New Issues in Peacekeeping

A research project of the International Peace Institute

TRACKING THE BLUE:
Phone and Vehicle Location Systems for UN Peacekeeping

A. Walter Dorn, Canadian Forces College

and

Christoph Semken, Montreal Institute for Genocide and Human Rights Studies

April 2015

EXECUTIVE SUMMARY

Situational awareness is a key to success in UN peacekeeping operations. A basic but as yet unachieved goal for UN missions is to know the exact position of their peacekeepers at any given time. Blue force tracking can help to plan missions, send reinforcements, retrieve wounded peacekeepers, avoid and respond to ambushes, kidnappings and friendly fire, and, ultimately, save lives. This article explains the benefits, drawbacks and challenges of various phone and vehicle tracking systems, surveys available technologies and looks at the political considerations. Fortunately, commercially solutions for real-time vehicle and smartphone tracking have become available at reasonable cost and with increasing accuracy and sophistication, while still being user-friendly. The United Nations can benefit from the advantages of modern blue-force tracking, without having to develop costly, customized solutions. Such an initiative should not encounter any political obstacles.

1 INTRODUCTION

UN peacekeepers risk their lives trying to save others. Many technologies can help the blue helmets protect themselves as well as others, and advance their multidimensional mandates.[1] But the United Nations is traditionally under-equipped, 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. The United Nations has not yet established 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 highly effective and cost-effective. Over the past decade, costs have decreased by a factor of ten while accuracy has increased several-fold. In addition, electronic miniaturization and the “convergence” of formerly disparate technologies means that modern devices often contain location systems along with many other components. For instance, many smartphones contain GPS receivers, signal transmitters, cameras, accelerometers, compasses and gyroscopes, as well as finger-print scanners and sensors.

This paper explains the benefits, drawbacks and challenges of various phone and vehicle tracking systems, analyses the requirements, and surveys available technologies. We show that practical tracking solutions are readily available to enhance both the security and efficiency of UN peacekeepers at very low cost, thanks to the revolution in communications and information technology. These real-time tracking solutions can save lives and alleviate much human suffering.

Fatalities are too common among UN peacekeepers. The number of fatalities for the decade 2004-14 is shown in Figure 1. Since 2010, the number of fatalities due to malicious acts has been rising both absolute and relative to the other causes. The number of UN personnel killed in attacks has risen from 37 in 2012 to 58 in 2013, with the trend continuing.[2] Of the 58 people killed in 2013, half died in ambushes on UN convoys. When peacekeepers are under attack—as in the ambush in Jonglei State, South Sudan, on 9 April 2013 during which five peacekeepers, two UNMISS national staff and five civilian contract employees died[3]—immediate situational awareness, including the position of the convey and nearby forces, is urgently needed. The information can help the United Nations to more quickly reach and rescue beleaguered staff, sending reinforcements more rapidly and assessing the battlefield situation even before arrival. Reinforcements sent in the past—for example, during the attack on a UNAMID convoy in South Darfur on 13 July 2013 that, despite reinforcements, left seven peacekeepers and one police advisor dead[4]—would have benefitted from a detailed map showing the exact positions of vehicles and peacekeepers to aid them faster and more effectively.

The benefits of tracking are not confined to providing effective reinforcements. In the attacks on the UN Common Compound in Mogadishu, Somalia, on 19 June 2013, knowledge of the staff's exact positions by tracking their smartphones could have been used to evacuate the area and retrieve wounded soldiers. Eight UN staff were killed in the attack.[5] Live-tracking can also help commanders who plan and carry out operations, allowing them to optimize their forces in places where they are most needed. In combat situations, "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, they would not have fired upon the Canadians, thereby saving one life and much injury.[6]

Live-tracking can also be used for early warning and prevention by identifying areas that peacekeepers are about to enter and alerting them of potential dangers, based on information stored in a Geographical Information System (GIS). Similarly, tracking can help to counter human smuggling since movements of blue or friendly forces can be distinguished from others.

In other emergencies, such as when peacekeepers are lost or their convoys are held up by locals, tracking can allow rescue teams or reinforcements to find them more rapidly. In some cases, the nearest peacekeepers can be identified and ordered 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 (if their phones are still transmitting). Stolen vehicles can be recovered more easily in order to combat the rise in carjacking incidents. For instance, in Darfur, dozens of carjackings occur each year, targeting vehicles of the mission and agencies of the United Nations and international non-governmental organizations.[7]

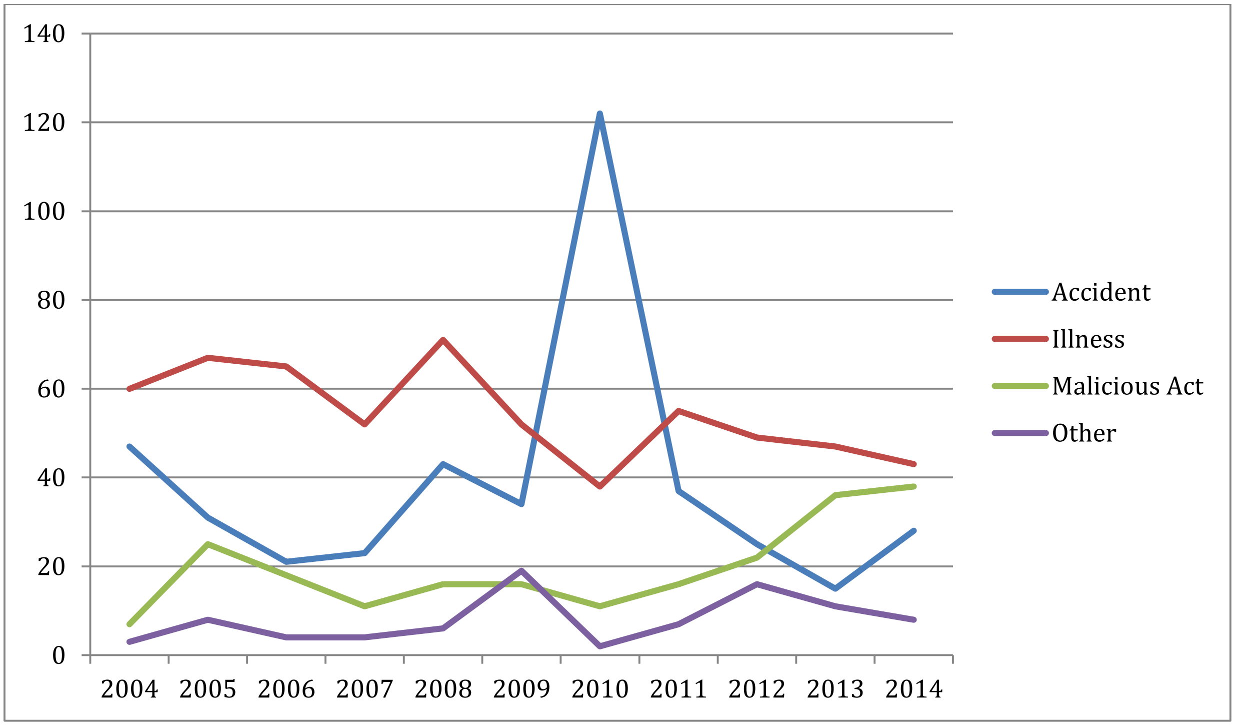

Figure 1: Number of UN peacekeeping fatalities by incident type[8]

Military tracking is often divided into blue, 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 force tracking, including all vehicles and personnel—military, police and civilian—of the UN mission. However, green, red and white force tracking are important too, and are taken into consideration in our discussion of the advantages and disadvantages of developing a customized UN tracking system.

The United Nations has already made some advances in 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 meters) to a receiving antenna, usually at UN facilities. The vehicle's Carlog device uploads a log of the vehicles locations/route since the last upload. It also sends information on distances travelled and driving behaviour. While operating the vehicle, Carlog is used for driver authentication (swipe card used in the Carlog device before ignition), speeding alerts (beeping), and fuel optimisation. 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 in addition to swipe cards). 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 forces are located at any one time, including the present. Carlog provides a historical record and it does not help when a vehicle is missing.[9]

For both safety and effectiveness, the United Nations should employ a modern tracking system for real-time awareness of vehicles and personnel locations. Such systems are used by advanced militaries but is it achievable within the limited resources of the United Nations? Fortunately, recent commercial advances make a UN tracking system entirely realistic, as proposed here. By combining tracking information from two different types of devices, cell phones and vehicles, a cost-effective system can be achieved with valuable redundancies. Vehicles can be located with new off-the-shelf tracking devices in the vehicles. These can offer mission commanders the accurate location of all mission vehicles at any given time on a map. This map 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. This way, all UN vehicles and most peacekeepers could be located at any given time in a flexible and cost-effective manner.

All tracking solutions surveyed by the authors use a similar architecture. Multiple clients, vehicles and/or smartphones, send their location updates to a server with GIS software. The system is designed to capture, store, illustrate, analyse, manage, and present the location data as a layer on top of various geographic data. The layers can include roads and route maps or more sophisticated ones showing the topology, satellite imagery, locations of local buildings and shops, friendly forces, humanitarian organisations, industries, or the possible presence of hostile elements, when such information is available. In commercially available solutions, the GIS is usually owned and operated by the company providing the solution—a business model called Software-as-a-Service (SaaS).

Different technologies can be used to locate tracking devices and then transmit the data to the centralized GIS. Most tracking devices use a Global Navigation Satellite System (GNSS), most often the Global Positioning System (GPS), to determine their position. It typically comes in the form of network-Assisted GPS (AGPS), which uses the mobile network to increase precision. When no GPS signal is available on the smartphone or vehicle, most devices use Cell Global Identity (CGI), provided by the mobile network, as a fallback technology. But because mobile network cells can be very large (up to 70km in diameter), other technologies are, again, used to get a more accurate position. These include Cell Global Identity with Timing Advance (CGI+TA), Uplink Time of Arrival (TOA), Angle of Arrival (AOA), and Observed Time Difference (OTD). Additionally, non-mobile network-based methods such as infrared/RFID, Ultra-WideBand, Smart Space Platform, Wi-Fi, Bluetooth, and sensor networks can also be used to determine a device's location.[10]

GNSS-based	Mobile network-based	Other
GPS	CGI	Wi-Fi
AGPS	CGI+TA	*Ultra-WideBand**
GLONASS†	TOA	*Smart Space Platform**
*Galileo**	AOA	*RFID**
	OTD	*Bluetooth**
		*Sensor-network**

Table 1: Enabling technologies for location-dependent querying based on Ilarri et al.[11]
*** Not widely used in smartphones or vehicle tracking devices**
† Not widely used in smartphones or vehicle tracking devices outside of Central Asia

2 MOBILE NETWORK AVAILABILITY

Some communications systems have built in tracking, as usually found in TETRA radios, so the information is communicated as part of the radio signal. But most tracking solutions utilise mobile phone networks to transmit the data to the central system. Such mobile networks are now cheap and widely available in both high- and low-income countries. The progress in the latter has been encouraging. For instance, in the developing world, the number of phone subscriptions per 100 inhabitants has grown to 90 in 2014 from only 10 in 2001. But because UN peacekeeping is often done in far-away regions where mobile networks have not yet reached, other technological solutions need to be explored.

The Global System for Mobile Communications (GSM, originally *Groupe Spécial Mobile*) is generally available and the primary standard for mobile communications in all fifteen countries where peacekeeping missions presently operate. Table 2 shows the coverage of GSM networks in six countries that host selected UN peacekeeping operations. In none of these countries did GSM cover the entire area as of 2009, as shown in the third column of the table. Another measure, with higher figures, is the percentage of the population with access to GSM shown in the last column of Table 2.

Country	UN Mission	GSM Coverage, % of Area	GSM Coverage, % of Population
C.A.R.	MINUSCA	N/A	21%
Côte d'Ivoire	UNOCI	22%	60%
D.R. of the Congo	MONUSCO	20%	53%
Haiti	MINUSTAH	68%	78%
South Sudan	UNMISS	N/A	N/A
Sudan (Darfur)	UNAMID	4%	43%
Average	Six missions	29%	51%
Average	All 14 missions	36%	58%

Table 2: GSM coverage in selected countries with UN peacekeeping missions[12]

Generally, GSM coverage is comparatively low in countries with peacekeeping operations: for all missions, the coverage averages at around 36% of the countries' area and 58% of the countries' population. Furthermore, in some missions, peacekeepers tend to patrol in remote parts of the country where there is less coverage. In Mali, GSM networks covered only 1% of the area but 19% of the population, given the heavy concentration in the south-west part of the country and the sparse desert areas of the north. The peacekeeping mission must, however, operate in the north where the rebel forces are based. In short, network coverage tends to be comparatively low for conflict regions. But the Table 2 data was compiled in 2009 and coverage has increased significantly. Since 2009, mobile-cellular subscriptions jumped from 58 to 90 per 100 inhabitants in the developing world.

In sum, GSM is not a reliable technology for *all* countries and regions hosting UN peacekeeping missions. With the exception of a few countries, such as Lebanon and Haiti, mobile network coverage is not complete and connectivity can easily be lost due to the lack of reliable networks. The United Nations has to consider each country individually and use complementing technologies in some missions. To this end, satellite communication modules can be added to most tracking devices. They are a more costly but readily available alternative, as we discuss below once the full set of technical requirements are covered.

3 TECHNICAL REQUIREMENTS AND POLICY RECOMMENDATIONS

Five main issues need to be considered for vehicle and smartphone tracking solutions in UN operations: reliability; update frequency; data privacy/encryption; personal privacy; and cost. Because of the challenges and potential vulnerabilities, these issues are worth considering in detail.

3.1 Reliability

Reliable tracking solutions are needed, especially when human lives are in danger. For this, all parts of the system have to be reliable.

As mentioned, most tracking solutions use GPS, a GNSS operated and maintained by the U.S. Air Force. The space segment of the GPS is very reliable. To be able 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.[13] The reliability of the space segment notwithstanding, the GPS system is still vulnerable to control and ground-receiver issues. In 2010, a software problem "rendered as many as 10,000 U.S. military GPS receivers useless for days."[14] Other events could result in a blackout, such as solar storms, volcanic eruptions, intentional destruction of satellites, technological problems, technological aging, collision of satellites in earth orbit, intentional and unintentional interferences, military conflicts and financing issues.[15] Since the US government has full control over GPS it could potentially decide to partially or fully prohibit usage to gain a military advantage or to save money. Although "selective availability," with its reduced accuracy, is currently turned off and economic interests make a return to this US practice unlikely, the US government in 2004 stated that the "the president could decide to disable parts of the network for national security purposes."[16] This deactivation is politically very unlikely though it is still technically possible, at least until the expected launch of new GPS satellites in 2017.[17]

Despite the risks, there is currently no feasible GNSS alternative to GPS. The Russian GLONASS system is only optimised within Russian boarders due to its low number of satellites;[18] and the deployment of the European GALILEO and the Chinese BeiDou systems will not be completed until 2019 and 2020, respectively.[19] Moreover, the above-mentioned issues are likely to affect all GNSS in much the same way.

To transmit location updates to a centralized GIS, most commercially available systems rely on mobile communications networks. As mentioned, GSM is the mobile network technology that would likely be used in the countries hosting a peacekeeping mission. Our study on network availability (above) shows that GSM networks are not a reliable option for all areas. Additionally, governments in political crises could shut down mobile networks and/or internet accessibility. For instance, this happened at least twice in the Syrian Arab Republic during its ongoing civil war.[20] While a smartphone tracking solution, at present, will have to rely on mobile networks, satellite-based devices can be used for vehicle tracking in countries with low or no GSM reliability. The devices send signals directly to satellites. They are more expensive but positional coordinates do not take up much data (typically less than 100 Bytes per transmission) and costs can be controlled by sending the coordinates less frequently (e.g., once every minute instead of every few seconds). The United Nations should utilize tracking solutions that incorporate satellite communications.

A further imminent risk to both GNSS and mobile network availability is the intentional jamming of signals by hostile forces. Both GSM and GPS signals can be jammed effectively.[21] How to mitigate the risks associated with electronic warfare is beyond the scope of this paper. In any case, deliberate jamming of GPS signals and mobile systems is rare and the spoilers sometimes found in UN mission areas would be unlikely to use such techniques.

In addition to the GNSS and the mobile network, the GIS must also be reliable. Without redundancies, the GIS can constitute a single point of failure. The tracking system could be rendered ineffective if the server is comprised. A number of different threats to this part of the system exist. First, denial of service attacks might make the server inaccessible. Second, viruses, worms, cross site scripting, and social engineering could be used to steal and manipulate data and/or shut down the system. Third, pharming and other man-in-the-middle attacks could be used to view and to alter the map.[22] However, there are measures that can be taken to prevent and mitigate such calamities.

As discussed in more detail below, encryption as well as uptime and security guarantees ensure data privacy and reliability for the GIS. Additionally, the United Nations itself has to ensure that systems for GIS access are secure. This requires the necessary software and adequate training for UN officials, about which the organization has already shown a basic level of competence.

Finally, 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, e.g., layers showing the security concerns or any other relevant factors. We consider a number of such desirable features below in our survey of commercially available solutions.

3.2 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, 800 m under BFT1).[23] For vehicles driving at 100km/h, location updates need to be sent with a frequency of up to one minute to achieve an accuracy of 800 m or five seconds for an accuracy of 100 m.

For cost-efficiency, the location updates can be minimal. Of the six countries with current peacekeeping operations studied above (CAR, DRC, Côte d'Ivoire, Haiti, South Sudan, and Sudan), only two (Haiti and Sudan) have significant 3G networks. Thus, most mobile network data connections will occur through the slower GPRS standard. Because of the small amounts of data that need to be sent for a location update (less than 100 Bytes), a GPRS connection with more than one kilobit per second already allows for updates to be transmitted within seconds. Usually, GSM-powered tracking devices use text messages as a fallback technology for location transmission.

3.3 Data privacy & encryption

Data privacy is vital for any UN tracking solution in a conflict zone. Leaked data could aid hostile forces in locating UN troops or persons. Even outdated or incomplete geolocation data could be used to analyse UN patrol patterns and operation procedures. Over 200 threats to a GSM/UMTS-network communication have been identified in the literature.[24] Data privacy needs to be ensured throughout the entire communication process, including the mobile tracking devices, mobile network, internet communication and the local network. For clarity, we will look at these four stages separately.

First, the mobile device needs to be secure. This is especially critical for phone tracking. Modern smartphones running operating systems such as Apple's iOS, Google's Android or Microsoft Windows are vulnerable to a variety of threats. Devices can be compromised by malware, wireless network attacks, denial of service, break-ins, malfunction, phishing, loss, or platform alteration.[25] A compromised device could be used to either send incomplete or wrong information to the server and/or to perform red force tracking, for example, by an opponent, a peace accord violator or by an international criminal network. However, phone system modifications, add-ons and applications, such as anti-viruses, can be used to protect smartphones against some of these threats. Most importantly, the user needs to be aware of the threats and countermeasures.[26] Therefore, the United Nations needs to train peacekeepers on smartphone security.

Second, since GSM and 3G networks are used for 95% of global calls and by all operators in the selected peacekeeping operations studied above,[27] their vulnerability is of concern. Older GSM networks can be hacked through active attacks with equipment costing less than

$1,500.[28] Passive attacks on GSM networks, in which the hacker merely eavesdrops the communication, can be achieved even without the use of expensive equipment since the release of some of the encryption keys on the internet.[29] Moreover, the Signaling System 7, used to communicate between different mobile networks, is vulnerable to eavesdropping, which is why neither GSM nor 3G networks can be considered secure.[30]

Third, much like the mobile network, the *internet* can be used for various types of man-in-the-middle attacks. For example, hostile forces could have access to a server through which the location update is being routed. The communication could then be eavesdropped and/or modified. Fortunately, both mobile network and internet communication privacy issues can be addressed by providing end-to-end encryption so intercepted communications cannot be read. The United Nations should use tracking solutions that provide end-to-end encryption.

Fourth, data can be stolen from the *tracking server* or the *local network*. Access to the tracking server needs to be limited to relevant personal. Additionally, the company running the server has to enforce encrypted communications, encrypted data storage, and up-to-date systems, especially when hacking is known to occur. This is a standard commercial function for which many solutions are available.

3.4 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 for most missions. However, supplementing vehicle tracking with smartphone tracking means that supervisors would be able to track peacekeepers at any time.

Location tracking can be an issue between the employer and employee (or officer and soldier) because the former can track the latter without their knowledge, 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 has been used to fire government employees.[31] Two types of safeguards can ensure the protection of individuals from an abuse of the tracking data: privacy policies and laws/regulations.

In the field, the UN missions reserve the right to know the location of their staff at all times, particularly during dangerous times or in dangerous places. However, the authors are unaware that the United Nations has any privacy policies in place. None of the "policy and guidance" documents published by the DPKO and the DFS set out privacy guidelines. Moreover, the UN Staff Regulations do not mention privacy or data handling.[32] In the absence of UN privacy standards, it should at least be ensured 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. For example, when employees are on leave (vacation) and out of the mission area, their device locators could 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 this with regards to the use of new technologies. Although none of the studied countries restrict the usage of positioning system for tracking purposes, the United Nations needs to ensure compliance with the law prior to implementing a tracking system.

3.5 Cost

The United Nations cannot afford the expensive, customised technology that some advanced national armies use because the world organization operates on a relatively constrained budget. Fortunately, for tracking there are many inexpensive, commercial solutions available. Previously, the United Nations deployed the Carlog system in its peacekeeping operations. For instance, in 2006, MONUC bought 336 Carlog devices for $173,100, or $515 per device.[33] This amount was used as a baseline value for our study of available products. The Carlog system is not able to give real time awareness, so an upgrade is needed or new options have to be explored. This paper shows there are quite inexpensive options.

In addition to the procurement costs for the devices, the United Nations will need to pay for the data connections. In the DRC and Haiti monthly mobile network data subscriptions with large data allowances (3-7 GB) are available for about $7 and $22 per phone, respectively. Except for the CAR and South Sudan, we also found data options for all other countries considered above, ranging from $0.06 to $2.07 per MB. In the absence of a deal with a local provider, tracking one vehicle every five seconds for twelve hours would cost the United Nations under $2 per unit, even with the most expensive mobile data provider. Satellite communication can be much more costly but they are almost always offered directly by companies with tracking solutions.

Commercially available products are generally much cheaper than military systems but, thanks to the commercial technology revolution, they offer many of the same features. Basic devices 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. Such devices 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. Server licences are sometimes included in the price (for devices over $1,000) or otherwise they range from $15 to $35 a month. The transmission costs of tracking devices with satellite modems are often included in either the server license or the price of the device. Where the number of satellite messages is limited, additional location updates from one provider are $0.0025 each. An hour of vehicle tracking (with an update once a minute via satellite communication) would thus cost only $0.15. The server licenses for smartphones, which would only use cellular networks, are typically lower than for vehicle tracking devices and range from $5 to $25.[34]

4 SURVEY OF TRACKING SOLUTIONS

Tracking peacekeepers can be affordable and can be done through cell phone tracking, vehicle tracking or hybrid systems. The following gives a sense of the types of products currently available, with or without satellite communications.

4.1 Cell Phone tracking

At present, hundreds of tracking applications ("apps") are available for smartphones, some for free, as illustrated in Table 3. Tracking apps typically use the phone's GPS receiver and the Cell Global Identity to send updates to a centralised server. Most commonly, consumer apps are being used for personal reasons such as parental control, tracking of partners and friends, and locating lost devices.

App	Primary purpose	Number of downloads[35]	Platforms	Additional features	Costs[36]
Glympse	Instant location sharing	5,000,000	Android, Apple, Windows Phone	No sign-up required	Free
Find My Phone	Locate lost devices	13,000,000	Android		Free-$4.99/month
Family Locator	Location sharing, parental control, lost device	14,000,000	Android, Apple, Windows Phone	Location alerts, messaging	Free-$5/month
Find My Friends	Location sharing, parental control	2,500,000	Apple	Location alerts	Free
iSharing	Location sharing, parental control	617,000	Android, Apple	Voice messaging, location & panic alerts	Free-$3.99/month

Table 3: Free tracking apps

Similar solutions are 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 so they can be sent to the next job more efficiently.

4.2 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; an estimated 200 software products are available to that end.[37]

In military operations, different systems can be used to achieve secure and reliable vehicle tracking. The Carlog system, currently used by the United Nations and already described above at the basic level, provides a secure offline tracking method. The devices are permanently attached to the vehicle dashboard and allow for driver authentication, route reporting and driving behaviour. 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), strong encryption mechanisms and fail-safe networks. Unlike GSM phones, TETRA radios can share channels directly in the absence of a mobile cell network. The standard is used in many public safety operations, including some UN peacekeeping missions. Many modern TETRA ratios include GPS receivers, allowing the operator of a TETRA network to locate and track the radios. Some of the available TETRA tracking applications are Motorola’s *MOTOLocator*, Airbus’ *Imp@ct* and Sepura’s *SICS-NET Visualise*.[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.

4.3 Hybrid systems

Most commercially available fleet management systems now allow for hybrid solutions in which both vehicle and smartphones can be tracked. The company typically provides the tracking devices, GIS and smartphone apps under one system. Only a few companies support devices made by other vendors.[41] 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.

Encryption is available for many commercial tracking solutions. The encryption between tracking devices, including smartphones, and the server depends on the protocol used. Encryption can be provided through either 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 server and the client cannot be eavesdropped. Additionally, Service-Level Agreements (SLAs) can be used for both uptime and security guarantees. The *standard* SLA of one company guarantees an uptime of 99.99% and includes penalties against the company in case of outages.[42]

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 US and Europe,[43] some companies have experience in or near conflict regions. Geothentic, for example, has customers in Mali, and Mix Telematics is based in South Africa and operates another data center in the Middle East.[44] Some products allow the grouping of vehicles and persons to create a command and control hierarchy.[45] 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").

5 DEVELOPING A CUSTOMIZED SYSTEM?

Aside from purchasing products currently available on the market, the United Nations could develop its own tracking solution. Many national military forces have developed their own systems for tracking vehicles and personnel.

The advantages of a customized and fully integrated system, developed for the specific needs of the United Nations would be numerous. First, all available geospatial data could be shown in one map, not just the information obtained from tracking devices. An integrated solution could also display aircraft, intelligence findings, and other force tracking; leading to an even more effective and efficient command and control. Second, more advanced technology could be used that allows for precise, 3-dimensional location tracking. As a result, tracking could help protect peacekeepers lives in urban warfare, building-clearance operations and underground/cave operations.[46] Third, physiological monitoring could be added to allow mission control to check peacekeepers status, including camera imagery or data from sensors worn by the peacekeepers themselves. With the rise of wearable technology an expanding range of sensors can feed into the system, including sensors relating to health. Fourth, automatic data exchanges with other UN agencies and friendly forces could be used for white force tracking. This would reduce the risk of friendly fire and allow peacekeepers to rescue civilian workers more efficiently. Lastly, a UN-specific product would be independent from the product lines of a specific company. Modifications could be made in a timely manner to reflect changes in operational procedures or the overall security situation.

Developing a new and independent tracking solution does have potential disadvantages. First, the software needs to be constantly maintained. A team of developers would have to provide security and general updates. Second, the United Nations would have to ensure the security and reliability of more systems. Developing a new system with limited resources would mean having to compromise on security. Finally and most importantly, developing a new solution would be more costly. The commercial-off-the-shelf solutions studied above benefit from economies of scale, resulting in small prices for server licenses. Developing a customized UN tracking solution, on the other hand, would likely cost tens of millions of dollars. By way of comparison, the United States spends approximately $20,000 per vehicle on its Force XXI Battle Command Brigade and Below (FBCB2) blue force tracking and Future Combat Systems (FCS).[47] Orders from one contract for encryption devices, software, maintenance and customer support for the FBCB2 system alone exceed $100 million.[48] Similarly, the contract value for the NATO GPS Force Tracking System amounts to approximately $84 million.[49] 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 the UN GIS cells.

6 POLITICAL CONSIDERATIONS

As shown, the technological obstacles to a new UN tracking solution can be easily overcome. Both security and reliability concerns could be addressed if the United Nations decides to opt for real-time vehicle and phone tracking. After having ensured the 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, are there any political obstacles?

The United Nations would have to ensure that a new tracking solution is worth the cost and effort. We have shown that the costs for real-time vehicle tracking devices are comparable to what the United Nations has previously spent on offline tracking, and that smartphones can be added cheaply. The UNAMID example of at least 37 carjacking incidents in 2014 shows a direct economic benefit—recovering stolen vehicles. But more importantly, real-time tracking can save peacekeepers lives in cases of ambushing, kidnapping, friendly fire, to retrieve wounded soldiers or send reinforcements, and because of an overall better command and control structure.

Troop contributing countries are unlikely to resist an improved UN tracking system too, given that it offers greater security for their peacekeepers in the field. Some extra training might be necessary but it would be minimal and should be welcome as giving additional skills to national forces; a half-a-day seminar might be needed. Some contingents may be concerned that a UN tracking system would be able to show if they have not been completing their patrols or reacting as requested but that information is mostly available through Carlog already.

The host state should have no objections to a better tracked UN mission. It could even help the UN respond to state queries over the positions of peacekeepers. Some states may not want UN peacekeepers to go into certain areas (e.g., near military bases) and tracking can help the United Nations to avoid such areas. Tracking is a communications technology and "unrestricted communications" are a right under the model Status of Forces Agreement that the UN uses as a basis for agreements with host countries.[50] Furthermore, having data centres in multiple countries and supporting both mobile networks and satellites can mitigate connectivity problems in, or disagreements with, host countries. In any case, it is hard for a host country to complain that the United Nations knows the location of its peacekeepers: the country's sovereignty will not be affected.

Countries that are the major contributors to the peacekeeping budget are also unlikely to resist the step to 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 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.[51] 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 process. The UN's 2009 New Horizon non-paper states: "The UN … needs access to new technologies for better situational awareness in the field."[52] The Departments of Peacekeeping Operations and Field Support (DPKO/DFS) have accepted the 2015 report of the Expert Panel on Technology and Innovation in Peacekeeping. The report stated: "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."[53] Of the many technologies advocated in the Expert Report, tracking would be one of the "quickest wins."

7 CONCLUSION

Fortunately for the United Nations, the basic requirements for a UN tracking system can be fulfilled by many off-the-shelf commercial products. Most companies offer agreements guaranteeing the reliability of their system, whether purchased by the United Nations or operated for the United Nations by the companies. For areas with poor GSM coverage, satellite tracking devices can be used. Many products offer important features, such as encrypted updates, panic buttons, flexible update frequencies, driver authentication, fuel management, speeding alerts, and more. Smartphone apps allow for the tracking of individual peacekeepers to add to vehicle tracking information. Maps and GIS can be edited on a basic level to display UN compounds, mission boundaries, and relevant objects. More sophisticated GIS can show both human and geographical terrain.

An independently developed solution could have certain advantages over readily available products: aggregation of all intelligence findings; white force tracking; use in indoor and underground operations; and inclusion of health information. The costs of such a solution, however, probably exceed the UN's budgetary restrictions.

Affordable tracking solutions exist and they will benefit UN peacekeeping operations in many ways. Cost-efficient tracking of vehicles and peacekeepers ensures personal security, command efficiency 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—Meagan Boissé, Neeko Collett, Ecem Oksay, and Marie Lamensch— and the International Peace Institute—Adam Smith and Michael Snyder.

[1] See: A. Walter Dorn, *Keeping Watch: Monitoring, Technology and Innovation in UN Peace Operations* (New York: United Nations University Press, 2011). United Nations, Expert Panel on Technology and Innovation in UN Peacekeeping, *Performance Peacekeeping: Final Report of the Expert Panel on Technology and Innovation in UN Peacekeeping*, 19 February 2015, http://www.performancepeacekeeping.org/offline/download.pdf.

[2] United Nations, Secretariat, *Increase in Deadly Attacks against the United Nations Claimed More than 58 Lives in 2013, Staff Union Says*, Press Release (New York: United Nations, 8 January 2014), http://www.un.org/press/en/2014/org1576.doc.htm. Malicious acts against peacekeepers (but not all UN staff) up to 30 November 2014 already exceeded those of 2013, see United Nations, DPKO, 'Fatalities by Year and Incident Type', 30 November 2014, http://www.un.org/en/peacekeeping/fatalities/documents/stats_5.pdf. See also Figure 1.

[3] United Nations, Secretariat, *Increase in Deadly Attacks against the United Nations Claimed More than 58 Lives in 2013, Staff Union Says*.

[4] Ibid.

[5] Ibid.

[6] David Pugliese et al., 'Canadian Commandos Gunned down despite Prearranged Code Words', *Ottawa Citizen*, accessed 9 March 2015, http://ottawacitizen.com/news/national/canadian-soldier-dies-in-friendly-fire-incident-in-iraq-dnd-says.

[7] Between 1 January and 15 November 2014, the number of carjacking incidents was 37, compared to 27 in 2013 and 22 in 2012. United Nations, General Assembly, *Report of the Secretary-General on the African Union-United Nations Hybrid Operation in Darfur*, 26 November 2014, http://undocs.org/S/2014/852. 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.

[8] United Nations, DPKO, 'Fatalities by Year and Incident Type'.

[9] Dorn, *Keeping Watch*, 49–50.

[10] Sergio Ilarri, Eduardo Mena, and Arantza Illarramendi, 'Location-Dependent Query Processing: Where We Are and Where We Are Heading', *ACM Comput. Surv.* 42, no. 3 (March 2010): 12:1–12:73, doi:10.1145/1670679.1670682.

[11] Ibid.

[12] GSM Association, 'GSM Coverage', *Mobile for Development Impact*, 2009, https://mobiledevelopmentintelligence.com/statistics/66-gsm-coverage-area.

[13] Analytical Graphics, Inc., 'GPS Satellite Outage Information', *AGI Developer Network*, 20 December 2014, http://adn.agi.com/SatelliteOutageCalendar/SOFCalendar.aspx.

[14] Dan Elliott, 'Air Force GPS Problem: Glitch Shows How Much U.S. Military Relies On GPS', *Huffington Post*, 6 January 2010, http://www.huffingtonpost.com/2010/06/01/air-force-gps-problem-gli_n_595727.html.

[15] Miikka Ohisalo et al., ‘Risks and Vulnerabilities of Future Satellite-Based Tracking Systems’, *International Journal of Geology* 5, no. 4 (2011): 142–49.

[16] CNN, ‘Bush Plans for Shutdown of GPS Network during Crisis’, 18 December 2004, http://web.archive.org/web/20041218020813/http://edition.cnn.com/2004/TECH/12/16/positioning.satellites.ap/index.html.

[17] US government, ‘Selective Availability’, *GPS.gov*, accessed 8 March 2015, http://www.gps.gov/systems/gps/modernization/sa/; Mike Gruss, ‘Launch of First GPS 3 Satellite Now Not Expected Until 2017’, *Space News*, accessed 8 March 2015, http://spacenews.com/launch-of-first-gps-3-satellite-now-not-expected-until-2017/.

[18] Pasi Kämppi, Jyri Rajamäki, and Robert Guinness, ‘Information Security Risks for Satellite Tracking’, *International Journal of Communications*, no. 1 (2009): 9–16.

[19] Chinese Government, ‘BeiDou Navigation Satellite System — System Introduction’, 14 December 2012, http://www.beidou.gov.cn/2012/12/14/2012121481ba700d7ca84dfc9ab2ab9ff33d2772.html; European Commission, ‘Galileo: Satellite Launches’, 2012, http://ec.europa.eu/enterprise/policies/satnav/galileo/satellite-launches/index_en.htm.

[20] BBC News, ‘Syrian Internet Back after Blackout’, 8 May 2013, http://www.bbc.co.uk/news/world-middle-east-22447247; Iain Thomson, ‘Syria Cuts off Internet and Mobile Communications’, *The Register*, 29 November 2012, http://www.theregister.co.uk/2012/11/29/syria_internet_blackout/.

[21] Hui Hu and Na Wei, ‘A Study of GPS Jamming and Anti-Jamming’, in *2009 2nd International Conference on Power Electronics and Intelligent Transportation System (PEITS)*, vol. 1, 2009, 388–91, doi:10.1109/PEITS.2009.5406988; M. Petracca et al., ‘Performance Evaluation of GSM Robustness against Smart Jamming Attacks’, in *2012 5th International Symposium on Communications Control and Signal Processing (ISCCSP)*, 2012, 1–6, doi:10.1109/ISCCSP.2012.6217797; J. Rantakokko et al., ‘User Requirements for Localization and Tracking Technology: A Survey of Mission-Specific Needs and Constraints’, in *2010 International Conference on Indoor Positioning and Indoor Navigation (IPIN)*, 2010, 1–9, doi:10.1109/IPIN.2010.5646765.

[22] Kämppi, Rajamäki, and Guinness, ‘Information Security Risks for Satellite Tracking’.

[23] ViaSat Inc, ‘Faster, More Effective Situational Awareness from the New U.S. Army FBCB2’, *Youtube*, 16 July 2012, https://www.youtube.com/watch?v=XDdZGiy8Luw.

[24] Daniel Fischer et al., ‘A Survey of Threats and Security Measures for Data Transmission over GSM/UMTS Networks’, in *2012 International Conference for Internet Technology And Secured Transactions*, 2012, 477–82.

[25] Woongryul Jeon et al., ‘A Practical Analysis of Smartphone Security’, in *Human Interface and the Management of Information. Interacting with Information*, ed. Michael J. Smith and Gavriel Salvendy, Lecture Notes in Computer Science 6771 (Springer Berlin Heidelberg, 2011), 311–20.

[26] Giles Hogben and Marnix Dekker, *Smartphones: Information Security Risks, Opportunities and Recommendations for Users*, Report/Study (European Union Agency for Network and Information Security, 10 December 2010), http://www.enisa.europa.eu/activities/identity-and-trust/risks-and-data-breaches/smartphones-information-security-risks-opportunities-and-recommendations-for-users.

[27] Cellcrypt, *Cellcrypt Voice Security Brief*, May 2013, http://www.cellcrypt.com/sites/default/files/users/Cellcrypt%20Voice%20Security%20Brief%20FINAL%20LE%20V5%20010513.pdf.

[28] Bill Ray, ‘Hacking into GSM for Only $1500’, *The Register*, 2 August 2010, http://www.theregister.co.uk/2010/08/02/gsm_cracking/.

[29] The attacker only needs a laptop, a programmable radio receiver, and pre-computed A5/1 keys which are freely available on the internet.

[30] Craig Timberg, ‘German Researchers Discover a Flaw That Could Let Anyone Listen to Your Cell Calls.’, *The Washington Post*, 18 December 2014, http://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/.

[31] M. G. Michael, Sarah Jean Fusco, and Katina Michael, 'A Research Note on Ethics in the Emerging Age of Überveillance', *Computer Communications*, Advanced Location-Based Services, 31, no. 6 (18 April 2008): 1192–99, doi:10.1016/j.comcom.2008.01.023.

[32] United Nations, Secretariat, *Staff Regulations* (New York, 2008), http://www.peacekeepingbestpractices.unlb.org/PBPS/Library/N0832434.Staff%20Regulations.pdf.

[33] MONUC, '2006-7 Acquisition Plan - United Nations Mission in the Democratic Republic of Congo', 27 September 2006, http://web.archive.org/web/20060927081538/http://www.un.org/Depts/ptd/2007_monuc.htm.

[34] Catherine Lewis (Executive Vice President of Mix Telematics), interview by Christoph Semken, 28 July 2014; Philippe Bisson (Business Development Director at Geothentic), interview by Christoph Semken, 22 July 2014; Jason Koch (President and Manager of Telogis Fleet at Telogis), interview by Christoph Semken, 24 July 2014; Ron Konezny (Vice President for Transportation & Logistics at Trimble Navigation Limited), interview by Christoph Semken, 21 July 2014.

[35] Estimated as of 17 December 2014, source: Xyo.net

[36] As of 17 December 2014

[37] As of 04 July 2014, Capterra was listing 274 fleet management software products at http://www.capterra.com/fleet-management-software/; C.J. Driscoll and Associates has published a 241-page report called the "2013 Fleet Operator's Guide to GPS Fleet Management Systems" which covers company background, key contacts, target markets, core features, distribution, installed base, key customers, and available hardware and service pricing information for 120 Mobile Resource Management (MRM).

[38] Dorn, *Keeping Watch*.

[39] Webpages for these technologies can be found at: http://www.motorolasolutions.com/XU-EN/Product+Lines/Dimetra+TETRA/TETRA+Applications/Motorola+TETRA+Applications/MOTOLocator; http://www.defenceandsecurity-airbusds.com/fi/web/guest/c4isr-solutions; http://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, http://www.psni.police.uk/costs_radio_equip.pdf.

[41] Jason Koch (President and Manager of Telogis Fleet at Telogis), interview.

[42] Catherine Lewis (Executive Vice President of Mix Telematics), interview.

[43] Clem Driscoll (C.J. Driscoll & Associates), interview by Christoph Semken, 10 July 2014.

[44] Philippe Bisson (Business Development Director at Geothentic), interview; Catherine Lewis (Executive Vice President of Mix Telematics), interview.

[45] Jason Koch (President and Manager of Telogis Fleet at Telogis), interview.

[46] Rantakokko et al., 'User Requirements for Localization and Tracking Technology'.

[47] Army Times, 'Army Integrating FCS, Blue-Force Tracking', 10 August 2008, http://archive.armytimes.com/article/20080810/NEWS/808100314/Army-integrating-FCS-blue-force-tracking.

[48] Harris Corporation, 'Harris Corporation Receives New Orders to Deliver Programmable Encryption Devices to U.S. Department of Defense Blue Force Tracking Network', 22 June 2011, http://harris.com/view_pressrelease.asp?pr_id=3257.

[49] Globecomm, 'NATO GPS Based Forced Tracking System', 27 May 2014, http://www.globecommsystems.com/in-the-news/press-releases/press-release-5-27-contract-extension-nato.shtml.

[50] United Nations, General Assembly, *Model Status-of-Forces Agreement for Peace-Keeping Operations: Report of the Secretary-General* (New York, 9 October 1990), http://undocs.org/A/45/594.

[51] United Nations, Procurement Division, 'Request for Expression of Interest: Provision of Fleet Management and Vehicle Tracking Systems for DFS', 13 January 2015, http://www.un.org/depts/ptd/pdf/eoi10644.pdf.
[52] United Nations, DPKO and DFS, 'A New Partnership Agenda: Charting a New Horizon for UN Peacekeeping', 2009, 32, http://www.un.org/en/peacekeeping/documents/newhorizon.pdf.
[53] United Nations, Expert Panel on Technology and Innovation in UN Peacekeeping, *Performance Peacekeeping: Final Report of the Expert Panel on Technology and Innovation in UN Peacekeeping*, 19 February 2015, 27–28, http://www.performancepeacekeeping.org/offline/download.pdf.