Cite as www.jha.ac/articles/a060.pdf

BEYOND SECURITY *PLANNING*: TOWARDS A MODEL OF SECURITY MANAGEMENT

COPING WITH THE SECURITY CHALLENGES OF THE HUMANITARIAN WORK

Luis Enrique Eguren

SUMMARY

The challenges faced by humanitarian agencies working in violent scenarios pose the need for comprehensive and dynamic systems to cope with the security requirements. Security planning cannot answer all the questions: we must take a step further and discuss a model for security management. In this paper we propose an overall framework for a security management process and an incremental approach to security management. Both topics should allow agencies and practitioners to better undertake strategies for coping with the security challenges of humanitarian work.

SECURITY MANAGEMENT *VERSUS* SECURITY PLANNING

Some of the most effective humanitarian agencies have a Security Plan carefully stored in the fifth drawer of the senior manager desk (of course in many agencies that fifth drawer is full with other documents, and there is no a drawer for security plans). Even that Security Plan may consist of a series of protective measures, contingency plans and safety rules, which may be useful as security guidelines but do not grasp the fact that that security requires an adequate overall management, and it means much more than a security plan. Security cuts through all aspects of an agency´s work in a conflict scenario: it has to do with operations (as any targeting the agency may suffer can be consequence of its operations), with assessing a changing context (and conflict scenarios can change quickly), with flows of information (recording and assessing security incidents), with personnel (from recruiting to training and team building), with budgeting and funding and so on (for an in depth analysis of security management see Koenraad van Brabant´s manual[1] and other relevant initiatives[2]).

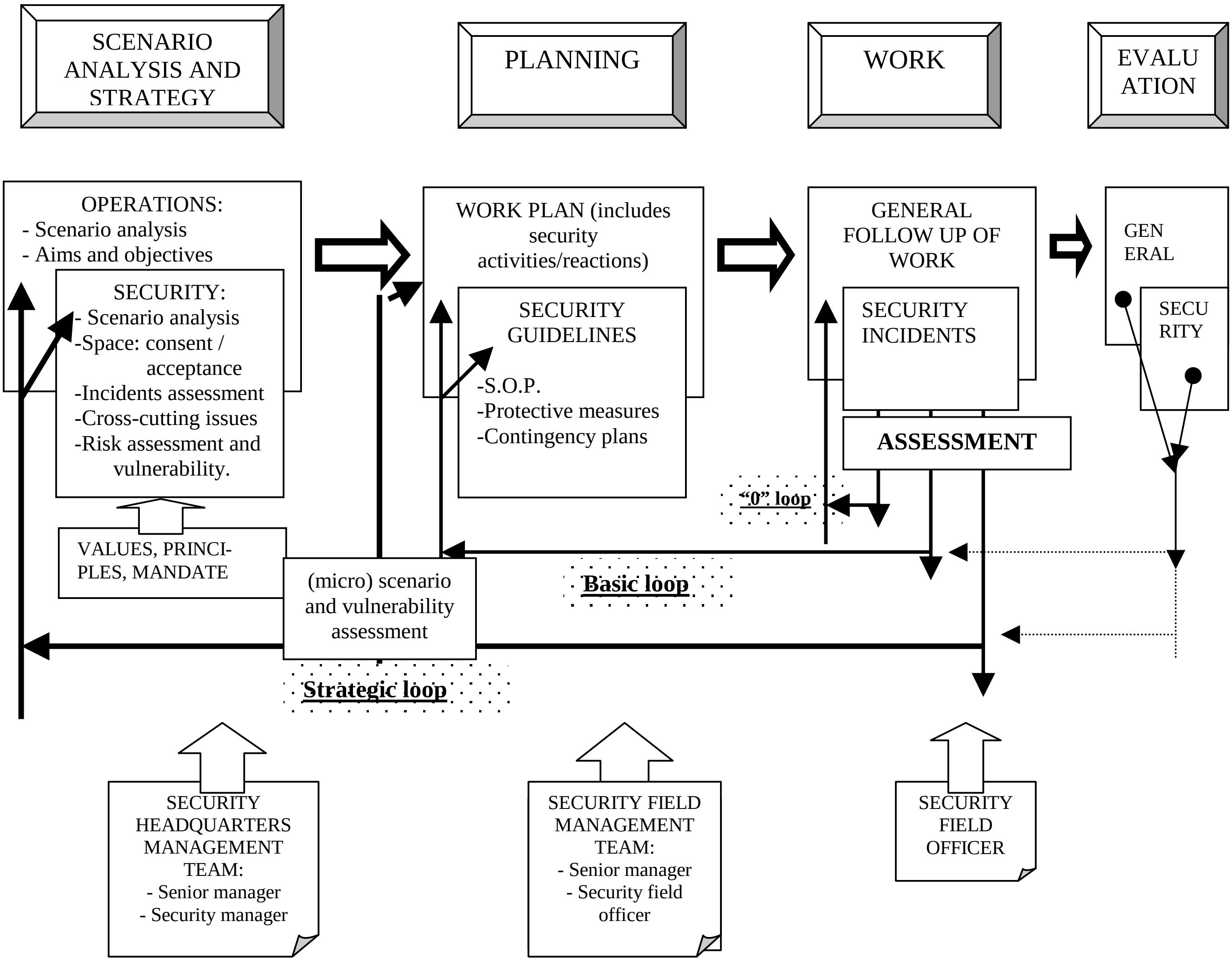
The still pending question now is: how can we handle the necessary integration of security in all the management levels of an agency´s work? We have already mentioned the security plans, which usually run separatedly from the work plans and often become a static document, disconnected from the operations or from the headquarters management activities and far from the dynamic approach security requires. But having such plans may lead to a sense of good practice in security which may prevent agencies from undertaking the necessary holistic approach to security. In other words, what we are posing here is that such security *plans* may actually be an obstacle in achieving a real level of security while working in a violent enviroment: We

[1] "Operational Security Management in Violent Enviroments" (2.000), Koenraad Van Brabant, Overseas Development Institute, London.

[2] We can quote at least the leading work in training in security management done by REDR (Registered Engineers for Disasters Relief, London) and the Interaction/OFDA initiative for developing a training curriculum in security.

need to manage security issues, instead of planning for them. Let´s visualize in the following diagram how can we achieve it[3].

MANAGING FOR SECURITY: A DYNAMIC APPROACH.



We can read this diagram from left to right, following the standard management lines (from scenario analysis to work planning, execution and evaluation). From this diagram we can visualize how security can be fully integrated into the management process of a project: Security occupies a specific niche when analyzing the scenario and setting the aims and objectives of the work, as well as when planning the work, following it up and evaluating its results. The security guidelines occupy a specific place (in the planning stage) in the overall process, where they become alive working documents which receive feedback from the follow up and evaluation stages.

[3] This diagram has benefitted from the invaluable input from Koenraad van Brabant, Jan Davis and the other attendants to a REDR workshop on reviewing REDR security management course (May 2000).

We can also read the diagram looking at the three security loops, which feed into the process from the records and assessment of the security incidents.

The “0” loop means that no action is taken after a security incident: it may be because there is no need for a reaction or because no action is taken.

The “basic loop” allows for the assessment to feed into either the security guidelines (at least) or the work plan (preferably). The basic loop allows for producing certain security actions and reactions which may create or develop the security guidelines; this is the case, for example, when after a security incident (let´s say a bomb threat) the agency prepares a standard operation procedure for dealing with bomb threats and an evacuation plan. If the basic loop feeds into the work plan, it may allow the agency to consider changes or adaptations in its work plan, so that it can react to the bomb threat and perhaps stop the activity that prompted an armed actor to threaten the agency in the first place.

The “strategic loop” takes the process a step further, allowing the security incident assessment to feed into the scenario analyses and strategy stage; following the former example, if the agency has the mechanisms for the strategic loop to function (work teams and ad hoc agendas), it would allow the agency to consider the impact of its programme on the objectives and interests of the armed actors, and design an ad hoc strategy to either continue with its programme whilst protecting its space of work or to change its programme, taking into account other variables (like vulnerability) as well as its principles and mandate.

As we can see, the basic loop is the minimum process for allowing an also basic security process to work (provided that some basic documents and procedures -like contingency plans or protective measures- exist and are complied with). This basic loop is the one you can find functioning in most of the institutions in the field, often in an incomplete way (for example not having some contingency plans, or not having established mechanisms for the assessment to feed into the work plan). The basic loop is also important because at least it allows the agency to have an incremental process for developing security procedures: no agency starts working in the field with an overall security process, and the capacity to improve it gradually is fundamental for achieving a basic security practice.

The strategic loop (assuming that the basic loop is also working) is a powerful tool which provides the agency with the right approach to security management, as it allows managers to make well informed decisions to prevent the main aspects of vulnerability when designing the programme (especially the impact of the programme in the conflict scenario).

The lower layer of the diagram allows us to see who is in charge of what in security management, from the field to the headquarters level. Sometimes there is a field security officer in an agency, but less often you can find a security field level management team (and rarely you can find such a security team at the headquarters level). These teams play fundamental roles in allowing the feedback mechanisms to work.

The time sequence shown in the diagram may suggest that the security management team can only analyze the scenario and make major decisions once or twice a year. For the sake of clarity, the diagram is designed showing one cycle of the process. But of course the cycle can be repeated (fully or partially) several times a year, provided it is necessary (for example in a high risk area): that is the function of the diversion of the "strategic" loop, named "(micro)scenario and vulnerability assessment". Its position (in the middle between the programme level –headquarters- and field level –work plan-) means that such assessment may require the participation of the field level security management team, as the leading team for this purpose, together with the security officer at headquarters

COPING WITH SECURITY CHALLENGES: SECURITY MANAGEMENT AS AN INCREMENTAL PROCESS

In terms of security so much cannot be predicted that it is essential to be able to react rapidly when a security incident occurs. Security management is never finished and is always partial and selective. It rarely can attempt a comprehensive, long-term view: Its contribution relies on its ability to prevent incidents and to point to the need for organizational integration and coordination to cope with such incidents. Maybe this is not very ambitious, but we also have to take into account that few resources are usually allocated for security, so that we never can be comprehensive. Pragmatism is a must in security management.

As we mentioned before, when reviewing the security practice of an agency you always find some kind of security guidelines or plans or measures or patterns of behaviour in progress. There are many forces at stake, from stereotypes about security practice to a reluctance to increase the existing workload by incorporating new security activities. Security practice is typically fragmented, evolutionary and largely intuitive. In terms of security management it is necessary to proceed step by step, making incremental changes to improve performance. Security strategies and procedures tend to emerge from "strategic subsystems", each of which covers a specific area of work (logistics, a field team specially concerned with its security, a headquarters manager under pressure by donor´s concerns for security, etc.). Incrementalism[4] in security management opens the door to informal processes and allows space for nucleus of change agents at work. Precipitating events (such as security incidents) prompt urgent, interim decisions that shape the security practice and that, if properly managed, becomes part of a widely shared consensus for action among members of the field and management teams.

How can all this be managed in order to achieve a good security practice? There are limits that constrain the system[5]: cognitive limits (not all factors affecting security can be aggregated and treated simultaneously in order to arrive at a holistic decision) and process limits (the timing and sequence imperatives necessary to create awareness, develop consensus, train people, ensure an adequate personnel turnover, implement activities, etc.). Therefore almost all of these subsystems and practices must be managed and linked together by a conscious incremental approach: security can be dealt within

[4] There are many studies about incrementalism and strategic planning. The approach reflected in this document draws on the work by C.E.Lindblom and James B. Quinn, among others.

[5] Quinn, James B.: "Strategic change: logical incrementalism". Sloan Management Review Summer 1989 (pp. 45-60)

the logic of each "subsystem", so that a consistent pattern can be maintained among the security decisions and activities implemented in that subsystem. In the overall system, broad security goals and policies will be set, so that they can accomodate a variety of specific activities and proposals from below, handle urgent matters, respond to unforeseen events and react to security incidents. Adequate security management links together and brings order to a series of security processes and decisions spanning years, learning from failures and building on good practices and succesful outcomes. As shown in the previous diagram, such security management follows a dynamic process with neither a real beginning nor a real end, but one which develops into a highly efficient and cost-effective system.

For a system of security management to be incremental, it requires that the basic and strategic loop are in operation. The basic loop can be developed improving the existing security practices and allowing and promoting the implementation of new ones, as well as making space for this loop to feed into the work plans (down-top approach). The strategic loop requires headquarters management decisions to be implemented (top-down approach), generally involving several management bodies (policy, programmes, funding, etc.). These relationships can be reflected in the following matrix, showing the incremental levels of implementation of security management activities:

		minimum	low	medium	high
Strategic loop	Scenario and programme assessment periodical and adaptable	Not in operation	Not in operation	Not in operation	Working
	Scenario and programme assessment in fixed terms	No security as a regular point on the agenda	Incidentally security is a point on the agenda	Security as a point on the agenda	Security as a point on the agenda
Basic loop	Work plans reviewed according to security	Work plan reviews prompted occasionally by security incidents	Periodical work plan reviews under the point of security	Periodical work plan reviews under the point of security	Periodical work plan reviews under the point of security
	Security guidelines and procedures	Some security guidelines in operation	Many security guidelines in operation. Security officer assigned.	Most (reviewed) security guidelines in operation. Security officer Compliance checked	Most (reviewed) security guidelines in operation. Security officer Compliance checked
		Basic security management		Strategic security management	

CONCLUSION

Security management confronts the risk of violent and rapidly changing scenarios and addresses the vulnerability of humanitarian agencies in the midst of such a risk: It therefore must be a dynamic and “ever green” system, a framework to guide and provide consistency for future decisions made incrementally. To act otherwise would be to deny that further information could have a value. Security management becomes the interface where strategies and work plans meet armed and violent challenges, the “living” interface which allows the agency to cope with unforeseen events and at the same time provide a sense of stability to humanitarian work.

Luis Enrique Eguren, MD, works as Coordinator of the Colombia Project of Peace Brigades International. He is also an independent consultant and trainer in several areas, being among them security and protection in humanitarian work.

(Note: with thanks to Julia Metcalfe, who reviewed the translation and style of the first version in English)