Blue Mission Tracking: Real-Time Location of UN Peacekeepers

A. WALTER DORN and CHRISTOPH SEMKEN

A basic but as yet unachieved goal for UN missions is to know the exact locations of their peacekeepers at any given time. Such tracking would help field missions plan operations, avoid and respond to ambushes, kidnappings and friendly fire incidents, rapidly send reinforcements and retrieve wounded peacekeepers, ultimately saving lives. Improved effectiveness could be obtained from 'precision peacekeeping', where soldiers, police and civilians are deployed to precise locations and events, while operational leaders follow their movements. Fortunately, tracking technology has improved considerably so that commercial solutions for real-time tracking of personnel and vehicles are now available at lower cost and increased accuracy and sophistication, while being more user-friendly. The advances in phone and vehicle tracking systems are reviewed here to identify the benefits, drawbacks and challenges, especially any political ones, for the United Nations. The world organization can benefit from modern blue mission tracking, without having to develop costly, customized solutions. Such initiatives have few technological or financial hurdles but the politics and institutionalization of continuous positional surveillance needs policy modernization, guided by a nuanced understanding of technological empowerment.

UN peacekeepers risk their lives trying to save others. Technology can help the blue helmets protect others as well as themselves, and advance their multidimensional mandates.[1] But the United Nations is traditionally under-equipped and under-resourced, even when it comes to life-saving technologies. Fortunately, one long-desired technology is now easily within reach: live tracking of UN vehicles and personnel. So far, the United Nations has not been able to establish a system for real-time tracking of the movements of its military, police and civilian personnel. But thanks to recent breakthroughs in both positioning and communications technologies, the available solutions have become more effective, including cost-effective. Over the past decade, costs have decreased by a factor of at least ten while accuracy has increased several-fold. In addition, electronic miniaturization and the 'convergence' of formerly disparate technologies means that modern devices like phones often contain location systems along with many other components. For instance, many smartphones contain positioning systems, signal transmitters, cameras, accelerometers, compasses and gyroscopes, as well as finger-print scanners and various sensors.

Just as positioning technologies have caused a revolution in military affairs (RMA) in modern forces, some of these same technologies can create a revolution in peacekeeping affairs. With exact location information, it is possible to carry out 'precision peacekeeping', where the military, police and civilians in the missions are deployed to the areas where they are most needed. But, as with the

International Peacekeeping, Vol.22, No.5, 2015, pp.1–20
http://dx.doi.org/10.1080/13533312.2015.1094192

RMA, a peacekeeping revolution needs a change in doctrine and policy to make use of the new technology.

This article examines the requirements, benefits and challenges of phone and vehicle tracking systems. It looks at the ways and impediments to realize the recommendation of the UN's Expert Panel on Technology and Innovation in Peacekeeping: 'tamper-resistant tracking technology should be installed on all vehicles and heavy weapons systems […] it is now imminently practical to locate all vehicles and peacekeepers in a mission at any given time, including in emergencies, in a flexible and cost effective manner'.[2] In agreement with the panel, practical tracking solutions were found to be readily available to enhance both the security and efficiency of UN peacekeepers, thanks to the revolution in communications and information technology. As the United Nations tackles the technical, political and privacy concerns, these real-time tracking solutions can save lives and alleviate much human suffering.

The Need for Tracking

Fatalities are too common among UN peacekeepers. Since 2010, the number of fatalities due to malicious acts has been rising both in absolute terms and relative to the other causes.[3] The number of UN personnel killed in attacks has risen from 37 in 2012 to 58 in 2013 to 62 in 2014.[4] Of the 58 people killed in 2013, half died in ambushes on UN convoys. One tragic example took place in Jonglei State, South Sudan, on 9 April 2013 when five peacekeepers, two of the UN mission's national staff and five civilian contract employees were ambushed.[5] When such peacekeepers are under attack, immediate situational awareness, including the positions of the convoy and nearby UN forces, is desperately needed. The information can help the United Nations to reach and rescue beleaguered staff more quickly, to send reinforcements and to assess the situation even before arrival. Reinforcements sent in the past – for example, during the attack on a UN convoy in South Darfur on 13 July 2013 that left seven peacekeepers and one police adviser dead[6] – would have benefitted from a detailed map or Geographical Information System (GIS) showing the exact positions of vehicles and peacekeepers to aid them faster and more effectively.

The benefits of tracking are not confined to providing rapid reinforcements for beleaguered convoys. In the attacks on the UN Common Compound in Mogadishu, Somalia, on 19 June 2013, knowledge of the staff's exact positions could have been used to evacuate the area and retrieve wounded peacekeepers. Eight UN staff were killed in the attack.[7] Live-tracking can help commanders who plan and carry out operations, allowing them to optimize their forces in places where they are most needed. In combat situations, both hostile fire and 'friendly fire' accidents can be reduced. For instance, if Kurdish soldiers at a checkpoint in Iraq had properly tracked or identified Canadian trainers arriving for a meeting at night in March 2015, it is unlikely they would have fired upon the Canadians, thereby saving a life and reducing injury.[8]

Live-tracking can also be used for early warning and the prevention of firefights by identifying areas that peacekeepers are about to enter and alerting them of potential dangers, based on information stored in a GIS. Similarly, tracking can help to counter human and arms smuggling since movements of blue or friendly forces can be distinguished from others, especially at night or in the rugged terrain preferred by smugglers.

In less dire emergencies, such as when peacekeepers are lost or their convoys are held up by locals, tracking can also allow the United Nations to find them more rapidly. In some cases, the nearest peacekeepers can be identified and sent to the area. Alternatively, quick reactions forces can be dispatched. Such reinforcements can be sent without the need for time-consuming and sometimes inaccurate location descriptions. The last known locations of kidnapped peacekeepers can be used in rescue operations. They may even be tracked in real time after being taken hostage, provided their tracking devices (e.g. within smartphones) are still transmitting. Stolen vehicles can be tracked and recovered more easily, an increasing challenge in missions. For instance, in Darfur, dozens of carjackings in 2014, in which vehicles of the mission, UN agencies and international non-governmental organizations were stolen.[9]

Contingents commanders need to know the positions of peacekeepers from other contingents, especially in overlapping areas of responsibility. In the Cambodia mission in 1993, the battalion commander from The Netherlands, Colonel (at the time) Patrick Cammaert, complained that he knew too little not only about the locations of the Khmer Rouge rebel forces but also about the other UN battalions and workers near or within his area of operation.[10] This is a problem of blue force tracking that now finds a technological solution.

Military tracking is commonly divided into blue, green, red and white force tracking. Blue force tracking refers to the movements of one's own forces – a particularly appropriate colour for the UN – whereas green refers to friendly forces and red to hostile forces, which are becoming all too common in the UN's areas of operation. Finally, white force is commonly understood as individuals or organizations somehow associated with the blue force, such as humanitarian agencies or non-governmental organizations. The civilian population can be represented by other colours (e.g. purple). In our analysis we focus on 'blue mission tracking', including all vehicles and personnel – military, police and civilian – of a UN mission. However, green, red and white force tracking are important too, and are discussed briefly in this article.

The United Nations has already made modest advances in UN vehicle tracking over the past decade. Currently, it uses an offline vehicle tracking system in most of its peacekeeping missions. The 'Carlog' devices in UN vehicles record position information while the car is operating and transmit the data when the vehicle is close (within about 150 metres) to a receiving antenna, usually at UN facilities. The vehicle's Carlog device transmits a log of the vehicle's locations and routes since the last upload. It also conveys information on distances travelled and driving behaviour. In addition, Carlog is used for driver authentication (swipe card used in the Carlog device before ignition), speeding alerts (beeping) and fuel optimization. The reported benefits of the Carlog system include: reduced accidents and injuries; improved driving performance; better fuel efficiencies; reduced repair costs; more regular vehicle maintenance; a reduced number of unauthorized trips; and improved vehicle security (using ID pass codes). Carlog also reduces paperwork since no manual trip-tickets need to be filled out. Overall, the Carlog system has proven itself a major aid for vehicle allocation and fleet management. However, the system does not provide an accurate picture of where vehicles or persons are located at any one time. Carlog only provides a historical record that does not help for urgent live operations or when a vehicle is missing.[11]

For both safety and effectiveness, the United Nations can employ a modern tracking system for real-time awareness of vehicles and personnel locations. Such systems are already used by advanced militaries, but is this achievable within the limited resources and politically constrained environment of the United Nations? By combining tracking information from two main types of devices, cell phones and vehicles, a cost-effective system can be achieved with valuable redundancies. Other location devices can also be added for other equipment, including heavy weapons, or for persons not carrying smartphones. Positions can be displayed on screens with a dynamic GIS at mission and regional headquarters, and made accessible to peacekeepers in the field. The vehicle tracking data could be supplemented by location updates sent from peacekeepers' smartphones and devices.

Technical Requirements

Three particular technical issues need to be addressed to verify the effectiveness of tracking solutions: reliability; update frequency; and data security/encryption. Because of the challenges and potential vulnerabilities, including from opposing or hostile forces, these technical aspects need to be understood so they are not exploited. They also impact on the political and privacy considerations discussed later.

Reliability of the System

Obviously, a UN tracking system needs to be reliable. Mission leaders and military commanders have to be certain that they can access accurate tracking information at all times. Loss of signal, interference by hostile forces or corrupt devices could all lead to confusion, loss of control and thus put peacekeeper lives at risk. Reliability will depend on the basic parts of the system.

Most tracking solutions use the Global Positioning System (GPS), a Global Navigation Satellite System (GNSS) operated and maintained by the US Air Force, to determine an individual's or object's location. The GPS space segment is very reliable. To provide an accurate position anywhere on earth, 24 GPS satellites are required. Since 2009, the number of healthy GPS satellites has always been between 28 and 31.[12] The reliability of the space segment notwithstanding, the GPS system is still vulnerable to ground control and receiver issues. In 2010, a software problem 'rendered as many as 10,000 U.S. military GPS receivers useless for days'.[13] Other events could result in a blackout, such as solar storms, volcanic eruptions, intentional destruction of satellites, technological problems, collision of satellites in earth orbit, intentional or unintentional interferences, military conflicts and financing issues.[14] Since the US government has full control over GPS it could potentially decide to prohibit usage partially or fully to gain a military advantage or to save money. Although 'selective availability', which reduces positional accuracy, is currently turned off and economic interests make a return to this practice unlikely, the US government in 2004 stated that 'the president could decide to disable parts of the network for national security purposes'.[15] Such deliberate deactivations are politically very unlikely though it is still technically possible, at least until the expected launch of new GPS satellites in 2017.[16]

Despite the risks, there is currently no feasible GNSS alternative to GPS. The Russian GLONASS system is only optimized within Russian borders due to its low number of satellites;[17] and the deployment of the European Galileo system and the Chinese BeiDou system will not be completed until 2019 and 2020, respectively.[18] Moreover, the above-mentioned issues are likely to affect all GNSS in much the same way.

Once position is determined on the mobile device, individual or vehicular, there are generally two means to transmit the position to a centralized GIS: mobile networks (for both radios and cell phones) and satellites. The reliability of mobile networks varies across countries. Networks in many large developing countries have traditionally only covered a small proportion of national territory, usually through the Global System for Mobile Communications (GSM, formerly *Groupe Spécial Mobile*).[19] Progress has been encouraging as indicated by the increasing number of cellular subscribers: since 2009 the number of subscriptions jumped from 58 to 90 per 100 inhabitants in developing countries.[20] However, even when data- or text-enabled mobile networks are accessible and reliable, governments in political crises could shut down the mobile networks and/or disrupt internet access. For instance, this happened at least twice in the Syrian Arab Republic during its ongoing civil war.[21] Unlike mobile networks, satellites have almost universal coverage. Therefore, satellite communication is recommended for vehicle tracking, at least as a backup possibility. Updates via satellite for smartphones would be desirable too but they are not yet cheaply available, though individual tracking devices are on the commercial market.

A potential risk to both mobile network and satellite communications is the intentional jamming of signals by hostile forces. Both GSM and GPS signals can be jammed effectively.[22] How to mitigate the risks associated with electronic warfare is beyond the scope of this article. In any case, deliberate jamming of GPS signals and mobile systems is rare and the spoilers in UN mission areas would be unlikely to use such techniques.

The systems used to store and view tracking information need to be reliable as well. Service-Level Agreements (SLAs) with industry can be used for both uptime and security guarantees. The *standard* SLA of one company guarantees an uptime of 99.99 per cent and includes penalties against the company in case of outages.[23] UN devices have to be free from malware, and redundancies should be provided. Finally, the GIS maps need to be sufficiently detailed for the given country or area, which is less likely for conflict areas. Maps should be editable so UN staff in the field and at headquarters can add details relevant to the mission; for example, layers showing the security concerns and many other relevant factors.

Bandwidth and Update Frequency

In peacekeeping, the update frequency of a vehicle/phone position will be determined by need, including the type of UN activity and the potential for problems. Ideally, the UN would want a system comparable to the US military system, which updates vehicle positions every 100 metres under Blue Force Tracking 2 (BTS2, 800m under BFT1).[24] For vehicles driving at 100 km/h, location updates need to be sent with a frequency of up to one minute to achieve an accuracy of 800m or five seconds for an accuracy of 100m. Even though bandwidth is a continual problem in peacekeeping missions, the GPS signal information will not put a strain on UN computers, given that they need only a few kilobytes per second, even with a multitude of devices.

Data Security and Encryption

Data security is vital for any UN tracking solution in a conflict zone. Leaked data could assist hostile forces in locating UN troops or persons.[25] Even outdated or incomplete geolocation data could be used to analyse UN patrol patterns and operation procedures. Over 200 threats to a GSM-network communication have been identified in the literature.[26] Data security needs to be ensured throughout the entire communication process, including the mobile tracking devices, the mobile network, the internet communication and the local UN network.

First, smartphones should be secured using appropriate software and, more importantly, by providing adequate training to peacekeepers.[27] The security of vehicular devices, on the other hand, can be ensured through contracts with the supplier. Second, encryption must be used in the connection between the GIS and the mobile device, as well as any separate devices used to view the locations on a map.

GSM and the newer '3G' network communications can be eavesdropped,[28] as can regular internet connections. Data and voice encryption is available for many commercial tracking solutions. The encryption between tracking devices, including smartphones, and the server depends on the protocol used and whether it is done through proprietary or standard encryption methods. All products studied used either Transport Layer Security (TLS) or Virtual Private Network (VPN)-encrypted connections for accessing the web interface, meaning that a connection between the GIS and the client cannot be eavesdropped.

Access to the GIS also needs to be restricted and the computer networks themselves have to be safe. Again, data security can be achieved at the supplier's end using contracts with penalties. For the United Nations, strong security policies need to be put in place for all devices that could be used to access the GIS.

Cost

Another key consideration is affordability. The United Nations cannot afford the expensive, customized technology that some advanced armies use because the world organization operates on a constrained budget. Fortunately, for tracking there are many inexpensive commercial solutions available.

The commercial-off-the-shelf solutions studied by the authors benefit from economies of scale, resulting in lower prices for server licences. Developing a customized UN tracking solution, on the other hand, would likely cost tens of millions of dollars. For instance, the United States spends approximately $20,000 per vehicle on its Force XXI Battle Command Brigade and Below (FBCB2) Blue Force Tracking (BFT) and Future Combat Systems (FCS).[29] Orders from one contract for encryption devices, software, maintenance and customer support for the FBCB2 system alone exceed $100 million.[30] Similarly, the contract value for the NATO GPS Force Tracking System amounts to approximately $84 million.[31] The United Nations will not be able to spend that much money on a tracking solution. However, this does not mean that the United Nations has to give up all the advantages of an integrated solution. Once new tracking devices have been deployed in the field, it will be easy to integrate location updates into the maps created by the UN cartography and GIS cells.

Even basic smartphones allow live cellular tracking in addition to the features that the Carlog vehicular system currently provides, namely fuel management, driver authentication, speeding alerts, maintenance scheduling and logging driving behaviours. Basic vehicle tracking devices that include these features can be acquired for $350–550 per device. More advanced devices that also support satellite communication, panic buttons and other features are available for under $1,000.[32]

Monthly costs for server licences and data connections are added to the procurement costs. However, the former does not usually exceed $30 for both vehicle tracking devices and smartphones while the latter can be kept low through deals with local network providers. Even satellite tracking can be achieved for $0.15 per hour when sending an update once a minute.

The costs for real-time vehicle tracking devices are comparable to what the United Nations has previously spent on offline tracking, and smartphones can be added cheaply.[33] Thus, the costs for such systems are not expected to be a barrier and should easily pass through the UN procurement and management system. If there are questions in the General Assembly's Fifth Committee or the Advisory Committee on Administrative and Budgetary Questions (ACABQ), it is unlikely to be about cost. Political and privacy issues are more likely to be of concern.

Personal Privacy

Vehicle tracking will not be considered a privacy issue here because the vehicle is UN property and such tracking is already being done by the United Nations, albeit not in real time. However, supplementing vehicle tracking with smartphone tracking means that supervisors would be able to track peacekeepers at any time.

Tracking can be an issue between the employer and employee (or even officer and soldier) because the former can potentially track the latter, including on off-time. The collected data can be used to exercise control, affecting both trust and the tracked individual's privacy. In the United States, for example, tracking data have been used to fire government employees.[34] But safeguards can ensure the protection of individuals from an abuse of the tracking data, including privacy policies and regulations. In the field, the UN missions reserve the right to know the location of their staff at all times. This is particularly important during dangerous times or in dangerous places. However, the authors are unaware that the United Nations has any privacy policies in place, including for 'positional privacy'. None of the 'policy and guidance' documents published by the Department of Peacekeeping Operations (DPKO) and the Department of Field Support (DFS) set out privacy guidelines. Moreover, the UN Staff Regulations do not mention privacy or data handling.[35] In the absence of UN privacy standards, the United Nations should at least ensure that UN personnel are aware of the privacy implications of tracking applications. One way of achieving this would be a disclaimer that warns users about privacy issues when they first use the tracking application. Also, cell phone tracking can be turned on or off according to the situation and policy. For example, when employees are on leave (vacation) and out of the mission area, their device locators could certainly be turned off.

UN missions need to act in compliance with laws and regulations of the state that they are working in, including any privacy laws. The General Assembly's Special Committee on Peacekeeping Operations has continually affirmed host nation consent with regards to the use of new technologies. Although none of the studied countries restrict the usage of a positioning system for tracking purposes, the United Nations needs to examine the national laws prior to implementing a tracking system.

Survey of Tracking Solutions

Tracking of peacekeepers can be done through separate cell phone and vehicle tracking devices or, alternatively, hybrid systems. There are many types of products commercially available.

Cell Phone Tracking

At present, hundreds of tracking applications ('apps') are available for personal smartphones. Tracking apps typically use the phone's GPS receiver and the Cell Global Identity to send updates to a centralized server. Most commonly, consumer apps are used for personal reasons such as parental control, tracking of partners and friends and locating lost devices. Consumers can often track their phones free of charge and more advanced applications are available for just a few dollars, showing how readily available this technology is. When suitable smartphones are not available, pocket-sized tracking devices can be commercially purchased for peacekeepers.[36]

Similar tracking is used for many commercial purposes. Firms use field service management apps to access work order details, create invoices, manage customer histories and process payments. Wholesale distributers, construction workers, health care providers and other field workers have their location displayed on a map in real time so they can be sent to the next job more efficiently.

Vehicle Tracking

Today, vehicle tracking solutions are commonly used in a whole range of industries, including taxis services, construction, delivery, field services, heavy equipment, oil, gas and government. 'Fleet management' is an increasingly well developed field of commercial activity; over 200 software products are available to that end.[37]

In military operations, various systems can be used to achieve secure and reliable vehicle tracking. The Carlog system, currently used by the United Nations, as described above, provides at the basic level of secure offline tracking method. The devices are permanently attached to the vehicle dashboard and allow for driver authentication, route reporting and driving behaviour recording. Vehicle drivers identify themselves by swiping their licence card through the Carlog reader and entering a passcode. As mentioned, the device records position while the car is in motion but it does not convey such information until it is close to a receiving antenna.[38]

One important opportunity for real-time tracking of vehicles is provided by Terrestrial Trunked Radio (TETRA), which also serves as a communication system. TETRA is a European Telecommunications Standards Institute (ETSI) standard specifying secure mobile radio communication. TETRA networks are similar to GSM networks but allow for significantly larger cells (the area covered by one cellular radio tower, though communication is also possible directly radio-to-radio), strong encryption mechanisms and fail-safe networks. Unlike GSM phones, TETRA radios can also share channels directly in the absence of a mobile cell network. The standard is used in many public safety operations, including a few UN peacekeeping missions. Many modern TETRA radios include GPS receivers, allowing the operator of a TETRA network to locate and track the radios. Motorola, Airbus and Sepura all offer tracking applications as part of their TETRA solutions.[39]

TETRA constitutes a reliable and secure option for blue force tracking, but it is also costly. Apart from the cost for the radio devices, it requires the maintenance of a mobile radio network. For instance, the running costs of all TETRA terminals (handhelds, mobile and base units, etc.) operated by the Police Service of Northern Ireland (PSNI) in the one year period 2009–10, was £392,000 (or US$ 600,000).[40] The costs for running a TETRA network in countries with peacekeeping may be a lot higher due to the large size of many mission territories.

Hybrid Systems

Most commercially available fleet management systems now allow for hybrid solutions in which both vehicles and personal devices, including smartphones, can be tracked. The company typically provides the tracking devices, GIS and smartphone apps under one system. Satellite vehicle tracking is offered either on frequency bands leased by the company itself or in cooperation with a partner company. Smartphone tracking apps are usually available for the most common phones and can be used on the same system.

Almost all GIS allow for a variety of mapping materials such Google Maps, Bing, TomTom Maps and Navteq. The maps can usually be modified to include geographical fences, buildings, shapes, critical information and more. While most market leaders focus on the USA and Europe,[41] some companies have experience in or near conflict regions.[42] Some products allow the grouping of vehicles and persons to create a command and control hierarchy.[43] The structure can be used to reflect battalions, missions and countries, with access rights set accordingly. It is also generally possible to have location updates triggered by events in addition to periodic updates. For example, a peacekeeper's location could be updated in the event that he leaves a certain area ('geofencing').

Beyond the Blue

In the digital age, mission tracking results can easily be merged with an abundance of other information sources to create a more sophisticated and complete picture. An obvious addition is the location data from other UN agencies and friendly organizations. The locations of their vehicles and persons could be integrated into a GIS for greater situational awareness. From within the mission, the UN cartography and the GIS cells can add high quality mapping material, showing relevant infrastructure, mission boundaries, UN structures, difficult terrain and more. Joint Mission Analysis Cells (JMACs) and Joint Operations Centres (JOCs), which are found in almost all peacekeeping missions, can contribute their geospatial intelligence findings for display as 'layers' in the GIS. This can include any information on dangerous forces who threaten the civilian population. In Haiti, JMAC 'target packages' describing the likely whereabouts of violent gangs were successfully used for precision operations as well as the quick arrest of gang members.[44]

Even friendly locals can be added to the tracking system. This could include leaders and VIPs from the host state who may seek UN protection. Though local UN staff would already be covered, selected non-staff could be added. The UN's mission in the Congo established a Community Alert Network where local leaders can call the mission in case of impending attacks or other emergencies. Adding positional information would help respond to these locals as it would for UN staff. All of the UN's twenty-first-century multidimensional missions have a mandate for protection of civilians (POC).

Information collected by a range of other organizations can also increase the scope and effectiveness of real-time tracking. Indeed, many of the goals formulated in current mandates make co-operation between the mission and other actors essential. The United Nations Multidimensional Integrated Stabilization Mission in Mali (MINUSMA), for example, is mandated to coordinate with the Malian Defence and Security Forces, support rebuilding the police and gendarmerie (including through co-location), to provide support for the government more generally and to collaborate with bilateral partners, donors and international organizations 'through enhancing information sharing and joint strategic planning'.[45] The Security Council further demanded intermission cooperation between MINUSMA and both the United Nations Mission in Liberia and the United Nations Operation in Côte d'Ivoire). It also called upon the EU, African Union and Economic Community of West African States to coordinate with MINUSMA; and authorized French forces to intervene in support of MINUSMA.[46] Sharing location data with at least some of these agencies would drastically improve the effectiveness of the mission. In addition, geolocated intelligence findings from member states have in the past been an important source of information, including in Haiti and Kosovo.[47] Such findings, voluntarily shared by member states, could be readily integrated into tracking systems.

The maps can also include satellite imagery and other imagery provided, for example, by the Operational Satellite Applications Programme (UNOSAT), which is sponsored by the United Nations Institute for Training and Research. Disaster alerts and weather forecasts from the Global Disaster Alert and Coordination System (GDACS) can be included. Other UN agencies – including OCHA, UNHCR and the World Food Programme (WFP) – have used the help of volunteering networks and crisis mapping. The Standby Task Force (SBTF), for example, is a group of volunteers that has provided the United Nations with real-time crisis mapping and situational awareness support in over a dozen cases.[48] Ushahidi is one of the platforms frequently used by volunteers to create crisis maps – a form of 'crowdsourcing'. Furthermore, satellite imagery from both publicly available (Google Earth) and commercial sources (DigitalGlobe) has been used by Harvard's Satellite Sentinel Project to monitor atrocities in Sudan and South Sudan. All of these technologies are designed to be easily sharable and could be integrated into a UN tracking/GIS system.

Information sharing with many humanitarian organizations is possible where they have already embraced real-time monitoring. Oxfam and other NGOs use HELIOS for supply chain management in humanitarian relief operations. Sahana Eden is an open source software platform for rapid deployment of humanitarian operations, including live tracking. It was used to coordinate the help of about 700 organizations during the 2010 earthquake in Haiti. The International Federation of Red Cross and many other organizations use FleetWave to manage their vehicle fleets.[49] All these systems make it possible for humanitarian organizations to share their location information automatically or selectively with UN peacekeeping.

Despite the technical feasibility, many humanitarian organizations may be reluctant to share their information with UN peacekeepers. Too close cooperation could threaten their principles of independence and impartiality, lead to disagreement with funding sources and create tensions over the vital 'humanitarian space', especially when armed forces create their own humanitarian programmes. However, cooperation is possible if there is no cooption; automatic information sharing can be on a voluntary basis for the benefit of the NGOs as well UN peacekeepers.[50]

The Politics of Positioning

As shown, the technological and financial challenges to a new tracking solution for UN missions can be easily overcome. Both security and reliability concerns could be addressed, as can information sharing. After having ensured the electronic security of trackable phones, a tracking app can be installed within minutes. New vehicle tracking devices could be mounted onto any existing UN vehicle. Both smartphone tracking apps and vehicle tracking devices are easy to use. However, what are the political obstacles?

Troop contributing countries are unlikely to resist an improved UN tracking system, given that it offers greater security for their peacekeepers in the field. Some extra training might be necessary but that would be minimal and should be welcome as giving additional skills to national forces; a half-day seminar might be all that is needed. However, some contingents might want the tracking information to be contained only within their own units because, otherwise, the mission leadership could discover how little patrolling they are doing, especially at night or in more dangerous areas, precisely where UN patrolling is most needed. On the other hand, some contingents might welcome the tracking system to show how much patrolling and activity they are doing for proactive peacekeeping. Tacking systems will certainly increase accountability.

Since tracking will also provide higher commanders with more detailed knowledge about the positions of individual peacekeepers, the temptations for the 'tactical general' can arise. Officers high up the chain of command might attempt to issue orders to much smaller units or individuals in the formation, jumping levels of decision making. While the commander should be adequately informed – and tracking can help – the new technology should not be an excuse for an overly zealous commander to direct units tactically at more subordinate levels. With some discipline, the appropriate levels of decision making can be maintained.

The host state, which has given consent for the deployment of the peacekeepers, should not have objections to a better tracked UN mission. On the contrary, mission headquarters would be better able to respond to state queries over the positions of peacekeepers. Some host states may not want UN peacekeepers to venture into certain areas (e.g. near military bases) and tracking can help the United Nations to avoid such areas, if required. Besides, tracking is legally permitted as a communications technology. 'Unrestricted communications' are a right under the model Status of Forces Agreement that the UN uses as a basis for agreements with host countries.[51] It would be hard for a host country to complain that the United Nations knows the location of its own peacekeepers: the country's sovereignty is not affected.

The host state may seek to receive the UN tracking data in real time but, except on common exercises or operations, this should be resisted. Often the host state has activities it seeks to hide from the UN or there are informants within the state, loyal to a hostile party. It would be unwise to let wrongdoers know when the UN patrols are coming. In Western Sahara, it is well known that Moroccan troops timed certain violations to occur (e.g. berm construction and expansion) when peacekeepers were not present to observe or complain about the activity.

Major financial contributors to the peacekeeping budget are also unlikely to resist real-time tracking given the low costs for a commercial system – less than $500 per vehicle using GSM, roughly $1,000 when using satellite transmission and $10/month per smartphone. The financial benefit of combating carjacking alone is likely to offset much of these costs. The UNAMID example of at least 37 carjacking incidents in 2014 exemplifies this direct economic benefit by recovering more stolen vehicles. But more importantly, real-time tracking can save peacekeepers' lives in cases of ambushes, kidnapping, friendly fire, retrieval of wounded soldiers or the dispatch of reinforcements.

The readiness of the UN Secretariat to adopt a real-time tracking solution, at least for vehicles, is exemplified by its 2015 Request for Expression of Interest (EOI) on the matter.[52] Adding smartphones and using tracking data are new ideas that can also be implemented, particularly given the willingness of the United Nations to make technological progress. The UN's 2009 New Horizon report states: '[t]he UN […] needs access to new technologies for better situational awareness in the field'.[53] More recently, the DPKO and DFS have acknowledged the need for tracking technology by accepting the 2015 report of the Expert Panel on Technology and Innovation in Peacekeeping.

Some UN workers may feel uncomfortable with a tracking function that is always on, giving their location at all times. Though the envisioned system would be far from 'big brother' or 'panopticon' surveillance, any overbearing watch function could be counter-productive. So policies and arrangements could be made to allow personnel to turn off the tracking devices at certain times or during certain activities, for example, during off-times or while on leave. There are also certain professional activities for which it would not be helpful to be tracked; for example, informal meetings at bars, where the UN staff or local interlocutors (e.g. informants) might not want their location to be revealed.

Related Operational Experience

Evidence for the operational effectiveness and challenges of a blue force tracking (BFT) system comes from the US Army. The FBCB2 BFT system was developed in the late 1990s for continuous vehicle location. Computers with touchscreens and keyboards display the vehicle's position, other FBCB2 vehicles nearby, known 'enemy' units and static objects such as minefields and bridges on a map or satellite imagery.[54] Recently, a handheld version of FBCB2, the Joint Battle Command-Platform, was developed that allows for secure third-party applications to be installed.[55] In addition to blue force tracking, FBCB2 can be used to send electronic messages, orders and requests to any other FBCB2 unit.[56] Originally, all FBCB2 communication was to be communicated over terrestrial radio networks.[57]

The system was first used in the Balkans; however the mountainous geography of Bosnia and Kosovo proved to be an obstacle to the radio-based communication. Satellite communications were added to mitigate this issue and to allow communication over vast distances.[58] A ‘guard computer’ was added as a gateway between the commercial satellite network and the US classified network to enhance data security.[59] In Iraq and Afghanistan, FBCB2 was often the only way of determining one’s own position, for example at night or during sandstorms. Additionally, blue force tracking cut radio traffic, freed up time, allowed for the transmission of messages and graphics to multiple recipients, accelerated the distribution of orders and allowed for the reading of maps without a flashlight.[60] In 2007, US General Bryan D. Brown described the experience with the tracking system during Operation Iraqi Freedom in glowing terms:

> The overall effectiveness of Blue Force Tracking (BFT) in support of special operations was exceptional. While not all SOF [Special Operations Forces] were equipped with BFT devices, BFT systems facilitated coordinated events during combat operations, enhanced tactical resupply efforts, reduced recovery time for SOF extractions (both extremis and scheduled) and saved lives. BFT proved to be an outstanding control mechanism.[61]

The US experience, however, also showed some of the operational problems. First, returning soldiers reported that the system was too difficult to use. It was difficult to locate messages, the system did not work as expected and some soldiers had problems creating an operations order. In addition to unneeded mandatory fields in forms, the system did not have the features they were accustomed to (cut and paste, drag and drop, a right click menu).[62] Second, soldiers were experiencing inoperability problems with the different tracking systems used by logistics, combat and coalition forces:

> The inability to produce a single, accurate, common operational picture at any strategic, operational or tactical level limited the overall utility of BFSA [Blue Force Situational Awareness]. Additionally, when a warfighter did have access to limited BFSA he still experienced a challenge in using the data because he was unable to select and display data that was relevant to his mission.[63]

Another problem with blue force tracking is the risk associated with using outdated tracking information. Bryant and Smith find that providing participants of a battle simulation in an urban environment with real-time blue force tracking devices dramatically enhances their ability to distinguish between friendly and enemy forces. However, showing participants position information that is 10 seconds old (a typical latency time) resulted in significantly more false alarms (fratricide), regardless of whether participants knew about the latency or not.[64] Therefore smartphone tracking should, on an individual level, not be used to decide whether to shoot or not. Other uses do not depend on small latencies; for example the USA uses Personnel Recovery Blue Force Tracking to rescue pilots.[65]

In an analysis of the effectiveness of network-centric operations, Gonzales *et al.* compare the performance of different US army units during the US occupation of Iraq following Operation Iraqi Freedom.[66] The effectiveness of the 101st Airborne Division (ABD) was measured against those of two Stryker brigades – 3/2 SBCT and 1/25 SBCT – operating in the same area. The three units were carrying out stability operations in Mosul in 2003, 2004 and 2004/05, respectively. They constitute a relevant case study because of their very different endowments.

The 101st ABD had blue force tracking (FBCB2-BFT) only in some command and control vehicles and helicopters while all others relied on legacy radio equipment. Significant location information was available to the commanders only at the battalion level and the Division had limited information about enemies and the civilian population. The 3/2 SBCT, on the other hand, 'had the FBCB2-Enhanced Position Location Reporting System [. . .] on most platforms, allowing visibility and messaging with most tactical units. It also had a high-bandwidth satellite communications [. . .] to provide communications between the brigade's battalion-level units and higher headquarters.' However, the 3/2 SBCT still had very little information on the whereabouts of enemy forces and civilians. This changed when the 1/25 SBCT took over. The 1/25 SBCT had access to more human intelligence and used signals intelligence equipment, video links between aircrafts and ground commanders, as well as voice-over-IP conferencing which allowed battalion-level units to participate in commanders' conferences.[67] Thus, the 101st ABD had only basic tracking capabilities (comparable to what the UN uses now), the 3/2 SBCT was equipped with a blue force tracking system (similar to the one proposed in this article) and the 1/25 SBCT used a more advanced tracking system encompassing intelligence findings.

The result was a reduction in the average number of soldiers killed per enemy attack from 0.10 (for the 101st ABD) to 0.01 (for both SBCTs). Similarly, the number of soldiers wounded in enemy attacks decreased from 0.60 to 0.09 (for the 3/2 SBCT) and 0.05 (for the 1/25 SBCT). The same effects where observed in the number of US personnel killed per offensive operation. Caveats exemplifying the effect included the fact that the 101st ABD mostly fought dismounted and that the SBCTs were equipped with electronic counter measures against improvised explosive devices (IEDs). Yet, even in comparison with the average casualty numbers of all units deployed in Iraq the two SBCTs had between half and a fiftieth of the casualties.[68] Together with improvements in doctrine, tactics, techniques, procedures and training, the tracking system and digital communications have resulted in an orders-of-magnitude reduction in the number of casualties.

Gonzales *et al.* conclude that blue force awareness enabled 'a number of advanced tactics, including accelerated planning, dynamic force retasking, self-synchronization, and swarming, which in turn led to improvements in performing tactical defensive missions'.[69] The better situation awareness, increased speed of command and dynamic small-unit synchronization helped respond to ambushes and attacks, thus reducing the number of soldiers killed and wounded. Though peacekeeping does not involve such high levels of combat, it does require peacekeepers who are situationally aware in dynamic and dangerous environments.

Conclusion

The requirements for a real-time UN tracking system can currently be fulfilled by off-the-shelf commercial products. Most companies offer agreements guaranteeing the reliability of their system, whether run by the United Nations itself or by the companies as a service. For areas with poor GSM coverage, satellite tracking devices can be used, at least for vehicles. Many products offer important features, such as encrypted updates, panic buttons, flexible update frequencies, driver authentication, fuel management, speeding alerts and more. Maps and GIS can be edited on a basic level to display the positions of vehicles and smartphones in relation to UN compounds, mission boundaries and relevant objects. More sophisticated GIS can show both local human and geographical terrain.

Unlike some surveillance systems, the mission tracking system should not find much objection from police and troop contributing countries, nor from the host states. After all, the UN has a right and a responsibility to know where its peacekeepers are in the field. There may be some cases where the tracking devices should be switched off, possibly at that initiative of peacekeepers, as an aid to their privacy or to prevent this information from disseminating to hostile groups. But such measures can be built into the system and into UN policy, as well as mission-specific guidelines. Similarly, appropriate sharing of tracking information with UN agencies and cooperating NGOs is possible while respecting the needs for 'humanitarian space'. One or more 'technology contributing countries' could help the UN Secretariat to pilot and field test a workable system for the UN's diverse missions.

Affordable tracking solutions exist and they will benefit UN peacekeeping operations in many ways. Cost-efficient tracking of vehicles and peacekeepers helps ensure personal security, create efficiencies and can ultimately save the lives of many peacekeepers, as well as the people they are charged to protect.

ACKNOWLEDGEMENTS

The authors are most appreciative of the useful comments and support received from researchers at the Montreal Institute for Genocide and Human Rights Studies – Kyle Matthews, Meagan Boissé, Neeko Collett, Ecem Oksay and Marie Lamensch – and the International Peace Institute – Adam Smith and Michael Snyder.

ABOUT THE AUTHORS

A. Walter Dorn is a Professor of Defence Studies at the Royal Military College of Canada, and teaches mid-career military officers at the Canadian Forces College. He served as a member of the UN's Panel of Experts on Technology and Innovation in UN Peacekeeping. His latest book is an edited volume, *Air Power in UN Operations: Wings for Peace* (Ashgate, 2014).

Christoph Semken is a researcher at the Montreal Institute for Genocide and Human Rights Studies. He previously served as an Assistant for Information Technology and is currently completing his Master of Arts in International Relations and Economics at the University of Aberdeen.

NOTES

1. See UN, 'Performance Peacekeeping: Final Report of the Expert Panel on Technology and Innovation in UN Peacekeeping', 19 Feb. 2015, pp.27–8 (at: www.performancepeacekeeping.org/offline/download.pdf); and A. Walter Dorn, *Keeping Watch: Monitoring, Technology and Innovation in UN Peace Operations*, New York: United Nations University Press, 2011.
2. UN (seen. 1 above), pp.27–8.
3. In 2014, 39 peacekeepers died in Malicious Acts as defined by the Department of Peacekeeping Operations (DPKO), more than in any other year except 1961 and 1993. Source: UN, DPKO, 'Fatalities by Year and Incident Type', 31 Mar. 2015 (at: www.un.org/en/peacekeeping/fatalities/documents/stats_5.pdf).
4. These numbers include all UN associated personnel that were killed in attacks according to the Staff Union. Source: UN, 'With Increased Number of United Nations Personnel Deliberately Killed in 2014, Staff Unions Calls on Organization to Do More towards Protecting Lives', UN doc., ORG/1593, 13 Jan. 2015 (at: www.un.org/press/en/2015/org1593.doc.htm).
5. UN, 'Increase in Deadly Attacks against the United Nations Claimed More than 58 Lives in 2013, Staff Union Says', UN doc., ORG/1576, 8 Jan. 2014 (at: www.un.org/press/en/2014/org1576.doc.htm).
6. Ibid.
7. Ibid.
8. David Pugliese, Ian MacLeod, Mark Kennedy and Norman Provencher, 'Canadian Commandos Gunned Down despite Prearranged Code Words', *Ottawa Citizen*, 9 Mar. 2015 (at: http://ottawacitizen.com/news/national/canadian-soldier-dies-in-friendly-fire-incident-in-iraq-dnd-says).
9. Between 1 Jan. and 15 Nov. 2014, the number of carjacking incidents was 37, compared to 27 in 2013 and 22 in 2012. Source: UN, 'Report of the Secretary-General on the African Union–United Nations Hybrid Operation in Darfur', UN doc., S/2014/852, 26 Nov. 2014. Data compiled from S/013/852 and its predecessors S/2014/515, S/2014/279, S/2014/26, S/2013/607, S/2013/420, S/2013/225, S/2013/22, S/2012/771, S/2012/548 and S/2012/231.
10. Patrick Cammaert, communication to one of the authors after his return from Cambodia, Geneva International Peace Research Institute, Geneva, 25 Aug. 1993. General Cammaert was later appointed Military Adviser to the Secretary-General and then Force Commander in several peacekeeping missions.
11. Dorn (see n.1 above), pp.49–50.
12. Analytical Graphics, 'GPS Satellite Outage Information', AGI Developer Network, 20 Dec. 2014 (at: http://adn.agi.com/SatelliteOutageCalendar/SOFCalendar.aspx).
13. Dan Elliott, 'Air Force GPS Problem: Glitch Shows How Much U.S. Military Relies on GPS', *Huffington Post*, 6 Jan. 2010 (at: www.huffingtonpost.com/2010/06/01/air-force-gps-problem-gli_n_595727.html).
14. Miikka Ohisalo, Otto Tiuri, Tatu Urpila, Pasi Kämppi and Jyri Rajamäki, 'Risks and Vulnerabilities of Future Satellite-Based Tracking Systems', *International Journal of Geology*, Vol.5, No.4, 2011, pp.142–9.
15. CNN, 'Bush Plans for Shutdown of GPS Network during Crisis', 18 Dec. 2004 (at: http://web.archive.org/web/20041218020813/http://edition.cnn.com/2004/TECH/12/16/positioning.satellites.ap/index.html).
16. US government, 'Selective Availability', accessed 8 Mar. 2015 (at: www.gps.gov/systems/gps/modernization/sa/); Mike Gruss, 'Launch of First GPS 3 Satellite Now Not Expected until 2017′, *Space News*, accessed 8 Mar. 2015 (at: http://spacenews.com/launch-of-first-gps-3-satellite-now-not-expected-until-2017/).
17. Pasi Kämppi, Jyri Rajamäki and Robert Guinness, 'Information Security Risks for Satellite Tracking', *International Journal of Computers and Communications*, Vol.3, No.1, 2009, pp.9–16.
18. Chinese government, 'BeiDou Navigation Satellite System – System Introduction', 14 Dec. 2012 (at: www.beidou.gov.cn/2012/12/14/2012121481ba700d7ca84dfc9ab2ab9ff33d2772.html); European Commission, 'Galileo: Satellite Launches', 2012 (at: http://ec.europa.eu/enterprise/policies/satnav/galileo/satellite-launches/index_en.htm).
19. The GSM Association (GSMA) has created coverage maps for all its members (at: www.m4dimpact.com/data/networks-coverage). Coverage is very poor in countries such as the Central African Republic (CAR), the Democratic Republic of the Congo (DRC), Cote d'Ivoire and Sudan. However, the maps produced by GSMA are from 2009; up-to-date coverage maps are not publicly available.

20. ITU, 'ICT Indicators Database', 23 Dec. 2014 (at: www.itu.int/en/ITU-D/Statistics/Documents/statistics/2014/ITU_Key_2005-2014_ICT_data.xls).
21. BBC News, 'Syrian Internet Back after Blackout', 8 May 2013 (at: www.bbc.co.uk/news/world-middle-east-22447247); Iain Thomson, 'Syria Cuts off Internet and Mobile Communications', *The Register*, 29 Nov. 2012 (at: www.theregister.co.uk/2012/11/29/syria_internet_blackout/).
22. Hui Hu and Na Wei, 'A Study of GPS Jamming and Anti-Jamming', Proceedings from the 2009 2nd International Conference on Power Electronics and Intelligent Transportation System (PEITS), Shenzhen, 19–20 Dec. 2009, Vol.1, 2009, pp.388–91; M. Petracca, M. Vari, F. Vatalaro and G. Lubello, 'Performance Evaluation of GSM Robustness against Smart Jamming Attacks', Proceedings from the 2012 5th International Symposium on Communications Control and Signal Processing (ISCCSP), Rome, 2–4 May 2012, pp.1–6; J. Rantakokko, P. Handel, M. Fredholm and F. Marsten-Eklöf, 'User Requirements for Localization and Tracking Technology: A Survey of Mission-Specific Needs and Constraints', Proceedings from the 2010 International Conference on Indoor Positioning and Indoor Navigation (IPIN), Zurich, 15–17 Sept. 2010, pp.1–9.
23. Interview by one of the authors by Skype with Catherine Lewis, Executive Vice President of Mix Telematics, 28 Jul. 2014.
24. ViaSat Inc, 'Faster, More Effective Situational Awareness from the New U.S. Army FBCB2′, *Youtube*, 16 Jul. 2012 (at: www.youtube.com/watch?v=XDdZGiy8Luw).
25. In Bosnia, UN peacekeepers communicated 'in the clear' (unencrypted messaging) the landing positions from mortar fire. The Serb attackers used this information to correct their fire to make it more lethal. This is a clear example of the need for encrypted communications. A. Walter Dorn, 'The Cloak and the Blue Beret: The Limits of Intelligence-gathering in UN Peacekeeping', *International Journal of Intelligence and Counterintelligence*, Vol.12, No.4 (Winter 1999), p.416.
26. Daniel Fischer, B. Markscheffel, S. Frosch and D. Buettner, 'A Survey of Threats and Security Measures for Data Transmission over GSM/UMTS Networks', Proceedings of the 2012 International Conference for Internet Technology and Secured Transactions, London, 10–12 Dec. 2012, pp.477–82.
27. Woongryul Jeon, Jeeyeon Kim, Youngsook Lee and Dongho Won, 'A Practical Analysis of Smartphone Security', in Michael J. Smith and Gavriel Salvendy (eds), *Human Interface and the Management of Information. Interacting with Information*, Berlin: Springer Berlin Heidelberg, 2011, pp.311–20; Giles Hogben and Marnix Dekker, *Smartphones: Information Security Risks, Opportunities and Recommendations for Users*, European Union Agency for Network and Information Security, 10 Dec. 2010 (at: www.enisa.europa.eu/activities/identity-and-trust/risks-and-data-breaches/smartphones-information-security-risks-opportunities-and-recommendations-for-users).
28. Craig Timberg, 'German Researchers Discover a Flaw that Could Let Anyone Listen to Your Cell Calls', *The Washington Post*, 18 Dec. 2014 (at: www.washingtonpost.com/blogs/the-switch/wp/2014/12/18/german-researchers-discover-a-flaw-that-could-let-anyone-listen-to-your-cell-calls-and-read-your-texts/).
29. *Army Times, 'Army Integrating FCS, Blue-Force Tracking', 10 Aug. 2008 (at:* http://archive.armytimes.com/article/20080810/NEWS/808100314/Army-integrating-FCS-blue-force-tracking*)*.
30. Harris Corporation, 'Harris Corporation Receives New Orders to Deliver Programmable Encryption Devices to U.S. Department of Defense Blue Force Tracking Network', 22 Jun. 2011 (at: http://harris.com/view_pressrelease.asp?pr_id=3257).
31. Globecomm, 'NATO GPS Based Forced Tracking System', 27 May 2014 (at: www.globecommsystems.com/in-the-news/press-releases/press-release-5-27-contract-extension-nato.shtml).
32. Price estimates based on interviews by one of the authors by Skype with Jason Koch, President and Manager of Telogis Fleet at Telogis, 24 Jul. 2014; Catherine Lewis, Executive Vice President of Mix Telematics; Philippe Bisson, Business Development Director at Geothentic, 22 Jul. 2014; Ron Konezny, Vice President for Transportation & Logistics at Trimble Navigation Limited, 21 Jul. 2014.
33. For comparison, in 2006, MONUC bought 336 Carlog devices for $173,100, or $515 per device. Source: MONUC, '2006–7 Acquisition Plan – United Nations Mission in the Democratic Republic of Congo', 27 Sept. 2006 (at: http://web.archive.org/web/20060927081538/ http://www.un.org/Depts/ptd/2007_monuc.htm).
34. M. G. Michael, Sarah Jean Fusco and Katina Michael, 'A Research Note on Ethics in the Emerging Age of überveillance', *Computer Communications*, Vol.31, No.6, 2008, pp.1192–9.

35. United Nations, Secretariat, ‘Staff Regulations’, New York, 2008 (at: www.peacekeepingbestpractices.unlb.org/PBPS/Library/N0832434.Staff%20Regulations.pdf).
36. The SPOT personal tracker, launched in 2007, claims to be the ‘world’s first Satellite GPS Messenger’ which provides ‘location-based communications to friends, family or professional services’ from virtually anywhere. A SPOT device weighs only 200g and can be kept in a shirt or pants pocket or in a bag. Source: Spot LLC, ‘The SPOT Personal Tracker’, 2015 (at: www.findmespot.com/en/index.php?cid=101).
37. As of 4 Jul. 2014, Capterra was listing 274 fleet management software products (at: www.capterra.com/fleet-management-software/www.capterra.com/fleet-management-software/).
38. Dorn (see n.1 above).
39. Online descriptions can be found for Motorola’s MOTOLocator (at: www.motorolasolutions.com/XU-EN/Product+Lines/Dimetra+TETRA/TETRA+Applications/Motorola+TETRA+Applications/MOTOLocator), Airbus’ Imp@ct (at: www.defenceandsecurity-airbusds.com/fi/web/guest/c4isr-solutions) and Sepura’s SICS-NET Visualise (at: www.sepura.com/products/tetra/applications/command-control/sics-net-visualise/).
40. PSNI, ‘Freedom of Information Request F-2010-03334: Running Costs of Radio Communication Equipment’, 2010 (at: www.psni.police.uk/costs_radio_equip.pdf).
41. Interview by one of the authors by Skype with Clem Driscoll, C.J. Driscoll & Associates, 10 Jul. 2014.
42. Geothentic, for example, has customers in Mali, and Mix Telematics is based in South Africa and operates another data centre in the Middle East.
43. Interview by one of the authors by Skype with Jason Koch, President and Manager of Telogis Fleet at Telogis.
44. A. Walter Dorn, ‘Intelligence-Led Peacekeeping: The United Nations Stabilization Mission in Haiti (MINUSTAH), 2006–07′, *Intelligence and National Security*, Vol.24, No.6, 2009, p.826.
45. UN, ‘Security Council Resolution 2164′, UN doc., S/RES/2164, 25 Jun. 2014, sec. 12.
46. Ibid., sec. 10, 25–27. Another example is the UN Mission in the Central African Republic and Chad (MINURCAT) which coordinated with at least 20 agencies, including: the Chadian army; the gendarmerie; police forces; the government; the UN High Commissioner for Refugees (UNHCR); the United Nations Peacebuilding Support Office in the Central African Republic (BONUCA); the Multinational Force of the Central African Economic and Monetary Community (FOMUC); and the Community of Sahelo-Saharan States (CEN-SAD). Jim Rolfe, ‘Partnering to Protect: Conceptualizing Civil–Military Partnerships for the Protection of Civilians’, *International Peacekeeping*, Vol.18, No.5, 2011, p.567.
47. A. Walter Dorn, ‘United Nations Peacekeeping Intelligence’, in Loch K. Johnson (ed), *The Oxford Handbook of National Security Intelligence*, Oxford: Oxford University Press, 2010, p.293.
48. The United Nations Office for the Coordination of Humanitarian Affairs (OCHA), UNHCR, UNOSAT and the World Food Programme (WFP) asked for the help of the SBTF in, for instance, Colombia (2010), Libya (2011), Somalia (2011), South Sudan (2012), the Philippines (2013) and Pakistan (2014).
49. See Linet Özdamar and Mustafa Alp Ertem, ‘Models, Solutions and Enabling Technologies in Humanitarian Logistics’, *European Journal of Operational Research*, Vol.244, No.1, 2015, pp.55–65; M.T. Ortuño, P. Cristóbal, J.M. Ferrer, F.J. Martín-Campo, S. Muñoz, G. Tirado and B. Vitoriano, ‘Decision Aid Models and Systems for Humanitarian Logistics: A Survey’, in Begoña Vitoriano, Javier Montero and Da Ruan (eds), *Decision Aid Models for Disaster Management and Emergencies*, Paris: Atlantis Press, 2013, pp.17–44.
50. Rolfe (see n.46 above), p.566.
51. UN, ‘Model Status-of-Forces Agreement for Peace-Keeping Operations: Report of the Secretary-General’, UN doc., A/45/954, 9 Oct. 1990.
52. UN, Procurement Division, ‘Request for Expression of Interest: Provision of Fleet Management and Vehicle Tracking Systems for DFS’, 13 Jan. 2015 (at: www.un.org/depts/ptd/pdf/eoi10644.pdf).
53. UN, DPKO and DFS, ‘A New Partnership Agenda: Charting a New Horizon for UN Peacekeeping’, 2009, p.32 (at: www.un.org/en/peacekeeping/documents/newhorizon.pdf).
54. B.T. Robinson, ‘Who Goes There?’, *IEEE Spectrum*, Vol.40, No.10, 2003, p.45.
55. Claire Heininger, ‘Army Develops Smart Phone Framework, Applications for Battlefield Operations’, *Army Communicator*, Summer 2011, pp.56–7.
56. Richard J. Dunn, III, ‘Blue Force Tracking: The Afghanistan and Iraq Experience and Its Implications for the US Army’, Reston: Northrop Grumman Mission Systems, 2003, p.4 (at: www.

northropgrumman.com/aboutus/analysiscenter/documents/pdfs/bft-afghanistan-and-iraq-exper.pdf).
57. Robinson (see n.54 above), pp.45–6; Dunn (see n.56 above), p.4.
58. Robinson (see n.54 above), p.46; Dunn (see n.56 above), pp.5–6.
59. Robinson (see n.54 above), pp.46–8.
60. Dunn (see n.56 above), pp.7–12; John W. Charlton, 'Digital Battle Command Baptism by Fire', *Armor*, Vol.112, No.6, 2003, p.28.
61. Bryan D. Brown, 'Statement of General Bryan D. Brown, US Army Commander United States Special Operations Command before the House Armed Services Committee Subcommittee on Terrorism, Unconventional Threats and Capabilities on the Current Manning, Equiping, and Readiness Challenges Facing Special Operations Forces', 2007 (at: www.globalsecurity.org/military/library/congress/2003_hr/brown.pdf).
62. Pamela A. Savage-Knepshield, 'Adaptive Soldiers: Overcoming Obstacles Imposed by New Technology', Proceedings of the Human Factors and Ergonomics Society Annual Meeting, Vol.50, No.23, Orlando, 26–30 Sept. 2006, pp.2514–5; Charlton (see n.60 above), p.29.
63. John Brophy and Preston A. Cooper, 'Joint Blue Force Situational Awareness: Helping Save Warfighter Lives and Improve Operations through Information Integration', *Army Space Journal*, 2005, p.2; Timothy L. Rider, 'Blue Force Tracking to Expand across Force', *Army AL&T*, Sept.–Oct. 2004, p.3.
64. David J. Bryant and David G. Smith, 'Impact of Blue Force Tracking on Combat Identification Judgments', *Human Factors: The Journal of the Human Factors and Ergonomics Society*, Vol.55, No.1, 2013, p.88.
65. Michael M. Sweeney, 'Blue Force Tracking: Building a Joint Capability', DTIC Document, 2008, p.12 (at: http://handle.dtic.mil/100.2/ADA482366).
66. Daniel Gonzales, John Hollywood, Jerry M. Sollinger, James McFadden, John DeJarnette, Sarah Harting and Donald Temple, *Networked Forces in Stability Operations: 101st Airborne Division, 3/2 and 1/25 Stryker Brigades in Northern Iraq*, Santa Monica: Rand Corporation, 2007.
67. Ibid., pp.xvii–xxvi.
68. Ibid., pp.115–20.
69. Ibid., p.119.