9

Challenges and problems

To deploy effective and appropriate monitoring technologies to the field, a range of issues and obstacles must be considered, including operational, technical, legal, political, institutional/cultural and financial challenges. Examining the desired characteristics and the practical problems helps identify potential pitfalls and promote potential solutions.

Operational

First and foremost, technologies must be operationally *useful*. They must provide increased situational awareness in important locations and of significant activities. They must not be purchased simply because they are appealing in an abstract sense. Hardware development in some nations is driven by a “technological imperative” – simply because it *can* be done. The United Nations cannot afford to adopt unproven technologies. As shown in previous sections, even the United Nations’ limited technological experience demonstrates the utility of many monitoring technologies such as night-vision goggles for night patrolling, aerial cameras to spot advancing threats, satellite imagery for mapping, and tracking systems to monitor UN vehicles.

Fortunately, technology is, in general, becoming increasingly *user friendly*, especially through the use of on-screen icons and menu-driven interfaces. But even user-friendly devices require testing and practice runs to

Keeping watch: Monitoring, technology and innovation in UN peace operations, Dorn, United Nations University Press, 2011, ISBN 978-92-808-1198-8

overcome potential problems. For example, depth perception can be a problem with night-vision equipment but to trained users these problems are manageable.[1]

To be *practical*, technologies must be reliable, accurate and easy to operate by the UN mission, if not plug-and-play. The modern experience with some technologies in UN and other operations – for example, those of the North Atlantic Treaty Organization (NATO) – has also shown that this is achievable, though special expertise is often required. For instance, expert analysts may be needed to recognize target signatures and to discard artefacts in imagery, especially with techniques such as synthetic aperture radar. Technical expertise may also be needed to calibrate equipment and adjust threshold levels, for example, to separate background "noise" from actual "signals" (the classic "signal to noise" problem). To accommodate the extra data from sensors, the United Nations would also need to increase the bandwidth, speed and reliability of its electronic transmission channels (for example, information technology networks).

In harsh peacekeeping environments, for example in hot climates or under rough handling, devices need to be *robust and durable*. Most military equipment is ruggedized to allow for difficult conditions, even combat. Ruggedization may increase the cost of the equipment, but not necessarily by a large factor.[2]

Terrain type and sensor range are key factors in technology selection.[3] In flat areas where the line of sight is long, such as in deserts, open fields and bodies of water (lakes, rivers and oceans), long-range sensors are best. These technologies include radar, high-zoom cameras (still and video) and laser range-finders, preferably on elevated towers or aerial platforms. Conversely, in terrain typified by a short line of sight and many obstacles – as found in jungles, rapidly undulating areas and built-up urban regions – numerous short-range sensors, spaced at regular intervals, might be needed to cover the area. Short-range devices typically include seismic, acoustic, magnetic and infrared break-beam sensors.

Weather conditions also play a role in the choice of sensors. Like human eyes, cameras operating in the visible part of the electromagnetic spectrum can become virtually useless in heavy fog or rain. Other devices, such as radar, are much less susceptible. For night vision, image intensifiers work better when there is more ambient light, for instance from a full moon on a cloudless night. Infrared devices give the clearest signals in cold weather when there is a greater temperature difference between the targets (warm bodies) and the background. Acoustic sensors sometimes have difficulty distinguishing target sounds (for example, rifle fire) from noise caused by thunder, rain or even wind, although automated acoustic analysis can supplement the human ear to identify the types, locations and sources of particular sounds.

The challenge is to achieve technological proficiency among a wide range of peacekeepers. Military, police and civilian personnel in UN missions have a wide diversity of computer and technical skills, especially as the majority come from the developing world. There is a constant and critical need to train and to integrate users. Both actions are needed to make effective use of technology in the organization's daily operations (Schwabe et al. 2001: 97). Without a process of integration, even the most powerful technological system would be ineffective if the intended users cannot take the results and apply them to the challenges of violent conflict.[4]

Some monitoring devices such as video cameras are now widely used consumer items and are designed to be "user friendly". Consequently, there is a reduced training need.[5] The challenge is to integrate video cameras into daily operations so that many can benefit from the imagery.

Interoperability – defined as the ability of one group to exchange information or equipment with another group for a common end – within peacekeeping missions is an ongoing challenge, given the various nations and nationals participating. Interoperability is not simply a technical challenge. Language barriers, different methods, national caveats on the use of force, lack of confidence and trust in the United Nations, and absence of familiarity are all obstacles to effective integration and cooperation.

Monitoring technologies are typically susceptible to false alarms, usually by responding to events the devices are not designed to detect: the "false positives". False alarms may also be caused by equipment malfunctions, poor maintenance, incorrect installation or calibration, improper usage, lack of training and other factors.

Outdoor motion sensors are an example of a monitoring/detection technology that has traditionally been inadequate in discriminating between real targets and nuisances such as wandering animals. One of the most effective means to counter false alarms is through dual technologies, that is, using systems or devices that incorporate at least two detection methods. For example, dual-mode motion detectors use both passive infrared (PIR) and microwave signals. PIR is used to detect the movement of warm objects against a background level. Microwave sensors transmit an electromagnetic pulse and analyse the reflected echo. PIR and microwave operate in different portions of the spectrum. In addition, one is passive, catching only the emissions from the monitored object, and the other is active, sending out a signal and catching the reflection. Consequently, they are not subject to the same types of false alarm. Combined, they usually give a better result. Similarly, "layering" of technologies for short-, medium- and long-distance viewing can result in "smarter" and more effective systems.

Technical

Technical problems are frequently encountered in the field. In remote locations, especially conflict zones in the developing world, challenges include:

- intermittent power;
- unreliable telecommunications;
- computer workstations that are stand alone and are not linked to any network, the Internet or even each other.[6]

The Achilles' heel of most technologies in remote locations is their dependence on reliable electrical power. Peacekeeping missions often operate in areas where a robust electrical infrastructure is lacking. Some areas have intermittent power for only a few hours a day, and other areas have no electrical grid at all. Fixed installations can mitigate some of this using gas/diesel-powered generators or alternative energy sources such as solar panels or more expensive wind turbines.

Mobile devices often rely on small portable generators or batteries. However, the reliance on rechargeable and/or disposable batteries entails logistical and environmental considerations. Older models of many technologies, including night-vision devices, quickly run through many batteries for normal operation. The absence of reliable power may require a cost/benefit analysis before deploying technology that is heavily power dependent. One consideration is the noise and high visibility of generators. In some UN situations, the covert/discreet operation of electrically powered devices may be needed.

A hopeful trend is the increasing use of solar power. Some smaller electronic devices can already be solar charged during travel. Cell phones with built-in solar panels are available. For instance, the "Surge" from US start-up Novothink provides a solar back cover for iPods and iPhones that generates about half-an-hour of talk time for two hours of charging (Donoghue 2009a, 2009b).

Even when power is available, a communications infrastructure is required to link computers, networks, databases and assorted sensors together effectively. Sensor or surveillance technology can be a powerful force multiplier but, for it to be effective, the data must be delivered to human operators and for interpretation and response by leaders.

Developing a communications infrastructure requires a highly skilled maintenance workforce and can be expensive to build and operate if no existing infrastructure can be leveraged or if the cost of bandwidth is exorbitant. Fortunately, the Communications and Information Technology Service of the Department of Field Support runs a communications network that is world class.

Furthermore, commercial cell phone networks have been spreading fast in the developing world. These telephone services, which are multiplying even in conflict-ridden parts of the world, can be extremely useful to UN operations. Most networks are engineered and built to ensure a high degree of reliability, driven by the business competition for market share and profit. As a result, the infrastructure tends to be robust and possesses significant redundancies, so that if one part fails a similar system can take over. A dedicated cell/radio system for tactical purposes can create an "all-informed net" where one station/transmission is heard by all others. Using cell phones can be useful in the policing context when one-to-one communications are sufficient and appropriate.

Cell phone coverage is rapidly expanding in the developing and the developed world (as shown in Figure 4.2). Even in many remote parts of the Democratic Republic of the Congo (DRC), cell phone service is available. This provides an additional means to communicate by voice to officers deployed in the field on operations or patrols. Equally important, it can provide data access and services to those same officers without the need to deploy a complex private data network or to rely on satellite phones, which can be very expensive. As an example, officers can use cell phones or iPhone/BlackBerry® type devices to capture and transmit photos directly from the scene or to exchange text/SMS messages and email for operational purposes, as well as to enter information into centralized databases while deployed.

An advanced smartphone now incorporates a still and video camera, voice recorder, calculator, weather forecaster, and a Global Positioning System (GPS) with maps and provides links to the Internet.

Legal

From a legal perspective, there are relatively few obstacles to deploying monitoring technologies in UN field operations, provided that the equipment serves the purpose of the mission. The UN Charter (Article 105) states that "the Organization shall enjoy in the territory of each of its Members such privileges and immunities as are necessary for the fulfilment of its purposes". The 1946 Convention on the Privileges and Immunities of the United Nations further declares: "The property and assets of the United Nations, wherever located and by whomsoever held, shall be immune from search, requisition, confiscation, expropriation and any other form of interference" (United Nations 1946: Section 3).[7] In the Status-of-Forces Agreement (SOFA), which the United Nations negotiates with the host state, the state almost always recognizes the United Nations' right to import equipment as well as the state's own responsibility to promptly grant all needed authorizations and licences. The SOFA also provides reassurance to the host state:

> The United Nations peacekeeping operation and its members shall refrain from any action or activity incompatible with the impartial and international nature of their duties or inconsistent with the spirit of the present arrangement. The United Nations peacekeeping operation shall respect all local laws and regulations. (United Nations 1990: Article 6)[8]

Because local laws may sometimes include restrictions on certain monitoring – for example, of military activities – a legal dilemma could potentially arise, but experts in the United Nations' Office of Legal Affairs differ over the legal response. For some, the United Nations' fulfilment of its mandate would take precedence under the legal principle of "factual displacement".[9] Others see the host state, no matter how fragile or failed, as sovereign and having the final say in matters of monitoring. In any case, even if legally permissible, the issue can become a political challenge (see below).

For UN aerial reconnaissance, the host states' guarantees in the SOFA of unrestricted freedom of movement should normally apply.[10] But the United Nations would probably develop a kind of "modalities arrangement" for purposes of air traffic control.

The United Nations respects human rights law, which includes provisions to respect individual privacy. In carrying out monitoring activities, the United Nations must "avoid arbitrary interference with [the] privacy, family, home or correspondence" of individuals, in accordance with the Universal Declaration of Human Rights (United Nations 1948: Article 12). In its monitoring work, the United Nations would need to uphold privacy rights except in "non-arbitrary" cases where the actions of the targeted individuals or groups affect the mandate of the mission. The United Nations can take measures to ensure it respects privacy during its surveillance.[11] In general, legal instruments are not impediments to the United Nations' work but, rather, enablers of it. Nonetheless, lawyers within the United Nations have complicated the matter on occasion, placing a legal straitjacket on UN activities, much to the consternation of UN commanders.

Political: The conflicting parties

Since peacekeeping operations (PKOs) are designed primarily to achieve or contribute to a political outcome, notably a sustainable peace between conflicting parties, political considerations play a major role in the selection of monitoring methods and technologies (Diehl 2002).

Ideally, technical monitoring, like UN observation in general, should have a confidence-building effect on the conflicting parties. Accordingly, opposition should come only from individuals and groups who oppose the peace agreement or process. All committed parties should see that it is in their own interest for the United Nations to identify violations and provide early warning of threats.

In reality, parties usually sign peace agreements reluctantly because they are unable to achieve their desired outcome through armed conflict (for example, a one-sided victory). They often remain deeply suspicious and accuse each other of all manner of violations. The parties rely on the United Nations to provide objective verification of the compliance of the other side, but often prepare for the possibility of renewed violence, especially by hiding their weapons. They frequently push the limits of the peace agreement and test the limits of the United Nations' verification capability. Violations may range from marginal to substantial: from delays in implementing peace accords to political manipulation/intimidation; from arms smuggling/stockpiling to deliberate killings for political ends.

For these reasons, some parties may not wish the PKO to deploy a comprehensive monitoring system that could readily detect their own infractions of the peace accords. They might complain that the United Nations is interfering, infringing or "spying" on them, or accuse the United Nations of violating its standard of impartiality. Here, technology can both help and hinder UN deployment. Imagery or other technical evidence of illegal activities can provide objective proof beyond the verbal or written reports from UN officers. But if the parties know that the United Nations can accomplish this level of verification, they may be less interested in bringing the organization into the peace process or allowing it freedom of observation. In the end, the acceptance by the parties of objective but intrusive monitoring is one important test of their political commitment to put the peace accords into practice.

In environments of tenuous commitment where the United Nations has to investigate both major and minor wrongdoings, a "cat and mouse" game is often played in which the conflicting parties try to hide violations and accuse one another in a "blame game". In the end, it is the duty of the United Nations to establish the most rigorous verification system possible. The world organization cannot afford to be an impotent bystander in areas of violent conflict where innocent lives are at stake. If the United

Nations wants more than a purely symbolic presence, it must be ready and able to identify significant violators of peace accords and perpetrators of human rights abuses. When warranted, it must be willing to "name and shame" such individuals and groups. Even more proactively, it must help locate and help arrest war criminals and major violators of human rights.

The parties may also have legitimate concerns about UN monitoring. They might fear that the PKO could gain compromising information about them that could lead to a loss of security, especially if the information were to be obtained by the other side.[12]

The United Nations has dealt with the parties' fears by reassuring them that it will act impartially, with the required level of confidentiality and in accordance with its mandate. The United Nations can alleviate fears associated with new technologies by providing similar assurances and guarantees, as well as detailed explanations of the United Nations' methods.[13] Information technology improves the ease of information transfer, but it also provides the tools to prevent and catch such unwanted transfers.

Although the United Nations' methods are transparent, collected raw data are generally not openly available. The United Nations can explore the concept of cooperative monitoring in which interpreted data or even imagery are provided regularly to all parties as a confidence-building measure (Dorn 2004). Other options for sharing information from video cameras and sensors are as follows:

- *all* information is provided to *all* parties for *all* events:
  - on a real-time basis
  - periodically (daily/weekly/monthly)
- only violations, major or minor, are reported:
  - to *all* parties
  - to the offending party only (as a protest)
  - to *all* UN member states
- violations are reported:
  - with *all* supporting evidence (information essential to demonstrate non-compliance)
  - with only supporting evidence that will not affect the military security of the offending party
  - with no supporting evidence

In some cases, conflicting parties have even considered allowing the United Nations to place real-time video feed on the Internet for public access, that is, using web cameras to view a hotspot. For instance, in the negotiations of the 2006 Comprehensive Peace Accord in Nepal, the parties asked the United Nations to install cameras for 24/7 surveillance of weapons storage depots of both Maoist insurgents and government forces. This was to help ensure that these arms were not removed. In the end the video imagery was not made public but kept on UN computers at the weapons storage site. But this example showed how technology was applied and how it was envisioned. The system included continuous video recording of the fenced-off storage sites, a series of floodlights for illumination and a means for UN civilian observers to sound the alarm in the event of unauthorized withdrawal of the weapons (Government of Nepal 2006). This example demonstrates that technology is so widely recognized as a tool in modern life that parties have requested the United Nations to deploy it in support of peace accords.

Political: The contributing states

Nations contribute military and police personnel to UN PKOs for a variety of reasons. These include: to make a contribution to international peace and security, to foster a national role and reputation in the world ("show the flag"), to gain experience for their troops in multinational forces serving in conflict zones and to earn additional income.[14] Consequently, some contributors might not want a decrease in the number of peacekeepers in the field. They might fear that technology could bring such reductions, just as some people feared that office automation technology would lead to empty offices. Such fears are unwarranted.

In most cases, technology would not result in decreasing troop numbers but would rather lead to their more effective employment. Most UN missions are already overstretched, with too few soldiers and civilians to carry out all the tasks mandated and implied in Security Council resolutions. Robust multidimensional operations in particular are difficult to staff and support. Technology would, in most cases, take away some of the tedium of routine observation and allow PKOs to shift peacekeepers into more proactive roles, such as rapid reaction forces. By facilitating greater situational awareness, including better early warning, technology would enable reaction forces to intervene in a more targeted fashion in crisis or volatile situations. Far from creating a bunker mentality, technical means can make UN peacekeepers more proactive because the responders would benefit from increased knowledge of their local areas and could adopt preventative tactics when venturing into new ones.

Some troop contributors have little or no monitoring technology in their national inventories. Their doctrine, training and technical experience may have been limited to binoculars. Being unfamiliar with advanced technologies, these contributors might resent or envy the employment of technologies by more advanced contingents. Technology could conceivably introduce an imbalance between national contingents. One solution is to raise the capacity of these developing-nation forces by providing them with the devices and training needed to meet a standard technological level. The technology gap that exists between contributing states should not mean that the United Nations has to operate at the lowest common denominator. Rather, the United Nations should strive to operate at the most effective level for reasonable cost and effort. The soldiers of developing nations have in the past shown great eagerness to try out new tools. "Strategic partnerships" to bridge the technology gap can be adopted between nations to address the equipment and training needs of developing nations.

Some developed nations have re-engaged in peacekeeping (for example, certain European nations deployed in Lebanon) and have shown that they are willing to bring in the technologies and capabilities that they feel are necessary, irrespective of whether the United Nations will reimburse them. The United Nations' Memorandum of Understanding with troop contributors allows for such National Support Elements and equipment. Sharing a range of technology and expertise with developing nations would raise the standard of UN missions.

Political: UN member states

Some technologically advanced states have sought to prevent the proliferation of certain monitoring technologies, fearing that these might fall into non-friendly or enemy hands. One example is the stringent US export control regime on its night-vision equipment.[15] This has prevented UN headquarters from answering calls from field commanders for third-generation (Gen 3) night-vision equipment. Thus, the UN missions must, at present, be satisfied with the generation 2+ (Gen 2+) equipment in UN stockpiles, although more advanced devices are still being brought to the field as Contingent-Owned Equipment.

More generally, some states would not want the United Nations to have "information power" that might challenge their intelligence dominance in certain areas. This is particularly true in strategic conflict zones where economic interests are at stake and/or where covert operations are taking place. On the other hand, there are many examples where major powers have shared sensitive information with the United Nations in order to help bring a more durable peace to war-torn regions. This includes imagery from satellites and over-flights. When the success of a PKO is in the interest of all member states, as PKOs usually are, support is often provided.

Nations that host future PKOs on their territory may harbour exaggerated fears that technology could be used to pry into their affairs or that the United Nations might overstep the bounds of proper behaviour by interfering with national sovereignty and possibly engaging in dubious or covert intelligence-gathering. UN peacekeeping history has few incidents on record of such deviant behaviour. In practice, the United Nations has tended to be overly cautious and sensitive, avoiding anything controversial, even if the stakes have been high. Furthermore, the United Nations can institute internal checks and balances to prevent the potential misuse of monitoring. As noted, the United Nations has pledged to observe legal prohibitions and international norms.[16]

Institutional and cultural

Amid the conflicting interests and demands of UN member states, the UN Secretariat impressively manages a large number of PKOs in some of the most difficult conflict regions of the globe, using troops and civilians from over 100 disparate nations. The Department of Peacekeeping Operations (DPKO) in New York struggles to provide the field with the resources needed to do the job satisfactorily while also developing general policy, doctrine and training materials for PKOs, starting at the most basic level.

Field personnel, especially from developed nations, often complain that they are deployed in UN missions without sufficient tools, particularly the ones to which they have grown accustomed under national or allied arrangements. In the case of the UN mission in the DRC (MONUC), military commanders pleaded for modern surveillance technologies to carry out their ambitious monitoring mandates over vast territories. The UN system at headquarters, which must budget, fund and procure the technology, has often been slow or inadequate in its response. When not all UN actors sense the urgency and also face member state demands to decrease the overall cost of peacekeeping, it has been difficult to justify significant purchases of monitoring technology despite their potential or proven utility.

The military staff at UN headquarters are generally quite aware of the role that monitoring technology can play in PKOs and are sympathetic to the calls from the field. Soldiers are accustomed to seeking operational advantage from technology, whether in war-fighting or peacekeeping. Officers with NATO experience are aware that the alliance has over a dozen agencies devoted to technology and over 20 military advisory groups and committees (see the list in Table 7.4) to deal with science and technology issues. By contrast, military technologies are foreign to most civilians in the UN Secretariat. Staff who have never used or seen technologies in operation are only vaguely aware of the benefits/limitations and often exhibit a degree of “technophobia”. They might even fear that technology is too military for peace. The solution is, of course, to raise awareness of technological options through education.

Some UN officials may also be concerned that member states would complain that the United Nations was overstepping its bounds in deploying sophisticated watching devices, despite the monitoring mandates. New information gained from technologies may also pressure and raise expectations for the United Nations to respond to early warning signals, removing the option of pleading ignorance about past or present threats. In the end, technical signals should help the United Nations become more proactive and responsive to the needs of inhabitants in conflict areas.

Humanitarians speak of the need for "humanitarian space" and worry about the possible over-militarization of operations. Some may not be aware that monitoring technologies can also be civilian run. In fact, humanitarian space relies extensively on communications technologies and many life-supporting devices such as water purification units. Using cameras instead of heavily armed soldiers can even reduce the level of military presence. When demilitarization is required, the step to civilian or appropriate joint civilian–military technology should not be difficult.

Financial

The cost of most monitoring devices is no longer a major obstacle. Prices have plummeted in recent years owing to advances in science and technology, as well as to the growing commercial marketplace. At the very low-cost end, motion detectors/illuminators can be obtained for as little as $20 and solar-powered versions are available at less than $50 per unit. This makes them cheap enough to use widely in refugee camps and even unattended places. Theft could be a problem, but at this low price there is little lost.

More expensive items such as video cameras (typically $500–2,000 each) for closed-circuit television (CCTV) systems and night-vision devices ($2,000 for Gen 2+ goggles) are well within normal discretionary budgets, as are hand-held metal detectors ($1,500) and acoustic/seismic systems ($1,500 for a set of a dozen sensors). Satellite imagery ($300–3,000 per image) becomes costly only when purchased in quantity or in near real time. (Some imagery, as in the older imagery on "Google Earth", is free.) Thermal (far-infrared) imaging devices are more expensive ($5,000 and above) and X-ray screening machines considerably more (over $25,000), as are various ground/aerial surveillance and artillery-locating radars (over $30,000).

The purchase of these devices, however, is only part of the overall cost, which must cover the entire lifecycle of the equipment. This includes procurement, transportation, installation, maintenance, repair, storage and disposal. Fortunately, the United Nations has become much better at equipment management over the past decade, especially through the development of better inventory methods and maintenance capabilities at the UN Logistics Base in Brindisi, Italy.

The most expensive types of surveillance are those involving aircraft (typically $1,000–2,500 per hour of flight for a wet lease[17]). When MONUC sought a commercial airborne surveillance service, DPKO budgeted $10–20 million per year, though the system was not deployed. If extensive use is to be made of aerial reconnaissance in several missions for several years, it might be cost-effective for the United Nations to procure one or more small aircraft and train its own civilian crews.

For unmanned aerial vehicles (UAVs), the United Nations might initially rely on certain troop-contributing countries that are rapidly gaining experience in deploying UAVs to operations. For instance, Belgium has deployed UAVs in Bosnia and the DRC under the UN-assisting European Union Force. As mini-UAV costs decrease and capabilities increase, the United Nations could consider purchasing some in the future.[18] A set of three mini-UAVs could be purchased for less than an annual dry lease for one manned aircraft.[19]

More challenging than equipment costs, however, can be the specialized training programmes for UN personnel to operate more advanced equipment. As mentioned, data analysis needs trained specialists. Several weeks of training and testing are required to operate even relatively simple systems, such as the ones used for X-ray screening.[20] This would be necessary for the equipment to become part of a standing "UN capability". Trainers from private corporations, including the equipment manufacturers, can be used to meet some of the training needs.

By using troop-contributing countries or wet-lease contractors, the training of military or contracted personnel can be done outside the United Nations, though such loans and leases may be more expensive than UN-owned and UN-operated equipment.[21] When the United Nations Interim Force in Lebanon was substantially expanded and upgraded after the 2006 war, the United Kingdom offered to provide UK-manned AWACS surveillance aircraft[22] – an offer that the United Nations had to turn down because of cost. Germany deployed frigates to patrol the coastline in the Mediterranean Sea and France sent a squadron of advanced UAVs. The full cost to lease such items would be millions of dollars a month, so the United Nations agreed to pay only a relatively small portion of the real cost.

Although monitoring is an essential, if not primary, function of all missions, monitoring equipment costs are currently not even 1 per cent of UN mission costs. The equipment costs are also minimal in comparison with the amounts the United Nations currently pays for aerial transport and personnel costs.[23] The United Nations spent over $8 billion on peace operations in 2009–2010. By contrast, a substantial increase in monitoring equipment in several missions could be gained with several million dollars. In short, the financial aspects of most monitoring technologies should not pose a significant obstacle, given the significant force-multiplier effect.

Other problems, pitfalls and hazards

Additional problems can be associated with technical monitoring:

- *Over-reliance*. If the United Nations were to become largely or completely dependent on technology, this would be a vulnerability. If devices malfunction or break down, experience a failure of electrical power or provide false information, the United Nations could find itself in difficult or embarrassing situations. Thus there is a need for constant testing, evaluation and cross-referencing with other sources, and for creating natural redundancies in the system. Direct human observation must continue to play a major part in the United Nations' information-gathering efforts.
- *Countermeasures*. Some technologies are susceptible to countermeasures that parties may take to evade detection. For instance, overhead nets can provide camouflage against day and night surveillance and GPS signals can be jammed. The United Nations should be aware of these possibilities, although most potential adversaries are not capable of sophisticated countermeasures.
- *Industrial lobbying*. DPKO already finds itself the target of lobbyists and commercial vendors who seek to promote their wares. Technologies cannot be justified for their own sake. They need to fulfil a definite purpose in peacekeeping (see Chapter 3). Commercial agents with past or present links to the organization may seek to exert undue influence on technology purchases. Given the strong defence lobby in some countries, particularly the host country for UN headquarters (the United States), it is likely that a more technologically receptive United Nations would find itself the object of greater lobbying. This, however, could have a side benefit of increasing awareness of technologies, although with some nuisance.
- *"Middleman" corporations*. Such companies are an integral part of the defence lobby in many nations, and the firms often charge substantially marked-up prices for coordinating delivery of products produced by others. This sometimes results in cost inefficiencies and a lack of direct accountability.

Though the challenges of employing technologies are great, the benefits are greater. The costs of not using technology are far higher in terms of UN effectiveness and of possible lives lost. Given the many obstacles identified above, what can be done to improve UN capacity? The penultimate chapter provides both general and technology-specific recommendations.

Notes

1. Night driving on roads with no street lighting (e.g. jungle roads) is possible with night-vision goggles but users should first gain experience in simpler environments. Users need to be aware that night-vision devices can alter depth perception and exhibit distortions such as curving at the edges and phenomena such as "blooming" (halo effects around bright lights), "scintillation" (temporary bright spots) and black spots (small but often permanent).
2. For instance, commercial water-resistant global positioning devices used for hiking and climbing expeditions can be purchased for under $200.
3. Terrain can impose other limitations on the choice of sensors. In the open desert, where there are many, if not an infinite number of, possible paths through the sand, point sensors are of limited value because they measure signals at one small location only. Seismic devices are rendered ineffectual in the desert because seismic waves are quickly absorbed by the sand. Similarly, in difficult mountainous terrain where vehicles are unlikely to pass, buried magnetic sensors are of limited value.
4. This notion is well captured by General Alfred M. Gray: "Intelligence without communications is irrelevant; communications without intelligence is noise" (quoted by Robert David Steele in "Intelligence & Information: The Debate Continues", available at <http://www.oss.net/dynamaster/file_archive/050305/fa8baa703790c82a5afbb1ada54e96db/Steele%20on%20Intelligence.doc>, accessed 7 February 2011). See also Steele (2010b).
5. In the same study (Schwabe et al. 2001: 102), a survey of US police officers revealed: "Relatively few local police (less than 10 percent) felt that training requirements were an important factor with respect to the use of video cameras either in patrol cars or in fixed or mobile surveillance. Only 10 percent of departments considered training to be key with respect to acquisition of night vision/electro-optic devices, smart guns, and for most vehicle stopping/tracking devices (tire deflation spikes, stolen vehicle tracking) and digital imaging devices (fingerprints, mug shots)."
6. Email from Dan Hefkey, Ontario Provincial Police Inspector, to Michael Dube, Toronto, Canada, January 2009. Inspector Hefkey had served as the detachment/station commander for the Hinche and Thiotte detachments in Haiti in 1995.
7. Also the 1994 Convention on the Safety of United Nations and Associated Personnel states that "their equipment and premises shall not be made the object of attack or of any action that prevents them from discharging their mandate" (United Nations 1994).
8. The right to import is provided in Article 15. This document also serves as the basis for Status of Mission Agreements in cases where UN civilians and unarmed military observers, but not UN forces, are deployed.
9. Personal interview with David Hutchinson, Senior Legal Officer, Office of Legal Affairs, United Nations, New York, 26 January 2007.
10. "The United Nations peacekeeping operation and its members shall enjoy, together with its vehicles, vessels, aircraft and equipment, freedom of movement throughout the

[host country/territory]. The freedom shall, with respect to large movements . . . be coordinated with the Government" (United Nations 1990: Article 12).

11. The United Nations could use lower-resolution cameras so as not to identify individuals (unless required) and exercise "shutter control" over the cameras and devices to ensure that the peacekeeping operation does not unduly observe innocent commercial or private activities.
12. This happened in one Bosnian city. As soldiers of the United Nations Protection Force observed the landing areas of mortar fire, they communicated these locations to regional headquarters by radio in the clear (non-encrypted). They did not know that Serb artillerymen were listening to the communications and using the information to correct their fire in order to make it more deadly. In such cases, encrypted communications are a must for the United Nations.
13. The United Nations could, for instance, outline the types of information that would be sought and the general methods and devices that would be employed. Furthermore, it could provide the parties with regular reports on its monitoring activities in a way that would not threaten the parties' security. At meetings of joint commissions or other bodies that bring all parties and the United Nations together, a regular feature could be the presentation of the results of UN verification in general terms.
14. For some states, peacekeeping is revenue generating.
15. To export night-vision equipment from the United States to the field, the United Nations would need an export licence from the US State Department under the US Government International Traffic in Arms Regulations rules. The US government allows third-generation technology to be exported to all NATO countries, plus Japan, South Korea, Australia, Egypt and Israel. So far, the requests of the Supply Section in the United Nations' Logistics Support Division for licences have all been turned down, on the basis that nations other than those listed above might gain access to the technology once it is deployed to the field. The United Nations currently gets most of its night-vision equipment (generation 2+) from a Canadian company.
16. There are examples, however, where nation-states have used UN peacekeeping and other operations as a cover to introduce their own intelligence personnel into the mission area. The United Nations Special Commission in Iraq is a likely case of this (Ritter 1999).
17. A wet lease for an aircraft arrangement would include at least some of the costs for crew, maintenance and fuel, as well as the lease of the aircraft itself. See <http://www.globalplanesearch.com/view/aircraft/aircraft-leasing-def.htm>.
18. The UAV would need to be certified for airworthiness, possibly by the nation that produced it.
19. A dry lease for an aircraft does not provide aircraft insurance, crew or maintenance services.
20. MONUC procured X-ray machines at a cost of over $500,000 for baggage-handling at the MONUC-run airports in the DRC. Many months after they were installed at airport departure areas, they had not been brought into use because the local personnel had not been trained to operate them.
21. For instance, the United Nations pays over $8,000 per month for two ground surveillance radars used by the Quick Reaction Force in the United Nations Mission in Liberia.
22. Airborne Early Warning and Control System aircraft cost over $200 million each to procure and between $10,000 and $25,000 per hour to operate (Beattie and Greenaway 1986).
23. It is estimated that almost a quarter of MONUC's annual budget of $1.1 billion is spent on aircraft and fuel.