

*Faculty of Informatics*

*Faculty of Informatics - Papers*

---

*University of Wollongong*

*Year 2006*

---

Realized Applications of Positioning  
Technologies in Defense Intelligence

K. Michael\*

A. Masters†

\*University of Wollongong, [katina@uow.edu.au](mailto:katina@uow.edu.au)

†University of Wollongong, [am16@uow.edu.au](mailto:am16@uow.edu.au)

This book chapter was originally published as: Michael, K & Masters, A, Realised applications of positioning technologies in defense intelligence, in H. Abbass & D. Essam (eds), Applications of Information Systems to Homeland Security and Defense, Idea Group Publishing, 2005, Chapter 7, 167-195. 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</a>.

This paper is posted at Research Online.

<http://ro.uow.edu.au/infopapers/370>

# Realized Applications of Positioning Technologies in Defense Intelligence

Katina Michael, Amelia Masters

## INTRODUCTION

It has been since the turn of the millennium that terrorist attacks have triggered heightened interest in homeland security issues. Terrorism is defined as “a form of political or criminal violence using military tactics to change behavior through fear” (Wang, 2004, p. 22). The September 11 (9/11) attacks marked a new phase of warfare, forcing U.S. president George W. Bush to respond with an Executive Order establishing an office of homeland security (White House, 2001). One can ponder as to why the Executive Order did not come any earlier, given the frequency of hijackings and bombings by extremist groups during the 1980s and 1990s. One can also question why other states, even the most remote nations, have begun to concern themselves with homeland security. What was it about 9/11 that caused such a ripple effect in defense strategy worldwide? Was it that a ‘successful’ terrorist attack was launched on what is perceived by many to be the most powerful nation in the world? Was it the nature of the attack, the element of shock created by a passenger airline flying into the Twin Towers and destroying them that was morbidly ‘revolutionary’? Or was it the sheer number of civilians that were impacted by the aftermath in New York City? Independent of the answer, believing that heavily investing in homeland defense security measures will curb all future attacks is foolish. In some respects it is analogous with searching for a needle in a haystack- the odds of complete success are low, although the effort is still warranted. Justification of this effort is only furthered by the implementers and the tools and strategies they use to maintain homeland security.

Technologies, particularly those that incorporate positioning intelligence, have an important role to play here. They are not foolproof but they go a long way toward aiding preventative and responsive measures in critical situations. The real concern however is how to ensure that the use of these technologies for the purpose of homeland security does not compromise citizen rights. Until now, the world has survived without explicitly detailed nation-specific homeland security strategies, thus heightening the challenges in implementation. These challenges escalate when it is considered that for the greater part, the need for homeland security has been fuelled by want. As initial desires were contained to a small number of developed nations, only a few have led and implemented advancements in defense. Since events like 9/11 have proven that the great nations are still penetrable however, a need for greater global security and defense intelligence has emerged.

The purpose of this chapter is to investigate the adoption of positioning technologies specifically used for defense intelligence, where defense is defined as the act of making safe from attack (Saydjari, 2004, p. 53). Defense intelligence in the context of homeland security is the act of gathering, processing and managing information to provide resistance against attack or to protect citizens from further harm. It involves having knowledge of an event that is likely to take place or which has already happened. A variety of breaches are possible, each affecting a different level of security, and not all concerned with the safety of citizens. Defense intelligence is therefore not just about filtering information that may be useful against an enemy but includes the distribution, dissemination and communication of findings to a variety of stakeholders. Various means

can be used to achieve this, but here we concentrate on positioning technologies. These are devices and systems that allow for the identification of a relative location of a living or non-living thing on the earth's surface, in a given outdoor coverage area or even within a building. The main positioning technologies that can be used for defense-related location-based intelligence services and those that will be discussed in this chapter include: 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). The main objectives of this chapter are: i) to provide a background of the main positioning technologies and how they relate to defense intelligence; ii) to give examples of how positioning technologies are being applied today both in the commercial and government sectors; and iii) to explore the use of complementary and supplementary technology innovations for homeland defense.

## HIERARCHICAL POSITIONING TECHNOLOGY

Positioning technologies differ in their capacity to identify. Some technologies work well outdoors while others are tailor-made for the in-building environment. Independent of the positioning technology application, location information is being sought to allow the furthering of processes such as seemingly simple "am I on the right track" or "where am I" queries. In some instances the value returned to the end-user is a latitude and longitude coordinate, in other instances it is the nearest base transmission station (BTS), nearest building or a specific location within an area. Spatial data plays an important role in visualizing location information, whether this is in hardcopy or on digital maps. Knowing where things are, where one has been, and where one is going can be vital. Defense has

long realized this potential and was preoccupied with positioning techniques even before digital technologies became available. Automation however, has realigned the importance of knowing where things are, especially for the purposes of gaining advantage over one's adversaries.

### Global Positioning System (GPS)

In the 1960s the idea of using space technology for telecommunications was explored by the U.S. government and the concept of a satellite was born. Satellites had unlimited prospects for defense, from gathering intelligence information to global broadcasting capabilities. Both uplink and downlink transmission were possible, taking information to and from Earth ground stations using radio waves. By 1974, the U.S. Air Force together with other U.S. military branches, were hard at work on the Navstar Global Positioning System (GPS) project. The project is estimated to have cost the U.S. Department of Defense (DoD) ten billion dollars to develop and was officially launched in April 1995. The system works by using twenty-eight satellites circling the Earth every twelve hours to broadcast radio navigation signals to an unlimited number of GPS receivers anywhere in the world. A GPS receiver is an end-user device that can be hand-held, mounted on a vehicle or found in a plane. Receivers can calculate location information to as close as between one and fifteen meters, this accuracy largely improved since selective availability (SA) was turned off. For a long time SA ensured that the accuracy of GPS readings for civil users did not correspond with that of military users. Given civilian users were achieving increasingly accurate readings through Differential GPS (DGPS) however, in some cases even better than that of their military counterparts, it is arguable

that SA would have been made redundant in the medium to long-term anyway. The main limitation of GPS is that it does not work well in all environments, especially from within dense vegetation, tall buildings or dwellings. Other more recent attempts at creating similar global positioning systems include the Russian Federation effort of GLONASS (Global Orbiting Navigation Satellite System) and the European Union effort of GNCC (Guidance, Navigation, Control and Communications) scheduled for completion in 2008.

### Mobile Voice and Wireless Data Networks

Mobile telephony has revolutionized the way people communicate. From 11 million mobile subscribers in 1990 to 300 million in 1998 and an estimated 1.2 billion in 2005, it is not difficult to see why location information is becoming increasingly important (ITU, 1999a). First generation mobile networks (1G) were based on analog transmission using frequency division multiple access (FDMA). Second-generation systems (2G) were later introduced to allow digital applications and to work towards a single standard. The latter aim did not eventuate however as even more applications were introduced. These included the global system for mobile (GSM), which used time division multiple access (TDMA), and the introduction of other frequencies like code division multiple access (CDMA). In addition, different variations of second-generation mobile networks sprouted up around the world, predominantly in the United States, Europe and Japan. The typical network elements have stayed the same however, and generally include mobile switching centers (MSC), base station controllers (BSC) and base transmission stations (BTS). Each MSC, usually located in a city center, has associated registers, including the home location register (HLR) and the visitor's location register (VLR). These electronic

directories help to identify the position of an individual all the way down the hierarchy to a single BTS or cluster of BTSs. In 2000, an initiative called International Mobile Telecommunications (IMT)-2000 began with the purpose of not only offering mobile subscribers higher transmission rates but of working towards achieving a global standard for third generation mobile networks (3G). The concept of a *family* of standards was then adopted by the International Telecommunications Union (ITU) to bring different types of networks together. These included macrocell, microcell, picocell, terrestrial cellular systems; cordless systems; wireless access systems and satellite systems. The ITU (1999b) have stipulated that the main aim of 3G is to introduce “seamless global roaming which enables users to move across borders and to make and receive calls while using the same number and handset.” If this is achieved, it will mean that every subscriber, independent of their network provider, will be locatable and universally identifiable, independent of where they are. 3G also gives service providers the opportunity to offer subscribers location-based services (LBS) like field service personnel management. There are present limitations to existing LBS however, including coverage availability, lack of appropriate content provision, cost, subscriber demand, and worldwide access equality.

#### Radio-frequency Identification (RFID)

Radio Frequency IDentification (RFID) in the form of tags or transponders can be used to detect, track and control. According to Stanford (2003, p. 9) “[c]onceptualizing them simply as ID tags greatly underestimates their capabilities, considering some have local computing power, persistent storage, and communications capabilities.” One of the first

applications of RFID was in the 1940s within the U.S. Defense Force where transponders were used to differentiate between friendly and enemy aircraft. Later, transponders continued to be used mainly by the aerospace industry (and in niche applications) until the late 1980s when the Dutch government voiced their requirement for a livestock tracking system. The commercial direction of RFID changed at this time and the uses for RFID grew manifold as manufacturers realized the enormous potential of the technology. The two most common RFID devices today are tags and transponders but since 1973 other designs have included contactless smart cards, wedges (plastic housing), disks and coins, glass transponders, keys and key fobs, tool and gas bottle identification transponders, even clocks. An RFID system has three separate components- a base station, a transponder and a communication interface in between. It is most commonly seen as a reusable and programmable tag that is placed on the object to be tracked, an antenna that transmits information contained within the tag, a reader that captures it, and a computer used for interpretation. Transponders, unlike tags, are not worn on the exterior of the body or object. On humans or animals in particular, they are injected into the subcutaneous tissue. In terms of further distinction, depending on their power source, transponders can be classified as active or passive. Active transponders are usually powered by a battery that operates the internal electronics. Some obvious disadvantages include cost, the need for replacement, and the additional weight that batteries add to the transponder unit. A passive transponder on the other hand has no internal power source. It is triggered by interrogation from a reading device emitting radio-frequency power. This causes the passive transponder to excite and reply. For this reason, passive transponders cost less and are longer lasting. As a further advantage, both types of RFID transponders

permit remote, non line-of-sight (LoS) automatic reading. This allows RFID to be used in a wide range of systems though typical implementations include wireless fidelity (wi-fi) campus networks, local area networks (LANs), and personal area networks (PANs). It should be noted that RFID infrastructure and the wireless local area network (WLAN) will be separate initially but with time will become highly integrated. “The existence of a robust and pervasive dual-mode communications infrastructure for WLAN and RFID tags will trigger numerous opportunities for applications around m-commerce.

Consumers will eventually utilize PDA-size multi-technology mobile computers that incorporate both wireless network connectivity and RFID tag communications” (Bridgelall, 2003, p. 2041). Branching out, large companies like Wal-Mart, Gillette, Proctor & Gamble, Unilever and Pepsi have announced plans to adopt RFID, as has the Department of Defense. Looking holistically then, it is the aim of non-affiliated institutions like the Auto-ID Center to make an *internet of things*. “By putting a radio-frequency identification (RFID) tag on every can of Coke, every pair of jeans and every bottle of shampoo in the world, companies will be able to track their products from manufacturer to consumer- and potentially even through to recycling” (Atock, 2003, p. 24).

### Geographic Information Systems (GIS)

Geography is a fundamental element in the majority of public and private datasets. Everything in the world has a relative global position but until recently, data in spreadsheets was not studied in the context of location. Increasingly, geographic information systems (GIS) are becoming important as a tool for analysis and decision-

making in strategy and planning. GIS can be viewed as an integrating technology, which merges the “precise location and associated attributes of natural and man-made features. This combination conveys the “what” and “where” of a feature or object on the Earth's surface and is the foundation upon which a wide range of information can be integrated and displayed” (DIGO, 2002). GIS allows for a sophisticated method of data mining because it grants an end-user a two dimensional (2D) representation of their data through the use of thematic mapping. The power and flexibility of visual representation allows the analyst to interpret and quantify raw and aggregated data like never before. GIS also allows for the geocoding of custom individual or business data to a fixed location on the earth’s surface, and it can do this for a diverse range of coordinate systems. It enables the seamless integration of geographic information sets ranging from topographical to social to political to telecommunications-specific, and much more. The strength of GIS is in helping to shed light on the overall environmental challenges and benefits by converting them into uniquely viewable spatial data which can come in two main formats, including vector and raster. Vector maps contain polygons, lines and point information that are measurable in terms of surface area, length and specific latitude and longitude. Raster maps are undivided images that can be registered as a backdrop to vector layers of information. Raster maps more often than not are aerial photographs or satellite images that reveal what would otherwise be hidden detail. The quality of images has been vastly improved since September 1999 when IKONOS, the first 1-metre commercial remote sensing satellite was launched. Today it is possible to acquire satellite imagery at a resolution precise enough to identify unique attributes of a private dwelling, including the presence of a swimming pool, barbecue area or clothes line. Although such imagery can

be processing and storage intensive, embedded GIS systems mostly used for mobile navigation require only basic spatial layers given the output is displayed on smaller screens. It is now not an uncommon practice for automobiles to be equipped with GIS mapping units for driver navigation.

## TECHNOLOGICAL EVOLUTION

### Complementary and Supplementary Innovations

Thus far the chapter has described important location positioning technologies that are relevant to homeland defense security. While they have been introduced individually, their definitive value becomes apparent when they are considered together, as complementary and supplementary innovations. GPS, mobile networks, RFID and GIS can be used together to solve complex location problems or to generate geographical intelligence with the assistance of additional peripheral devices. Macario (1997, p. 263) describes hierarchical cell-based location plans in the traditional macrocell, microcell, picocell arrangement within a geographic context. “A macrocell would give overall area coverage, and take command of traffic motoring past. A microcell area... would focus on slow moving subscribers moving between high-rise buildings, for example; while a picocell focuses on the foyer of a theatre, or exhibition centre.” When using these geospaces in real-time applications, together positioning technologies can overcome one another’s limitations, from global to local levels of detail. Recognizing this, Varshney (2003, p. 244f) puts forward an integrated location management architecture that consists of several heterogeneous wireless networks including satellites, cellular, PCS and 3G networks, and wireless LANs and PANs to support every possible level of user request.

He explains, “[t]he location precision requirement can be satisfied by using one of several wireless networks, which provide different levels of location accuracy. An extensive wireless coverage is achieved by providing indoor and outdoor coverage to fixed and mobile users in local as well as wide area environments. Access to multiple wireless networks also enhances the infrastructure’s dependability.” Li et al. (2004, p. 1015) agree that “[b]y using wireless technology like GSM, GPRS, PHS, CDMA and RFID... the communications over applications is unbounded.” In another paper, Siegemund and Flörkemeier (2003, p. 378) describe the important role that mobile phones will play in location applications in the future. They believe that their ubiquitous nature and economic success means, “mobile phones [will] serve as the major platform for users to communicate with smart objects because they are also present when an interaction with a smart object is to take place.” They propose that mobile devices like phones, PDAs and digital cameras will increasingly become Bluetooth-enabled and allow for direct communications between BTnodes and mobile device features like SMS (Short Messaging Service). Interestingly enough however, very few have published papers on the potential of mobile location technologies for homeland defense, save for the application of battlefield operations and management during actual combat, and what is increasingly being referred to as network-centric warfare (NCW).

Other key components employed in compound systems include: automatic identification to allow user access, handheld or wearable devices that act as GPS receivers and mobile voice/data transmitters, a Mobile Location Centre (MLC) that identifies devices in a mobile network, an Information Management System (IMS) to ensure the capture of

location and identification information in a format that is reusable to system workflows, and web-based intelligent applications that can be viewed by those who need to build the strategies for homeland defense or who need to respond to breaches in security. In these intelligent applications, the representation of maps can show coarse scales of regional administrative boundaries, or can be increased in granularity to show particular locales, such as troubled hotspots or war zones. End-users can then change the zoom level in order to identify an individual dwelling or, identify particular features of a floor plan within a building. The most important operating criteria for such a system are whether or not the data is readily available, whether it is in the appropriate format, and how it can be built dynamically with links back to the IMS via radio signals. There are two methods for sending this information to storage; either directly to a host computer through a standard interface, or in a portable reader for upload at a later time. In addition to the above, other information technologies considered important in counterterrorism include:

“categorizing/clustering, database processing, event detection and notification... predictive modeling, publishing, searching, semantic consistency/resolving terms, video processing, visualization, workflow management” (Popp et al., 2004, p. 39). Kun (2004, p. 30) adds “... simulation... data mining/data warehousing, intelligent agents, decision support/expert systems... and link-analysis” to the list. It is through the combined use of these tools that massive amounts of data are transformed into intelligence. To aid in this transformation, what becomes crucial is the use of semantic techniques. These “are extremely useful in organizing and structuring data into information that would facilitate effective decision-making and in extracting contextually relevant information and knowledge” (Laxminarayan & Kun, 2004, pp. 25f; Avant et al., 2002). The big picture

thus shows that it is information and communication technologies that will play and *need* to play a pervasive and central role in overcoming informational challenges in homeland defense. According to Congress's Joint Inquiry into the 9/11 attacks, if U.S. intelligence agencies had made better use of information technology, September 11, 2001, might have been "just another day" (Popp et al., 2004, p. 36).

### Commercialization

The technologies described above have mostly stemmed from defense initiatives. GPS for example, had a military origin, and its research and development was an effort to support strategic nuclear and tactical military missions. Foundations in defense mean the technology can be employed against an enemy and it can be considered controlling by nature. In 1983 however, GPS was opened up to civilians, whereas previously it had been solely for military use. This change had major implications as it meant that governments other than the United States and its allies could use the capabilities of GPS. Further, the commercial sector did not take long to embrace the military technology and the number of GPS applications grew exponentially. What is ironic is that commercial applications are now, again, being considered for their original purpose within defense. But is it too late? In the case of GPS especially, what was originally protected so that it would not be used against the U.S., has been declassified and given over willingly. The possibility is that GPS will now be used against its creator. Kun (2002, p. 31) supposes, "[i]f we know where we are through a GPS/GIS system, so does someone else who can intercept such information. If we can control every single device at home or at work, or do financial transactions electronically remotely, so can someone else claiming to be us." In the same

vein, satellite imagery can be acquired *over-the-counter*, allowing information to be accessed by an enemy who may have previously known very little about the country's terrain and key locations. Of course one could argue that paper maps are just as accessible as their digital counterparts but few would disagree that the power of digital mapping is many times greater than that of its hardcopy equivalent.

### Location-Based Services (LBS)

Commercial applications that utilize positioning technologies are diverse and range from child monitoring devices used to ensure safety to care-related devices for Alzheimer's sufferers who may lose their way. Humans are not the only living recipients of positioning technologies though, animals too are increasingly finding themselves implanted or tagged to prevent the extinction of species, to encourage better agricultural practices and even to track food down the chain to the point of consumption. Objects are also being equipped with GPS units and RFID tags. It is now possible to get directions from in-car GIS applications, objects on-the-move, and from stolen vehicles being tracked. There exist niche LBS companies that specialize in offering fleet management services incorporating vehicle navigation and property asset tracking via air, ship and road. In addition, mobile handsets can even be tracked, either by the use of an in-house GPS chipset or by the current zonal information acquired by nearby BTSs. The general method of network triangulation however can only identify the mobile device as being inside the BTS coverage area, and this could be right next to the BTS or over 30 kilometers away. In 2003 the Federal Trade Commission in the U.S. asked that wireless operators provide Automatic Location Identification (ALI) for persons making

emergency services calls. The resultant Public Service Answering Point (PSAP) now allows wireless operators to accurately identify the location of an individual to between 50-150 meters.

Some of the more notable LBS applications on the market today include: iMode by NTT DoCommo, mMode by AT&T Wireless, the Personal Locator by WherifyWireless, and the VeriChip by Applied Digital Solutions. iMode and mMode offer consumer and business users a diverse range of mobile commerce applications, including LBS functions to find people nearby, find facilities nearby, and get directions, weather and traffic reports. The Personal Locator uses a GPS wristwatch and additionally takes advantage of the wireless operator's footprint within the coverage area to identify an individual's latitude and longitude coordinates. The VeriChip device on the other hand allows for identification of a user in a building and can be used for offender monitoring and patient-supplied healthcare-related information. VeriChip's VeriTrack application offering is marketed as the "who, what and where of your company... VeriTrack is designed to track, monitor and protect all assets within an organization or company, including people." Other niche LBS are those such as the DestronFearing Corporation offering for animal ID, Skye-Eye for asset tracking, SnapTrack for fleet tracking, Starmax's Startrax monitoring system, and CarCom as a locator for cars. LBS applications are not confined to land; RFID and satellite shipboard transponder systems are also being used at sea. The Automatic Identification System (AIS) for example, has the ability through a VHF transponder to "repeatedly broadcast the ship's name, position and other details for automatic display on nearby ships" and for coastal states to log ship routing information (Moutray & Ponsford,

2003, p. 386). There are two ways that LBS can be deployed- one mode requires environments be context aware, the other mode is triggered on demand by a tag worn by the user. There are advantages and disadvantages to both of these approaches in gathering defense intelligence. Regardless, the types of applications that are currently being developed will be aiming at fulfilling control, convenience and care-related product innovations (Michael & Masters, 2004). With the ability to know where someone is 24x7 however, opportunities for any breach in security can be considered serious.

### Systems Integration and Convergence

While each of the positioning technologies discussed above can be used individually, integrating them with each other and additional network-centric devices increases their power manifold. For example, consider the Wherify Wireless GPS Universal Personal Locator phone that contains an atomic clock, GPS chipset, and telephone capability, including a 911 emergency button, concierge service, and two-way speaker. The all-in-one combo device can fit in one's purse and has been made possible by advancements in electronics, computing and telecommunications. Miniaturization and increases in processing power and storage have given rise to numerous product innovations.

Depending on the level of service being offered to the subscriber, completely disparate network types can now operate in tandem. GPS and 2G/3G networks can now work harmoniously toward fulfilling an application goal. The Globalstar operator for example, offers dual CDMA/GPS coverage on the same plan with a different pricing structure. Subscribers use a multimode phone which first attempts connection using terrestrial links; if that fails, a satellite link is used instead. Handheld devices can also be used in a

variety of wireless solutions. Industry convergence is occurring at just about every level of the positioning technology value chain, as combinations of technologies are being brought together and applied to offer completely new capabilities. Kurzweil (1999) has called this phenomenon the Law of Accelerating Returns, while Ni et al. (2003, p. 407) refer to the “growing convergence among mobile computing devices and embedded technology” describing the union as sparking “the development and deployment of context-aware applications, where location is the most essential context...” Sangani (2004, p. 26) also notes that “it [is] abundantly clear that digital convergence has well and truly arrived and is here to stay” in discussing the increasing phenomenon of digital device convergence. He adds that Bluetooth and wireless LAN are “complementary” technologies. Cohen (1999) describes these dynamics as the *push-pull* effect in technological innovation. In the first instance, advanced technologies serve the specific needs of new operational tasks (push effect), namely, the technologies have been created or combined for the purpose of fulfilling a new requirement. In the second instance, when new technologies or existing technologies are combined in new ways, a trigger pull effect can occur, leading to the development of new military systems. Positioning technologies act to fulfill both push and pull effects. One need only consider the role that GPS has played in spurring on future development. It was initially built to serve a military requirement for navigation and once achieved, it was not long before it was recombined with other techniques such as RFID and suggested for a diverse range of applications, including intelligent transportation. Generally, “[t]he proliferation of wireless technologies, mobile computing devices, and the Internet have fostered a growing interest in location-aware systems and services” (Ni et al., 2003, p. 407).

## THE LINK BETWEEN POSITIONING TECHNOLOGIES AND DEFENSE INTELLIGENCE

Nine months before September 11<sup>th</sup>, the United States' defense program developed by the Defense Department's Quadrennial Defense Review (QDR) was criticized for not being the "strategic blueprint needed to meet... emerging threats" (Kosiak et al., 2001). These warnings went unheeded until the 9/11 attacks took place. According to Kosiak et al. the major flaw with the QDR program was that it merely pointed to transformation but did not actually stipulate how it would be achieved in reality. The QDR simply paid homage to such terms as 'information warfare' and 'network-centric warfare', and rather than a proactive approach to defense planning, the U.S. took a *business-as-usual* approach. The U.S. learnt a grave lesson the hard way, that in these times of global uncertainty, a sit-back-and-wait approach is fatalistic. Just because a nation has enjoyed relative peace for some time, especially a powerful nation like the U.S. who has made ample developments in weaponry and stealth, it does not mean that relative calm will be enjoyed indefinitely. In fact today, the mightiest can fall subject to the most unimagined enemy. Terrorist organizations or cells have been behind some of the most heinous crimes the world has seen yet, but these individuals are most effective when they are at work "inside" the borders of a nation, not outside. When we reflect on 9/11, what we must remember is that, independent of their nationality, it was U.S.-trained pilots that steered an airplane into each Tower. The U.S. granted them residency, but the government did not know their real motive for entry or their day-to-day exchanges. This is what was perhaps most alarming to citizens of the U.S.- the lack of intelligence about the events that were to

unravel, and the lack of communication and warning to citizens of Manhattan. Worse still (at least in terms of national security) was the targeting of the Pentagon itself, and the alleged targeting of the White House. In a single moment the attack made a mockery of U.S. defense and multibillion dollar early-warning programs. What it demonstrated was the fragility of any country under attack, and more so, that there are no longer any limits to terrorism. How is it possible, for instance, to defend against suicide bombers?

#### Areas of Concern

Since the turn of the millennium the world has witnessed occasions where technology, especially positioning technologies, could have been used to aid governments, potential victims, or civilians at large against prospective threats or conflicts. These threats are not merely linked to the trafficking of weapons of mass destruction (WMD) or the much discussed stockpiling of nuclear, biological and chemical (NBC) warfare. Beyond WMD and NBC is a nation's broader scope of concern for homeland defense including maintaining an anti-access/area-denial environment, carrying out urban eviction and control, and the management of space and information. All of these require geographic information in order to trace an individual's tracks or to identify when suspicious behavior is taking place so as to allow for immediate response. Consider for example, the 'successful' production of WMD or NBC as a failure in defense intelligence. It is generally too late once weapons have been produced because inevitably they will be used by someone, somewhere, sometime. The window of opportunity that is most important to a defense intelligence community is that time between the terror plot being conceived and its planning. One cannot stop an individual from conceiving to kill others but one can

stop a perpetrator from carrying out these machinations, given enough advanced warning. Ideally a robust defense intelligence system should be able to detect and identify the group that is considering producing NBC weapons or that is in the process of procuring materials to produce WMD. In broader terms, the intelligence system would be focused on preventative measures and rarely with taking responsive action in terms of battlespace strategies. Taking a utopian view, with such a full-scale system in place there would be minimal conflict or none at all. The aim of a geospatial defense intelligence system would be to detect unlawful activity both from within a nation's borders, and wherever feasible and relevant outside its national borders. Examples of what this managed and integrated system could do include:

- identifying potential threats to the safety of civilians in public space, such as
  - on public transport in key traffic hotspots (including air, ship, rail and road)
  - around major landmarks, government buildings, and entertainment venues
  - places where people congregate like shopping malls, schools, universities, hospitals, churches and banks
- predicting the likelihood of hostage crises, and other terrorist actions
- identifying potential assassination attempts of very important persons (VIPs)
- aiding in the prevention of environmental disasters such as
  - the deliberate poisoning of major waterways and dams
  - the spraying of crops with harmful chemicals (i.e. food contamination)
  - toxic fumes released in closed areas like subways
- preventing the disruption of services, which cause major outages in utilities like
  - electricity; gas; water; telecommunications; nuclear power plants; refineries

- avoiding the blanket coverage of harmful unconventional warfare to major centers
  - biological: dissemination of anthrax spores; small pox unleashed
  - chemical: dirty bombs
  - radiological
- containing virus outbreaks and other health concerns
  - contagious and non-contagious disease control
- infiltrating international organized crime syndicates such as
  - underground trading of materials and skills
  - money laundering rackets
- intercepting trafficking in
  - drugs; people smuggling; border control/customs control
- controlling influx in
  - illegal immigration; asylum seekers
- maritime surveillance issues
  - illegal fishing; illegal dumping; piracy
- countermeasures for cyberterrorism
  - intercepting communications such as email, CDs or digital messages
- preventing fraudulent activities
  - social security benefit overestimation
  - multiple identities claimed by the same individual
- proactively identifying organizations that are opposed to law and order
  - including religious organizations with extremist beliefs; and
- responding to other human emergencies.

## Realized Defense Intelligence Applications

Operation Iraqi Freedom was lauded as the first real war of the 21<sup>st</sup> century and, as such, was seen by many as the first opportunity to implement and utilize new positioning technology strategies in a real-time environment. The outcome was to be determinative of whether advancements had indeed created a better, more efficient fighting force. Among the new capabilities trialed were:

- Several new types of unmanned aerial flight vehicles whose capabilities ranged from tactical extended vision over short distances, to strategic systems that could provide GIS images from 65,000 feet (Moutray & Ponsford, 2003).
- Imaging of targets in near-real-time, and email transmission of the GIS photos and GPS co-ordinates to bombers in flight.
- A real-time computerized display of land, sea and air forces, shared by component commanders and tailored to specific viewing needs.
- Force movements shown on real-time computer displays carried by battalion brigade and division commanders (Caterinicchia & French, 2003).

These enhancements to the type and coordination of assault meant that the time needed for quick targeting was reduced to 45 minutes. This is a vast improvement on the four-day turnaround of Operation Desert Storm in 1991. Despite the progress however, some difficulties were evident. Foremost, there is a communications problem for those who range too far from the central technology hub. For those fighters in Iraq who were out of contact, problems were encountered because the bandwidth needed to carry data on

systems other than satellites was not available. This shows that the size of the information generated by positioning technology can be unwieldy, especially where the quality of GIS images or positioning messages is paramount. Further, the actual information itself was not propagated appropriately throughout the military ranks. Though higher ranks had access to real-time spatial data, broadcasting of this information to the front-line defense was irregular at best. Whereas in battle it is this front-line who must make instant decisions based on known circumstances, it is arguable that they have the most need for the information. Lastly, many believe that the Iraqi conflict was not a real test of advanced positioning systems as the Iraqi soldiers were not a suitable opposition. Indeed, the Iraqi forces “did not blow up bridges or use chemical weapons... [They] did not exploit the lack of a coalition offensive from the northern front or take advantage of their dug-in urban positions” (Caterinicchia & French, 2003). Dealing with an unskilled enemy then, it would be unwarranted to conclude beyond doubt that their defeat gave a true picture of the worth of the new technology-embracing strategies.

It is important to note that the implementation of any positioning technology application still cannot provide one hundred percent read or identification accuracy in all cases in the current state of development. The RFID reading process may, for instance, encounter interference from other wireless systems or nearby metals. Nevertheless, this does not detract from the ability of RFID to provide efficiency through automated tasking. In one instance, this may include the coordination of objects and relationships. In an airport environment for example, dependant on information stored on a transponder, the use of RFID on luggage can allow airline personnel to link travelers to their luggage, to flight

manifest logs, and to law enforcement databases. In other scenarios, RFID can facilitate the coordination of access restrictions. Many smart-card access systems in use today employ RFID technology to associate the cardholder with access permissions to particular locations. Commonly used as a means of building control, the boundaries of this application extend to the general regulation of space. Traffic management is one extended use with RFID vehicle identification schemes such as the Australian eToll initiative, operating on major Sydney, Melbourne and Queensland roads, being used to improve transportation efficiencies. Employed to bypass toll payments, drivers purchase a uniquely identifiable RFID tag that is placed in the front window of their vehicle. RFID readers sit at unmanned tollbooths and, upon recognizing a nearby transponder, allow vehicular access to the motorway, bridge or tunnel. The unique identifier stored in the eToll transponder is then logged for billing purposes. Similar automatic vehicle identification schemes have also emerged in military circles. Boundary control at U.S. military bases in New Jersey and Massachusetts have both, at different times, employed passive UHF RFID devices on military transport to denote 'cleared' vehicles and to allow them access to the facility. These simple implementations of positioning technology support defense intelligence initiatives by automating the access control process, increasing efficiencies- as much as possible- without reducing pre-existing security measures.

Outside distinctly military circles, positioning technologies still have great realized impacts for homeland securities. To illustrate, we look to the prison system. In 2002, 27 of 50 American states were using some form of satellite surveillance to monitor parolees.

Similar schemes have been used in Sweden since 1994. In the majority of cases, parolees wear wireless wrist or ankle bracelets and carry small boxes containing the vital tracking and positioning technology. The positioning transmitter emits a constant signal that is monitored at a central intelligence point. Economic benefits exist, as it is cheaper for parolees and minor offenders to serve their sentences from home, than to be tax-funded members of the prison population. In Sweden, savings were said to have been between 8 and 16 million U.S. dollars for the 1997 calendar year alone. Social benefits are also present. On the one hand, because of the accuracy of GPS, there is a level of defensive certainty involved in identifying and monitoring the whereabouts of so-called 'threats' to society. On the other hand, there is a level of privacy afforded to the parolee. Where the tracking devices are cumbersome, there is some stigma of an external tag, but there are realized means for the GPS component to be in inconspicuous form. Digital Angel for example, entered into an agreement with both California Governor's Office of Criminal Justice and Planning and Department of Corrections to undertake a one year pilot program in which the movements of Los Angeles County parolees would be monitored using wearable devices. Taking this one step further, the use of *implantable* RFID for tagging prisoners or parolees is a similarly realized application of positioning technology in the homeland security arena. Moral concerns however, make this distinctly humancentric use of the technology unlikely in the existing climate. VeriChip especially, a current forerunner in implantable RFID sales and manufacturing, is attempting to dissociate itself from any promotion of involuntary identification. This shows the obvious conflicts with allowing technology to empower the wrong people. Certainly, there is no real technological difference between a democratic government implanting parolees, and

a totalitarian government implanting political activists and minority groups. As Kun (2002, p. 31) has foreseen, “[p]erhaps one of the greatest challenges of this decade will be how we deal with this theme of privacy versus national security.”

### The Vision: Geospatial Intelligence

Prior to 9/11 very little was written about homeland security. Since this time however, the number of academic works has exploded. These articles envision that technological advancement will play an integral role in solving a plethora of defense issues. Already millions of dollars are being allocated to the research and development of programs for transitioning military defense away from conventional warfare (e.g. Command and Control Research Program). While there are peripheral issues such as strategic directions, choosing the right leadership, building agile organizational units, enhancing procurement methods and funding the right projects, it is technology which is being heralded as the way forward to 2010 and beyond. The vision rests in an evolving area known as ‘information intelligence’, which is now increasingly being considered in the context of space (geographic location) and time (mobility). The terms ‘information intelligence’ and ‘geospatial intelligence’ can be used interchangeably. DIGO (2002) defines geospatial intelligence “as the collection, exploitation and analysis of imagery and geospatial information to locate, describe, assess and visualize physical features, observable phenomena and geographically referenced activities over time and space.” Information systems which are then affected by geospatial intelligence include: “navigation systems, command support systems, surveillance systems, weapons platforms, mission planning systems, war games, simulators, and facilities/range management systems” (DIGO,

2002). With regard to homeland security and defense specifically, the future focus is on how best to utilize positioning technologies and associated geospatial systems to prevent *standard*-type attacks or to respond to *non-standard*-type attacks which need ad-hoc specifications or require rapid response in an emergency situation. This vision, encompassing the process of not just intelligence gathering but the use of surveillance and reconnaissance, would require that timely, accurate and relevant information be collected and assessed on a citizen-by-citizen basis. The idea might sound Orwellian (because it is), but governments have been conducting small-scale surveillance through the use of data matching programs for decades, often for the sake of reducing social security benefit fraud. The question is, at what lengths are we as citizens willing to go to for the sake of peace, albeit a peace which cannot yet be guaranteed, irrespective of the measures taken?

#### Practical Commercial Positioning Applications Linked to Defense

For the time being, positioning technologies for civilian safety have existed purely in the commercial arena. Consider the GPS Locator for Kids application marketed by WherefyWireless, which is used to locate a Personal Locator wrist-worn device anywhere, upon a subscriber's request. Not only is the exact position of the individual identified but a breadcrumb of that individual's path can also be displayed using the World Wide Web. As has been noted already in the chapter, the company recently launched the Universal Locator Phone, marketed as a safety solution for both families and businesses. WherefyWireless believe the solution is useful for "kids and teens on the go, executive security, Alzheimer's patients, working women, hikers and joggers,

vacations, fleet management, mobile work force, commercial fleets, theft prevention and tracking of stolen assets, vehicles, briefcases and laptop bags, cargo, heavy equipment, marine equipment, and many other uses” (WherifyWireless, 2004). Many of these applications can be tailored toward the implementation of defense strategies. It is not impossible to think that in the future all citizens may wish to adopt this kind of device for convenience or safety reasons, or that alternatively a government may impose its use on its own citizens.

When the Severe Acute Respiratory Syndrome (SARS) epidemic began to spread in various parts of Asia, it was mobile service providers who contributed to the dissemination of important information through SMS. Sunday Communications, a Hong Kong mobile operator, and Starhub a Singaporean mobile operator, provided up-to-date information about SARS-infected buildings, giving travelers and locals the ability to reduce the risk of becoming infected. By ringing the SARS number subscribers would request that their phones be tracked and sent a warning of the potential risk of being in a particular calling zone (Lui, 2003). In both instances the SARS-related data was taken from the country’s Department of Health, and included “locations visited by suspected SARS patients and updated names of buildings within one kilometer of the subscriber’s calling area in which there ha[d] been confirmed cases” (Staff, 2003). As important as outdoor tracking of SARS cases was, the indoor “hospital-centric” tracking was even more vital. Ling (2003) describes the use of the Contact Track & Trace system, and the Hospital Movement Tracking System, based on RFID technology used to monitor visitors, patients and hospital staff. The system worked as follows. Every individual

given physical access to the hospital was issued with a RFID sensor card to be worn around the neck. As people walked around the hospital, data was captured via RFID readers and stored in the central computer's database. Information about an individual's contact in the hospital was stored for 21 days after each new contact point. The information was then widely used to create intelligence surrounding the SARS outbreak and potential spread of new infection. This brings us to an interesting point, the future need for cooperation between commercial and government bodies. Where the government was once depicted as a provider of *all* services, current commercial realities show that the government must outsource or deregulate in order to gather useful data and fulfill its main objectives. Cohen (1999), speaking from a U.S. perspective agrees, stating that, "[d]efense against hostile information operations will require unprecedented cooperation among Services, defense agencies, commercial enterprises, and U.S. allies." This corresponds with an interesting mix of interests. In one respect, private entities are helping the government and citizens of the nation by providing important information to those who want it. On the other hand, they are generating extra revenue from their existing subscriber base for using network airtime.

In a further stage of advancement the VeriChip company has also put forward the use of a positioning technology for the safety of individuals. In this instance, the device is not wearable or luggable but implantable. RFID transponders for humans, implanted in the subdermal layer of the skin, are the latest in ID technology; the innovation being not in the actual device but in the way it is housed underneath the skin. In response to the 9/11 tragedy, VeriChip M.D. Director of Medical Sales, Dr Richard Seelig had a chip

implanted in his hip and another in his arm to demonstrate its prospective use in such situations, particularly for research and rescue operations. Senior Vice President of Technology Development, Keith Bolton, told Murray (2002), “[Seelig] was motivated after he saw firefighters at the World Trade Center in September writing their Social Security numbers on their forearms with Magic Markers... He thought that there had to be a more sophisticated way of doing an identification.” Very Important Persons have also adopted the technology to decrease the likelihood that they will be kidnapped. As Scheeres (2002a) reported “[f]oreign executives and other individuals who are frequent kidnapping targets in Latin America will soon be able to use implantable ID chips and personal GPS devices in an attempt to thwart their abductors.” Cunha Lima, a Brazilian politician of more than twenty-two years believes the technology will contribute to public safety and security- “I believe this technology will act to deter the shocking rise of kidnapping of the children of businessmen” (Scheeres, 2002b; Horn, 2000). RFID implants are most useful when the bearer is unable to communicate and requires to ‘be found’ without seemingly sending out an intentional signal. Closed campus environments are best suited to the technology but all that is required for open environments is that the transponder is within the range of a reader. The high water content of the human body however, deems this to be quite a short range where RF signals are concerned. In a less pervasive compromise, longer reading distances are available using RFID transponders in bracelets or interwoven into clothes or shoes. These external devices have already been used in a variety of vertical sectors including for low-risk criminals serving their sentences from home, for new-born babies or children who are in hospital or daycare and

subject to possible kidnapping, and in aged care facilities particularly for sufferers of dementia.

Positioning techniques are useful but only so long as information can be captured and processed immediately or at a later point. One proposal for data capture involves a supplementary innovation to fixed or mobile positioning techniques, in the form of identification cards. While national ID schemes have been debated since the inception of citizen ID numbers, it is now likely that smart cards will be introduced widely, especially given rising concerns over fraudulent activities related to social security benefits. In fact, in December 2001 there was a proposal put forward to the United Nations by Pascal Smet to register every human in the world with their biometric. At first the system was proposed solely for the European Union but later was discussed as a global initiative (Hawthorne, 2001). Some proponents of a UID believe that, “[f]ears of terror and identity theft, as well as the complexity of multiple databases make the prospect of using a single identifier look very attractive... While expensive and difficult to implement, a universal identifier makes control of personal information much easier, both for governments wishing to provide services and to protect citizens, and the individuals themselves trying to control their personal information” (Friedman & Wilford, 2003).

In the U.S., biometric systems have been used for electronic benefits transfer and other social services such as the Immigration and Naturalization Service Passenger Accelerated Service System (INSPASS) for over ten years. One of the first counties to introduce biometrics for social services was Los Angeles County in California for their General

Relief (GR) program. Among the problems of the legacy system outlined by county supervisors were the falsification of photos, signatures and social security numbers that were encouraging applicants to sustain multiple identities. In the past, governments worldwide have been criticized for their inefficiencies regarding the distribution of social services. There are still many developed countries that use paper-based methods in the form of vouchers, coupons, ration cards, concession cards to operate large-scale federal and state programs. Singapore, Taiwan, the Philippines, Malaysia, Thailand, Saudi Arabia, Spain, Germany and the Czech Republic were some of the first countries to introduce national ID smart cards. One of the largest-scale smart card projects was begun in China, led by the China Citizen Card Consortium. The plan is to have one integrated card for citizen identification, health care and financial purposes. “The smart card is set to store the bearer’s ID number, health care code, address, birthdate, parents’ names, spouse’s name and a fingerprint” (Valles, 1998, p. 7). The U.S. Department of Defense has similarly instituted a multiapplication smart card to replace the various military paper records, tags and other cards. The MARC (Multi-Technology Automated Reader Card) was distributed to all 1.4 million active duty armed forces personnel. Coordinator, Michael Noll said that the ultimate goal of MARC was: “[a] single standard, multiple-use card that [could] be used across the government... for applications such as payroll, employee records, health care and personnel assignments” (Jackson, 1996, p. 41). MARC was first used during the Gulf War crisis. The card contains a magnetic-stripe and integrated circuit, as well as a photograph and embossed alphanumeric text and it can handle up to 25 applications.

In Britain, beyond biometrics, chip implantation was suggested for illegal immigrants, asylum seekers and even travelers. The problem of migration is not an easy one to solve, people regularly move from one country to the next, often retaining dual citizenship. In addition to this, blocs like the European Union have now made it easier for people to roam freely between countries, giving rise to difficulties in tracking inflows and outflows of people from one place to the next. Being able to manage these flows would be crucial to prospective defense plans. Smet argued the following (Hawthorne, 2001), “[i]f you look to our societies, we are already registered from birth until death. Our governments know who we are and what we are. But one of the basic problems is the numbers of people in the world who are not registered, who do not have a set identity, and when people move with real or fake passports, you cannot identify them.” To aid in alleviating this problem, the notion of Universal ID numbers (UID) or “follow-me” numbers is one embraced by numerous governments and has been supported (to an extent) by such legislation as the Electronic Digitized Signature Act of 2000 in the U.S. The only problem for implementation is the great divide between wealthy nations and those with either poor infrastructure or who are strongly opposed to the idea. Herein lies the additional question, what good is a UID smart card to citizens of a lesser developed country, especially where the multitude of services the UID proposal embraces are not available to them? Independent of this, national person-number systems are not the only issues that governments are grappling with. In response to 9/11, several bills were passed in the U.S. Congress to allow for the creation of the Enhanced Border Security and Visa Entry Reform Act. The U.S. now demands the use of biometrics for incoming and outgoing travelers, and aliens must either comply with the new rules or forgo visiting

altogether. Many civil libertarians were astounded at the pace at which these bills were passed and relevant legislation created, however this reflects one strategy to help minimize the risk of potentially harmful people entering the U.S.

## CONCLUSION

There is an increasing trend toward the commercialization of military technologies for civilian use. Technologies once developed by the military for the sole purpose of defense are now being embraced by private companies who recognize their potential widespread application in new mass market areas like Location-Based Services. Interestingly, the military who were once considered the end-to-end service providers of their own needs, has now acknowledged that it too must rely on the private sector not only to fulfill but progressively to advance its main line delivery. This latter trend has coincided with the perceived need for ensuring homeland defense through the use of integrated management systems. Knowledge based on geospatial information will serve as the hub for intelligence gathering activities. The concept of a hierarchical positioning technology system, as presented in this chapter, will pave the way forward for location intelligence that can assist in the prevention of breaches in homeland defense- from small-scale social security fraud to high impact terrorist attacks. This subject is explored further in the chapter titled *The Advancement of Positioning Technologies in Defense Intelligence*.

## 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>

- Atock, C. (2003). Where's my stuff. *Manufacturing Engineering*, April, 24-27.
- Avant, D. et al. (2002). Semantic technology applications for homeland security. *Proceedings of the Eleventh International Conference on Information and Knowledge Management*, 611-613.
- Bridgelall, R. (2003). Enabling mobile commerce through pervasive communications with ubiquitous RF tags. *IEEE Wireless Communications and Networking*, 3, 2041-2046.
- Caterinicchia, D. & French, M. (2003, June 19). Network-centric warfare: not there yet. *Federal Computer Week*. Retrieved June 18, 2004, from <http://www.fcw.com/fcw/articles/2003/0609/cov-netcentric-06-09-03.asp>
- Cohen. W. S. (1999). *Annual report to the President and the Congress: the defense strategy*. Retrieved June 3, 2004, from <http://www.pentagon.gov/execsec/adr1999/chap1.html>
- DIGO. (2002). *Defense imagery and geospatial organization*. Retrieved June 5, 2004, from <http://www.defence.gov.au/digo/>
- Friedman, A. & Wilford, S. (2003). *Universal national identifier*. The virtual citizen: identity, autonomy and accountability workshop. Retrieved June 1, 2004, from [www.sccs.swarthmore.edu/users/02/allan/UID\\_scenario.doc](http://www.sccs.swarthmore.edu/users/02/allan/UID_scenario.doc)
- Hawthorne, M. (2001, December 14). Refugees meeting hears proposal to register every human in the world. *SMH*. Retrieved June 20, 2004, from <http://www.iahf.com/other/20011219.html>
- ITU. (1999a). *Satellite systems— from VSAT to GMPCS*. Retrieved June 10, 2004, from

[http://www.itu.int/telecom-wt99/press\\_service/information\\_for\\_the\\_press/press\\_kit/backgrounders/backgrounders/satellite\\_systems.html](http://www.itu.int/telecom-wt99/press_service/information_for_the_press/press_kit/backgrounders/backgrounders/satellite_systems.html)

ITU. (1999b). *World Telecommunication Development Report 1999: Mobile Cellular*.

Retrieved June 13, 2004, from [http://www.itu.int/ITU-D/ict/publications/wtdr\\_99/page1.html](http://www.itu.int/ITU-D/ict/publications/wtdr_99/page1.html)

Jackson, W. (1996). The MARC card gets smarter. *Government Computer News*, 15(1), 41-43.

Kosiak, S., Krepinevich, A. & Vickers, M. (2001). *A Strategy for a Long Peace*.

Retrieved June 1, 2004, from [http://www.csbaonline.org/4Publications/Archive/R.20010130.A\\_Strategy\\_for\\_a\\_L/R.20010130.A\\_Strategy\\_for\\_a\\_L.htm](http://www.csbaonline.org/4Publications/Archive/R.20010130.A_Strategy_for_a_L/R.20010130.A_Strategy_for_a_L.htm)

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

Kun, L. G. (2002). Homeland security: the possible, probable, and perils of information technology. *IEEE Engineering in Medicine and Biology*, 21(5), September/ October, 28-33.

Kurzweil, R. (1999). *The age of spiritual machines: when computers exceed human intelligence*. New York: Viking Books.

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

Li, C-J. et al. (2004). Mobile healthcare service system using RFID. *Proceedings of the 2004 IEEE International Conference on Networking, Sensing and Control*, 2, 1014-1019.

- Ling, T. C. (2003). Contact track and trace. *Electronics Review*, 16(2).
- Lui, J. (2003, April 18). Cell phone firm offers SARS alerts. *CNETAsia*. Retrieved June 23, 2004, from [http://zdnet.com.com/2100-1103\\_2-997457.html](http://zdnet.com.com/2100-1103_2-997457.html)
- Macario, R. C. V. (1997). *Cellular radio*. New York: Macmillan.
- McDonald, M. D. (2002). Key participants in combating terrorism. *IEEE Engineering in Medicine and Biology*, 21(5), September/ October, 34-37.
- Michael, K. & Masters, A. (2004). Applications of human transponder implants in mobile commerce. *Proceeding of the Eighth World Multiconference on Systemics, Cybernetics and Informatics*, Orlando, Florida, 505-512.
- Moutray, R. E. & Ponsford, A. M. (2003). Integrated maritime surveillance: protecting national sovereignty. *Radar*, 385-388.
- Murray, C. (2002, January 7). Injectable chip opens door to human bar code, *EETimes CMP Media*. Retrieved April 8, 2003, from <http://www.eetimes.com/story/OEG20020104S0044>
- Ni, L. M., Liu, Y., Lau, Y. C. and Patil, A. P. (2003). LANDMARC: indoor location sensing using active RFID. *Proceedings of the First IEEE International Conference on Pervasive Computing and Communications*, 407-415.
- Popp, R., Armour, T., Senator, T. & Numrych, K. (2004). Countering terrorism through information technology. *Communications of the ACM*, 47(3), 36-43.
- Sangani, K. (2004). RFID sees all. *IEE Review*, 50(4), April, 22-27.
- Saydjari, O. S. (2004). Cyber defense: art to science. *Communications of the ACM*, 47(3), 53-57.

Scheeres, J. (2002a, January 25). Kidnapped? GPS to the rescue. *Wired News*. Retrieved October 15, 2002, from <http://www.wired.com/news/business/0,1367,50004,00.html>

Scheeres, J. (2002b, February 15). Politician wants to 'get chipped'. *Wired News*. Retrieved October 15, 2002, from <http://www.wired.com/news/technology/0,1282,50435,00.html>

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.

Staff. (2003, May 1). Operator delivers SARS updates. *Wireless Week*. Retrieved (June 23, 2004, from <http://www.wirelessweek.com/article/CA295478>

Stanford, V. (2003). Pervasive computing goes the last hundred feet with RFID systems. *Pervasive Computing*, 2(2), 9-14.

Valles, E. (1998). Smart ID cards to guarantee privacy: national card plans get underway amid anxieties. *China News*, October 7, p. 7.

Varshney, U. (2003). Location management for mobile commerce applications in wireless internet environment. *ACM Transactions on Internet Technology*, 3(3), August, 236-255.

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

WherifyWireless. (2004). *Wherify's GPS locator phone*. Retrieved June 20, 2004, from <http://www.wherifywireless.com/univLoc.asp>

White House. (2001, October 8). *Executive order establishing office of homeland security*. Retrieved June 15, 2004, from

<http://www.whitehouse.gov/news/releases/2001/10/20011008-2.html>

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.