12th International Conference on Information Fusion
Seattle, WA, USA, July 6-9, 2009

Estimation of adversarial social networks by fusion of information from a wide range of sources

John R. Josephson jj@cse.ohio-state.edu
Joshua Eckroth eckroth@cse.ohio-state.edu
Timothy N. Miller millerti@cse.ohio-state.edu
Laboratory for Artificial Intelligence Research
Computer Science & Engineering Department
The Ohio State University

Abstract – *A data structure is described that serves to define a target structure for estimating social networks. It represents who knows whom, the strength and polarity of associations, and levels of confidence that linked individuals are actually personally acquainted. This network, which represents social structure, is embedded in a more inclusive network structure that also represents vehicles, places and organizations. This broader structure can be used to accumulate information to enable automated inferencing to assist human processing in estimating the social network of interest. How portions of this inferencing can be done is briefly described, and a scenario is given that illustrates the use of this kind of fused information to make a decision. We also review a range of hard and soft information sources with emerging value for estimating adversarial social networks, and describe how these sources can be used for the purpose.*

Keywords: Information fusion, soft information, social networks, biometrics, asymmetric warfare, urban operations

1 Introduction

The attacks of 9/11 challenged the United States with a massively distributed, decentralized, and somewhat amorphous global adversary, who is still at war with America, and continues to be a threat. To respond appropriately, defense intelligence is needed at the level of individual human beings and their relationships. Fortunately, recent rapid progress in technology has produced reliable biometric sensors, along with new sensors of many kinds, backed by new algorithms, faster computers, and better networking. Progress has also been made in technologies for databases, enterprise-level computing, natural language processing, internet search, and information display. As a result, a wide range of information is now readily available for defense intelligence that previously was not recorded, or not recorded in digital form, not accessible through information networks, or not processable. And the information revolution continues. Thus, there is a need, and an opportunity, for rapid progress in providing decision makers with needed information regarding individual humans and their relationships.

Relevant information occurs in many forms, but to be useful, it must be gathered, combined, abstracted, provided, and presented. Where this processing of information is not automated, much relevant information will remain beyond reach, because it has such high requirements for the relatively scarce available resources of trained, and informed, human attention. Thus, automation is needed to enable effective use of the abundance of available, relevant information–for defense intelligence in general, and for estimating adversarial social networks in particular. (We use the term 'estimating' here, rather than, for example, 'determining,' to suggest that often best-guess hypotheses are already useful for decision making, and in any case, higher levels of confidence will commonly come to best-guess hypotheses by accumulating additional supporting evidence.)

Adversarial social networks are presumably embedded in larger networks of social relationships about which information is available, and estimating who is an adversary may be a large part of the problem. Adversarial social networks are presently estimated almost exclusively from human sources of information, "soft" sources, such as informants, detainees, and field reports, augmented with intelligence from captured documents and intercepted communications that has been human-processed to extract the relevant pieces. In this paper, we suggest ways to use various types of 'hard' information, processed automatically from physics-based sensors, to build, augment, and annotate social network representations that also rely on evidence from soft sources. We review a range of enabling technologies that are either presently in use, or presumably will soon be available.

However, social network information is not easily found in hard information sources, so one main function of this pa-

per is to point out some available sources, and suggest ways to extract relevant information. Automatic extraction of information about social networks from soft sources will often depend on natural language processing, which attempts to extract references to human individuals, and infers relationships from proximity in the text, or by using linguistically more sophisticated methods to estimate what is being asserted about the individuals referred to. Difficulties in processing text, and speech, come from many sources, including the use of different names to refer to the same individual, the difficulty of processing pronouns, and inconsistent transliteration of non-English names [9, 22]. As a result, at the present time, practical use of soft sources usually requires manual tagging of input data and manual generation of thesauri to relate similar names [9].

Drawbacks of individual technologies can presumably be mitigated by fusing information from many sources, which permits more reliable information to override less reliable information, as well as opportunistic gathering of information wherever it appears, and exploitation of the sheer abundance of information to overwhelm and correct mistakes.

The remainder of this paper is organized as follows. In Section 2, a relatively simple data structure is described for representing social networks, along with a more inclusive data structure for representing related information expected to be useful for inferring social relationships. Suggestions are given for elaborations of the data structure, and for metadata annotations to support automatic processing and human oversight. In Section 3, we review a range of hard and soft sources of information, and describe how the information can be used for estimating social networks. This is followed, in Section 4, with an example scenario that illustrates the use of this kind of fused information to make a decision.

2 Data structures

We begin by representing a "social network," as such, as a network data structure (a mathematical graph), where the nodes represent human individuals, and the presence of a link between two nodes represents the fact that the corresponding individuals are personally acquainted, either face-to-face, or by bidirectional communications. That is, the intended semantics of a node is to represent a human individual, and the intended semantics of a link is to represent the relationship of being personally acquainted.

In addition, we suppose that a link has positive or negative *polarity*, respectively indicating that the individuals have a cooperative/trusting relationship, or an antagonistic relationship. A link also has a *strength*, which represents the strength of the relationship, which, for positive polarity, is the degree of trust or active cooperation, and for negative polarity, the degree of mistrust or active antagonism. We suppose that the default for an existing link is positive polarity with weak strength.

Nodes in this network, representing individuals, are associated with representations for various attributes of the individuals, such as name and biometric identifiers, while links are associated with specifiers for polarity, strength, and (optionally) type of relationship. The following attributes are initially provided:

- *Person attributes* — name, aliases, fingerprint pattern (for each finger), face pattern (for facial recognition), voice pattern (for voice recognition), iris pattern, biometric ID.

- *Person–person link attributes* — polarity, strength, type (close relative, friend, neighbor, superior-subordinate, customer, comrade, ...)

This network represents the target structure for estimating a social network. It defines what we want to estimate, and defines the data structure for representing and storing the results. These results will presumably be provided to intelligence analysts and decision makers through software tools that enable browsing, searching, inspection, and hand correction.

We suppose that this network structure, for representing individuals and their relationships, will be embedded in a more inclusive network data structure, for linking the social information with additional information expected to be useful for inferring relationships of individuals, and for other purposes related to potential actions. Thus, we suppose other types of nodes representing other types of entities, specifically, vehicles, locations, and organized groups of individuals, and appropriate types of links, initially as follows:

- *Vehicle attributes* — type (auto, truck, bus, donkey cart, APC, boat, ...), owner, license plate jurisdiction and number, vehicle identification number, make, model, year, color, photograph.

- *Location attributes* — name, aliases, address, geolocation (latitude, longitude, altitude), boundaries, extent (person capacity, physical area), floorplan.

- *Group attributes* — name, aliases, type (family, political party, faction, sect, tribe, militia, insurgent group, ethnic group, tactical unit, government, ...), number of members.

Each attribute will have associated metadata, including an estimate of reliability. When nodes are merged (described below), this estimation of reliability will be considered when attributes contain conflicting information.

Links represent relationships between entities represented by nodes. Links also have attributes. We provide for potential links between the following pairs of node types:

- *Person–location link attributes* — Person was at the Location (at a certain time), Person resides at the Location, Person is frequently at the Location.
- *Person–vehicle link attributes* — Person owns Vehicle, Person rode in Vehicle (at a certain time), Person drove Vehicle (at a certain time), Person frequently rides in (or drives) Vehicle.
- *Vehicle–location link attributes* — Vehicle was at Location (at a certain time), Vehicle is frequently parked at Location, Vehicle exploded at Location (at a certain time).
- *Person–group link attributes* — Person is a member of the Group (or Person is antagonistic to the Group), role of Person in Group (leader, follower, patriarch, donor, fighter, ...).
- *Vehicle–group link attributes* — Vehicle belongs to Group.
- *Group–Location link attributes* — Group has significant presence in Location (a region), Group has headquarters at Location, Group has facility at Location.
- *Location–Location link attributes* — Location overlaps with Location, Location is contained in Location, Location is contiguous with Location, routes from Location to Location.
- *Group–Group link attributes* — Group overlaps with Group (has common members), Group contains Group, Group is allied with Group, Group is hostile to Group.

The existence of entities, and of relationships among them, change with time, as do the attributes of entities and relationships. We presume that it will be useful to keep track of this kind of historical information by recording it in the data structure, but we will not address these complications in this paper. Also, different relationships may imply different timespans, such as the implied short timespan of "vehicle X was near road sensor Y at time T" versus the implied perpetual timespan of "person X is the cousin of person Y." Again, we will not address these complications. Note that it is important to distinguish changes in entities and relationships, from changes in the data structure representing them. The latter may represent only changes in the available information, or changes in estimates of ground truth.

We presume that, when the data structure is modified, the provenance of the information causing the modification is recorded. For example, if a person-person link is created because of a report of two persons riding in the same auto at the same time, then a hyperlink to the report is saved in a log associated with the link, which is created along with the link. This log, and information about provenance, is made available for analysis, allowing users to judge the truthfulness or reliability of the information. Additional informative information might also be recorded in the log, such as, "Person A received weapons from Person B."

When a new node is a candidate for inclusion in the network, the possibility must be considered that the node would be a duplicate of one already present. In general, a node will be added when a matching node is not found (e.g., a person with that name is not found). However, because names may be spelled differently, or a name may be an alternative name for the same entity, mistakes will inevitably be made, and, at some point, it will be necessary to merge two or more nodes into one, after concluding that they represent the same entity. This process might be performed manually or automatically. As long as there are no contrary attributes, nodes can be merged by taking the set union of their links and attributes. Nodes might be merged automatically when an existing node's attributes are updated, and when those new attribute values cause the node to be a duplicate of another node. For example, a person node might be updated to include a fingerprint pattern. The system will attempt to match this fingerprint pattern with those of other person nodes. If a match is found, then these two nodes will be merged. If the same attribute of the nodes have contrary values, the attribute with the higher confidence will prevail. The system thus avoids duplication of nodes by merging nodes whenever enough information exists to determine that they probably refer to the same entity.

It is also possible for a single node to mistakenly refer to two different people or objects. A node can be automatically marked for suspicion of being a duplicate based on information such as that recording the same person as being in two non-overlapping locations at one time. Under some conditions, the node could be automatically split in two by replaying logs of reports and assigning attributes to the most compatible candidate. As more information is added to the network, the identities will presumably further diverge, and misattributed metadata might be corrected.

Reliability or credibility tags also permit views of the network that filter out all but the "hard core" consisting of the most reliable information (e.g., relying on biometrics or high-reliability soft sources providing structured information, with no intervening unreliable processing). After viewing "hard core" information, views showing information of lesser reliability might be incrementally shown. In this way, decision makers would be able to judge whether the information is reliable enough for actions being considered. For

example, lethal force should only be applied based on information of high reliability, while information of much lower reliability might be the basis for decisions about reconnaissance priorities.

In the following section we review a range of hard and soft sources of information, describe related technologies, and describe how information from these sources can be fused to estimate a social network, represented in the data structure just described.

3 Fusion of hard and soft information

3.1 Hard information

We first address 'hard' information sources, which are typically excluded from social network estimation because social relationships are difficult to detect. With the development of biometrics, license plate recognition, RFID, and other technologies, automated analysis of social relationships in hard information sources is becoming feasible.

3.1.1 Biometrics

Biometric technologies have recently become available that are sufficiently reliable for military uses. They are highly practical and effective for the myriad of tasks that require high-reliability human identification and identify verification. Their benefit to national defense is well-understood: the Department of Defense has created the Biometrics Management Office and the Biometrics Fusion Center [38] in their pursuit of 'identity dominance' [37]. Additionally, since 2004, the Pentagon has been building an enemy biometric database [30]. It is clear that accurate estimation of social networks depends on accurate estimation of human identities, and biometric technologies play a key role.

A range of biometric technologies are available. Fingerprint identification, the oldest such technology, is also one of the most reliable and distinct. Hand and finger geometry (measuring the widths and lengths of various portions of the hands and fingers) and voice recognition, however, suffer from less distinctiveness [39]. Less distinctiveness means that several people might share the same measurements, so specific identification becomes impractical, although verification is possible when membership in a particular measurement class is rare.

Facial recognition is moderately distinct but can be performed at great distances. We discuss this technology more in Section 3.1.2. Iris and retinal scans, on the other hand, are highly distinct, and iris scans may even be performed at highly practical distances (3–6 meters), and simultaneously for multiple subjects [1]. The iris may also indicate ethnicity [29] and gender [33]. Retinal scans are less common and are considered more intrusive upon medical privacy because retinal changes can reveal medical conditions, such as pregnancy or AIDS [25].

Biometric	Identify/ Verify	How Distinct	How Intrusive
Fingerprint	Both	High	Touching
Hand geometry	Verify	Low	Touching
Facial recognition	Both	Moderate	300 meters
Voice recognition	Verify	Low	Remote
Iris scan	Both	High	3–6 meters
Retinal scan	Both	High	1-2 inches

Table 1: Comparison of biometric technologies (Adapted from [39])

Most technologies require subject cooperation during enrollment (the process of obtaining a pattern for purposes of future identification or verification). Enrollment for facial recognition is possible even for non-cooperating subjects [23].

A summary of these popular biometric technologies is provided in Table 1. From the table, we see that hand-geometry recognition and voice recognition are better suited for verification than for identification. Verification technologies are most useful for corroborating other evidence. That is, when voice data or hand geometry data is available, the reliability of an identification may be increased by relying on one of these technologies.

Each technology can be deployed in a range of situations. Gathering fingerprints is standard behavior in police and military forensics. Hand geometry recognition may be used to protect access to restricted areas. Facial recognition systems can be used to monitor crowds, roads, and other public areas. Voice recognition can be used on eavesdropped conversations and broadcasts. Finally, iris scans are possible in any area that attracts a subject's gaze, such as ATMs, storefront windows, tollbooths or checkpoints.

The Department of Defense has found success with its Biometrics Automated Toolset (BAT) and peripheral Handheld Interagency Identity Detection Equipment (HIIDE). These devices provide an all-in-one fingerprint, iris, and photograph enrollment system. The BAT unit can perform the full range of identification and verification tasks, while the portable HIIDE can verify identities against a watchlist [3]. As of late 2007, over 2,000 units have been deployed with more than 560,000 enrollments [2].

Whenever biometrics are used, the network representation may be augmented to include information about persons (individuals who have been identified or verified) and places (where the identification or verification took place). Additional examples of the use of biometrics appear in following sections.

3.1.2 Video surveillance

Video surveillance is a widespread technology of increasing maturity. Many algorithms exist for tracking moving entities. Finding social relationships in video, however, requires additional capabilities that can identify persons, vehicles, and places, and recognize social behavior such as engaging in conversation, or walking together.

Face recognition and gait analysis are the best candidates for automatically identifying persons in video. Reasonably reliable algorithms exist for face recognition at a distance (up to 300 meters outdoors) [40] and under various lighting conditions, often on-par with, or surpassing, human abilities [27]. Modern approaches may involve single-camera 2D images or multi-camera 3D reconstructions, and may pair visual and infrared spectra [5, 19]. Although gait recognition is not as mature as face recognition [4], high reliability can be obtained, even at large distances, and from arbitrary points of view, by combining the two methods [10, 8].

Vehicles are of interest when estimating social relationships because a social relationship can usually be inferred when two people ride together in the same vehicle. Moreover, vehicles are relatively easy to track and may lead to key places. They are also relatively easy to identify. License plate recognition can be performed with high accuracy [7], very rapidly [41], even in complicated, poor-quality images [17]. Multiple license plates with various orientations can even be detected in a single image [14]. Once a vehicle's license plate is identified, the owner of the vehicle may be identifiable by database lookup.

3.1.3 Unattended Ground Sensors

A variety of unattended sensors in common use today fall under the label 'unattended ground sensors' (UGS). Typical sensors include seismic, acoustic, infrared, and optical sensors, and are often small, lightweight, wirelessly networked to a common processing system, and deployed over vast regions. With such sensor networks, algorithms exist to identify, classify, and track targets [16, 12, 34]. Although UGS are used in a variety of applications, it is clear that social relationships and other information such as vehicle movements may be estimated from sensor networks. Vehicles or persons may be identified and/or tracked (with, say, seismic sensors [12]) and associated in the social network data structure with other relevant information (such as the vehicle's estimated occupants or owner).

3.1.4 Phone call logs

Phone calls between two individuals indicate the individuals share a certain kind of relationship. Land-line and cell-phone records may be processed to relate the calling and receiving persons. The strength of such relationships may be estimated from the number and duration of calls. This technique, among others, was used by Krebs to construct the social network of 9/11 terrorists [20].

3.1.5 Passenger lists

Travel by plane, rail, or boat often requires the purchase of tickets. Passenger lists for these modes of travel can be acquired, and will associate persons with places. Sometimes information is recorded about reserved seats (as typically for air travel), so who sits next to whom may also be considered, with a positive social relationship between individuals being inferred with low confidence based on a single occasion of adjacent seating, and with high confidence if it reoccurs. Such inferences may augment existing databases, such as the United States Terrorist Screening Center's 'watch list' [35], by adding estimations of social relationships between, say, an individual found on such a watch list and individuals not yet suspected.

3.1.6 Passports

Persons and places may be linked through the obvious means of tracking passport holders as passports are presented for identification at borders and other places.

3.1.7 RFID tags

RFID (radio frequency identification) tags are small, unique identifiers that can be read from a distance of about 3 meters. Tags with tiny batteries can be read from farther distances. The tags respond to radio frequencies emitted from the reader; their response is then detected by the reader. These emissions correspond to the tag's unique identification [36].

This technology will likely become very important for asymmetric urban operations [18]. They are particularly useful in estimating social networks. RFID tags can be embedded in tires (covertly when a vehicle drives over RFID 'dust') or placed in or on clothes, baggage, and so on [28]. When vehicles or persons pass near an RFID reader, they can be uniquely identified.

Other suggested uses of RFID tags include RFID-enabled license plates [42]. These enhanced license plates further ensure accurate identification. Passports have also been fitted with RFID tags, though recent demonstrations indicate a passport may be covertly read by an attacker [31].

3.1.8 Geolocation of IP addresses

Internet hosts (clients, servers, routers, etc.) all have an associated Internet protocol (IP) address. If the host is publicly accessible, then it is possible the host can be geolocated by searching for its address among a geographic database, such as *GeoURL* [11] or *Net World Map* [24]. Usually, this database associates blocks of IP addresses to cities, counties, or larger areas, so a geolocation lookup of a particular IP address is not necessarily accurate (wrong location) nor

precise (multiple connections from the same host may be geolocated differently) [13].

Locating a host of interest, such as a web server or client computer, may be useful if the host is known to be related to a person or persons. Geolocation information may corroborate various links between persons and places, but suffers from relatively low accuracy and precision.

3.2 Soft information

Soft information differs from hard information in that soft information is commonly less reliable, and it is difficult to extract useful information automatically unless it has been recorded in structured forms. Soft information consists primarily of human-generated language in written and spoken modalities. Sometimes it is possible to identify between which persons the communications occur. Yet estimating social relationships and relationships between persons and places will often require the use of currently-immature natural-language processing technology.

Research in textual analysis is an active field, and its successes and failures will not be reviewed here. The following sections briefly describe how automatic analysis of soft information may help in estimating social networks.

3.2.1 HUMINT collection

Human sources may directly provide information about social relationships, and collectors can ask about social relationships explicitly. As well, friendly forces may observe and report social interactions. Collectors may be employed at roadblocks, refugee collection points, and detainee collection points, for example [15]. Subsequent analysis of information obtained during such interrogations and debriefings may yield valuable information about social relationships and relationships between persons and places. High-reliability information relating two individuals might come from them being captured together, with identity being reliably established using biometrics.

3.2.2 Email, chat, newsgroups, blogs

Analysis of computer-mediated communication (CMC) typically aims to estimate group membership, inter-group relationships, and group influence. CMC is social in nature, but nevertheless often involves anonymous agents. Social relationships may be estimated from these kinds of sources, but determining the identities of the actors may require additional information from other sources.

3.2.3 Open source information

The wider category of open source information (or open source intelligence, OSINT) includes soft information that is publicly accessible, dynamic, and sometimes contradictory [32]. The degree to which sources of such information may be trusted may be difficult to assess [26].

The data structure described here is essentially one possible ontology. It defines relationships between persons, vehicles, places, and groups. Tools like AutoMap [6] can assist in extracting social relationships in text by identifying proximally-occuring names (and aliases with the aid of a thesaurus), and places.

3.3 Management of the network

Social networks evolve over time. Relationships strengthen or weaken, positive relationships may turn adversarial, and vice-versa. This complicates matters. Estimation of social networks additionally suffers from perpetually incomplete information. From any one information source or any short period of time, only a fragment of the complete social network of interest can be estimated. Individuals may be tracked via video surveillance, for example, but remain unidentified. As well, a single individual may be referenced in text or interviews by two different names; the estimated social network would, we might expect, represent two distinct individuals rather than one.

To mitigate these difficulties, automated processing should correct false beliefs and resolve conflicting information whenever possible. As noted previously (Section 2), each attribute is tagged with a reliability measure. Attributes obtained from highly reliable sources, and attributes whose values have been corroborated, will have high reliability measures. Conflicts between attributes may occur when the social network is updated. Such conflicts can be resolved by retaining the more reliable attribute and deleting the less reliable attribute. The provenance of such a change will be recorded, with any previous value of the attribute (and its reliability measure) saved as part of the attribute's provenance.

Entities that have not yet been identified will be retained in the social network as anonymous entities (albeit with unique IDs). If, for example, an anonymous entity is tracked from point A to point B, and is identified at point B, then all occurrences of this anonymous entity in the social network (including its relationship with point A and point B) will be updated to reflect the entity's identification.

All sources of information, including biometric identification, tracking, and textual analysis, are subject to false matches, false non-matches, human miscoding, and other forms of error. By drawing upon large amounts of information from multiple sources of disparate types, it should be possible to correct many errors by overriding less reliable information with more reliable information, and by overwhelming mistaken information with a preponderance of contrary information.

3.4 Inferring social relationships from co-location

When information is available that associates two individuals with the same location at the same time, a social relationship between them can be inferred, if the location is relatively small or exclusive. Two people being present in the same house at the same time can be presumed to be acquainted, with a confidence that increases markedly if the event is repeated. On the other hand, two people being simultaneously present in the same office building, or city, cannot be confidently associated.

3.5 Inferring group membership and coordinated behavior

Group-membership might be inferred by analyzing the strengths and polarities of links between persons. Strong links with positive polarity provide some evidence that one person also belongs to a group to which the other belongs. The basis for the strong association needs to be considered, for example, close kinship does not imply political affiliation, whereas co-presence at meetings with politically similarly affiliated individuals does provide significant evidence of political affiliation.

Coordinated behavior might be inferred from similar simultaneous changes in the network. For example, Krebs [21] discovered that many people joined the social network of the 9/11 terrorists just before the attack.

4 A scenario

To illustrate how hard and soft information may be fused to estimate social networks in such a way that supports decision making, imagine the following scenario.

The geographical area of the operations is Turkmenistan and Afghanistan, specifically near the border between these two countries. An open source report by an NGO organization active in the region reports an increase in the flow of opium from Afghanistan into Turkmenistan. Two independent HUMINT sources report the same. Intelligence analysts suspect that opium is being bartered for materials to make improvised explosive devices (IEDs), and for small arms and larger weapons to use against coalition forces. Consequently, analyst attention is drawn to Turkmenistan, where several HUMINT sources report rumors that a provincial governor (G-1) has been brokering deals between the Russian Mafia and Afghan drug lords.

The intelligence requirements are to determine if weapons have been acquired, from the Russian Mafia, by what means they are being transported, and to where.

An individual, whom we label Person X, is known (via previous HUMINT reports) to be either an Afghan drug lord or a first-order association with Afghan drug lords. That is to say, Person X is already represented in the estimated social network. Moreover, Person X has been associated with the Russian Mafia as a result of automatic inferencing based on video surveillance that detected Person X, on three separate occasions, in the same location (within speaking distance) with three other individuals (the same people in each instance) who are known, from previous intelligence, to be members of the Russian Mafia. The video surveillance that detected the repeated co-location of the four individuals used face recognition to establish identities. The video surveillance was put in place because of earlier interest in the activities of various members of the Russian Mafia, and all four people had already been enrolled into the facial recognition system from photographs provided by human informants and by Interpol from previous arrests in the Balkans.

Examining the estimated social network for clues for possible connections between the Afghan drug trade and the Russian Mafia thus turns up Person X who is linked with both groups. While examining surveillance photos of one of the events where Person X was co-located with the Mafia members, an analyst notices that Person X has been photographed using a cell phone. Consequently, the analyst manually tags the image as showing Person X using a cell phone. In response to this tagging, automatic inferencing examines SIGINT data recording cell phone usage at the time the photograph was taken and in the vicinity of the location. The inference engine finds that only one cell phone call was recorded at the time, and in the approximate location, so it associates Person X as a participant in the call. The call was recorded as taking place between the cell phone at that location, with unknown ownership, and a phone registered to a rug merchant's at his business location in Herat, in Afghanistan. So the inference engine links this unknown cell phone number to Person X. Since two other calls were made from this phone to the same phone associated with the rug merchant, and one call was made in the reverse direction, Person X is associated with the rug merchant.

Moreover, trucks owned by this rug merchant were previously stopped at checkpoints between Gushgy in Turkmenistan and Herat in Afghanistan. The drivers of these trucks were asked to provide information about their destinations and owners. The rug merchant, being the owner of these particular trucks, had already been represented as a node in the social network before this particular investigation began. Thus, intelligence analysts, when browsing the network of associations with Person X, turn up the rug merchant, who owns several trucks that travel between Turkmenistan and Afghanistan, and is consequently suspected of transporting opium, or IED materials and weapons, or both.

As a result, the decision is made to locate these trucks, and others owned by the rug merchant, and track their move-

ments, particularly across the border. Additionally, these trucks will be monitored to determine where they are loading and unloading their payloads, especially in Afghanistan. Surveillance will be maintained on the trucks, and on the rug merchant's phone, Person X's cell phone, and the provincial governor (G-1).

In this particular scenario, the social network was mostly estimated before it was known to be useful, largely by automated inferencing from both hard and soft sources. The estimated social network provided information to intelligence analysts that was critical for pursuing their objectives.

Acknowledgments

This research was supported through participation in the Advanced Decision Architectures Collaborative Technology Alliance (CTA) sponsored by the U.S. Army Research Laboratory under Cooperative Agreement DAAD19-01-2-0009. The views and conclusions contained in this document are those of the authors and should not be interpreted as representing the official policies, either expressed or implied, of the Army Research Laboratory, Defense Department, or the U. S. Government.

References

[1] F. Bashir, P. Casaverde, D. Usher, and M. Friedman. Eagle-Eyes (TM): A System for Iris Recognition at a Distance. *IEEE Conference on Technologies for Homeland Security*, pages 426–431, May 2008.

[2] Biometric Automated Toolset (BAT) and Handheld Interagency Identity Detection Equipment (HIIDE): Overview for NIST XML & Mobile ID Workshop. Biometrics Task Force, September 19, 2007.

[3] BAT Upgrades Tested in the Field. Biometrics Task Force: The Biometric Scan, January 2008.

[4] N. Boulgouris, D. Hatzinakos, and K. Plataniotis. Gait recognition: a challenging signal processing technology for biometric identification. *IEEE Signal Processing Magazine*, 22(6):78–90, 2005.

[5] K. Bowyer, K. Chang, and P. Flynn. A survey of approaches and challenges in 3D and multi-modal 3D+2D face recognition. *Computer Vision and Image Understanding*, 101(1):1–15, 2006.

[6] K. Carley and J. Diesner. AutoMap: Software for Network Text Analysis. http://www.casos.cs.cmu.edu (Accessed February 22, 2009).

[7] S. Chang, L. Chen, Y. Chung, and S. Chen. Automatic license plate recognition. *IEEE Transactions on Intelligent Transportation Systems*, 5(1):42–53, 2004.

[8] R. Chellappa, A. Roy-Chowdhury, and S. Zhou. Human Identification Using Gait and Face. In *IEEE Conference on Computer Vision and Pattern Recognition, 2007 (CVPR'07)*, 2007.

[9] J. Diesner and K. Carley. Revealing Social Structure from Texts: Meta-Matrix Text Analysis as a novel method for Network Text Analysis. *Causal Mapping for Information Systems and Technology Research: Approaches, Advances, and Illustrations*, pages 81–108, 2005.

[10] X. Geng, L. Wang, M. Li, Q. Wu, and K. Smith-Miles. Adaptive Fusion of Gait and Face for Human Identification in Video. In *IEEE Workshop on Applications of Computer Vision (WACV 2008)*, pages 1–6, 2008.

[11] GeoURL. http://www.geourl.org (Accessed February 22, 2009).

[12] G. Goodman. Detection and classification for unattended ground sensors. In *Proceedings of the Information, Decision and Control Conference*, pages 419–424, 1999.

[13] B. Gueye, S. Uhlig, and S. Fdida. Investigating the Imprecision of IP Block-Based Geolocation. *Lecture Notes in Computer Science*, 4427:237, 2007.

[14] C.-T. Hsieh, Y.-S. Juan, and K.-M. Hung. Multiple License Plate Detection for Complex Background. *International Conference on Advanced Information Networking and Applications*, 2:389–392, 2005.

[15] FM 2–22.3 (FM 34–52)—Human Intelligence Collector Operations.

[16] L. Kaplan. Node selection for target tracking using bearing measurements from unattended ground sensors. In *Proceedings of the IEEE Aerospace Conference*, volume 5, 2003.

[17] S. Kim, D. Kim, Y. Ryu, and G. Kim. A Robust License-Plate Extraction Method under Complex Image Conditions. In *International Conference on Pattern Recognition*, volume 16, pages 216–219, 2002.

[18] K. Kirby. RFID Meets GWOT: Considering a New Technology for a New Kind of War. Storming Media, 2006.

[19] S. Kong, J. Heo, B. Abidi, J. Paik, and M. Abidi. Recent advances in visual and infrared face recognitiona review. *Computer Vision and Image Understanding*, 97(1):103–135, 2005.

[20] V. Krebs. Mapping networks of terrorist cells. *Connections*, 24(3):43–52, 2002.

[21] V. Krebs. Uncloaking Terrorist Networks. *First Monday*, 7(4), 2002.

[22] B. Malin, E. Airoldi, and K. Carley. A Network Analysis Model for Disambiguation of Names in Lists. *Computational & Mathematical Organization Theory*, 11(2):119–139, 2005.

[23] M. Murtuza, Y. Lu, N. Karampatziakis, and T. Theoharis. Three-Dimensional Face Recognition in the Presence of Facial Expressions: An Annotated Deformable Model Approach. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 29(4), 2007.

[24] Net World Map. http://www.networldmap.com (Accessed February 22, 2009).

[25] E. Newton. *Strengths and Weaknesses of Biometrics*, chapter 12. Economics of Identity Theft: Avoidance, Causes and Possible Cures. Springer, 2007.

[26] D. Noble. Assessing the reliability of open source information. In *Proceedings of 7th International Conference on Information Fusion*, 2004.

[27] A. O'Toole, P. Phillips, F. Jiang, J. Ayyad, N. Pénard, and H. Abdi. Face Recognition Algorithms Surpass Humans Matching Faces over Changes in Illumination. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, pages 1642–1646, 2007.

[28] R. Pruett. Identification-Friend or Foe? The Strategic Uses and Future Implications of the Revolutionary New ID Technologies. Storming Media, 2006.

[29] X. Qiu, Z. Sun, and T. Tan. Global Texture Analysis of Iris Images for Ethnic Classification. *Lecture Notes in Computer Science*, 3832:411, 2006.

[30] J. Sherman. U.S. Creates Enemy Biometric Database. *International Biometric Group*, October 18, 2004.

[31] F. Size. Expert pushes envelope with passport RFID crack. *Network Security*, 2007(3):2–20, 2007.

[32] R. Steele and M. Lowenthal. *Open Source Intelligence: Executive Overview*. OSS Academy, 1998.

[33] V. Thomas, N. Chawla, K. Bowyer, and P. Flynn. Learning to predict gender from iris images. In *First IEEE International Conference on Biometrics: Theory, Applications, and Systems (BTAS 2007)*, pages 1–5, 2007.

[34] Y. Tian, H. Qi, and X. Wang. Target detection and classification using seismic signal processing in unattended ground sensor systems. In *IEEE International Conference on Acoustics, Speech and Signal Processing*, volume 4, pages 4172–4175, 2002.

[35] United States Government Accountability Office. Terrorist watch list screening: Opportunities Exist to Enhance Management Oversight, Reduce Vulnerabilities in Agency Screening Processes, and Expand Use of the List (GAO-08-110), 2007.

[36] R. Want. An Introduction to RFID Technology. *IEEE Pervasive Computing*, pages 25–33, 2006.

[37] J. Woodward. Using Biometrics to Achieve Identity Dominance in the Global War on Terrorism. *Military Review*, 85(5):30, 2005.

[38] J. D. Woodward and S. Cava. DoD Biometric Conformity Assessment Initiative. Technical Report RP-1182, RAND Corporation, 2005.

[39] J. D. Woodward, K. W. Webb, et al. Army Biometric Applications. Technical Report MR-1237-A, RAND Corporation, 2001.

[40] Y. Yao, B. Abidi, N. Kalka, N. Schmid, and M. Abidi. Improving long range and high magnification face recognition: Database acquisition, evaluation, and enhancement. *Computer Vision and Image Understanding*, 2007.

[41] H. Zhang, W. Jia, X. He, and Q. Wu. Real-Time License Plate Detection Under Various Conditions. *Lecture Notes in Computer Science*, 4159:192, 2006.

[42] Z. Zhou, W. Li, C. Deng, T. Li, and Y. Li. Secure Design of RFID Tags in the New Type License Plates Automatic Identification System. *International Symposium on Computer Science and Computational Technology (ISCSCT '08)*, 1:694–697, December 2008.