HARVARD PROGRAM
ON HUMANITARIAN POLICY
AND CONFLICT RESEARCH

TOWARDS A COMMON SECURITY FRAMEWORK: SECURING ACCESS AND MANAGING RISKS IN HAZARDOUS MISSIONS

By

Claude Bruderlein

PROGRAM ON HUMANITARIAN POLICY AND CONFLICT RESEARCH
Harvard University
1033 Massachusetts Avenue · Fourth Floor · Cambridge, MA 02138 USA
Tel: (617) 384-7407 · Fax: (617) 384-5908 · hpcr@hsph.harvard.edu

Summary

International agencies are facing increasing levels of threats against their staff and activities in many of their operations. Since the end of the Cold War, these agencies, inter-governmental and non-governmental alike, have been called to work more intensely in conflict areas.[1] These areas have become singularly more dangerous in recent years, exposing staff to greater risks. The threats of attack, as well as recurring levels of criminal violence, are now part of the daily life of international agencies' workers in many of these situations, hindering their work and limiting their access to people in need.

Although significant resources have been invested recently in building the security capabilities of international agencies, **the escalation in security threats has not been matched with the development of corresponding institutional strategies to mitigate operational risks** and reduce the exposure of international agencies. Despite serious flaws in existing security systems, international agencies have been inclined to expand their security capacity at a technical level rather than reviewing the relevance of their security strategies.

As a response to the attacks against United Nations (UN) headquarters in Baghdad and other field missions, the United Nations is planning to expand significantly the capacity of the UN security system by creating a Directorate of Security, which will centralize all UN security systems, and by adding a number of staff and layers of technical responsibilities to an already bureaucratic and over-procedural security apparatus. While most operational managers agree that the security environment of UN agencies has evolved considerably over the recent years, this significant expansion in security capabilities is being considered without a clear and proper understanding of the types or sources of threats the UN will face in the coming decades.[2] There are few discussions on global and local threats against UN operations or the role that agencies can play to mitigate exposure to risks.

Similarly, other agencies, such as the International Committee of the Red Cross (ICRC) or Médecins Sans Frontières (MSF), are increasingly tying their security response to conservative interpretations of their mission — relying significantly, in the process, on the neutral character of their activities and the acceptance of the communities. **Many organizations, however, fail to acknowledge the changing perceptions of international assistance in some areas of the world and the changing profile of the security threats that endanger not only their operators but the recipient communities as well.** For these agencies, the current security developments represent a major challenge

[1] International agencies are understood here as those organizations involved in international efforts to provide assistance (developmental, humanitarian, technical, or political) to governments, civil societies and populations affected by an armed conflict. These include United Nations (UN) and non-United Nations agencies, International Red Cross organizations, non-governmental organizations (NGOs), charitable groups and foundations that operate internationally, and engage actively in conflict environments. Although these organizations may function under specific and divergent mandates, their staff and activities often face similar security challenges. Such list does not include peacekeeping, peace enforcement, or other military-type operators.

[2] See upcoming Secretary General's Report to the UN General Assembly, "Strengthened and Unified Security Management System for the United Nations".

not only to the safety of their staff, but, equally, to the traditional humanitarian and neutral character of their operations and their ability to operate independently from integrated political and security missions.

Present security challenges raise difficult questions regarding the ability of international agencies to operate in conflict environments and mitigate the sources of insecurity. New security threats associated with global terrorism, collapsed or fragmented states, the proliferation of small arms, the privatization of conflicts, rising economic depredation or environmental degradation in some conflict areas are forcing a re-evaluation of the core objectives of these agencies, their dependence on current security systems and the impact new security methods may have on the perception of their constituency and beneficiaries. **A strictly technical response to the new sources of insecurity is unlikely to provide a secure environment. An in-depth debate and a practical agenda on a common security approach of international agencies active in high-risk environment are urgently warranted**.

This paper addresses the strategic components of the current security approaches of international agencies and reviews some of their shortcomings. It provides preliminary elements of new and more integrated security strategies to ensure that international agencies are able to respond to upcoming security threats. In the first section, the paper presents some of the critical factors pertaining to the increased exposure of international agencies to security threats. Section II reviews the two dominant schools of thought among international agencies in addressing insecurity, namely the system-based and the community-based security approaches. In section III, the paper introduces a model for the development of an integrated security management system (ISMS) accompanied by succinct and practical recommendations on the professionalization of security management of international agencies.

The paper concludes that **one of the most pervasive aspects of the existing security crisis lies with the eminent sense of threat to the distinctiveness of humanitarian and development organizations from political and security operations**. This systemic threat should by no means prevent such agencies from adapting their operational strategies to these new environments. **Unless these organizations can develop professional security response mechanisms to address these threats, it is unlikely that they will be able to oppose the integration of their operations into centralized system-wide security systems,** further linking their missions to dominant security and political agendas.

I. Security environment of international agencies in the twenty-first century

Before reviewing current strategies to address the security challenges faced by international agencies, it is important to identify at the outset the factors that have played a key role in the increased exposure of agencies' staff to insecurity. These include:

- Increased international involvement in conflict areas

Over the last decade, international agencies have been called to deploy their humanitarian and development activities in a growing number of hazardous locations ranging from unstable political situations to outright civil or international wars.[3] Upon the request of donor governments to amplify synergies between assistance and peace efforts (for instance, strategic framework activities in Afghanistan)[4], international agencies also had to expand their engagement to include right-based and conflict prevention/resolution activities (for example, the promotion of gender issues and human rights in Taliban Afghanistan). This increasing international involvement in conflict prevention, management, and resolution caused agencies to deploy more staff in a growing number of conflict situations, thereby increasing their exposure to insecurity.

- Fragmented and complex political emergencies

If the overall number of conflicts decreased since the early 1990s, the remaining and emerging conflicts take place against the context of endangered or collapsed states. The fragmentation of the states — with its various manifestations in terms of ineffective government control over territory and people, warlordism, repression of minorities and resulting movement of internally-displaced and refugee populations — contributes to the complexity of conflicts. International agencies must cope with these factors of uncertainty by developing programming strategies that allow for the necessary flexibility to address divergent needs in a way that, ideally, remains impartial and amenable to all the parties to the conflict. The performance of these agencies in preserving the integrity of their programs and maintaining the acquiescence of all the parties to the conflict amounts, for a large part, to their security.

- The blurring of the distinction between combatant and civilians

Traditionally, wars have been fought among combatants, for the most part sparing civilian populations. Since the Second World War, however, conflicts have increasingly engaged civilians, both as active participants in hostilities and direct targets of attack. Since then, civilians have constituted the overwhelming majority of war casualties. With the waning of the Cold War, a pattern of deliberate war against civilians, waged by relatively untrained

[3] In 2003, for example, the United Nations deployed over forty thousand UN staff in ninety-one hazardous missions. This deployment represented a twenty-five per cent increase since 1999. See the *Report of the Independent Panel on the Safety and Security of UN Personnel in Iraq* (hereafter Ahtisaari Report), New York, 20 October 2003, p. 26.

[4] See Alan Kreczko, *The Afghan Experiment — The Afghan Support Group, Principled Common Programming, and the Strategic Framework*, Disasters, Vol. 27, Issue 3, p. 239, September 2003.

forces wielding relatively light arms, has persisted. Assisting civilians can, arguably, be perceived by parties to a conflict as a gesture of political and security significance. Despite the humanitarian character of their endeavor, international agencies run the inherent risk of being perceived as taking part in the conflict — and thus become the subject of attacks simply by deploying their humanitarian operations for the benefits of the civilian population. Such perception is emphasized further when agencies actually take widely publicized political positions linked to the political agenda of one party to the conflict.[5]

- The privatization of armed force and the increased availability of weapons

The proliferation of small arms has had a significant impact on both the political and security environments of contemporary conflicts. For a few hundred dollars, individuals can arm themselves and create an active military group. With a minimum of training they can engage other groups or government forces. This access to weapons has generated both the spreading of violence (criminal and political) and the leveling of political groups. Private groups can acquire substantial power and exert control over large territories and populations. International agencies' operators have to engage with these individuals to seek access to vulnerable populations and aspire to obtain credible security guarantees. Evidently, such enterprise has remained hazardous as demonstrated in several instances, such as civil wars in Liberia and the Democratic Republic of Congo.

II. CURRENT APPROACHES OF INTERNATIONAL AGENCIES TO THEIR SECURITY NEEDS

A striking aspect of the existing approaches of international agencies to security is the **dearth of strategic thinking** involved in the development of their security response. For the most part, current approaches have been elaborated as a series of technical responses to operational problems (e.g., security of individuals, premises, transport, or communication) without meaningful policy debates on coherent security strategies among international agencies. Only recently has the Office of the UN Security Coordinator and the Inter-Agency Security Management Network (IASMN) engaged in some reflection on security priorities and procedures for UN agencies working in hazardous environments. No other significant institutional policy mechanisms address, in a coordinated manner, the security risks incurred by international agencies.

This lack of debate is particularly surprising in light of the lengthy discussions among international agencies on accountability, the mainstreaming of human rights in their activities, or the nexus between rehabilitation and development. While security risks and capabilities have grown into a primary strategic factor allowing or prohibiting field operations, little has been published among agencies.

Several reasons account for the lack of development of cogent security strategies.

[5] See, for example, the statement of the United Nations High Commissioner for Refugees, Ruud Lubbers, calling, on September 24, 2004 for an autonomous status for the Western Darfur region while UNHCR has been involved as a lead agency in dealing with the refugee flow from the Darfur region.

A first aspect relates to the cultural gap between development professionals and the security world. Despite being active in conflict areas for years and carrying significant responsibilities in terms of security of staff, development and humanitarian professionals will generally balk at being perceived as knowledgeable in this area. The treatment of security issues has often been perceived as a military matter to be handled by 'security experts,' i.e., oftentimes former military or security officers. Such delegation of competence to military experts has contributed historically to the fostering of a sub-culture of security among former military officers. Within individual agencies, these would then focus on a narrow paradigm of security that, conceptually and practically, relates more to military operations than international agencies' activities. As a result, **security has been established as a technical field rather than a strategic and policy area** of an organization as a whole.

A second aspect refers to the critical nature of security obligations of individual agencies and the dilemmas they involve vis-à-vis the following three parties.

- *Host governments*

Host governments are, in principle, responsible for all security aspects of international agencies' operations. Such official security blanket is not necessarily welcomed by agencies as it may hinder the perception of neutrality of an individual agency, exert unwarranted control over the agency's movements and activities, and limit access to vulnerable groups. Rather than triggering undesired attention from state security services by being too concerned about security, agencies tend to understate their security needs to keep the host government at a distance.

- *Non-state armed groups and civil society*

In relation to non-state actors and civil society, international agencies are aware of the importance of remaining transparent and trustworthy in the eyes of local entities. Being too concerned about staff security, beyond the acceptable local norms pertaining to protection against criminal activities, can be perceived easily as hiding a more political agenda or, even worse, suspicions against local actors. Agencies will tend to model their security to local practices and customs, even though they realize fully that their security needs in conflict areas differ substantially from those of local private actors.

- *International agencies' staff*

Finally, security of personnel represents a direct liability of the agencies toward their staff under employment regulations. The determination of security risks may well trigger incommensurable consequences in terms of an agency's relationship with its own staff. In other words, the more determinate the security risks appear in any given situation, the more definitive the obligations of the agencies are to provide security to its staff. **Although agencies are understandably not requested to provide absolute security to their staff in conflict areas, there are no clear indications of the amount of security they *should* provide.** In this context, the professionalization of security can carry significant operational and financial liabilities for international agencies in terms of assessment, analysis, protection measures, and preventive evacuation and relocation.

Against this background and despite the growing need for coherent approaches to security management, international agencies have, nonetheless, spent limited time and resources in developing proper security strategies. Existing approaches are, as it is, a result of mixed operational practices that combine different sets of strategies, which vary from one agency to the next.

Current strategic approaches to security

The current strategic approaches of international agencies to security can be identified as deriving from one of two schools of thoughts (or a combination thereof): (i) a system-based security approach, and (ii) a community-based security approach.

System-based security approach

Under the system-based security approach, security relies on the implementation of strict security standards and procedures by all the agencies involved in a conflict area. In such an approach, the security of each member depends to a large extent on the security of all the others. System-based security is at the core of the UN security system where the UN Security Coordinator, the IASMN and the security apparatus in the field are designed to function as a network of security operators operating in parallel to UN operations and providing guidance and standards on all security issues. The key components of this approach are as follows.

- Security threats are perceived as a given reality against which agencies need to be protected. These threats need to be assessed and counter-measures need to be planned by security experts. The focus, here, is on the threats and on protection measures to be implemented, rather than the sources or motives of the threats.
- The security response is based essentially on centralized generic standards (e.g., the UN Minimum Operational Security Standards (MOSS)). Field operators are responsible to external/HQ entities for the proper implementation of these standards.
- The system is rational and easily scalable, depending on the amount of resources available to ensure compliance with system-wide standards and procedures. Security capabilities are easily deployable and mobile pending the availability of resources.
- The system is based on dedicated military or security expertise that can import and adapt lessons learned in military operations (on security of people, premises, transportation or communication).
- The system can easily be integrated into larger security systems of the international community. A system-based security is often driven by (or the result of) an already existing peacekeeping or peace enforcement mission, which can be activated in times of emergency (for example, to undertake an evacuation). It is also part of a modus operandi on security with political actors of a peace process that can guarantee a proper security environment for the international agencies. In this context, security of staff is not simply a mean to an operational end, but becomes an end in itself, as an integral part of a larger international political and security agenda. Inversely, a failure of the system can endanger wider humanitarian, development, and political efforts (e.g., deliberate attacks on UN HQ in Baghdad) and result in the withdrawal of staff.

The shortcomings of such system are threefold.

- A system-based security approach depends largely on quality risk assessments. System-based security requires strong intelligence capabilities to function properly. These capabilities can hardly be deployed by international agencies due to political and legal restrictions imposed by host governments, or at the level of the international community. As a result, military experts are often unable to take proper protection measures due to the lack of intelligence information. Paradoxically, the implementation of tighter security measures often results in limiting interactions with the population and potential sources of threats, hindering further the capacity of agencies to assess their security environment.
- System-based security responses are essentially reactive and amorphous. In the absence of proper intelligence on security threats and in view of limited capabilities to engage in a dialogue with the sources of the threats in a preventive manner, international agencies are easy ('soft') targets with few capabilities to build their security capital on a system-wide basis.
- Unless additional military capabilities are available, system-based security can easily be out-gunned or overrun by any armed group that finds it advantageous to chase the international agencies out of the conflict situation.

Community-based security

Community-based strategies adopt a different approach to security. Under this formulation, security is defined as the product of a relationship with the community of beneficiaries and actors to the conflict. Security of staff derives, in this context, from the *acceptance* of the presence and activities of international agencies by all those who can affect the security of these agencies. This approach has been adopted by such humanitarian organization as the International Committee of the Red Cross and other non-governmental NGOs active in conflict areas. The key elements of this approach are as follows.

- The security of staff starts with the prevention of threats, addressing directly potential sources of risks and negotiating access to vulnerable populations. The focus is on the sources of the threats and the means to prevent their emergence.
- Consultations with community interfaces as well as representatives of parties to the conflict are essential components of this approach. Communication and transparency are the primary tools of security management processes.
- In this context, organizations must be in a position to articulate a clear and acceptable mandate and explain the purpose of their activities to the communities involved. Their activities need to be focused on clearly identified humanitarian or developmental aims and maintain strictly neutral goals. The delivery of services must be recognized as impartial, following strict and transparent need assessments.
- The role of the humanitarian operators is central. Their expertise in building trust with the parties and within the population plays a critical role in securing the operational groundwork for the agencies' activities.
- Security is not an end in itself. It is aimed at providing life-saving assistance to vulnerable groups. It needs to be re-assessed constantly to determine the level of risks

any organization may tolerate regarding the critical nature of the needs to be served. Above a certain level, an organization may be willing to accept heightened security risks only in the face of critical humanitarian needs. As these needs are reduced, or in otherwise less dire circumstances, rational actors will demand a corresponding drop in their exposure to risk.

The shortcomings of this approach are fourfold.

- Community environment plays a central role in providing secure grounds for agencies to operate. However, international agencies are not community-based. Their agenda is defined most often by international entities and their funding is provided by foreign donors. The constant pressure for distinctiveness in terms of mandate and visibility contradicts, to some extent, the need for community adherence and exchanges.
- Communities are in a position to guarantee the security of agencies only to the extent they are themselves safe and secure. Global/foreign threats and organized crimes are often beyond the reach of community-based security guarantees. International agencies are especially vulnerable to external threats as the community-based security approach limits their ability to put together close protection measures in community settings. Once an agency turns to the community to ensure its security, it starts sharing the risks faced by community members.
- Acceptance by the community is elusive. A difficult notion to measure and test over time, it can also be misleading. Communities of beneficiaries may not have a choice of accepting or rejecting humanitarian assistance. Acceptance does not automatically engender security guarantees. Acceptances by governments and armed groups alike are also dictated by political and security strategies that evolve over time, further emphasizing the limited relevance of acceptance strategies as a long-term tool for security. Communication strategies and negotiation skills remain critical tools to enhance the security of staff in these circumstances
- Community-based security is not scalable and replicable without the availability of qualified individuals to engage in a dialogue with the parties to the conflict and develop the necessary personal networks. Community-based security remains most often centered on individual operators that are able to integrate communication, programming and security goals of agencies in a coherent manner. Experienced individuals are difficult to find and deploy on short notice. Furthermore, the reliance on individual professionals may mislead the organization in the belief that operational security results directly from the deployment of a specific group of experienced individuals, underestimating the evolution of the security risks and the need for institutional response and evaluation strategies.

III. DEVELOPING NEW SECURITY STRATEGIES FOR INTERNATIONAL AGENCIES

In view of the increased pressure on agencies at both the systemic and community levels to improve their security response, international agencies have to look for new strategies to enhance the protection of their staff. In recent years, international agencies have tended to develop hybrid approaches to security, relying at times on system-based strategies, and at other times, on community-based strategies (e.g., Military officers of the Provincial

Reconstruction Team (PRTs) in Afghanistan negotiating security arrangements with local militia leaders or, inversely, humanitarian operators in the Gaza Strip being outfitted with close protection equipment, such bullet-proof vests). Although this alternation has allowed agencies to gain much needed flexibility, it remains unsatisfactory over time, as it does not yield a coherent and replicable security strategy.

Ultimately, the two schools of thoughts are contradictory. On the one hand, system-based security is essentially reactive and relies mostly on external security resources, focusing on military aspects of security, and providing a centralized and coordinated system of protection. On the other, community-based security may offer the best-known method of prevention of threats. However, it remains rarely scalable and replicable. It also generates confusion in terms of security standards in any given situation. Locally devised strategies such as promoting the participation of communities in programming and enhancing the role of national staff in security management are not part of any systemic mechanism, leaving limited opportunities to evaluate their effectiveness in terms of security of staff over time and among agencies.

Evidently, neither approach offers a definite solution to the security needs of international agencies. The improvised mixing of the two is not a long-term solution. In fact, such mixing appears to have contributed to the current anxiety of international agencies regarding their security systems, where both community and standards-based approaches are no longer trusted to provide the necessary security for operational staff. Still, if combined properly, the incorporation of the two approaches could offer interesting synergies. However, such blending cannot be merely reactive to circumstances, setting up a wall here, developing a dialogue there. The approaches need to be married in the form of an integrated strategy for security, which can be evaluated and adapted to new circumstances.

What is specifically needed is an integrated security management system that can provide common professional and cultural grounds for the development of sound security strategies. This 'common' security culture must be based on the understanding of the composite nature of the mission of international agencies. International agencies, being humanitarian, developmental or political, are all driven by an internationalist agenda toward assisting local communities in times of conflict. The security of their operations depends as much on a standardized and well-integrated system-wide security strategy as on the support and participation of communities in implementing the security requirements of agencies.[6]

[6] This combination is, in that respect, akin to the work of public health organizations and their strategies. Like security strategies, public health strategies are not aimed at the eradication of specific threats or the treatment of specific illnesses. Rather, the strategies aim specifically at the *reduction of the vulnerability* of population to health threats. Threats to public health are not perceived as stand-alone risks but as the product of both external agents (bacteria, viruses) and communal behaviors that allow these agents to prosper and threaten the health of individuals. What brings public health together as a domain is the dedicated *professional character* of the field. A profession that is based on solid system-based replicable strategies (e.g., public health as a scientific and professional field) as well as community-based interventions (community health programs).

Modeling an Integrated Security Management System (ISMS)

Based on the preceding analysis, this paper suggests an innovative model for the creation of an integrated security management system (ISMS). Such system could be put into place within each agency to serve the needs of the respective agency for tailored security strategies, and to provide the common professional grounds for the establishment of a concerted security framework among international agencies.

The dynamic character of insecurity

The starting point of an ISMS is its ability to integrate all the elements of the security response of international agencies into a defined model, from the management of risks to the mitigation of damages. This integrated approach responds to the intrinsic dynamic of insecurity. The latter is the product of a dynamic sequence of factors and events:

RISK FACTORS ⇨ OPERATIONAL THREATS ⇨ SECURITY INCIDENT ⇨ LOSS and DAMAGES

Risk Factors: Any operation faces a series of risk factors, from the most benign (e.g., desert environment) to the most serious (e.g., proliferation of small weapons). These factors need to be assessed and analyzed continuously to provide the necessary information to the operational managers on the conflict environments in which their staff will operate.

Operational Threats: The risk factors become relevant to the security managers as they contribute to the emergence of actual operational threats against international agencies (e.g., threat of an attack against a relief organization.) The operational menace is the realization of several of the risk factors at a given time and location. Evidently, not all perils are stated expressly. However, depending on the location and various risk factors, operators will agree that most often threats are communicated to the agencies before a security incident occurs. It is important in this context to be able to interpret this communication and react to it in a proper and timely manner.

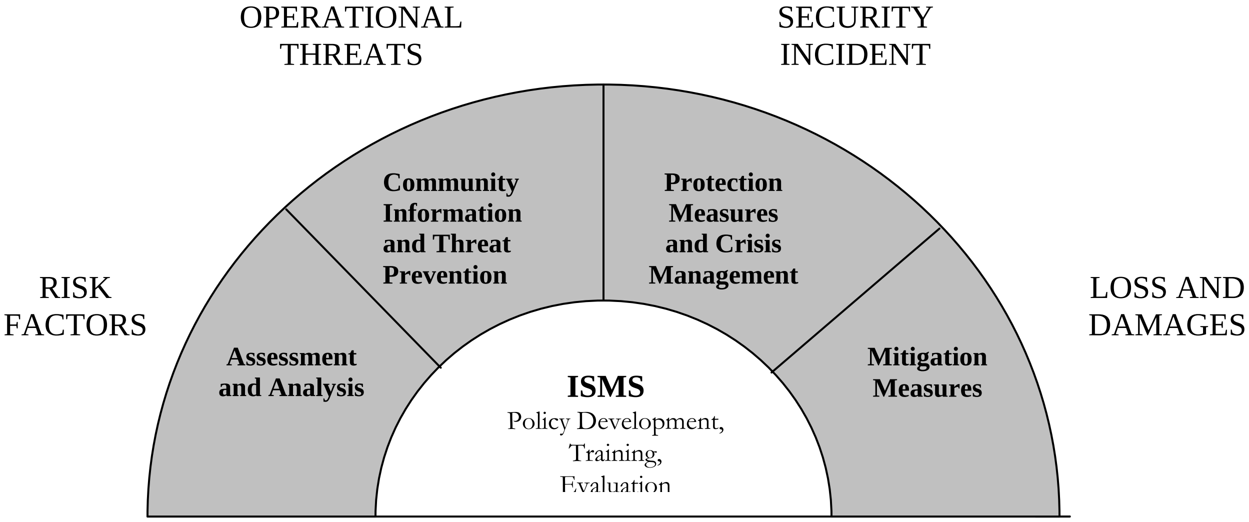
Security Incidents: Many threats are not carried out. Only a few result in security incidents (e.g., ambush of a relief convoy). A key aspect of security analysis is to evaluate the quality of the threats received and the capacity and willingness of the protagonists to implement their plans.

Loss and Damages: Finally, incidents result in various types and scope of loss and damages (e.g., injury to truck driver, stealing of goods). In some situations, protective measures may successfully prevent the occurrence of any substantial damages.

A key aspect of the dynamic of insecurity is the interdependence between the various sequences of factors and events. Evidently, not all risks factors will result in a security incident. However, all loss and damages resulting from a security incident can be traced to an actual threat and to a series of risk factors. This interdependence is at the core of an ISMS, as individual elements of the security response build on one another to create a common security strategy.

Building an Integrated Security Management System

Creating an integrated security management system does not require substantial new resources. It focuses mainly on making current resources and expertise work together.


OPERATIONAL THREATS
SECURITY INCIDENT
RISK FACTORS
LOSS AND DAMAGES
Community Information and Threat Prevention
Protection Measures and Crisis Management
Assessment and Analysis
Mitigation Measures
ISMS
Policy Development, Training, Evaluation

At the core of an ISMS stands a standard-based, centralized planning and policy structure that provides guidance and strategies to a set of security sectors located at the periphery. The central organ bears the responsibility of evaluating the performance of each security sector and, if need be, dispatching internal investigators to enquire on potential failures of the security system. The central ISMS should be staffed by security experts who can provide the necessary guidance and training to security and operational staff at the field level. This group of experts should be composed of both individuals with a military/police background and experienced operators from the humanitarian and development community.

Under such an ISMS, the responsibility for the implementation of the security measures is located at the field level (gray area) and implemented by field operators. These operators should be trained to fulfill security responsibilities; however, they do not need to have a military or security background.

Each of these security sectors has an equal value in terms of priority, as any gaps among them endanger the integrity and efficacy of the whole system. These responsibilities and competence per sector include:

Risk Assessment and Analysis

Security and operational managers should be entrusted with the responsibility of assessing and analyzing a series of identified risk factors according to policy guidelines from headquarters. These analyses should provide practical recommendations to operational managers at the local and regional levels to address the sources of insecurity through threat prevention or protection measures. These assessments should be conducted as part of the regular programmatic assessments undertaken by the agencies and should not revert to intelligence (i.e., covert) gathering methods. The results of these assessments should also be shared with other security sectors and organizations.

Community Information and Threat Prevention

Taking stock of community-based approaches and experiences, operational managers should be given clear objectives and messages in terms of communication to the community both at the capital and field levels regarding their operations. The results of these exchanges should be documented and shared with the other security sectors.

Protection Measures and Crisis Management

Based on the risk assessments and exchanges with community representatives, appropriate protection measures should be in place to ensure the security of staff, premises, transportation and communication. For each of these fields, specific standardized policies should be implemented based on the ISMS guidelines produced at headquarters. In time of crisis (i.e., in the course of a security incident), contingency planning should be implemented for the preservation of critical assets. Training and drill exercise are key components of such security preparedness.

Mitigation Measures

The responsibility of the security system does not end with the conclusion of the security incident. It must also address all the logistical aspects of the mitigation measures pertaining to minimizing the consequences of a security incident. In terms of human resources, these responsibilities may include emergency medical treatment, post-traumatic stress consultations and evacuation. In terms of physical assets, it may include collection of residual assets, upgrading of protection measures and security response, evaluation and investigation. The two last elements are of special importance both for dealing with the compensation of the injured parties and for the evaluation of potential security lapses that may have occurred.

This model for an ISMS puts into place both system-based and community-based approaches and merge them into a common security strategy for international agencies. Under an ISMS, operational security needs are divided into four discrete fields of activities, from risk assessment to mitigation measures, each with its dedicated policies and strategies. These respective activities provide for the establishment of a clear, credible, and professional security system based on scalable and replicable strategies. As with other security approaches, an ISMS is unlikely to provide absolute security, but it will provide **a coherent**

and integrated method to reduce the exposure of staff to security risks across agencies and situations.

Conclusions and recommendations

This paper has presented a first set of observations regarding the increased insecurity affecting international agencies working in conflict environments and their response mechanisms. It aimed to trigger a debate on common security strategies that will go beyond the reaffirmation of current approaches and will **generate the necessary prospective thinking to address emerging threats against the security of staff.** It proposed a model for an integrated security management system serving both system-based requirements and taking advantage of community-based strategies.

In the final analysis, one should note that emerging security threats present unique challenges to international agencies that not only endanger staff and operations, but affect as well their historical existence as independent organizations. It may be argued that the ultimate test of operational relevance resides with each organization's institutional capacity to protect its personnel. Political relevance and operational sustainability will, thus, require that international agencies engage seriously in developing both their security capabilities and their strategies to address the sources of insecurity for the sake of all staff engaged in current and future crises.

Recommendations

The establishment of a coherent and integrated security system is a long-term and demanding goal for international agencies. Presented here are some recommendations to orient the efforts of the senior management in terms of the development of the necessary strategic capabilities.

The centralized development of security standards

One of the strengths of system-based security strategies is the rational, scalable, and replicable character of systemic security arrangements. Although these systems have been using resources intensively, they have been offering demonstrable results over time and provided solid grounds for the development of a proper security culture. It is imperative that agencies allocate the necessary resources in the development of a set of robust security policies as well as training their personnel not only on security technique but also security management skills. Topics for policy research include:

- communication/negotiation techniques and strategies for seeking secured access,
- role of outsourcing and local participation in programming and security building,
- size and pattern of deployment as part of a security strategy (is smaller safer?),
- alternative methods for community-based security assessments,
- use of information technology in risk assessment and analysis,
- sharing of security responsibilities between headquarters and the field, and
- staff management in high-risk environments (issues of compliance with security regulations).

These security policies should be developed in an objective and critical manner, to be compared with other agencies and with other fields of international private and public activities. Equally, these policies should be evaluated by external authoritative experts from various fields of expertise (military, police, intelligence, private security firms, insurance companies, and so on). Agencies should also promote a scientific debate on security issues comparable to other fields of security studies, as a way to stimulate scholarly research on these issues at they pertain to their operations in conflict environments.

The professionalization of security operators

This effort relies largely on the creation of a professional security network engaging operational planners and managers at both headquarters and in the field. All senior managers with security responsibilities should be trained in security management, in addition to their all-staff training in security techniques (for instance, response to attacks, surviving hostage taking, and emergency procedures). These management skills should include:

- situation analysis and risk assessment,
- development of preventive security strategies,
- design and implementation of security regulations,
- provision of physical and psychological protection to staff,
- building crisis management capabilities,
- monitoring and reporting of security incidents, and
- managing the effects and consequences of security incidents.

To promote inter-agency cooperation and exchanges in this area, the senior management should consider submitting their training curriculum to a certification process by an independent board of experts that would review and advise agencies on the professionalization of their security system and activities. Donors could also play a role in promoting compliance of international agencies with the certification process.

The development of a common professional security culture

Finally, efforts should be devoted to promoting a new security culture among all professionals involved in conflict areas that would facilitate the integration of security considerations into the programming of the agencies' activities. The security of one is more than ever dependent on the security of all, regardless of the nature or scope of activities of international agencies involved in conflict areas. Assumptions that some organizations are safer or even immune from attacks because they carry a distinct emblem, or belong to a specific religion, ideology or national origin, have to be discarded. Evidently, different types of activities may warrant different security and operational strategies (for instance, ICRC frontline operations may require more stringent confidentiality rules than human rights observers in the country). However, the overall success of all these strategies depends ultimately on the professionalization of their management, the common recognition of their interdependence and the respect of core security standards in terms of training and behavior of staff at the field level. Professional training at all levels should incorporate these new security concepts and encourage a dialogue on the security of staff and its implications for all those concerned.