United Nations
Department of Peacekeeping Operations
Department of Field Support

Ref. 2010.34

Policy

Monitoring and Surveillance Technology in Field Missions

Approved by:	Alain Le Roy, USG/DPKO
Effective date:	1 November 2010
Contact:	Senior Policy and Doctrine Officer, Office of Military Affairs, DPKO
Review date:	1 November 2013

MONITORING AND SURVEILLANCE TECHNOLOGY IN FIELD MISSIONS

Contents:

A. PURPOSE

1. This Policy explains the context and the purpose of using Monitoring and Surveillance Technology (M&ST) for mandate implementation and protection of United Nations personnel and facilities. Instructions on implementation are provided by a related Standard Operating Procedure (SOP).

B. SCOPE

2. This Policy applies to DPKO Mission senior leadership, planners, and Field Support managers at UN Headquarters (UNHQ); Heads of Missions (HOM), Designated Officials (DO), Security Management Teams (SMT), Heads of Military Components (HOMC), Heads of Police Components (HOPC), Directors/Chiefs of Mission Support (D/CMS), Chiefs of Integrated Support Services (CISS), and UNLB.

3. It can also serve as a guide to the Department of Political Affairs (DPA) and DPA-led Missions and UN Country Teams and Chief Security Advisers/Officers (CSA/CSO).

C. RATIONALE

4. Taking decisions in complex situations requires a solid, current and unbiased picture of the situation. Vast mission areas and limited mission resources often do not allow having a comprehensive view and understanding of the situation and require that human assets be complemented by technological tools.

5. Further, aggressive behaviour and attacks against UN staff have increased in recent years, requiring enhanced protection measures for personnel and facilities.

6. Monitoring and Surveillance Technology can significantly improve capabilities of peacekeeping missions to generate a comprehensive picture of the operating environment, and ultimately enhance the quality of decision-making for a variety of mandated tasks, including the protection of UN staff.

7. The Maritime Component in UNIFIL is an example of usage of Monitoring and Surveillance technology, as ship-borne radars are used to detect un-identified vessels into ports. Another example is the use of Satellite Imagery for Haiti, where it contributed to situational awareness in planning in the aftermath of the earthquake.

D. POLICY

D.1 Purpose of Monitoring and Surveillance Technology

8. In UN peacekeeping, M&ST is used for two main purposes:

   - First, to support decision-making in complex environment. This requires a rich capability to collect information thereby supporting the implementation of mandated tasks, including protection of civilians. For this purpose, collected information is handled through a clearly defined and transparent process (see annex. The Information Cycle) that leads to an assessment to the mission leadership;
   - Second, protection and surveillance of UN local and international staff and facilities to prevent physical aggression on individuals, theft, intentional damages and other hazards.

9. Consequently, tasks to be performed by M&ST will derive from the mandated tasks and security needs of the mission. They comprise, but are not limited to:

   - Surveillance of high risk area in support of protecting civilian populations.
   - Locate and monitor armed groups.
   - Surveillance of UN facilities and of potentially dangerous areas where UN personnel is deployed.
   - Monitoring developments and damage assessment in natural disaster situations (flooding, volcanic eruptions, mud slides, etc.) in support of a mission and to affected populations;
   - Tracking of UN property for logistics management and retrieve personnel in case of carjacking or kidnapping.

10. The mandated task to monitor activities along a demilitarized zone, and redeployment or demobilization of forces in a given area undergoes a different collection and assessment process, which is not treated in this policy.

D.2 Principles

11. For the purpose of this policy, M&ST is defined as the technologies that may be used by peacekeepers to enhance their own capability to detect and monitor threats in their mission area. M&ST comprises systems such as Closed Circuit TV (CCTV), Remotely Piloted Vehicles (RPV), sound and radio listening devices, seismic detection devices, air reconnaissance systems, etc. This policy does not cover satellite sensing technology.

12. M&ST can be deployed at any stage of a field mission and must be integrated with other available resources of information.

13. Requirements for Monitoring and Surveillance Technology (M&ST) will be based on thorough mission analysis, taking into account the mandated tasks, the political environment, the security situation, the terrain, and the nature of

challenges to the mission. Needs have to be clearly identified and defined in order to formulate requirements for the most adequate M&ST combination, both in terms of quality (type of information to be collected) and quantity.

14. Formulation of requirements for M&ST will be the coordinated result of process between the joint (JOC and JMAC), military, police and security (DSS) and support (DMS incl. CITS) components of a Mission, under the overall guidance of the Head of Mission and DPKO to decide on the most appropriate technological solution[1].

15. Besides technical issues that need to be carefully coordinated with the host country, such as radio frequency allocation or air space management, M&ST requires careful political management as regards its potential intrusiveness and information sharing.

16. The Heads of Missions shall designate an entity or unit within the Mission, usually the JMAC, to store and secure data, as well as to oversee the analytical process.

D.3 Status of Mission / Force Agreement (SOMA / SOFA)

17. The UN acts according to the principle of impartiality and in full accordance with international and national laws and uses. They will not engage in illegal activity in order to collect information.

18. The use of M&ST will be formalized in the SOFA/SOMA or other bilateral arrangements.

19. The SOFA/SOMA acknowledges the UN's right to import, free of restrictions, equipment for official use by the mission and to communicate unhindered. It may have provisions for technical coordination on the use of communication equipment with the host government.

D.4 Information Processing

20. UN operating processes – including information management processes – are open and transparent. Information processing will follow the Information Cycle (Annex A). Data and information however may be sensitive in nature as they may contain unverified information (about individuals). In any case, information will be considered as sensitive – and handled as such - unless it has been analysed, sanitized from information that may endanger individuals and cleared for dissemination.

21. Sensitive information shall be classified as Confidential or Strictly Confidential, as per ST/SGB/2007/6, for proper storage, retrieval, archiving and disposal. The originator of the information concerned, or its recipient if the information is received from an outside source, under the overall supervision and guidance of the head of department or office, shall decide whether the information is sensitive and mark it with the appropriate classification as detailed in section 4 of ST/SGB/2007/6.

22. Sensitive information will be stored accordingly in protected databases and Missions shall establish procedures to define authorized users of relevant Information and Communications Technology (ICT) resources as per ST/SGB/2004/15. Missions shall ensure that automated information systems, including networks and telecommunications systems, that collect, create

[1] See SOP Annex A

communicate, compute, disseminate, process or store sensitive information, have mechanisms to prevent access by unauthorized persons, as per ST/SGB/2007/6.

23. Processed information will be shared within the UN only, including UN HQ. The Head of Mission will decide on the distribution list within the United Nations Country Team (UNCT) based on the "need-to-know principle", and taking into account safety and privacy of individuals.

24. Sharing classified information or downgrading security classification in order to share information with non-UN entities will require specific approval of the senior mission management in consultation with its originator and UN HQ.

D.5 Training

25. Training activities related to M&ST will address three levels:

- Technical skills of individuals responsible for operating monitoring and surveillance devices;
- Integration of M&ST in information management processes by Information Management Staff and/or JMAC personnel;
- Knowledge and integration of M&ST capabilities into decision-making process at Senior Management level.

E. TERMS AND DEFINITIONS

26. **Digital map** – a map of vector data files depicting geographic features that could be manipulated, analyzed and printed by geographic information systems.

27. **Joint Mission Analysis Centre (JMAC)** – an integrated structure to support planning and decision-making and to support the development of risk assessments by the Head of Mission and the Mission Leadership Team through integrated analytical products. In integrated missions, the JMAC has relations with the UNCT

28. **Joint Operations Centre (JOC)** – an integrated structure to support decision making by the HOM and the Senior Management Team with a focus on day to day operational activities. During a crisis, the JOC will operate the Crisis Management Team. The UNCT should share information with the JOC.

29. **Mission Leadership Team** - Includes the Head of Mission (HOM) (in many cases also the Designated Official for Security), heads of components and, in integrated missions, heads of agencies, funds and programmes. In some missions, the Deputy Special Representative of the Secretary-General/Resident Coordinator/Humanitarian Coordinator (DSRSG/RC/HC) may represent the heads of agencies funds and programmes.

30. **Monitoring** – Monitoring is the activities-based employment of sensors to follow the evolution of a situation. Monitoring includes tracking of UN property through locating devices (usually, GPS-based).The term "monitoring" as used in this document does not cover the mandated task to monitor activities along a demilitarized zone or in a given area: such activity undergoes different collection and assessment process.

31. **Risk** - The combination of impact and likelihood for harm, loss or damage to the United Nations system from the exposure to threats. Risks are categorized in levels from Very Low to Very High for their prioritization.

32. **Security Management Team (SMT)** – Comprised of the Designated Official, Heads of Agencies, Senior Mission Leadership and the CSA/CSO. Advises the DO on all security related issues.

33. **Security Risk Assessment (SRA)** – The process of identifying those threats which could affect UN personnel, assets or operations and the UN's vulnerability to them, assessing risks to the UN in terms of likelihood and impact, prioritizing those risks and identifying prevention and mitigation strategies and measures.

34. **Sensitive Information** – Information that, as determined by the United Nations with reference to the criteria set forth in ST/SGB/2007/6, may be classified as "confidential" or "strictly confidential". The designation of "confidential" shall apply to information or material whose unauthorized disclosure could reasonably be expected to cause damage to the work of the UN or third parties. The designation "strictly confidential" shall apply to all information or material whose unauthorized disclosure could reasonably be expected to cause exceptionally grave damage to or impede the conduct of the work of the UN. Classification should be used judiciously.

35. **Surveillance** - Surveillance is the space- and object-oriented employment of sensors by systematic observation of a given space (including, to a lesser extent, airspace) or objects by visual, acoustical, electronic or other means. Surveillance is performed openly by ground-based sensors, such as surveillance cameras or with air-based sensors, such as tethered balloons or drones.

36. **Technical Assessment Mission (TAM)** - Assessment made by UN experts to ascertain whether the minimum conditions for a successful UN peacekeeping intervention are or can be put in place. Addresses a mission's environmental conditions and emerging concept(s), in particular the managerial and integration aspects, with a view to formulating its Concept of Operations (CONOPS).

37. **Threat** - Any factors (actions, circumstances or events) which have the potential or possibility to cause harm, loss or damage to the United Nations system, including its personnel, assets and operations.

F. REFERENCES

- Integrated Mission Planning Process (IMPP) Guidelines endorsed in 2009
- Mission Start-Up Field Guide, Version 2, August 2010
- United Nations Field Security Handbook, January 2006
- Use of Information and Communication Technology Resources and Data (ST/SGB/2004/15)
- Information Sensitivity, Classification and handling (ST/SGB/2007/6)
- Record-keeping and the Management of United Nations Archives (ST/SGB/2007/5)
- DPKO Policies on JOC and JMAC, 05 Jan 2010
- DPKO Policy Directive on Strategic Deployment Stocks Operations, 30 January 2006
- United Nations Minimum Operating Security Standards (MOSS), 01 April 2004
- Planning Process for Military Operations, September 2001
- DSS Memo 20 April 2009, Entry into effect of new policies on Security Risk Management, Minimum Operating Security Standards and Guidelines for

determining Acceptable Risk

G. MONITORING AND COMPLIANCE

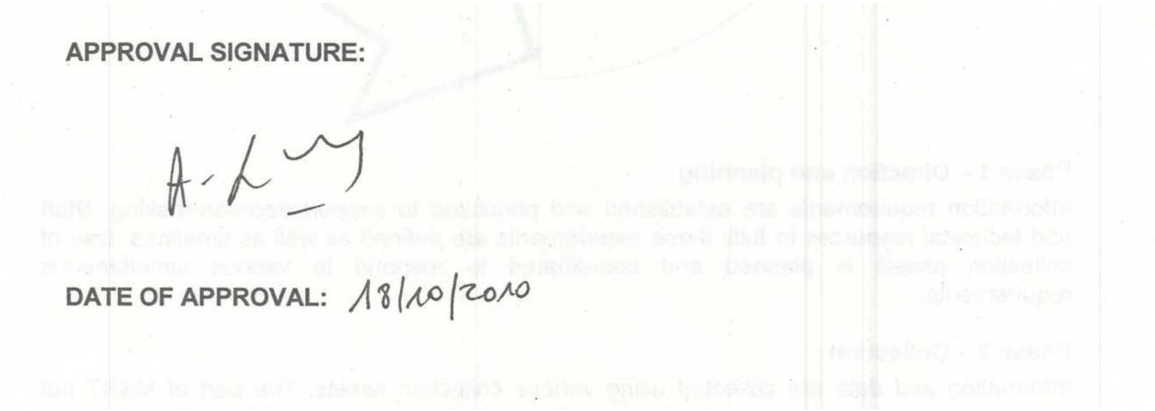
38. Implementation of this policy is monitored by DPKO and DFS.

H. CONTACT

39. The Office of Military Affairs (OMA) will coordinate monitoring and surveillance technology policy updates as required with stakeholders in DFS and DPKO for the approval by the Expanded Senior Management Team (ESMT). Informal consultations will be conducted with DPA and DSS. Senior Policy and Doctrine Officer, fax (+1) 212-963-9070.

I. HISTORY

40. This is the first issue of this Policy. It has not been amended.

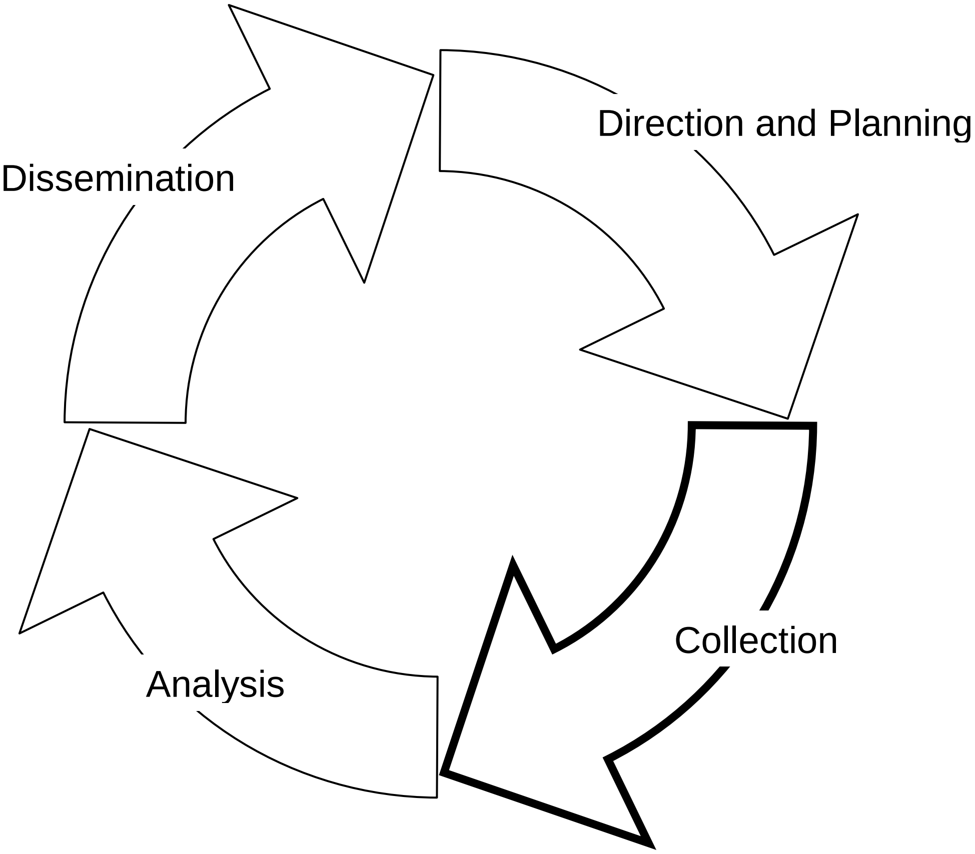


APPROVAL SIGNATURE:

DATE OF APPROVAL: 18/10/2010

ANNEX A

The Information Cycle



Phase 1 – Direction and planning

Information requirements are established and prioritized to support decision-making. Staff and technical resources to fulfil these requirements are defined as well as timelines. Use of collection assets is planned and coordinated to respond to various simultaneous requirements.

Phase 2 – Collection

Information and data are collected using various collection assets. The part of M&ST not devoted to protection is basically a part of the collection assets used by a Field Mission besides other human and open sources .There are no illegal collection activities in the UN practice.

Phase 3 – Analysis

Collected information is processed and analysed to address the needs and concerns of the Senior Mission Management and/or to identify issues that may become a matter of concern in the future.

Phase 4 – Dissemination

Results of the analytical process are disseminated to the Senior Mission Management and to other addressees through reports, presentations, briefings or database access.