

Faculty of Informatics

Faculty of Informatics - Papers

University of Wollongong

Year 2006

The advancement of positioning
technologies in defense intelligence

K. Michael*

A. Masters†

*University of Wollongong, katina@uow.edu.au

†University of Wollongong, am16@uow.edu.au

This book chapter was originally published as: Michael, K & Masters, A, The advancement of positioning technologies in defense intelligence, in H. Abbass & D. Essam (eds), Applications of Information Systems to Homeland Security and Defense, Idea Group Publishing, 2006, Chapter 8, 196-220. Original book available <[a href="http://www.idea-group.com/ebooks/details.asp?id=5710"](http://www.idea-group.com/ebooks/details.asp?id=5710)>here.

This paper is posted at Research Online.

<http://ro.uow.edu.au/infopapers/371>

The Advancement of Positioning Technologies in Defense Intelligence

Katina Michael, Amelia Masters

INTRODUCTION

Through a path of development and commercialization, systems integration and convergence, the use of positioning technologies in defense has become an accepted, if not standard, feature of intelligence applications. Explored in *Realized Applications of Positioning Technologies in Defense Intelligence* (the precursor to this chapter), four main positioning technologies are identified as being at the core of advancement. These are the global positioning system (GPS), second generation (2G) and beyond mobile telephone networks (including wireless data networks), radio-frequency identification (RFID) and geographic information systems (GIS). Alone, each technology presents a unique aid during responsive and preventative defense scenarios—ranging from warfare through to the dissemination of information- but when used together their force and reach are multiplied.

The control and command of this power is paramount as we note that, continuing into the 21st century, our global society is faced with an uncertain and wholly dynamic security environment. In addition to known geographic and cross-border aggressions, the hidden threats of terrorism and the complexities of information warfare also seem to be increasing. The result is that world governments now more than ever need to actively understand and monitor the environments in which they and their citizens participate. Where positioning technologies play a significant role in this environment, a context of use needs to be created whereby defense strategies are appropriate and security requirements are accordingly aligned.

Written to supplement the previous investigation of realized applications, this chapter is an exploration of the future evolutionary path of positioning technologies in defense intelligence. It seeks to provide insight into how positioning technologies could be used to prevent and respond to a breach in security, and will analyze these types of implementations from within a social context. Current awareness of positioning technology applications will then be used as the foundation for a predictive analysis of future trends, culminating in a final assessment of advancement.

PREDICTED DEFENSE INTELLIGENCE APPLICATIONS

While entirely hypothetical, a predictive investigation of positioning technology usage points to possible defense intelligence approaches using current technology. The applications are not spelled out as ‘this’ or ‘that’ application but rather follow a conjoining theme throughout. The predictive scenarios attempt to cover *pre* and *post* a breach in homeland security, from preventing a threat, to managing, responding and recovering from an attack. Thus they consider what is traditionally known as ‘contingency planning’ through to ‘emergency management and response’.

Preventative Scenario

The preventative approach proactively seeks ways to stop a potential terrorist attack or breach in security by using all the relevant information available to form intelligence about an event that has yet to occur. It is like bringing pieces of a jigsaw puzzle together to form a picture; only here almost certainly a large number of pieces are missing and the final picture to be represented is ambiguous. Intelligence is not merely about certainties,

as indeed questions will always be raised over even the clearest of intercepted data that shows how an adversary will strike. Increasingly, intelligence is about pulling a diverse range of data sets together in their native form, including video, audio, text, spatial and graphical, to create a big picture view of proceedings. It is not a 'crystal-ball' approach or the work of a good 'forecaster' - it is more about being alert to day-to-day happenings.

Popp et al. (2004, p. 36) use the analogy of *joining the dots*, only it is much more complex than that, given there is no specifically defined problem and very little is known about where to begin searching for the answer. Initially it may be a worthwhile exercise to study previous terrorist attacks and to consider these in light of the possibilities. This does not mean that all terrorist attacks and security breaches are executed in the same manner but it recognizes a benchmark for future attacks. It showcases what is possible, and gives warning that future attacks will grow in sophistication, process and magnitude.

Defense intelligence data that is gathered from different sources needs to be collected and analyzed holistically within a spatial Information Management System (IMS). This can be done using geographic classification as the primary key for creating relational links between database tables. Specific end-user applications can then be built which use a secure Web-based portal to run queries and generate relevant reports. High-level information can be nationwide, with the ability to zoom-in into state, postal code, street and individual dwelling levels with a mixture of satellite, aerial and vector-based data sets. Even though new dwellings are erected every day, land, sea and similar boundaries are for the greater part static. What constitutes Australia and Australian waters for instance will not change overnight. Independent of the data type, geospatial systems can

cope with a diverse range of information and act as the hub for comparison and decision-making. The reality is though that no single agency owns all the geographic content. There could be hundreds of suppliers in any given nation. An initiative like the National Imagery and Mapping Agency (NIMA) in the U.S. as a “national intelligence and combat support agency whose mission is to provide timely, relevant and accurate geospatial intelligence” is strongly recommended for any country concerned with national security. Independent of a united body however, there may still be problems with determining which spatial data set(s) to use. There can be conflicts between data sets that were created in different years and by different organizations. For example, town centers may shift, as may the size of postal codes within them due to processes such as gentrification. Annual spatial links between data sets thus need to be made to ensure that vintage data is not rendered completely useless to the situation at hand today. Making a decision on the government agencies that will be responsible for updating and maintaining each data set is also very important. Most likely, suppliers like the Lands Department in the local area will have accumulated thousands of different data sets since the inception of digitization. Being able to identify which maps are meaningful is a long and time-consuming exercise but it must be done by a specific taskforce who have the end result in mind. The aim is to build a standardized clearinghouse where defense intelligence personnel with access privileges can acquire this data. The facility may even allow for dynamic updates. A note here is required to state the obvious- that above and beyond the need for standardization of GIS, it is critical that the adversary does not gain access to defensive GIS data. There have already been several cases argued in the United States that show enemies of the

nation to be acquiring and using map data from public web sites for intelligence purposes. Terrorists too can utilize hi-tech to their advantage.

While defense intelligence is usually considered a multifaceted multipart problem due to the great number of unknowns, there are some general rules that apply. Foremost, defense intelligence is more about making use of valid information- one *can* act on 'fact' but can only *consider* acting on "incomplete, ambiguous and/or unreliable" intelligence (Yen, 2004, p. 34). And in terms of sureties, the only thing any nation can claim to know, at least to begin with, is its own geographic landscape. Knowing oneself is the beginning of wisdom. The question is how to know another? How can a nation predict terrorist attacks when terrorists continually conceive new ways to inflict terror? As Popp et al. (2004, p. 37) state, "...we are faced with a new world in which change occurs very rapidly, and the enemy is asymmetric and poses a very different challenge; the most significant threat today is foreign terrorists and terrorist networks whose identities and whereabouts we do not always know." Historically, though we can point to contemporary terrorist examples as far back as the 1960s, it has been recently that an escalation in activity has taken place. In Egypt a series of car bomb blasts targeted numerous luxurious hotels along the Sinai Peninsula (2004, October 8); in Indonesia a car bomb exploded in front of the gates of the Australian Embassy in Jakarta (2004, September 9); in Beslan in Russia, hundreds of schoolchildren and their parents were taken hostage and the crisis ended in bloodshed (2004, September 1); in Madrid ten explosives were detonated remotely by mobile phone hitting four trains at three stations (2004, March 11); a truck bomb exploded outside the UN headquarters in Baghdad (2003, August 19); a powerful car bomb was detonated

outside the Marriott Hotel in Jakarta (2003, August 5); in Russia civilians were taken hostage at a Moscow theatre venue (2002, October 25); in Bali it was several explosives in vehicles that were detonated remotely using a mobile phone aimed at a popular night venue (2002, October 12); the hijacking of planes in the U.S. and their use in bringing down the Twin Towers (2002, September 11); the utilization of the U.S. postal service to deliver mail containing Anthrax spores (2001, October); the destruction of the U.S. embassies in Kenya and Tanzania in 1998; the release of toxic fumes of sarin gas in a Tokyo subway station (1995, March 19); the countless suicide bombers in Israel that have attacked public venues and buses (2001, August 19 till today); the list goes on. Trying to find a common link between all of these breaches in security is difficult, even though traditionally terrorists use one of six tactics: bombing, hijacking, arson, assault, kidnapping, or taking hostages (Wang, 2004, p. 23). Independent of the type of attack though, if one reduces the events down to the lowest common denominator there are some commonalities. Foremost, that it is *people* that conceived and executed these attacks. The other two unknowns that need to be found to curb any attack are the proposed *timing* of the event and the proposed *location* of the event. Although an individual's mind cannot be read, there are technologies that can track where individuals are, when they are there, and with whom these individuals are communicating (either for personal or business transactions).

Notwithstanding the serious privacy implications, knowing an individual's community of interest (CoI) could probably reduce the number of terrorist attacks and breaches in security. CoI brings together important pieces of information: the location of a

caller/messenger (origination location and time), the actual traffic flow (how long a caller/messenger was involved in the transaction session and the type of transaction), and the destination location of the receiver whether it be local, long-distance or international. CoI is a term that can be found in teletraffic theory but its applicability here for preventative security purposes is equally relevant. Such telecommunications concepts as point-to-point communication matrices, network neighborhood analysis, homing patterns and topology layout, traffic analysis aggregation, payload demands, gravity models, internodal distances, shortest-path routes, points of interconnect, interconnect traffic, centralized or distributed traffic architectures, and logical and physical network views are useful in analyzing any type of people communications. Yen (2004, p. 34) describes the task of trying to detect suspicious activities of terrorist groups as social network analysis. For instance, an individual wishing to cause a major disaster in a location could not act alone. They will use some form(s) of communication- telephone, mail, email or fax. Being able to trace such information could help authorities identify possible suspects. Consider being able to trace every location visited by an individual, including homes, businesses, and public space. This information could be used to build not only a geo-profile of the individual but also some sort of psychological assessment. Already caller details records (CDR) are used to help police and federal authorities to catch criminals. Beyond CDRs, the mobile phone itself could be used to present typical routes taken by the individual. Things being sent by individuals, like mail or parcels, could also be tagged using RFID. Sender information is still optional in many countries but knowing where the package came from is important. Given the ability to back-track on historical exchanges

between suspected terrorists, it could help to decrease situations like the U.S. Anthrax scares.

There are different ways that CoI could work, and this in itself is a project for further research. CoI could be implemented by using an anticipatory approach or, as has been presented in this hypothetical scenario, it may be implemented in real-time. Among the prospective social models to implement such a system are (in order of invasiveness):

- i) one global 'follow-me' number is allocated to individuals at birth;
- ii) all citizens are required to carry/wear a permanent mobile tracking device; and
- iii) all citizens are implanted with a RFID transponder.

It is also possible to understand the social models as complementary to one another, evolving over time. Determining an accurate CoI matrix, requires the identification of at least two or more fixed geographic locations, as either originating or terminating nodes. CoI in the scenario given here would work with 'mobile' nodes, that is, tracking actual human beings as they go about their daily tasks. Knowing where a person has been does not necessarily make them a suspect, but given a series of circumstances they could be considered for deeper surveillance. There are already well-instituted person-number systems in the majority of nations, although these techniques are not entirely useful given the majority were created at a point when computing power was relatively primitive. In many instances, duplicate citizen numbers are creating grave problems for government data-matching programs. An alternate proposal is a universal ID (UID) at birth. This ID could be used for a plethora of applications, from an individual's telephone number or email address, to their fixed home address, dispelling the problem of inter-country

movements and intra-country location. The main argument for a UID is that it will eliminate the problem of false identities. The UID would have a wide-ranging use. Yasuura (2003) has put forward the idea of a Personal Identifier (PID) system for bidirectional authentication and an RFID tag system for a “new social infrastructure”. The “digitally named world” would require members of society to be identified by a PID/UID and for all goods and products to be identified by RFID. It would even be possible to know when an individual has entered a particular building or when they have purchased particular materials. The view of pervasive computing thus becomes “a world of omnipresent but invisible information technology embedded into products and everyday items” (Siegemund & Flörkemeier, 2003, p. 378). From here it is a small advance for users to interact with objects using mobile phones. The querying could happen via SMS and active tags could thereafter process the commands sent to the object. Apart from the RFID UID, a GPS wrist-worn device would also identify an individual’s exact whereabouts. As Werb (p. 52) speculated in 1999, “[i]n the not-to-distant future... GPS devices will become so small and affordable that monitoring and tracking of humans in real-time would be feasible.” The question that needs to be asked is why a strategy such as this should be instituted when it is such a small percentage of the world’s population that is causing breaches in security.

For now the approach seems highly unlikely, but in the event of terrorist strikes increasing in frequency and magnitude to include such things as ‘limited’ nuclear strikes causing global unrest, it is possible that the approach could be adopted by governments beyond the military needs of network-centric warfare. We need only consider what

happened during the worldwide SARS outbreak to comprehend the possibility of an ‘out-of-control’ global epidemic. In similar scenarios, positioning technologies would help in a better understanding of the epidemiology of disease transmission as relationships between sufferers could be geographically represented. Kun (2004, p. 41) recently demonstrated the “need of sharing surveillance and epidemiological information worldwide and in real time”. Also shown was “the need for standards, geographical information systems (GISs), geo-coded information, and even the use of handheld devices to input data with imbedded spatial information from areas where the need for recording geographical coordinates is a must, (i.e., places where a dead animal/insect may be found for certain diseases).” His message resulted in the Italian project titled GeoSARS (Georeferenced Surveillance of Acute Respiratory Syndrome). The idea has been referred to as ‘syndrome surveillance’ and records patient symptoms and signs combined with an individual’s geographic location. McDonald (2002, p. 35) concurs with Kun on the issue of biosurveillance. He writes that, “[p]ublic health surveillance of population and environmental data can significantly improve detection of weapons of mass destruction, while ensuring the maintenance of the fundamental rights of... citizens.”

Responsive Scenario

When describing responsive actions in homeland security, it is usually in terms of emergency management. According to the Federal Emergency Management Agency (FEMA, 2003) emergency management is “the process of preparing for, mitigating, responding to and recovering from an emergency.” Contingency planning, which focuses

on the “prevention of undesirable events and the mitigation of undesirable consequences,” comes before emergency preparedness (Wang, 2004, p. 22).

Laxminarayan and Kun (2004, p. 27) prefer to separate the measures taken by first responders (local fire, police, ambulance and search and rescue departments) as active or passive. Active measures are “those measures that include denying entry of a person or substance or delivery system to the continent or states, our island territories, or access to sources of water, clean air, and crops, to large buildings, airports, and population-gathering centers.” Passive measures on the other hand, “include rapid warning and evacuation, quarantining, mitigating through vaccines, health, fire, and police intervention.” Positioning technologies can address both of these types of measures. For instance, they could be used to send out different types of alerts. Dependent on the proximity of persons to target locations, various levels of alarms could be raised. A simple color-coded system could be devised such as the one cited by Wang (2004, p. 24) representing the different level of threat: “Green represents *normal*. Yellow means *access controlled*, under which security would increase patrols and ID would be checked at entrances. Red indicates *restricted access* by using one entrance to each building, with bags checked and visitors escorted. Black is the *highest alert* with campus closed.”

Key infrastructure and other points of interest could be identified and marked in a GIS. These may include government offices, telecommunication hubs, landmarks, dams, utilities, refineries, transport hubs like airports, depots, stations and places where people congregate like hospitals, universities and schools, and shopping malls. Hotspots would have determinable vulnerability levels that could be updated dynamically. See maps 1-6

for a hypothetical scenario of how GIS and other positioning technologies could be used for homeland defense in the future. In the event that an attack was launched, authorities would have the right to poll all active devices in the vicinity of the disaster. This would not only help local staff deal with a response effort to help the injured but also a containment effort to curb further disasters from occurring. The 9/11 attack could possibly have had fewer casualties if this kind of monitoring had taken place. Flight 11 took off from Boston International at 8 a.m. and impacted the World Trade Centre at 8.45 a.m., Flight 175 took off from the same location at 8.15 a.m. and impacted the World Trade Centre at 9.03 a.m., Flight 77 left Washington's Dulles Airport 8.21 a.m. and impacted the Pentagon at 9.45 a.m., Flight 93 left Newark at 8.43 a.m. and crashed at 10.10 a.m. The air traveling time of the shortest hi-jacking was 45 minutes. In future efforts, such events could be avoided by the use of positioning technologies. Containment could perhaps have been achieved on 9/11, even if terrorists had successfully impacted one of the Twin Towers.

Apart from outdoor monitoring, indoor monitoring may also be applied. Context-aware building environments with surveillance beyond video cameras will become commonplace. Communication in these in-building settings could occur between "smart objects, between smart objects and background infrastructure services, and between smart objects and their users" (Siegemund & Flörkemeier, 2003, p. 379). Wireless LANs could be used to monitor UIDs. Anyone who should not be in the building would be detected. As the tags would be invisible to users, there would be an implicit association between their actions and the system. Whether the user agreed or not, an unobtrusive sensor could

be triggered without their knowledge. This would be advantageous in the event of a breach in security but obviously unethical in any other circumstance.

People involved in response efforts would be more educated about unfolding situations if positioning technologies were used. Improved access could be given to, for example, building layouts, floor plans and stairways, location of gas lines, water lines and air ducts. During the 9/11 recovery and response, firefighters were not given the adequate information they needed and as a result many lost their lives trying to put out a fire that was beyond control. The response was conducted in a state of panic, rather than being led by logical plans. People that were in the World Trade Centre had little knowledge of what was occurring outside. Route information for all of the emergency services would have helped with treating the injured and to establish basic hubs for communication. In addition, and in any responsive scenario, knowing where people are positioned during or immediately after a terrorist attack could help them receive aid quicker. Loved ones trying to locate missing persons would have instant information about whether or not their family and friends were victims. The UID could be triggered and linked back to vehicle registrations, addresses or other useful information. In events that were mainly chemical-based or biological, geographic information systems could be used to represent the area of concern after dispersion analysis or other required analyses had been determined. Civilians could be messaged about the effects of a biological attack, using their UID, either to an email or mobile handset through SMS (beyond that of media reports via broadcasts). Positioning technologies could also be used to precisely identify the location of debris to help with the reconstruction of what took place, and assist with

clearing and rebuilding efforts. Cordoned off areas that were out-of-bounds for civilians could be identified on maps messaged to individuals affected by the disaster. In addition to this, information could be collected straight from field workers and sent via the appropriate applications to a secure government database, given the appropriate Web-based portals for communication. Participants in a pilot for mobility and emergency services, post 9/11, were found to be “hopeful about the roles that mobile devices and wireless access can play in making their work life safer and also better enable them to perform their duties” (Sawyer et al., 2004, p. 64). The major advantage of wireless computing that the pilot reaffirmed was in the speed that information flowed from person-to-person, and from person-to-system using existing processes at critical times. It is also important to highlight that participants were more concerned with reliable connectivity than upload and download speeds.

Taggart et al. (2003) have written extensively about the significance of satellite systems in emergency management. They describe that irrespective of how rapidly fixed and mobile operators get networks back in operation after a major disruption, that during terrorist attacks it is satellites that should be relied upon as an alternative system for communications. “The difficulty of many of the first responders... to communicate with themselves and to other federal agencies confirmed the need for an interoperable and flexible communication infrastructure... Since many of these agencies must make time-critical decisions, there may not be enough time for communication links to be restored using conventional mobile ground or airborne nodes” (Taggart et al., 2003, p. 1155). In the aftermath of the 9/11 attack, it was privately-owned satellites that provided

communications when landline and terrestrial networks failed. Some examples include the Iridium and Globalstar providers. Quite possibly first responders in the future will be equipped with GPS universal phones to allow for coordination, management and integration in the response effort. While Taggart et al. predict that only the key personnel will most likely be equipped with GPS phones due to the fact that first responders are already heavily equipped with other tools, the devices will likely be wearable (especially as the GPS chipsets get smaller). In addition to person-to-person communications and person-to-system communications, system-to-system communications could also take place. In the event of a radioactive, chemical or biologically exposed area, sensor data could automatically be collected and sent to laboratories for more detailed analysis.

According to Want (2004, p. 86), detectors could minimize the danger of “long-term exposure to such harmful agents, many of which are invisible and odorless. In addition, deploying such devices at national ports of entry could help identify potential terrorist activity before it occurs.” Saydjari (2004, p. 56) is correct in his summation that “[w]e need a spectrum of system models and an engineering framework analogous to the CAD/CAM framework used by hardware engineers. The community needs adequate threat models, adversary models, mission models, and countermeasure effectiveness models. Each type of model will require tremendous energy to produce, yet little effort is under way in these arenas.” Assuming these models are created and implemented, their success will lie in the ubiquitous adoption of positioning technologies in open and closed environments, by all people, things and infrastructure whether in the form of GPS, 2G/3G mobile, RFID, or other communication-based means. Success may also, at least in some respects, depend on the implementation of a priority system, whereby mobile technology

infrastructure allows government and emergency personnel communications access before civilians and businesses.

SOCIAL CONTEXT

Where positioning technologies play a significant role in homeland security environments and their monitoring, a social context needs to be created in which defense strategies are appropriate and security requirements are accordingly aligned. Current ventures have been fuelled by demand for increasing standards of protection, and have been propelled in advancement by events such as 9/11 in the U.S. and, in the Asia-Pacific region, by the Bali Bombing in 2002. In addition to this, the dual-use aspect of the technologies, where public and private implementations exist side-by-side, has led to interest and funding from commercial sectors. While the integration of positioning technologies in areas of defense remains a high priority, worldwide civil applications continue to develop, each one more innovative than the last. This commercial influence and the private use of defense technology (though arguably not the private use of defense systems themselves) are pushing advancement in directions that are totally incomparable to historical military and homeland security developments. Indeed, in the current information age, we are seeing an unprecedented development and dispersion of technology. This new investment however, despite its potential for success, is not necessarily the way to curb all future security breaches. Warranted as the effort may be, especially in terms of pure peace-keeping efforts, arguing that this set of advancements are better or more advantageous than previous developments simply because they are 'different' or more widely accepted

is erroneous. The odds of total success are still low and are marred by the fact that no system can ever be foolproof.

Faults in hardware and inaccuracies in software aside, positioning technology cannot exist in a vacuum. Most systems require a user, or, at the very least, some form of user input and it is here, in the realm of 'intelligence' that most problems lie. Indeed, we can build the technology but we often have problems utilizing it appropriately and effectively. The knowledge systems that are required to provide the scope for positioning technologies are often flawed. Take for example the 1999 bombing of the Chinese Embassy in Belgrade by United States military forces. On May 7th, at around midnight local time in Serbia, one of a fleet of American B-2 bombers dropped five Joint Direct Attack Munitions 2000-pound bombs on a target in Belgrade. The target had previously, and wrongly, been identified as the head office for the Yugoslav Federal Directorate for Supply and Procurement (FDSP). Instead, what actually stood in the target location was the Chinese Embassy. The bombs, all GPS-guided missiles set to operate "in all weather and at night using a satellite-based navigation system of a high order of accuracy", (United States Department of Defense, 1999) reached their geographic target successfully, killing three Chinese journalists and injuring twenty embassy staff. In later press releases and formal statements of apology, the U.S. government admitted that the bombing was both an error and an accident. The positioning technology had functioned correctly but the knowledge systems supporting it had failed. Official accounts pointed to three major intelligence faults. First, the technique used to locate the FDSP building was imprecise. The geographic co-ordinates of the building were produced using inexact land

navigation techniques to pinpoint a street address on out-of-date maps. Second, the databases used to correlate and cross correlate the location of the target and its surroundings housed incomplete and dirty data. With regard to the Chinese Embassy in particular, multiple databases within the U.S. Department of Defense showed it still to be in its pre-1996 location, even despite several visits to the new building by U.S. officials after 1996. Accordingly, the Embassy was never identified as being in the target location, and the FDSP building was never shown to be anywhere else. The third major intelligence flaw involved the focus of the attack. Pre-attack reviews had centered upon how to attack, the value of the target, and the possibility of collateral damage. The accuracy of the location was never questioned. The culmination of these events was that the bombing went ahead in error. U.S. officials had become complacent with the use of knowledge management systems and this was reflected in the way the positioning technology was applied.

Before we can really use the technology in its most beneficial capacity, we need to master the art of information intelligence. If the use of positioning technology is to be accepted, it needs to be employed using legitimate inputs. Indeed, though its use may be valid for homeland security purposes, it is not valid to use the technology improperly or to cause damage outside the immediate need for action, whether or not this action is protective. To create a positive process for use, a change in the culture surrounding information gathering and knowledge systems may be required. Indeed, when considering the issue of timeliness needed for knowledge gathering in the Information Age, Kun (2004, p. 35) writes, “[w]e need to change our methods, our systems, our infrastructures, our

procedures, and our policies.” Where this change is not incited, the impact and acceptance of positioning technology may be lessened. That there are gray areas and potentially unacceptable uses for it though does not convincingly indicate that we are concentrating on the wrong initiative. To ensure maximum benefit however, technology cannot be the only initiative on which progress in homeland security depends. The potential for human error in the operation of positioning technologies and the management of their associated knowledge systems means that the creation of checks, balances and support systems must become a vital part of the defense infrastructure. Not only this, but alternate and distinct initiatives in areas such as peacekeeping and economic controls (to name but two global areas for concern) must also share a critical focus. By creating this multi-faceted defense system then, some level of dynamism in security strategy is assured as varying options for action and reaction are available. This becomes paramount as, faced with nebulous enemies, “static preventative techniques, while important, are inadequate” (Saydjari, 2004, p. 54).

FUTURE TRENDS

The use of positioning technology as a means of automatic and location-based identification is set to increase exponentially. In line with the size of increase however, the rate of increase will depend greatly upon general agreements as to application quality and standards. For positioning technologies, especially those in dual public and private use, an assessment of application quality is often dependent upon commercial or application readiness. As such, applications being researched present different concerns to those products being sold in the marketplace. Further, technologies that utilise humans

as major elements (not simply as participants) in the overall system create additional issues. Take for example the Cyborg 1.0 experimentation conducted by British university Professor Kevin Warwick regarding human implantation with RFID transponders.

Though Warwick's implant created an unparalleled interactive environment within the confines of his laboratory, he was only able to keep the implant inside his arm for nine days in the first experiment. A direct blow to the transponder would likely have shattered the casing, doing irreparable damage to the surrounding nerves and tissue. Similarly, research in the area of location based services faces technological hurdles as combining GPS with humancentric RFID involves challenges of radiation shielding, miniaturization and power supply.

The first stage of evolution is therefore likely to be contained to the extended definition and tagging of inanimate and non-human objects. This will promote the creation of industry standards and allow appropriate advancement in quality to gain a foothold before we are faced with real debate over humancentric applications. In military circles, mass asset tagging has already begun. Both Operation Enduring Freedom in Afghanistan and Operation Iraqi Freedom in Iraq for example, used RFID tracking to identify and manage various cargo shipments. By January 2005, under mandate from the U.S. Department of Defense, all suppliers to the military will be required to use passive RFID tagging on shipments of goods. This condition exists at all packaging levels, with separate stringent requirements for the tagging of high-value assets. There are few exemptions. These efforts mirror progress in the private sector with recent moves by U.S. giant Wal-Mart to require that their top 100 suppliers implement systems for the RFID tagging of goods by

2005. Similarly, numerous manufacturers including Benetton and Gillette have already conducted RFID packaging trials, showing a move into the mainstream for this application of the technology.

If we take the commercialization of defense innovations such as GPS and the Internet as an evolutionary indicator, the dual use of technology will gain greater momentum. Where governments have previously opened up research to allow the private sector an autonomous strand of development, we are now seeing a re-convergence of application paths to create superior knowledge systems. Where defense-type positioning technologies were once a reserved realm of implementation, they are now on the brink of embracing a wider economic and managerial scope. To illustrate, prior to 1994 the Defense Meteorological Satellite Program (DMSP) run by the Department of Defense, and the Polar-orbiting Operational Environment Satellite Program controlled by the Department of Commerce existed as separate entities. In the early 1990s however, the potential cost efficiencies and performance improvements that the combination of the two systems might bring was identified. In May 1994, a convergence plan was submitted to the U.S. Congress and, four years later, was endorsed by the President. The result, in 1998, was the National Polar Operational Environmental Satellite System (NPOESS), a polar-orbiting environmental satellite system that capitalized on NASA's Earth Observing System to satisfy both civil and military requirements. Since that time it has successfully managed the command and control functions of both programs, and has arguably done so at a reduced cost. Convergence in terms of homeland security does have some disadvantages however. By integrating multiple systems into a singular entity it

compounds the number of operational facets that are susceptible to a breach in security. Further, where lines of demarcation are not clearly drawn between each system component, questions as to the involvement of non-defense agencies in homeland security may be raised. These considerations mean that the future effects of using homeland security systems for defense, or of them being targeted in a security breach, are amplified in comparison to current states. The use of hybrid knowledge systems widens the scope for social damage. The willingness to converge systems to gain economic and technological economies of scale must be tempered by a visible delineation of ownership and responsibility, and must be managed by appropriate implementation and recovery strategies if the future visions for convergence and heightened knowledge systems are to be successful ones. Nonetheless, it is questionable whether changes to current arrangements will actually take place, especially in the short term.

In supporting convergence and enhanced knowledge systems, we face a battle with bureaucracy as information sharing channels are still not currently suited to the free flow of information between government and law enforcement agencies. In the area of homeland security specifically, information sharing channels were dealt a serious blow after Watergate when new reforms prohibited the Federal Bureau of Investigation (FBI) from distributing the findings of criminal investigations to any other national security agency, including the Central Intelligence Agency (CIA). Though arguably implemented with good intention, the serious flaw in this development became obvious when several major terrorist attacks were staged in the U.S. during the early 1990s. The 1993 bombing of the World Trade Centre is a pertinent example. Six days after the bombing, the FBI

detained 26-year old Palestinian Mohammed Salameh for attempting to claim his rental car deposit on the van that had housed the bomb. Under the Watergate reforms though, post-arrest and so long as additional fugitives remained, the FBI could only concentrate on the prosecution of those captured and could not aid the investigations of any other agency. While progress in information sharing has been made since this time, many anomalies remain. To illustrate, though the U.S. Homeland Security Act of 2002 contains provisions that, “[e]xcept as otherwise directed by the President, the Secretary [of Homeland Security] shall have such access as the Secretary considers necessary to *all* information, including reports, assessments, analyses, and unevaluated intelligence relating to threats of terrorism against the United States...” senior government officials from within the Department of Homeland Security have confirmed that there are difficulties in extracting threat-related information from government agencies. This is in addition to a formal statement made by Jerry Berman, President of the Center for Democracy and Technology, during testimony before the Homeland Security Committee Subcommittee of Intelligence and Counterterrorism on March 25th 2004. Here he confirmed, “the sharing of terrorist-related information between relevant agencies at different levels of government has only been marginally improved in the last year, and remains haphazard. It is still comprised of multiple systems that cannot communicate with each other... It is not the result of a carefully considered network architecture that optimizes the abilities of all of the players.”

Further leaning toward a lack of successful convergence in the short-term, bureaucratic and legal systems are not suited to the rapid response needed in defense scenarios. The

wheels of justice turn slowly and the problem with treating a matter as purely a law enforcement issue means that it also becomes understood in this context. A division between what is legislated for and what can be achieved then becomes the practical reality. In terms of terrorism and homeland security, it is further detrimental as issues of intelligence, state sponsorship and individual freedoms can become secondary. The ramifications of this are not always obvious, especially when legislation is enacted as a reflexive and defensive measure. At the time of a breach in homeland security, the immediate benefits of the legislation in providing a solution or a means of retribution are those that are given attention. In time however, the more wide-ranging effects are seen. One of the most contemporary examples has been the enactment of the USA Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (Patriot) Act of 2001. Passed by Congress a mere 45 days after the 9/11 attacks in New York City, its progress through the parliament saw very limited debate. In a 342 page-long document, the legislation made sweeping changes to 15 other statutes plus enacted new provisions of its own. In this regard, the Act took vital steps toward providing for the victims of 9/11 and toward increasing and improving forensic capabilities toward cyber-crime.

Three years on however, investigations show that the long-term repercussions of the Patriot Act were, perhaps, not adequately considered and that the Act may indeed violate individual rights of citizens. The grim reality is that in order to improve homeland security, new powers were given to law enforcement and intelligence agencies, both domestic and international, at the cost of eliminating the controls that previously existed to ensure that courts had authority to regulate the abuse of such powers. With the

safeguards removed, various government agencies are now able to conduct covert searches without warrants, including wide-ranging telephone and Internet surveillance, and can access all financial, medical, mental health and student records which were previously unavailable to them. Investigation of American citizens may now occur where no probable cause of crime exists and non-citizens may be jailed or denied re-admission to the U.S. based upon mere suspicion of criminal intent (American Civil Liberties Union, n.d.). This shows a conundrum in assessing the true value behind many homeland security strategies. The turbulent social context in which the initial assessment of damage is made can lead to skewed notions of what is appropriate in response. Then, as Davies (2002, p. 37) states, “[h]ow do we distinguish genuine and meaningful public security proposals from those based on convenience and illusion, and yet avoid the appearance of ingratitude or cynicism toward those who might just be doing their best to help?”

It is impossible to tell whether the current lack of comprehension and unity in response to homeland security initiatives is a sign of things getting worse before they get better, or whether it simply shows that each new terrorist action will place greater restraints on freedom. What can be predicted with certainty is that the positioning technologies used to support defense and associated bureaucratic efforts will continue to advance. How they are implemented will be a product of the efficiencies that we are seeking to create at present. Thus, the structures that we are only now starting to build will reflect in the use of positioning technologies and their underlying knowledge systems. An absence of long-term studies makes the evolutionary path difficult to predict in this respect and can only be further complicated by any attempt to prejudge the ethics that will inevitably become a

part of all future security actions. The result is that though we can predict an application of technology, we cannot predict its effect or outcome.

CONCLUSION

There is no simple or singular solution to the current security crisis and with the increasing complexities of global advancement caution must be taken when formulating a response. Both cause and effect of action must be assessed. Here, let us compare two very different but equally devastating events. On the 26th of April 1986, a nuclear accident and fire damaged a power plant in Chernobyl. For days afterwards, a giant cloud of radiation hovered over much of Europe and today the consequences are still being felt through infertile land and human deformity. In citing an article by Reuters, Kun (2004, p. 42) writes that it took until 1990 for the Soviet authorities to realize the extent of the accident. After evacuating 100,000 people within a 20 mile zone a few days after the disaster, authorities evacuated another 14,000 at the end of 1990, for a sum total of 90,000 people in the years after the actual event had occurred. Though the damage was catastrophic and widespread, the global response was limited. Initiatives to make nuclear power and associated facilities safer received little attention and those who were not directly affected by the accident were able to ignore its occurrence without ramifications. In contrast, on September 11, 2001, two passenger jets flew into the Twin Towers in New York City. Though killing thousands, the geographic damage was confined to Manhattan. Emotionally however, the whole world was affected. Governments leapt into action and a new *Age of Terror* was declared. Why then, in two such catastrophic disasters, did the response differ so widely? Arguably, the vital difference between the two situations, and

the factor that caused such different reactions, was the element of intention. Where the disaster at Chernobyl was not the result of hostility, 9/11 was a political statement designed to invoke fear. As a result, the global response was rapid. Keeping in mind that terrorist attacks were not new to the world however, why was the response as large and as quick as it was? A new age perhaps, beyond that of the Information Age? Or did the new scale and magnitude of such nebulous hostility make us angry? And was our response tailored in a similarly heated fashion?

Leaving these questions unanswered, what we gain from the comparison is an understanding that where hostile elements are the force behind a disaster, governments are not immune to responding on similarly emotive grounds. This is often justified by an overriding want to protect its citizens. With no higher level of review than government itself however, this ability to be affected by emotion means that when taking action, appropriate safeguards must exist. This is especially true in the case of positioning (and other) technologies, as the effects of implementing technology are often greater than the technology itself. What we must ask therefore, in relation to the outcomes of the response and the further implementation of homeland security measures is whether a proactive approach to defense incites more hostile behavior? Does the use of new technology as a defensive measure provoke enemies by laying down a challenge? Imagine for example, if George W. Bush succeeded in his implementation of the Star Wars missile defense plan for the United States. Would this success reflect a “ready for anything” attitude? Would its very existence encourage attack? As McDonald (2002, p. 37) states, “[o]ur greatest paradox is that- if a massive security build-up in the United States is perceived as

insensitive and predatory- our defensive actions incite the type of attacks that we are trying to defend against.” And what to say if the satellite and monitoring systems were, like the advancement paths for the technology itself, to take on dual roles in both the public defense and the private commercial sectors? This immediately widens the effect of impact should the system be a target for, or the source of, an attack. Immense care must therefore be taken with the adoption of positioning technologies, especially since recent advancements in GPS, mobile telephony, RFID and GIS have made them a viable option for defensive implementations. As implementers, governments also need to provide support for the knowledge systems which underpin the technology. Without a strong information base from which to derive useful inputs, the positioning technology is rendered useless or, in a worst-case scenario, can create situations far more damaging than those ever imagined. This is because though it is easy to speculate over the path of advancement, the outcomes of adoption are never as simple to predict.

REFERENCES

American Civil Liberties Union. (n.d.). *USA Patriot Act*. Retrieved June 30, 2004, from <http://www.aclu.org/SafeandFree/SafeandFree.cfm?ID=12126&c=207>

Davies, S. (2002). A year after 9/11: where are we now? *Communications of the ACM*, 45(9), 35-39.

Federal Emergency Management Agency. (2003). *Emergency management guide for business and industry*. Retrieved August 28, 2003, from <http://www.fema.gov/library/bizindex.shtm>

Kun, L. (2004). Technology and policy review for homeland security. *IEEE Engineering in Medicine and Biology Magazine*, 23(1), January/ February, 30-44.

Laxminarayan, S. & Kun, L. (2004). The many facets of homeland security. *IEEE Engineering in Medicine and Biology Magazine*, 23(1), January/ February, 19-29.

Masters, A. (2003). *Humancentric applications of RFID: the current state of development*. Unpublished honor's thesis, University of Wollongong, Wollongong, NSW, Australia.

McDonald, M. D. (2002). Key participants in combating terrorism. *IEEE Engineering in Medicine and Biology*, 21(5), September/ October, 34-37.

Michael, K. (2003a). The rise of the wireless internet. In E. Lawrence et al. (Eds.), *Internet commerce: digital models for business* (pp. 291-294, 296). Australia: John Wiley & Sons.

Michael, K. (2003b). Trends in the selection of automatic identification technology in electronic commerce applications. In N. Cerpa & P. Bro (Eds.), *Building society through e-commerce: e-Government, e-Business and e-Learning* (pp. 135-152). Chile: University of Talca.

Michael, K. (2003c). *The technological trajectory of the automatic identification industry: the applications of the systems of innovation (SI) framework for the characterization and the prediction of the auto-ID industry*. Unpublished doctoral dissertation, University of Wollongong, Wollongong, NSW, Australia.

Michael, K. (2004). Location-based services: a vehicle for IT&T convergence. *Advances in e-Engineering and digital enterprise technology I. Proceeding of the Fourth*

International Conference on E-engineering & Digital Enterprise Technology, Yorkshire, UK, 467-477.

Michael, K. & Masters, A. (2004). Applications of human transponder implants in mobile commerce. *Proceedings of the Eighth World Multiconference on Systemics, Cybernetics and Informatics*, Orlando, Florida, 505-512.

Michael, K. & Michael, M. G. (2004). The social, cultural, religious and ethical implications of automatic identification. *Proceedings of the Seventh International Conference in Electronic Commerce Research*, Texas, US, 432-450.

Michael, K. & Michael, M. G. (n.d.). Rise of the *Electrophorus*. *Quadrant*. Accepted for publication in 2004.

Popp, R., Armour, T., Senator, T. & Numrych, K. (2004). Countering terrorism through information technology. *Communications of the ACM*, 47(3), 36-43.

Reuters. (1990, April 24). Wider Chernobyl evacuation ordered. *Washington Post*.

Sawyer, S., Tapia, A., Pesheck, L. & Davenport, J. (2004). Mobility and the first responder. *Communications of the ACM*, 47(3), 62-65.

Saydjari, O. S. (2004). Cyber defense: art to science. *Communications of the ACM*, 47(3), 53-57.

Siegemund, F. & Flörkemeier, C. (2003). Interaction in pervasive computing settings using Bluetooth-enabled active tags and passive RFID technology together with mobile phones. *Proceedings of the First IEEE International Conference on Pervasive Computing and Communications*, 378-387.

Taggart, D. et al. (2003). Usage of commercial satellite systems for homeland security communications. *IEEE*, 2, 1155-1165.

United States Department of Defense. (1999, May 8). Joint statement by secretary of defense William S Cohen and CIA director George J Tenet. Retrieved June 17, 2004, from <http://hongkong.usconsulate.gov/uscn/others/1999/0508.htm>

Wang, H-M. (2004). Contingency planning: emergency preparedness for terrorist attacks. *IEEE Aerospace and Electronics Systems Magazine*, 19(3), March, 21-25.

Want, R. (2004). Enabling ubiquitous sensing with RFID. *IEEE Computer*, 37(4), 84-86.

Werb, J. (1999). H-m-m-m-m... where is it? *Communications News*, 36(3), p. 52.

Yasuura, H. (2003). Towards the digitally named world- challenges for new social infrastructures based on information technologies. *Proceedings of the Euromicro Symposium on Digital System Design*, 17-22.

Biographical Notes

Katina Michael

Katina Michael is a lecturer in Information Technology at the University of Wollongong. In 1996 she completed her Bachelor of Information Technology degree with a co-operative scholarship from the University of Technology, Sydney (UTS) and in 2003 she was awarded her Doctor of Philosophy with the thesis “The Auto-ID Trajectory” from the University of Wollongong. She has an industrial background in telecommunications and has held positions as a systems analyst with United Technologies and Andersen Consulting. Most of her work experience was acquired as a senior network and business planner with Nortel Networks (1996-2001).

Amelia Masters

Amelia Masters completed her Bachelors Degree in Information and Communication Technology (Hons) at the University of Wollongong, writing her thesis on current development states for humancentric applications of RFID. She has been employed in both public and private sectors in R&D roles and currently works as a software engineer in the Automation and Control Systems industry sector, specializing in surveillance technologies. Amelia is currently completing a Bachelors degree in Law.