

FACT FINDING TRIP TO AFGHANISTAN AND INDONESIA

Prepared by Melissa Ong and Bob Schmitt, December 2, 2005

Background

The Crisis Management Initiative and the United States Institute of Peace have collaborated on a venture to improve the safety of civilian personnel responding to international crises. This venture is entitled the “Safety Information and Reporting Service” (SIRS). SIRS was developed as a response to a series of international conferences on the role of information and communications technologies in international crisis management.

The project team focused on a proposal to field an incident-mapping and reporting service. But in order to test the validity of this idea, the project team conducted a series of consultations with NGOs, UN agencies, other international governmental organizations, and national government officials. It became clear during the consultations that the idea of developing a “one-size-fits-all” was not feasible, and therefore the focus became attempting to identify a core suite of technologies that could be scaled to meet the demands of diverse safety environments based on the nature and intensity of perceived threat.

To better understand the issues involved in the venture, the project team decided to choose two contrasting safety environments to investigate the likelihood of the proposed core technologies to make an impact on improving the safety of civilian crisis response personnel in the field.

This decision led to the deployment of a fact-finding mission by the SIRS project coordinator, Bob Schmitt, and humanitarian consultant Melissa Ong. The team traveled to Afghanistan and Indonesia in October and November of 2005 to observe the operations of the Afghanistan Non-Governmental Safety Office (ANSO) and compare it with the operations of the NGO Security Forum in Banda Aceh, Indonesia.

Afghanistan and Indonesia were chosen as assessment targets primarily to compare and contrast the two different types of organizations (formal vs. ad hoc), and because they represented two contrasting examples of security/safety environments. Afghanistan would, by anyone’s measure, be classified as an insecure environment, with 24 violent aid worker deaths in 2004, and over 38 violent aid worker deaths in 2005.

Banda Aceh, by comparison, had fewer than a half-dozen aid worker deaths, primarily from accidents. In addition, the CMI/USIP team had developed good contacts with people in Afghanistan and Indonesia and it was felt that they represented a good starting point for the investigation of the feasibility of the SIRS concept.

Bob Schmitt, the project coordinator for SIRS, and Melissa Ong, a humanitarian consultant and former program manager of ANSO interviewed over 35 people from 30 organizations during a three-week trip to Afghanistan and Indonesia. Their findings and recommendations are summarized in this trip report.

Trip Purpose

The purpose of the trip to Afghanistan and Indonesia on 19 October to 3 November 2005 was to survey staff of civilian organizations participating in humanitarian activities to find out about how they acquire

and use safety information. The fact-finding team¹ examined existing civilian safety networks to learn details about how safety data is collected, analyzed, synthesized, disseminated and employed in the field in an effort to reveal opportunities for enhancing the effectiveness of existing safety information networks.

Definitions

Our working definitions for the concepts of “security” versus “safety” are:

- Safety information includes information relating to accidents, criminal activity, acts of intentional violence, and the outbreak of infectious disease, and
- Security information includes information about intentional and unintentional threats to safety related to criminal or political violence.

However, for the purposes of this paper, we will refer to “security” issues as covering both the security and safety domains, (unless specifically mentioned otherwise).

Method

We chose to go to Afghanistan and Aceh because they gave us an opportunity to look at two very different mechanisms that were in place for humanitarian organizations to share security information. Furthermore, the threats that faced agencies in both locations varied enormously, presenting a chance for us to examine the process in very different operating environments.

The NGO Security Forum offered another model, one less formal and more collaborative than ANSO, to determine if incident-mapping technologies would be useful to deploy in the context of a natural disaster response situation complicated by security concerns.

In Afghanistan we surveyed the Afghanistan NGO Security Office (ANSO), focusing on assessing the effectiveness of ANSO as a primary and highly regarded source of information about security issues affecting civilian humanitarian organizations. In Aceh, our focus was to understand how the NGO Security Forum worked. We also assessed the effectiveness of the forum in facilitating the sharing of security information.

We formally interviewed 35 people from 30 organizations in Kabul and Banda Aceh, and spoke with dozens more in informal settings. This included individuals from for-profit companies, NGOs, government officials and individuals working for private security firms as they also contributed to ANSO as a source of information and received reports as consumers. The organizations represented in the formal interviews included a diverse selection of NGOs, commercial concerns, national representatives and international agencies. We interviewed organizations of varying sizes and missions, some with multiple locations in country, others with single locations; organizations that had been on the ground prior to current events, those who came in after a trigger event (occupation of Kabul by Coalition Forces and tsunami in Banda Aceh), and those in the process of doing pre-deployment assessments. The individuals we interviewed all had some security responsibility (e.g. country directors, programme managers) or had security as their primary roles.

The interviewees were questioned about how they learned about security incidents, whether they shared information with other organizations, how they did it (email, phone, radio, web, satellite phone), their principal observations and concerns about their security situation, their security priorities, and suggestions they had to improve the sharing of security information.

¹ The team was comprised of Melissa Ong and Bob Schmitt. Melissa is the former Programme Manager of ANSO and Bob Schmitt is the project lead for the SIRS initiative.

Background on organizations surveyed and operating environments

Afghanistan Non-Governmental Safety Office (ANSO)

ANSO was established in 2002 by a group of NGOs who came up with funds to hire a security consultant for Afghanistan. Currently, it is a \$1.2 million per annum International Rescue Committee programme that has a staff of almost 50 people and is located in 5 offices around the country. The office in Kabul acts as an information center, collecting information from the Regional Security Advisors in each of the 5 operational regions (corresponding roughly to the north, south, east, west and central portions of Afghanistan).

ANSO staff are tasked with collecting reports of security incidents, disseminating news of those incidents, and attempting to investigate the underlying reasons for those incidents. ANSO does this through an email mailing list, a phone tree, personal phone calls (if specific organizations may be affected by specific threats), and they are experimenting with an SMS list (which has been problematic). At the end of each week ANSO creates a weekly brief that summarizes incidents that occurred during the previous week, follows up with incidents reported on during that week, provides a brief bit of analysis, and then produces a color-coded threat level map of each of its five regions. ANSO also manually maps incidents.

Security priorities in Afghanistan among NGOs were primarily focused on crime (kidnapping, banditry, extortion), accidents, illness, and close behind, being directly or indirectly targeted by insurgent groups through kidnappings, shootings, IED attacks, rocket attacks, and landmines. Clearly the consensus is that Afghanistan is a high-risk environment, and most people we spoke with took appropriate precautions.

Aceh NGO Safety Forum

The NGO Security Forum is voluntary and collaborative body that was started by the Security Coordinator of a large NGO. This was established in February 2005 by Alexandre Carle of CARE as a means of sharing information between NGO security focal points.

The security situation in Aceh was far less acute than in Afghanistan. The major focus of security plans and evacuation procedures was on how to deal with traffic accidents, earthquakes, mosquito borne disease, accidents in general and the conflict between the insurgent group the Free Aceh Movement (GAM) and the Government of Indonesia (GOI). Major incidents included injuries caused during earthquakes, medical emergencies requiring evacuation, drownings at a local beach due to strong currents and a couple of shooting incidents in the late spring involving NGO staff traveling on country roads late at night.

Principal Findings

Both environments vary dramatically therefore the kind of information shared and the method used varied substantially.

1. Need for independent NGO security focal point

The most common finding was the need for a strong, *independent*, and clearly identified NGO focal point that embodied security best practices. In Afghanistan, ANSO clearly provides that role and most are satisfied with the role it plays. People wanted reports of more consistent quality, and more statistical analysis, but everyone on the ground for any appreciable amount of time knew that ANSO was the security focal point for NGOs. The situation was very different in Banda Aceh. Some NGO's knew about the NGO security forum but few knew whom to contact about it. In both locations, participants uniformly mentioned the need for a clearly identifiable NGO security focal point. Difficulties stemming from mission dissonance between security focal points and host organizations were clear from the perspective of many organizations, and most felt that the NGO security focal points would be best served by being standalone organizations. Consequently we investigated it carefully, and became

convinced that an independent NGO security focal point makes the most sense, for the following reasons:

- Security issues are politically sensitive. Host organizations feel compromised by the risks that are required to be taken to do the job of collecting and analyzing security related information.
- The administrative requirements for a mobile, aggressive data collection effort are different from an institution that moves at a more measured pace. This is reflected in issues related to employee recruitment, intake, salaries, benefits, security standards, reimbursement/cash advances, contracting for shared services, and many other facets of program administration.
- Funding obligations of host agencies sometimes put them at odds with mission requirements of security focal points.
- Decision-making speed suffers due to internal bureaucracy of a large relief organization when a quick decision is needed. Staff on both sides often felt the process was too unwieldy for the benefits received.

2. Staff recruitment, handover, and training is a critical need

Almost every problem with data collection and delivery reduced down to a staffing problem: staff transition, inappropriate staffing, inappropriate handover and/or training. Every organization we spoke with found that it was difficult to find and retain qualified security offices due to competition with private sector (who are offering up to five times the salary for equivalent work, with better R&R schedules).

3. Reliable internet access and services are expensive, difficult to acquire, problematic and a critical component

Although every organization felt that internet access was critical to establishing sustainable administrative processes, every organization had difficulty obtaining internet access and felt that a central source of information about internet access would be helpful. Most access to the internet in both places was acquired through VSAT uplink to remote hosts, and most of the sites investigated were many “hops” away from primary internet backbones. Further, most organizations did not have expertise to acquire and retain reliable vendors. Consequently, we heard many stories of inaccessible mail servers, web servers that did not work or were not accessible for long periods of time, poor technical support, and unreliable access to the internet.

4. Field communications are problematic, especially backup communications

In both locations, commercial mobile phone services were the primary method of communications. In virtually every case for first responders, groups used satellite phones for initial communications and switched to mobile phones when the services became available. In both locations, the availability of radio communications was hampered by obscure government procedures and was characterized by lack of frequency coordination: frequencies are acquired on a first come, first serve basis.

Almost everyone surveyed admitted that mobile phone networks became useless in emergencies and that a radio backup would be extremely useful. However, there was significant disagreement about how it could be reliably implemented. Ideas ranged from the security focal point providing a set of NGO emergency frequencies and manning a 24 hour radio room to where people felt that if things got that bad, everyone would be evacuating making radios communications unnecessary.

Most NGO's were haphazard in their use of radios as primary or backup communication mechanisms. Many of the larger NGO's had formal radio check in processes, and their staff kept their radios handy, and charged. In other cases, staff had radios but never tested them and were never trained in how to use them.

A further finding was that lack of accessible radio management and programming skills, and host government bureaucracy/politics play a major discouraging role in developing this resource. Cost was

less an issue than coordination and access to expertise. Every organization interviewed felt it would be useful for the security focal point to have a strong IT / field communications component to help outline options for security communications.

5. Everyone used multiple sources of information, but relied on the NGO security focal points for the “first, best” information

In both locations, NGO’s (as well as other types of organizations) looked to NGO security focal points to provide the first information on incidents, and expected them to provide good analysis of those incidents. Further, especially in Afghanistan, the NGO security focal points were perceived as having some of the best information available related to civilian humanitarian security issues.

6. There was a willingness and expectation to share security information.

In Afghanistan, everyone we interviewed said they shared information with ANSO and people felt they were providing an appropriate and valuable service for the present conditions in Afghanistan. In Aceh, there was also a willingness to share information however there was some confusion as to how this should be shared due to a lack of NGO security focal point that is known to all.

7. Because security focal points exist, expectations for them to provide emergency response services is very high

In both locations, once an organization gained the reputation for being a security information focal point, expectations were raised among NGO staff that they could also serve as a an emergency response organization. This is a difficult expectation to counter, especially when the focal points often DO provide response services to some extent. One of the issues associated with ANSO’s position and success is that people expect them to deliver much more than they are set up to and can reasonably expect to deliver. We found that most NGO’s thought of ANSO as a first-line emergency dispatch operator if their staff encountered problems in the field (car wrecks, evacuation). Part of this has to do with the personal nature of the data exchanges: when people have something to report, they call. When ANSO has something critical to report, it calls affected parties. The relationships are primarily personal, and very distantly, institutional.

8. One of the responsibilities of NGO security focal points is civil/military/governmental liaison

Especially in Afghanistan, it was taken for granted, by everyone, that an appropriate role for ANSO was to work with all types of organizations that had a stake in humanitarian security. Many NGO’s were happy for ANSO to liaise with the international and national security forces, UN DSS and the embassies. ANSO has significant relationships with local government authorities and maintains significant contact with UN agencies, Coalition Forces and ISAF, and foreign government agencies. Similarly, people at the UN, in foreign embassies and in international military forces saw ANSO as being the NGO security focal point. Interviews with those agencies revealed significant respect for the work of ANSO and the professionalism of their staff and services. Everyone we interviewed ranked ANSO as the most reliable, consistent, and timely source of information about security incidents involving civilian humanitarian workers.

9. Funding mechanisms provide interesting obstacles and opportunities

The nature of donor funding results in highly creative responses to getting mission related needs met. Some organizations dump all of their computer and communications equipment in a ‘security’ budget, while others feel that they need to distribute hardware, training and staff costs to other programs. This often leads to strange management and reporting relationships. Perhaps more importantly, it obscures the “true” costs of providing effective security. There does not appear to be a standard approach for defining and funding security management.

10. Everyone had difficulties obtaining appropriate medical/evacuation insurance, and developing evacuation plans

Most organizations had some form of medical/evacuation insurance and evacuation plan, however it was clear that people were doing their work without much confidence that these would be much good in

case of an emergency. In Afghanistan, getting EMT and stabilization care is problematic, getting long-term care, unreasonable and getting evacuated quickly to a high-quality medical facility uncertain. Acquiring insurance is often a significant administrative hurdle, even for organizations that have standing relationships with insurers.

11. Everyone used some form of incident-mapping and it's value was perceived as critical but no one had the capability to continually provide updated maps and statistics

Virtually every interviewee felt that a current map that pinpointed recent incidents and included threat levels would be very useful as overview instruments. All offices that we visited had incident and security maps tacked up on walls. Most were hand drawn, with pins marking resource locations or incidents, or had areas marked off as insecure areas. Many directors complained of the volume of incident reports they received, and mentioned that they wished there was more focus on making relevant incidents (those that happened in the same locations as their field offices) more accessible.

UNIMS in Banda Aceh came the closest to providing high-quality incident reporting maps, but those were only available to UN agencies and were not to be distributed widely.

12. Almost every country director mentioned the need for incident statistics for assessing their own security plans and for inclusion in funding proposals.

Tabular reports of incidents by type and location were almost uniformly mentioned as being a data need that was not being filled.

13. Data management resources are primitive by European and US standards

It was clear that most organization's use of data management technologies were limited to the use of email and word processing documents, and the occasional spreadsheet for budget development. Neither the data providers nor the consumers made much use of existing data management tools to organize or add value to the data they routinely received.

14. Data security was a non-issue

Data that was considered to be highly sensitive was handled in face-to-face conversations, while less sensitive, but also critical information, was typically handled via a mobile phone call. Everything else was assumed to be public information. None of the individuals interviewed made use of encrypted storage, access and transmission.

15. There are few standard operation policies/practices for developing sources, collecting and reporting data

There were no little or no SOPs available for security focal points. At ANSO, interviews with regional security advisors (RSAs) revealed that while each did the same job in different ways. Therefore given the finding that one of the main complaints about ANSO was inconsistency, one must assume that the lack of SOPs is partially to blame. Given ANSO's size, responsibilities and the activity in its environment, developing SOPs is a significant and time-consuming task that is not top on the priority list. In Banda Aceh, the voluntary nature of the NGO Security Forum ensures that no SOPs have been developed.

17. Local media is a major source of information

Local media was seen as a major source of information about potential threats, actual incidents and gauging local attitudes. In both places, NGOs were actively scanning and translating local news stories however most were not sharing those translations and abstracts with each other or with their security focal points. In Afghanistan, media monitoring services were available. In Indonesia, virtually every NGO we talked to had a member of staff monitoring local media and translating significant articles.

18. Government corruption is a huge issue

In both places, had people been willing to go on the record, government corruption would have ranked at the top or near the top of security concerns. We heard story after story of extortion attempts, requests

for bribes or kickbacks, roadside “detainments” and appropriations by national police, military forces and civilian government officials. Although concerned about the subject, many interviewees were not willing to go into details for fear they would come out and they would be targeted for program termination, violence or expulsion from the country.

Relevant Observations

Afghanistan

The scope of security awareness of the people and organizations we interviewed was astonishing. Everyone was concerned about security, and for good reason. Five civilian humanitarian workers had been killed in the weeks just prior to our visit; there was a rocket attack on a town in the north that may have targeted the UN; there was a rocket attack on a CF convoy that killed civilians just outside of Kabul, and there was a threat that the criminal gang that kidnapped a CARE worker last summer was again planning to kidnap a female NGO worker.

Most NGOs observe travel restrictions and curfews, and only frequent dining establishments that appear on the UN’s “cleared” list, and even then, they are urged to stay in. Security precautions include dressing appropriately, not walking on the street individually, guards, hardened entrances to offices and living quarters, routine communication check ins, logging travel, and using approved drivers for transportation.

Nearly everyone we interviewed used ANSO as a primary source of information, both UN agencies and Coalition Forces, followed by their own sources, then UN DSS, then embassy briefings. Typically security focal points receive an ANSO report, and if it pertained to their staff, they would alert their staff and may get additional information in return. Most interviewees stated that if they learned more from their staff, they relayed what they learned back to ANSO, usually via a personal phone call to one of the staff with whom they had built up a personal relationship. The accuracy of their reports was rated consistently high by all of our interviewees with the notable exception of organizations who’s primary focus was military and UN security. ANSO was consistently rated highly, among all organizations, for being the first to report incidents and threats. There were many incidents that do not get reported, for a variety of reasons: the NGO didn’t feel it was sufficiently threatening to the NGO community as a whole or because people were afraid that the report would lead to further security restrictions.

Most interviewees stated that their preferred way to receive incident reports was by email or phone. Most preferred to report incidents by phone with someone they knew. The biggest needs expressed was more statistical analysis of threats, more investigation into specific threats, and more follow-ups on warnings and incidents.

People with a lot of experience in Afghanistan said that ANSO provide just enough information for them to be able to analyze various incidents with regards to their impact on their staff. People who had not been in country most frequently expressed the need for more analysis.

Banda Aceh

Everyone we interviewed felt that the NGO presence in Banda Aceh was welcomed by all levels of government and by the local people: a significant difference from in Afghanistan. Most people we spoke with were a little uneasy about the availability of high quality medical care, but most had plans to deal with medical emergencies. It was generally accepted that one did not drive outside the city much after dark as one would most likely encounter roadblocks by TNI or GAM setup to extort “road taxes” from vehicle occupants. People felt very safe on the streets, reporting a low crime rate due to the imposition of Sharia law. There was a strong feeling of the need to respect local customs for dress and behavior, but trying to figure out what local customs were was confusing. Cultural sensitivity has led to significant disagreements among NGOs and UN agencies and remains an area of concern.

Most interviewees felt that the peace process between GOI and GAM was proceeding better than expected, but most also felt the situation required close monitoring.

About half of the interviewees had heard of the Security Forum, but the majority did not know who the contact person was or who to contact if there was an incident or if they needed information. Most of the larger groups were following formal security procedures appropriate to the UN Phase 3 and Phase 4 designations, but most of the smaller organizations were taking few, if any, security precautions other than being culturally-sensitive, carrying a mobile phone, and avoiding country roads after dark.

One notably bright spot in Banda Aceh was the UN Information Management System (UNIMS), managed by UN OCHA. UNIMS (formerly HIC) is clearly the information focal point for relief and development efforts in Banda Aceh. This is partly the result of circumstance, and partly the result of planning and vision. The fortuitous circumstance was having staff with the right skills on the ground about 5 days after the tsunami hit, closely followed by a trailer packed with IT equipments: laptops, routers, switches, copiers, printers and an incredibly invaluable HP large-scale map printer.

UNIMS judged internet access to be less important than standing up a good field based information gathering and dissemination function, and the quickly established themselves as THE source of good information about who was doing what, where in response to the tsunami. Their most beneficial function was to run an information “kiosk” staffed by two attractive local “girls” who also knew what they were doing and were adept at extracting information from customers who stopped by to get maps, attend briefings, or use the kiosk facilities. The social aspects of the kiosk made it a catalyst for information-sharing.

When the scale of the international response became clear, UNIMS decided that it needed to transition into an organization capable of supporting long-term development efforts and began shifting focus from short-term interaction with NGO’s and UN agencies, to longer term efforts designed to strengthen the Indonesian governments ability to manage post disaster development. Towards this end, they have seconded staff to the Indonesian government relief agency, BRR to implement a national database launched on October 28 designed to register the activities, goals, and impacts of NGO activities in Banda Aceh. All NGOs are required to register their activities by November 18, in part, to allow the GOI to come up with an assessment of relief activities on the one-year anniversary of the tsunami (December 26).

ICT Observations

From the perspective of a technician specializing in structured data management systems, the degree to which ad hoc, personal, and manual processes are used to gather, process and disseminate information in the field is remarkable.

Difficulties with connectivity in the field, (bandwidth, technical support, cost) dramatically limit the degree to which these data collection and dissemination processes can be automated. But perhaps more importantly, there is general lack of understanding about how information technologies can be used to leverage existing collection and dissemination efforts. There is a strong desire in the field to be able to employ more systematic methods, but expertise and services are simply unavailable. The most advanced system we found amongst NGOs is a flat Access database that could only be queried by one person at a time.

There is a clear desire to be able to have some standards for classifying incidents, “threading” incidents, and reporting incidents so that they can be reported and compared over time and between different areas/regions/circumstances. However, there are no clear (public) standards to adopt that do this.

It was clear that larger organizations had better ICT capabilities as a result of foresight and planning. Further, the organizations that had the most to risk from security incidents (military, embassies, UN, and monitoring missions) had significant investments in ICT infrastructure and clear lines of ICT responsibilities.

A common observation was the lack of basic ICT infrastructure: electrical power, wiring, internet connections. Everyone experienced logistical difficulties getting appropriate amounts of primary or

backup power; getting generators installed; getting access to repeated frequencies, getting radios programmed, finding responsive VSAT service providers, and finding ICT technical support in general.

Conclusions

- 1) NGO security focal points were considered to be professional, reliable, and critical information providers who could be trusted to provide information critical to civilian relief and development operations. The level of professionalism we encountered was surprising and encouraging.
- 2) There was little resistance to the idea of sharing information. On the contrary, we found that the expectation was that it would be shared as long as it only reached affected parties.
- 3) There was strong support in the field for a neutral NGO security focal point whose sole mission and responsibility was to provide security information.
- 4) NGOs were still encountering significant ICT problems. Costs were still very high, and appropriate expertise difficult to find.
- 5) There was enthusiastic acceptance of the idea of incidence-mapping the point where many organizations were already doing some form of it manually, in collaboration with other actors, or had plans in the works to stand up some sort of GIS/mapping activity. The chief impediment was funding and expertise.
- 6) Staff turnover is a huge issue with organizations that led to poor institutional memory. Most felt it took a minimum of 2 months just to get oriented, and a couple more months to build effective human networks. Transitions do not typically overlap and led to a gap in the ability of various regional offices to effectively collect and analyze incidents.
- 7) There is little evidence of standard operating procedures and consistent approaches to incident reporting, security assessments and security management and planning. There were attempts to address this but with little actual results.

Given these findings, we propose the following course of action to systematically improve the safety of crisis responders on a global scale, and in Afghanistan and Sumatra in particular:

Recommendations

- 1. Establish an independent organization, governed by a board of directors of representative, principally affected organizations (NGOs, donor agencies and perhaps insurance companies) to begin to systematically address issues of standards, SOPs, pre-deployment tasks and contracting, deployment planning.**

There is a clear need for an authoritative body to begin to develop standard models for NGO security focal points, ranging from ad-hoc councils, to one/two person full-time functions, to ANSO like entities. It will take a minimum of 3 full-time staff to start this up, (probably more like 6-7 staff), to perform the following functions:

- Provide fiscal agency for NGO security focal points in the field.
- Develop fundraising proposals for rapid deployment operational modules as needed so that if there is consensus on the board for deployment, a well thought out proposals can be quickly shopped around to funders.
- Donor management and consensus building
- Board management and consensus building
- Provide management functions to quickly deploy field-based security focal point missions and increase effectiveness of security focal point service delivery in the field.

- Developing SOPs for mission deployment, network development, data collection, analysis and dissemination, and information management.
- Develop relationships with the global NGO community to promote best practices (similar to ECHO's work in this area, but applying general principals to specific environments, e.g. Afghanistan, Sudan, Indonesia, Nepal, Zimbabwe).
- Provide security education and specialized training functions in collaboration with service providers (like RedR) derived from field experiences.
- Provide ICT support to field missions.
- Negotiating IT/comms/equipment/services contracts in advance of mission deployments to jump-start the process of providing reliable ICT services.
- Provide back office logistical support for funded missions (transport, lodging, visas, insurance, supplies, services).
- Developing incident reporting and statistical data standards and tools that implement collection and reporting data standards in the field.

Deployment decisions would be made by the board and ongoing program funding would be separate from operational funding for field missions.

The three staff would be an Executive Director, a CTO, and a Development/marketing person. The main function of this staff would be creating the business model, documenting practices and creating SOPs, developing contractual relationships with data and ICT providers, building the technical infrastructure (servers, communications, data model/standards, applications); interfacing with nascent project areas (Darfur, Niger, etc) and fundraising

Once the independent organization is stood up, it would immediately pilot an NGO security focal point organization in the field.

2. Field three staff to provide ICT support to ANSO

Funding for three staff to help ANSO develop their IT functions in Afghanistan (incident mapping, website development, improve their IT and radio communications functions).

The staff would be:

- i. Trainer/documentation specialist/troubleshooter that would travel to regional offices to help with IT problems/issues and would pull together SOPs for RSAs and the Ops manager.
- ii. Database and content manager: keeps data clean, backed up, deals with servers and internet services issues.
- iii. Product manager: GIS specialist who uses data to create GIS (and other) products for dissemination:
 1. Tables of incident stats per province/region.
 2. Maps.
 3. Threat analysis charts.
 4. Security briefs that include overview plus updates on current situation for new staff AND beneficiary home offices. This would go to country directors and HQ staff.
 5. Develop an ANSO website to disseminate materials on the web.
 6. Improve management of ANSO alert lists (email, SMS, phone tree) to more carefully target customers of ANSO products.

3. Fund a two-person (one international, one national) field office in Banda Aceh to act as a full-time security focal point for the NGO community.

There is clearly a need for an identified NGO security focal point in Banda Aceh. A dedicated NGO security focal point in Banda Aceh would work closely with UNIMS to collect and compile existing incident data, security plans, foster other kinds of information sharing (e.g. a local media monitoring service), and would work with the NGO community in Banda Aceh to keep them connected with each other.

Key information products that are currently needed in Banda Aceh include:

- Medical facilities and evacuation procedures (there are significant issues getting people through Indonesian immigration and customs on emergency medical flights from Banda Aceh).
- Emergency points of contact
- Road conditions and road safety ratings
- Safety alerts and warnings: earthquake, tsunami, mosquito/water borne disease
- Incident reports in a standard format
- Incident statistics in a standard format
- Comparative threat assessments (UN vs. AMM vs. NGO)