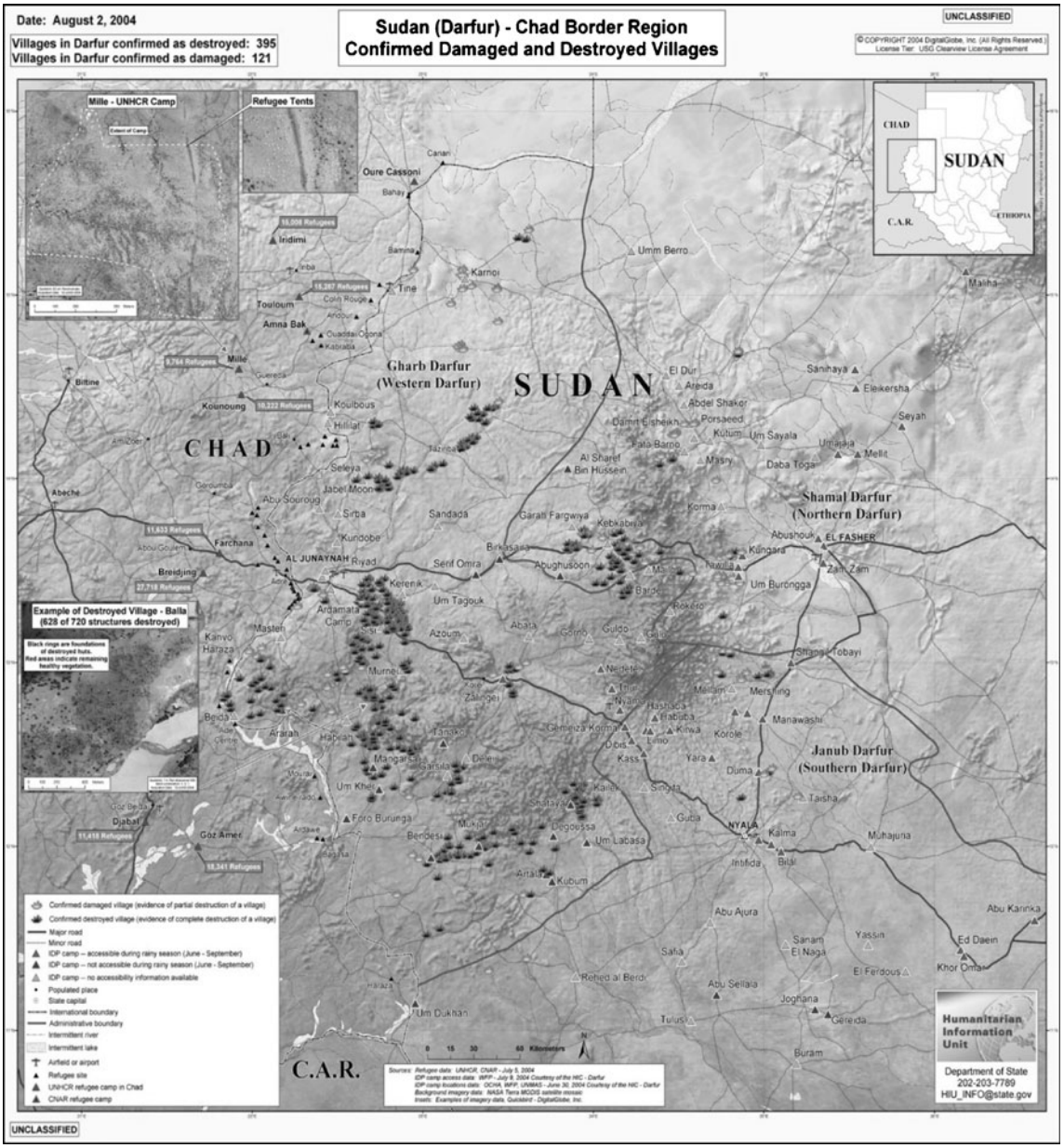

Fig. 5 Data fusion of human and geospatial data of the Sudan (My thanks to Ben Maitre for this representation of the destruction in Darfur.)

and terrorists. Sharing intelligence (data) among allied nations is difficult making analysis particularly problematic (pp. 26–28).

3 The future: Technological support and the new field of visual analytics

Getting the appropriate computer equipment with the appropriate software systems into the hands of those collecting and analyzing data is critically important in counterterrorism and counterinsurgency operations. Unfortunately, according to recent study by the National Visualization and Analytics Center (Thomas and Cook 2005), "current technologies do not address the needs for handling these massive, messy, diverse, and ever-changing volumes of information" (p. 2), nor do they provide support for the complex tasks involved in the analytical and discovery process. In fact, very few of technologies even address the need to communicate with their audiences about their analytical results and products. (p. 2). The study's authors further state that although we do have numerous hardware and software systems to help analysts process, organize, and explore data, we are "only scratching the

surface in terms of meeting the true analytical needs" (Thomas and Cook 2005, p. 23).

For Thomas and Cook and others, one solution is the creation of *software* that will support analysts in the most time consuming and complex aspects of the analytical process (p. 23). The software has to be built on the foundations of reasoning, sensemaking, cognition and perception in order to support collaborative analytical processes about complex and dynamic problems (p. 6). It must have better displays or "spaces" to contain the relevant data so analysts can visualize the connections among relevant information from the different source streams in order to integrate the data and gain insights from them (Thomas and Cook 2005, pp. 94–98). Furthermore, analysts must be freed from the constraints of current tools that require them to analyze data of different types separately. They need to be able to consider all information/data together, without being restricted by format, type, or source, including data in motion or streaming data so they can detect changes. Ultimately, analysts need to go beyond the current data-type-centric modes of analysis to support work with dynamic data of all types in a "seamless environment" (p. 127, p.131–133).

3.1 The discipline of visual analytics

In an effort to address these technological deficiencies, the Department of Homeland Security (DHS), under the leadership of the Pacific Northwest National Laboratory (PNNL), chartered the National Visual Analytics Center (NVAC) in 2004. NVAC provides strategic direction and coordinates activities to discover, develop, and implement innovative visual analytic methods. The Center's primary goal is to establish a long-term research and development agenda for Visual Analytics—specifically "the creation of *software systems* that supports the analytical reasoning process" (Thomas and Cook 2005, p. 34, emphasis added).

NVAC is central to the emerging science of Visual Analytics—a multidisciplinary field dedicated to improving data collection and analysis through the use of computer-mediated visualization techniques and tools. The purpose of visually-based analytical reasoning, or visual analytic discourse, is to maximize human capability to perceive, understand, make judgments and work collaboratively with multidimensional, conflicting, and dynamic data, such as terrorism data. Formally, Visual Analytics is defined as "the science of analytical reasoning facilitated by interactive *visual* interfaces" (Thomas and Cook 2005, p. 4, emphasis added). Visual Analytics concentrates on four major areas:

- *analytical reasoning techniques* (e.g. developing alternative explanations, hypothesis testing, developing scenarios) that enable users, both individually and collaboratively, often under extreme time pressure with limited and conflicting data, to probe data, gain insights and apply judgments in order to reach conclusions that will inform assessment, planning, and decision making;
- *Visual representations and interaction techniques* that enable users to see, explore, and process large amounts of data at once;
- *Data representations and transformations* techniques that convert all data types, including conflicting and dynamic data, in ways to support visualization and analysis;
- And *production, presentation, and dissemination techniques* that enable the user to transmit the results of the analysis to appropriate audiences (Thomas and Cook 2005, p. 4).

New visualization software tools are critical to the analytical reasoning process. The ultimate goal for visualization software is to maximize the human capacity to perceive, understand, and reason about complex data and situations. To reach this goal, software must be built on theoretical foundations and principles of reasoning (both convergent and divergent thinking), sense-making, cognition and perception. The software also needs to enable analysts to focus on what is important, solve problems at multiple levels of abstraction, reason about situations that can change rapidly, and collaborate with others who come from different organizations, backgrounds and levels of expertise.

3.2 Developing software platforms for analysis

Contributors to the growing multidisciplinary field of Visual Analytics are developing the software tools and capabilities to represent and integrate our data through layering and data fusion techniques. Two excellent examples of these types of software platforms are Palantir Technologies[24] and ORA.[25] Palantir Technologies is a leading company noted for its integration of structured and unstructured data sources and its ability to draw in all types of data, including message traffic, link charts, spreadsheets, text as well as SIGNINT, ELINT, and IMINT. Its capability of fusing geospatial and temporal data is particularly useful to commanders and field-based intelligence cells.[26]

ORA is a dynamic meta-network assessment and analysis tool developed by CASOS at Carnegie Mellon. It contains hundreds of social network analysis metrics and recently has added two new tools—Loom and ORAGis—to the ORA Platform that enable the analysis of spatially and temporally continuous data captured by sensor systems e,g,

[24] http://www.palantirtech.com/government/intelligence

[25] http://www.casos.cs.cmu.edu/projects/ora/

[26] For an example of a Palantir analysis see http://www.palantirtech.com/government/analysis-blog/afghan-conflict

GPS sensors embedded in vehicles or logs of activities. This capability has enabled researchers, for the first time, to fuse spatial, temporal and relational data.[27]

We have monumental data collection and analysis tasks before us in order to counter terrorism (Davis et al. 2004; Treverton 2009) and insurgencies (Perry and Gordon 2008). As summarized above, challenges are great and solutions will not be short-term or easy. Palantir and ORA, two software platforms developed for the intelligence community, are a good example of the way forward in Visual Analytics. Despite the challenges enumerated in this brief overview, they signal the progress made to date and illustrate the opportunities that await other IS researchers interested in applying their knowledge and skills to the tracking and disrupting of dark networks.

References

An Overview of the United States Intelligence Community (2007). Retrieved from http://www.dni.gov/overview.pdf, August 15, 2008.

Best, R. A. (2003). Military transformation: Intelligence, surveillance, and reconnaissance. *Report for Congress*, Order Code RL31425, January 17, 2003. (Updated Chizek, 2003 report).

Best, R. A. (2006). Intelligence Issues for Congress. *CRS Issue Brief,* IB10012. Updated May 9, 2006. Retrieved from http://fpc.state.gov/documents/organization/66506.pdf.

Carter, N. (2008). Joint Interoperability Division helps training take flight. Retrieved from http://www.jfcom.mil/newslink/storyarchive/2008/pa040808.html.

Chizek, J. G. (2003). Military transformation: intelligence, surveillance and reconnaissance. Order Code RL31425. Updated January 17, 2003.

Davis, L. E., Treverton, G. R., Byman, D., Daly, S. & Rosenau, W. (2004). Coordinating the war on terrorism. OP-110-RC. Santa Monica: RAND.

Department of Defense, *Joint Publication 1-02, DOD Dictionary of Military and Associated Terms*, 12 April 2001, as amended 15 Oct 2001.

Eick, S., & Karr, A. (2002). Visual scalability. *Journal of Computational and Graphical Statistics, 11*(1), 22–43.

Goodman, G. (2003). Introductory remarks Nov. 17 at ISR Integration 2003: The Net-Centric Vision. Conference. Retrieved from http://www.defensenews.com/promos/conferences/isr1103/2399864.html.

Hanneman, R. A., & Riddle, M. (2005). *Introduction to social network methods.* Riverside, CA: University of California, Riverside (published in digital form at http://faculty.ucr.edu/~hanneman/)

Larson, E. V., Eaton, D., Nichiporuk, B., & Szayna, T. S. (2008). *Assessing irregular warfare: A framework for intelligence analysis*. Santa Monica: Rand.

Lyman, P., & Varian, H. R. (2003). How much information. Available at http://www.sims.berkeley.edu/how-much-info.

Miller, G. A. (1956). The magical number of seven, plus or minus two. *The Psychological Review, 63*(2), 81–97.

Nagle, D. (2002). NNS020517-10. Naval Fires Network: The Transformation of Naval Warfare. Retrieved from http://www.globalsecurity.org/military/library/news/2002/05/mil-020518-usn01.htm.

Perry, W. L., & Gordon, J. (2008). *Analytic support to intelligence in counter insurgencies*. Santa Monica: RAND.

Rollins, J. (2006). "Fusion Centers: Issues and Options for Congress." RL34070. Updated January 18, 2008. http://www.fas.org/sgp/crs/intel/RL34070.pdf

Thomas, J. J., & Cook, K. A. (eds.). (2005). *Illuminating the path: The research and development agenda for visual analytics*. National Visualization Center.

Tenet, G. J. (1999). *Consumer's guide to intelligence*. Collingdale: Diane Publishing Company.

Treverton, G. F. (2009). *Intelligence for an age of terror*. Santa Monica: Rand.

Treverton, G. F. (2001). *Reshaping national intelligence for an age of information*. Cambridge: Cambridge University Press.

Treverton, G. F., & Gabbard, C. B. (2008). *Assessing the Tradecraft of Intelligence Analysis*. Santa Monica: Rand. http://www.rand.org/pubs/technical_reports/2008/RAND_TR293.pdf

Treverton, G. F., Jones, S. G., Boraz, S., & Lipscy, P. (2006). *Toward a theory of intelligence. Workshop report*. Santa Monica: Rand.

U.S. Department of Homeland Security. (2004). *Securing our Homeland: U.S. Department of Homeland Security Strategic Plan*. Washington, D.C: Department of Homeland Security.

Waltz, E. (2003). *Knowledge management in the intelligence enterprise*. Boston: Artech House.

Warrick, J., & Wright (2008). U.S. teams weaken insurgency in Iraq. *Washington Post*, Saturday, September 6, 2008; A01.

Wurster, D. (2004). Statement of Brigadier General Donald Wurster, U.S. Air Force Director, Center for Intelligence and Information Operations, United States Special Operations Command before the Strategic Forces Subcommittee for the Senate Armed Services Committee on the fiscal year (FY) 2005 Tactical Intelligence and Related Activities (TIARA) and Joint Military Intelligence Program (JMIP) Budget Requests, April 7. http://www.iwar.org.uk/sigint/resources/defense-intelligence/Wurster.pdf

[27] For an example of fused geospatial, temporal, and relational data, see http://www.casos.cs.cmu.edu/projects/ora/jfolson-SI08-poster-final.pdf.

Nancy Roberts is a Professor of Defense Analysis and Co-Director of the CORE (Common Operating Research Environment) Lab in the Defense Analysis Department, in the Graduate School of Operational and Information Sciences at the Naval Postgraduate School in Monterey, California.

Dr. Roberts received a PhD from Stanford University, a MA and BA from the University of Illinois, and a Diplome Annuel from the Cours de Civilization Francaise at the Sorbonne. Her previous faculty appointments have been at the Graduate School of Business at the Naval Postgraduate School, the Carlson School of Management at the University of Minnesota, and the Graduate School of Business at Stanford University as a visiting associate professor.

She has published extensively in the areas of public entrepreneurship and innovation, strategic management and planning, leadership, stakeholder collaboration, complex networks, dialogue and deliberation. Her current research focuses on "wicked problems" such as the tracking and disrupting of terror networks and the organizational challenges of post-conflict reconstruction. She is the co-author of *Transforming Public Policy: Dynamics of Public Entrepreneurship and Innovation* (1996) and editor of two books—*The Transformative Power of Dialogue*

(2002) and *Direct Citizen Participation* (2007). Dr. Roberts is also an Associate Editor of PAR, and serves on the editorial boards of *Public Management, The American Review of Public Administration, and International Public Management Review.*

Her current teaching assignments include three courses: *Visual Analytics; Planning and Organizing in Complex Networks*; and *Coping with Wicked Problems*. In her position as Co-Director of the CORE Lab, she created and developed the Defense Analysis course *Tracking and Disrupting Terror Networks*. Under the auspices of the Lab, she now leads teams in the investigation of the geospatial, temporal, and relational dimensions of terrorist networks and the development of strategies to counter them.

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.