[Part VI: Connectivity and security of the field staff]

Chapter 33: Mainstreaming security management

Summary

Security awareness and the management of risk should be a characteristic of responsible programme management. Yet there are "barriers to change" which need to be overcome for risk-management good practice to be firmly accepted.[1]

Mainstreaming good practice

RedR-IHE is a London-based NGO with over 25 years experience providing training and support services to frontline humanitarian aid agencies[2]. A strength of the RedR-IHE security programme since its inception in the mid-1990s as an inter-agency research initiative has been its focused relevance on the challenges faced by aid agencies in their increasingly insecure operating environments. The relevance has come from the way in which the training curriculum, and the management model that grew from it, framed itself as "*a research-led training project and a training-led research project*". Almost unknowingly it promoted an "evidence-based" approach to management that sought out good practice by reviewing the "science base" of thinking on security from several sectors (academic, military, police, private security firms), as well as harvesting the experience of the real-life challenges of aid practitioners.

This tradition of "learning through doing" has led to a focus on the need for mainstreaming good practice. Feedback from workshop participants over the years, and the observation of the trainers who have delivered these workshops all over the world, seem to be pointing in the same direction. Namely, that whilst almost everyone who attended the training valued the process, and could see why the approach was useful, the "reality" of organisational life would always be the most severe limitation to adoption of the good practice for security promoted on the training. There was a certain irony here: on the one hand organisations "valued" their people and their security enough to send them on a course, but their people-centric values seemed to run out of energy when it came to adapting organisational practice in the ways the training was suggesting.

Investing time

Individual managers, no matter how committed or attached to the approach, would invariably run into what we came to term "barriers to change" when they attempted to implement the approach within their organisations. They say that organisational values, known collectively as the organisational culture, are only really revealed when it comes to making resources available, especially in conditions of resource scarcity when choices have to be made between equally appealing organisational objectives. So the typical "barriers to change" that came back from frustrated practitioners were "we don't have enough time for this" and/or "we don't have enough money for this". But since good security management at field level is really about good programming based on holistic understandings of where we are working, it does beg the question "if we don't have time for this, then what do we have time for"?

To some extent this is inevitable when attempting to disseminate good practice. Similar challenges are faced by those trying to promote other forms of "good practice" with regard to staff management, gender equality or equal opportunities. Certainly there is a clear need to build up the awareness and knowledge of individuals as a means of developing a common language and approach to managing security throughout the sector. But until this language and approach is understood and accepted organisationally, and permeates the way an organisation thinks and acts from top to bottom, then the impact of training-based approaches are going to be partial and transitory. This is especially true in our sector, where staff turnover is one of the key challenges to organisational learning, memory and capacity development.

Championing change

In essence, for security good practice to be "mainstreamed" we are talking about significant cultural change within organisations. For this to

***Paul Davies**: has extensive experience in the humanitarian sector as a manager, trainer and media specialist. At the time of writing this article he was Good Practice Coordinator for the RedR-IHE Security Programme. Paul is currently Director of Navigator Communications (www.navigator-communications.com), working on a number of consultancies, including a global study on anti-vehicle mines and aid agency security for UK NGO, Landmine Action.*

1. *This article first appeared in the RedR-IHE Security Quarterly Review, Spring 2005 Issue.*
2. *See: www.redr.org/london*

occur, leadership needs to come from the top, and that means Chief Executive level. Senior leaders need to become "change champions". This is the starting point for the mainstreaming component of RedR-IHE's security programme: a series of one-day seminars and workshops for the senior leadership of aid agencies and consulting services at HQ level to assist and facilitate the development of a culture of good practice.

Finally, it is crucial to think of the "end state" to which this process is aspiring. What does it, or will it mean, to have "mainstreamed" good practice with regards to security management? It is clear that the definition of a successfully "mainstreamed" organisation will be rooted in the culture that pervades the organisation and its people, rather than a bureaucracy cluttered with endless checklists and procedures, all bound together in some oppressive ring-bound folder that will consume your excess baggage allowance. This is not to say that security policies, procedures and practices do not need to be formalised into a living security plan; of course they do, but rather that an organisation that has succeeded in mainstreaming security good practice will not be primarily defined by this.

Instead, security will be the lens through which all activities are seen, and decisions made. Security awareness and risk management good practice will be so ingrained in the organisational culture that it will simply be understood that "this is the way we do things around here". Equally, this will be a culture where people will not have to be told that we all have a responsibility for security: every member of staff will understand this, and act accordingly. For senior leadership, this mainstreamed culture of security good practice may be the source of further significant dilemmas, such as when to suspend an existing programme or turn down new donor money if the security conditions are not right. But nonetheless, an embedded security culture should make such demanding dilemmas into routine decisions, and provide a clear guide to action that will service the agreed and understood best interests of the organisation and all its stakeholders in the long term.

Central Risk Group
Practical steps for corporate-level crisis management

Control Risks *is an independent, specialist risk consultancy with 18 offices on five continents. They provide advice and services that enable companies, governments and international organisations to prepare for a variety of unforeseen and potentially financially damaging events. In the event of nightmare scenarios becoming a reality – an executive kidnap, devastation from natural disasters, extortion demands from local guerrillas – Control Risks enables its clients to respond quickly and effectively to preserve life and to secure operations and reputation.*

No two security crises are the same. Dealing with a terrorist attack targeted at your company poses completely different challenges to dealing with an attack aimed at the area in which you operate. Likewise, responding to a violent takeover of your company's assets is very different to responding to serious civilian unrest. Yet many private and public organisations maintain just one crisis-management plan, and it comes as a shock when, in the event of a crisis, they find it close to useless. That is why it is crucial that companies undertake risk assessments at an early stage in the investment cycle.

While there is no blueprint for a crisis plan, there are certain characteristics that all good plans contain. Below are a few of these characteristics.

1. Crisis plans should include clear lines of authority, a single coordinator, and provide for the rapid availability of resources in the event of an incident.

The early hours of an incident are crucial to establishing facts, avoiding miss-steps that could lead to an escalation of the situation, and mounting an effective communications campaign. Straightening out unclear or disputed lines of authority in the middle of a crisis will waste valuable time and create a sense of confusion that could complicate the response. To minimise the scope for such problems, private and public organisations should ensure that crisis-management procedures and lines of authority are agreed in advance by all relevant parties. Plans should provide explicit criteria for deciding when to delegate the role of crisis coordinator to an in-country manager or another party who may be in a better position to manage the situation.

2. The key players in any crisis plan should be evaluated to ensure that they are physically and mentally fit. Entities operating in particularly crisis-prone areas should assess the physical or psychological health hazards associated with a particular posting.

Candidates who suffer from chronic stress or anger-management problems can endanger themselves or others during an incident and, as such, can be unsuitable for deployment to high-risk countries. In some cases, companies may be able to address these problems by offering training to reduce high-risk behaviour. But in all cases, companies should conduct a security risk assessment for guidance in determining whether a given country or location should be classified as high-risk for the purpose of deployments.

3. Good crisis plans rely on up-to-date training for the key players. Private and public organisations should ensure that employees have the confidence to act individually and collectively to safeguard themselves and the company.

Employees selected for overseas assignments should receive a predeparture programme that includes a comprehensive security briefing. Frontline staff deemed to be at high risk by virtue of their location or their profile may require a supplemental hostile environment training (HET) course. Among other topics, the HET should teach staff how to calm a situation or prevent an escalation if they are involved in an incident. Local employees should receive training on security, emergency response procedures and avoiding high-risk behaviour during an incident. All employees should receive regular personal security briefings.

4. Good crisis plans require easy communications between the affected area and the crisis management teams. For high-risk assets, private and public organisations should consider the installation of silent alarm systems linked by satellite to a 24-hour monitoring system as a means of providing instant notification of an incident and communications during an incident.

Such alarms, already in widespread use in the shipping industry, allow an authorised on-site operator to send a coded distress signal without attracting the attention of an adversary. The 24-hour monitoring centre sends a coded reply to the operator and notifies company managers if it fails to receive a pre-agreed response from the affected site. Managers can then investigate the alarm and activate the crisis management and contingency plans if necessary. Private and public organisations should restrict knowledge of silent alarm systems, particularly in environments where local employees may pose a potential risk. Private and public organisations may also wish to consider installing concealed GPS systems in vehicles and marine vessels to assist in pinpointing their location during a crisis.

5. No matter how well organised a company's crisis planning is, without strong physical security nothing can be done to protect employees. Private and public organisations can install a variety of safeguards to restrict access to a high-risk site or limit movement within that site after a crisis. Design of these systems must strike a balance between security and safety.

Private and public organisations should consider the use of anti-intrusion devices, lockable gates, retractable stairways, caged stair heads, dazzle lights, manual or remotely operated water hoses, lockable doors and the creation of secure safe havens. Private and public organisations should ensure that security measures do not interfere with the ability to evacuate the asset quickly in the event of an accident or emergency.

Control Risks constantly reviews and updates its risk ratings. The map shows its ratings for risk in countries around the world as at March 2006. Businesses should regard all risk-mitigation measures with the same willingness to introduce changes as circumstances demand.

GEOS: MANAGING INTERNATIONAL RISK

Interview with Laurent Jacquet:

Summary

International terrorism and attacks on foreigners has made people think twice about travelling abroad and meant that companies sending staff overseas have stepped up their security assessments of a given country before their staff set foot on foreign soil. GEOS is the leading risk management group in continental Europe. Its main activity consists of protecting the business development of its clients through the provision of a global security package that includes audit, consulting, operational assistance and crisis management. GEOS offers a complete range of solutions that enables its clients to manage international risk (political, security, terrorism) and business risk (unfair competition, fraud and litigation). The organisation has a fulltime staff of 180, a turnover of €17 million, operations in more than 50 countries, 12 international branches (Algeria, Britain, Saudi Arabia, Colombia, Costa Rica, Denmark, United States, India, Russia, Venezuela) and over 200 clients in a variety of business sectors and industries.

Why are risks certain missions so often overlooked?

The risks involved in travelling abroad are often underestimated for a number of reasons. Firstly people are often unaware of the potential dangers of their country of destination. This could be a question of a "force of habit". If they are used to travelling to countries that have a reputation for being dangerous they may, or may not, take a few precautions during their first trip but if after that they have not experienced anything out of the ordinary they will be less inclined to take precautions for the next trip. Secondly, some countries may be risky but they may not have attracted as much media attention as other countries with media-grabbing risks such as for example the frequent kidnappings in Columbia or attacks on foreigners in Iraq. Lack of media attention also means that people are often ill-informed and therefore do not take any special precautions prior to setting off on their travels.

When is it excessive to be concerned about our own security while travelling and when is it perfectly justified?

People should always assess the security risks of the countries they are travelling to. Based on sound information about the actual risks and the specific cultural features of the country in question, they will be in a much better position to take appropriate steps to ensure their own security. . For example, the "bunker mentality" often adopted by expatriates in the Gulf states may be construed as a sign of a lack of confidence in the inhabitants or the police force particularly in the case of Africa (Algeria, Nigeria, Angola,…).

What makes, say, Cairo a dangerous destination and Mexico City a relatively safe one?

Cairo is definitely no more dangerous than Mexico City. When an assessment is made of the risks, the gap between reality and the common perception tends to increase. Increased publicity, reflecting cultural and emotional factors, for a number of developments, has a direct impact on the risk assessment process. This can often lead to a distorted assessment of the actual situation In reality, crime kills more people than international terrorism.

What parameters should one take into consideration to evaluate the risk of a given mission? Who is at risk? What sort of risks are we talking about?

Security risks are a growing concern not just for tourists but also for entities sending staff abroad to work or sending employees on business trips to foreign countries. Tourists and expatriates who fail to adopt a low profile or ensure that they are well informed before their departure are jeopardising their own and maybe others' security. Such risks to be aware of include the following:

Risk of crime

Expatriates and business travellers are all the more exposed to the risk of crime because their incomes and lifestyles often contrast sharply with most of the people living in the countries they are visiting. While their awareness of what types of behaviour to avoid is often relative. Consequently, they are exposed to several risks:

***Laurent Jacquet**: is currently Director of External Relations and Information Services at GEOS, a position he has held since March 2004. Prior to that he was Editorial Director for Le Moniteur du Commerce International (LeMoci), Paris, France.*

- **Personal security**: aggression, lynching, murder, rape…

- **Property**: intrusion, thefts of all kinds (burglary, car, extortion…)

Often such crimes are carried out by individuals or small groups of people. However, they can also involve large organised gangs or mafia-linked groups armed to varying degrees.

The following four indicators are useful in assessing the relative risk of crime: assess the risk of crime are:

- The number of murders.
- The number of thefts.
- The level of fraud.
- The number of rapes.

Social climate

The social climate should be monitored closely taking into account the possibility of attacks on expatriates and business travellers. Both tend to be prime targets for criminal gangs or terrorist organisations.

Social climate-related risks include the following:

- **Institutional risk**: this is an analytical survey of the indicators of corruption in the law enforcement and legal system, which provides a means of assessing how the rule of law operates in the country or city in question.

- **Government stability**: this assesses how effective the executive authority is, whether there are any rebel forces and whether changeovers in political power are peaceful or not.

- **Political violence**: this refers to all the various clashes between the different political groups (political parties, trade unions, partisans,…).

- **Ethnic, xenophobic and racist violence** assesses the current situation in relation to such crimes.

Terrorism

Terrorism-related risks are assessed in the light of the incidents and threats from local and international terrorists groups within a particular country.

Kidnappings

Such risks are assessed on the basis of the number of kidnappings involving nationals and expatriates carried out within the country. The reasons for such kidnappings (for example, political, mafia, financial, religious) should also be taken into account.

Geopolitical

The risks tied in with this factor reflect the country's strategic importance both regionally and internationally. It also reveals its political and diplomatic approach on the international stage. Other yardsticks taken into account are: border incidents, secessionist, independence or separatist activities.

Can you make a distinction between exposure to risk when travelling for a few days, when touring for several weeks and when living for several years in a given place?

The exposure to risk is not necessarily based on a length of stay but more a question of being in the wrong place at the wrong time. For example, risks linked to airports, access roads, particularly in Africa, or "express kidnappings", where travellers are abducted with the sole aim of securing a ransom quickly, do not have any bearing on the length of a trip but on the whereabouts of the person. Expatriates may be exposed to different risks such as those to their property, as well as aggression in the home but such crimes can also happen in the person's home country.

What would you recommend as a security checklist for travellers?

Before setting off, people should learn various items of information about their host country. For example, the history, geography, demography and general security of a country can tell us a lot about the potential risks.

GEOS also recommends that those travelling for business should find out about:

- The employer's travel security policy.
- The employer's country information database (if there is one).
- Feedback from previous trips made by members of staff.
- The advice the Foreign Office issues to travellers.

With regard to health advice, GEOS recommends that people should:

- Undergo a medical examination before departure.

- Take along a copy of their medical records.

- Check the validity of their international vaccination certificate and ensure that they are covered for the country they are visiting.

- Take along medicines that are suitable for the country of destination and their own requirements and habits. They should include any medical prescriptions relating to the products, as these will be routinely requested so as to ensure they are not narcotics.

As for the administrative formalities, GEOS urges people to:

- Check the validity of their administrative documents (passport, visa, identity card, international driving licence and so on).

- Take along photocopies of these official documents, but leave the original copies in the company or hotel safe.

What about staff working for NGOs are they more or less exposed? What should an NGO operating on the ground in a crisis area do to protect its personnel?

NGOs do not enjoy any favourable security treatment. In fact they are even more exposed: they are regarded as key targets owing to their operational vulnerability. Above all, warring factions and insurgents often consider NGOs to be "in the pay of the West", which frequently means being "dependent upon those in power". “Confessional” NGOs (those with religious affiliations) are, of course, the most vulnerable, according to this logic. Here, too, the best way of preparing yourself for any risk is to be informed about the local situation and cultures and, above all, the security conditions. The ethical scale of a mission often helps to cloud a person's judgment of the actual risk. Added to that is the fact that staff who are used to living in sensitive areas abroad may be a bit blasé about the actual risks. Management should bear this in mind and seek to impress upon them the importance of being properly prepared for every eventuality.

What would be the security profile to adopt when leaving for an ordinary study/assessment mission in Damascus, what should one do when assessing a tsunami/earthquake area, what should be done in a terrorist-prone country (Saudi Arabia, India, Bangladesh), etc.?

In Damascus, places that are immediately associated with the West, such as major hotels and diplomatic representations, should be avoided, and people should not wear anything or behave in any way that attracts attention for example. They should remain cooperative and comply with any requests made by police officers.

Travellers can reduce the risk of terrorist attack by steering clear of any target locations and adopting a low profile. There is no comparison between the situation in India and the one in Saudi Arabia. Westerners may be targeted just for being a Westerner in Saudi Arabia, while in India, you just have to take basic precautions about where you go and the company you keep. The risk of terrorist attacks cannot be measured in terms of the number of previous incidents or the number of victims. The key factor is whether a person is a target or not.

Chapter 34: Why aid agencies must strengthen security cooperation

Summary

Contemporary humanitarian aid personnel increasingly work in dangerous environments where the risks of being targeted by irregular forces with nil regard for human dignity are rife. These challenges have necessitated many international NGOs to pursue ways of promoting safety and well-being of staff working in high risk countries. This paper aims to highlight the benefits of establishing joint NGO security coordination networks as the way forward for dealing with those challenges within the context of a high risk country.

The number of humanitarian workers killed while working in high risk countries have increased dramatically in recent years. According to the Afghanistan Non Governmental Organisation Safety Office (ANSO), 37 humanitarian workers were killed in Afghanistan between 2003 and 2004[1]. Other criminal acts against Non Governmental Organisations (NGOs) have also been on the increase; these include hostage taking, sexual assault, armed robbery, and malicious damage. This has been exacerbated by the increasing prevalence of irregular forces whose moral values have been diminished after many years of civil conflicts, eroded perception of NGO neutrality, religious extremism, and chronic poverty, among others.

The aim of this paper is therefore to highlight the importance of developing networks for security collaboration and coordination as the way forward in tackling the emerging challenges described above. It is this writer's view that the successes of the Afghanistan NGO Security Office (ANSO) or the East Democratic Republic of Congo's (DRC) Centre de Communication, (CDC) and others, can form the basis for establishing similar networks in other countries where security is a big concern.

***Kiruja Micheni** is currently the Security Manager for Christian Aid, responsible for developing and managing the global security policy for the organisation and ensuring its implementation. He has extensive security management experience of NGOs and the private sectors, and served with the United Nations peacekeeping mission in the Former Yugoslav Republic of Macedonia, for two years including as the Chief Operations Officer.*

Need for Change

Traditionally, humanitarian agencies have depended heavily on acceptance as the key element of the security triangle; acceptance, protection and deterrence. Although this has previously worked well, recent experience in some complex emergencies such as Iraq, Afghanistan and others where the perception of neutrality has been lost begs humanitarian organisations to rethink their security strategies. As pointed out in the guidelines by the United Nations Office of the Humanitarian Coordinator for Iraq, "showing the flag is not sufficient in ensuring the security and safety of humanitarian personnel"; on the contrary, it could even attract attacks;[2] hence a need for broader approaches to security management. Furthermore, in some regions, anti-western terror groups don't draw a line between NGOs, multinational forces, UN agencies and government agents, and because the former are the comparatively under resourced, they are often most vulnerable. As way to meet these challenges, some agencies have adopted various strategies some of which are not consistent with core values of the sector. These include an increase in the use of armed protection as recently observed by the author in Afghanistan, Somalia and Haiti, or "embedding" agency vehicle in a UN convoy under military escort". The need for a review as proposed in this paper is driven by the following dilemmas:

- Growing need to increase protection and deterrent measures against the fact that humanitarian organisations cannot justify heavy expenditure on security.
- How best to maintain liaison with military actors without compromising neutrality; in complex emergencies sometimes NGOs have no choice but to seek the support or protection by military forces.
- The expanding need for NGOs to continue speaking out on behalf of those undignified by the scandal of conflict without seriously endangering their staff.

1. *ANSO Security briefing May 2005*
2. *United Nations Office of the Humanitarian Coordinator for Iraq (UNOHCI), 20 Oct 2004, www.reliefweb.int/rw/rwb.nsf/db900SID/HMYT-66BQU7?OpenDocument*

- Need for NGOs to remain focused on their objectives within the context of a high-risk environment.

Cooperation with UN

The UN security system is usually a focal point for coordinating security issues in many humanitarian emergencies. They are also helpful in sharing security information with the wider NGO community working in hostile environments, but realistically they cannot be expected to keep everyone in the loop without a functional security network. Where this exists, they have been noted to provide security alerts and updates, coordinate evacuations and other services as appropriate. Unfortunately formal security partnerships between the UN and NGOs currently don't exit, although occasionally, overzealous UN security staff have been known to give the impression that NGOs can be included as part of a wider security umbrella provided their organisations sign a memorandum of understanding (MOU) with the UN committing to meet the cost of evacuating their staff, but when this is pursued, you quickly learn that "the UN is not currently resourced to make such a commitment".

International military forces

Internationally mandated military force can be of great assistance to NGOs whenever there is an urgent need for evacuation of international staff or to help with search and rescue operations. For this reason, humanitarian organisations should establish appropriate means of dialogue with the military forces, but being aware that too much contact with them could be perceived as compromising NGOs' independence and impartiality. Therefore in order for humanitarian organisations to maintain and demonstrate their independents, such contacts should be made and maintained through a formal or informal NGO security forum. The forum/security coordination office will also ensure that any information given to the military is of general nature and that they are not construed to be providing intelligence to the military forces, noting that the divide between information and military intelligence is rather blurred.

Examples of existing NGO security offices

Afghanistan Non Governmental Organisation Safety Office (ANSO) model

The Afghanistan Non Governmental Organisation Safety Office (ANSO) was set up to provide up-to-date security information for the humanitarian community serving in Afghanistan. It is currently sponsored by the International Rescue Committee (IRC) and funded by ECHO, the Humanitarian Aid department of the European Union, SDC, the Swiss Agency for Development and Cooperation as well as donations by various NGOs. ANSO has a well established network comprising of the Head office in Kabul and 5 regional offices covering Central, East, West, North and South for coordination and information gathering, which enables them to provide timely security updates and advisory whenever they receive threat warnings or following a security incident. They also send out weekly security reports and coordinate weekly security briefings by each region. ANSO also help in coordinating evacuations; an example being the evacuation of NGO international staff from Jalalabad to Peshawar following violent demonstrations in Nangahar province on 11th May 2005[3]. The office has also helped in facilitating joint training in security awareness, first aid and defensive driving. These and many of its other achievements have made ANSO stand out as the most successful NGO security outfit in their category, so far. Indeed most NGO security managers that this author has interacted with agree that the organisation has played a key role in enhancing safety and security of national and international NGO workers in Afghanistan.

Centre De Communication (CDC) – East DR Congo

This NGO security Network for East DR Congo region was formed in 1997/8, following increased rebel activities by the movement Congolese Rally for Democracy (RCD). It brings together up to 28 INGOs currently operating in South Kivu province of Eastern DRC, most of which are based in Bukavu town. It was initially hosted by Safe the Children but now IRC plays host.

The mission of CDC is to collect, analyse and disseminate security information to all its members. It also provides a forum for NGOs to discuss security issues and agreeing a common strategy. For example, because of the chronic non-effectiveness of the Congolese police, CDC was able to arrange for the setting up of a small detachment of the local police to respond to security incidents affecting NGO staff and premises. The unit also conducts night patrols of NGO offices and residences of expatriate staff and carry out radio checks with guards at residences and

Hundreds of Afghans rioted over reports that American interrogators at Guantanamo Bay prison flushed at least one copy of the Koran down a toilet.

offices every two hours from 2000 to 0600 Hrs. CDC is also responsible for maintaining HF radio contact with staff travelling to and from the field.

CDC is funded through contributions from members. According to Chirha Murhambo, Christian Aid's Programme officer in Bukavu, the fee is currently US$190 per member. This is used for payment of salaries, equipment maintenance and purchase of stationery.

The office has been a good success as gathered by this writer during a security review of the region last year. At different one-on-one meetings with different agencies, all five representatives spoken to were in no doubt that it had helped to improve safety and wellbeing of NGOs in the area.

Joint Security Network for NGOs in Haiti

The Security network for Haiti, christened Systeme De Securite Inter-ONG (IOS) is probably the youngest such organisation. It started operating on 1 September 2005 with the appointment of a joint Security Officer. Currently there are 11 member agencies: Action Aid, Christian Aid, Oxfam GB, Concern Worldwide, German Agro Action, Lutheran World Federation, Acted, Initiative Developpement, Protos (Belgian), Helvetas (Swiss), and Diakonie (Germany). The office is hosted by Christian Aid in Port-Au-Prince. Funding is through contributions by members estimated at about US$2,000 per agency per year. According to Christian Aid's Haiti Country representative Helen Spraos, they started by "taking a conservative approach whereby each organisation that was definitely committed contributed US$1,565 for the first six months following which they were to review the way forward".

Keeping IOS afloat has been a great challenge. Although many of the smaller NGOs are keen to join, they have no provision in their budgets to support the initiative. Some of the big NGOs "have not felt" the need to join at this stage when the office is still considered under resourced.

It is hoped that once up-and-running, the initiative will go along way in establishing the bases for NGOs to share security information, including with other key players such as the UN and agreeing on common strategies. Unfortunately their funds are limited and could do with some support from donors. Efforts are ongoing to lobby support.

Sudan NGO Security Initiative

The idea of setting up of initiative for Sudan based on the ANSO model came up in May 2005 as a strategy to cope with a very difficult security environment. But this proved to be quite a challenge as no agency was willing to host the office fearing punitive response from the Khartoum government. Others argued that they already had own security officers and plans. However it did appear from the various emails flying about at the time that those who opposed the idea mistook the proposal for some form of privatisation of security management. Despite these difficulties more than 10 agencies have so far signed up; and enough funds have been pooled for an initial assessment. Like in the case of Haiti, optimists believe that once the initiative is up and running, others will want to be part of it, after seeing the benefits.

Suggested Roles for a Joint NGO security Office

Roles for a centralised security office would depend on respective local context. The list suggested below is therefore only a guide:

- As the focal point for security coordination with the UN, internationally mandated police forces and military, Embassies and other relevant security stakeholders.
- Maintaining a generic country security plan and coordinated contingency plans for the wider NGO community.
- Coordinating evacuations.
- Organising joint security training programmes; it is always cheaper when different organisations pool resources to carry out training.
- As the centre for receiving incident reports throughout the area of operations; this helps NGOs to learn from each other's experience and good practice.
- Receiving threat warnings from various sources and alerting NGOs accordingly
- Route assessments and classification.
- Host for meetings to discuss security and information sharing; such forums help to build solidarity between different NGOs.
- Assistance with security induction of newly recruited staff.

- Provide assistance to smaller NGOs in setting up their own security procedures as appropriate.

- Play a leading role in exploring opportunities for sharing of security resources, e.g. radio repeaters etc for the common good of all NGOs.

- Liaising with local police.

- Provision and manning of a dedicated security radio channel.

- Setting up and ensuring a functioning NGO "security tree;" for quick dissemination of critical security alerts and information.

Recommendations

There is no doubt that security cooperation between humanitarian organisations working in a high-risk country is very important. While recognising that field security is discussed at various forums on ad hoc basis, there is need to setup an office with responsibility for the coordination, bearing in mind that actions of one agency could have an impact on the security of others. Indeed, it should be remembered that local militants often cannot distinguish between different NGOs.

Those advocating for the setting up these proposals should not be discouraged by the fact that some agencies have appeared unconvinced of the relevance. This is likely to remain the case until there are more success stories like ANSO and CDC. The success of the Sudan and Haiti initiative is therefore very important for charting the way forward. If they succeed, more would want to be part of it. Alongside soliciting support from more NGOs, those spearheading the initiatives for the two projects should also explore options for donor funding.

Mercy Corps on the necessity of coordination and cooperation

Interview with George Devendorf

***George Devendorf**: is Director of Public Affairs at Mercy Corps. Between 2000-2003 he was responsible for directing Mercy Corps' disaster preparedness, assessment and response efforts worldwide. Prior to joining Mercy Corps, Devendorf worked with a variety of relief and refugee assistance organisations, including USAID/OFDA (Kosovo and Macedonia), ICVA (BiH), InterAction (Washington, DC), the IRC (Sudan), UNHCR (Sudan), and the IOM (Philippines).*

Can you briefly explain the work of Mercy Corps?

Mercy Corps is an international relief and development organisation based in the US and the UK. We're active in around 35 countries around the world and we've just celebrated our 25th anniversary. We've been directly involved in most major disaster response operations for the last 20 years or so, but we're also involved in longer-term community-based development in countries in transition – whether that be economic, political, or security-related transitions.

In your experience of emergency relief operations, what lessons can be learnt with respect to coordination and cooperation between different civilian, military and humanitarian actors?

We need to be careful here not to generalise. Since September 11 a disproportionate amount of attention has been given to a few operations – notably Afghanistan and Iraq - in discussions about coordination in emergency relief operations. This is not surprising given the funding and media attention given to these two emergencies, but they are not necessarily reflective of the so-called "normal" kind of emergency to which our agency responds. Throughout Africa – certainly in West Africa and East Africa – conflicts have been on-going for some time, and while some involve international peacekeeping forces or other international military forces, just as many don't. The lessons to be learnt on cooperation depend on who's there, and what kind of relief efforts are needed.

That said, cooperation and coordination continue to be the "holy grail" within the international community's crisis response efforts. Effective coordination is so difficult to achieve because it has to occur on so many levels: not just at the international and strategic level, but also at a regional level where the disaster or conflict has regional implications and all the way down through national capitals to the field level.

It's often at the field level that we find both the best and the worst examples of coordination. Where the different actors – governments, UN agencies and non-governmental organisations (NGOs) – face common challenges, we often find very good cooperation. This is true, for example, in areas where staff security is a prevailing concern. Inter-agency collaboration on security management is an area in which we've seen some progress in recent years. I expect that this trend will continue, and that we'll see more initiatives underway within both the NGO and the UN communities, particularly with regards to information sharing.

What role does ICT play in ensuring effective cooperation and coordination?

Information and communications technology is critical to every major aspect of a crisis response operation. Each operation is so inherently complex and interdependent that it places a tremendous premium on the integration of all the various interventions – whether they be political, military, social or human rights-related.

If we take the example of security coordination again – it's very clear that the ability of agencies to achieve effective security management depends largely on their communications infrastructure. If a host country wants to control the allocation of frequencies and communications practices, this can present enormous hurdles for security management. In some cases, the UN or major intergovernmental organisations can negotiate with host governments and include NGOs – all of them or some of them – under the UN's communications umbrella. But if there is no "empowered" state actor, you often have a "free-for-all". In that kind of environment, it is much tougher to develop and manage shared or consolidated communications systems. It is one of the greatest frustrations in our line of work that often you have staff in the most remote and insecure areas, and they are unable to communicate effectively with us or us with them.

Collective forms of communication can be very important tools for managing risk and improving security. They can take the form of a basic phone tree, a radio network – often administered by a UN entity – or websites that provide consolidated information on crisis situations that users can access on a demand basis.

Afghanistan is an interesting model. The primary service provider of security-related information, the Afghanistan NGO Safety Office (ANSO), has developed a cell phone SMS-based alert system for truly urgent security-related messages and behind that a much

larger and more extensive e-mail-based update that goes out every few days.

What about coordination and cooperation at a planning and strategic level – what lessons can be learnt there?

The real challenge here is that, however good an organisation is at performing its particular task, it will never be enough on its own because of the interdependence of the various issues and challenges associated with crisis management operations. I think more real world case studies would be very useful in this debate, to see where it worked and where it didn't.

Let's take Afghanistan as an example. In this case, different national groups took lead responsibility for different aspects of the reconstruction and development efforts. The Germans are responsible for police training, the Americans in charge of military training, and the Italians in charge of judicial reform – just three of several pillars of the overall reconstruction effort. But these tasks are so inter-related, that failure in any one of these areas directly impacts on the success of the others. What's the point of having an operational police force if there are no judges to prosecute cases or no prison space for those who are prosecuted? And if the army is developed more quickly than the police, it will soon find itself engaged in policing functions that can stretch its capacity and blur the lines between the responsibilities of the military and the interior ministry. So again it points to the need for close integration and coordination between initiatives in these situations.

Of course high level planning does go on, but there's no overall mechanism to ensure that progress is being made in a coherent way. The only body that could effectively play this role would be the national government of the host country – but in Afghanistan the government is the recipient of the capacity building we've just been talking about, so it's a catch-22 situation.

What about civilian-military cooperation? From your experience, what are the key issues?

The question of how closely civilian and military components can and should operate together is an important topic. How closely should they conduct planning, implement activities, monitor and evaluate them? Here, there are perhaps lessons to be learnt from the US experience since September 11.

For various reasons the US administrations turned to the Pentagon to serve as its primary implementing arm, not just for military tasks but also for state building and in some cases humanitarian activities both in Afghanistan and Iraq. I think there was a perception that the military had a unique ability to respond quickly and effectively to almost any challenge put in front of them. What this did was to circumvent the US State Department and civilian side of the US government that was primarily responsible for state building activities, democracy and governance support, and humanitarian assistance. It led to a gradual eroding of civilian state capacity that meant they have been less able to play the role for which they are mandated.

So while a few have talked of the need to have a seamless operation between civilian and military services – with no internal barriers – I would urge caution. I see the benefits of presenting a homogenous view of the EU from overseas, but in many of the situations where the EU is active there are good reasons why a visible separation between its civil and military sides is necessary - even if behind closed doors there is close cooperation. This applies must directly to operations in countries in crisis, where the creation of winners and losers is impacted by the behaviour of international actors.

Keep in mind that the EU itself doesn't do much on the ground, rather it contracts others to do it. Very often those implementing the work – whether it be peace building activities, humanitarian or reconstruction projects - are in fact NGOs. If the EU is relying on these entities to implement the bulk of its work overseas, it needs to think strategically how it can best ensure their success. And that's not just in terms of meeting programme targets and objectives, but also in keeping their staff safe. If one or two NGO workers are killed, it's likely that all civilian activities in that area will be either suspended or shut down. So, there needs to be great sensitivity around how NGO activities are perceived by the local population.

More often than not, the humanitarian community has sufficient capacity to address urgent humanitarian needs. In such cases, military involvement in humanitarian situations often complicates the issue and can inadvertently make our jobs tougher or potentially endanger our staff. There needs to be a clear distinction in the minds of local populations, not just in that country but also neighbouring countries, of the difference between humanitarian, unarmed, independent aid providers, on the one hand, and military forces pursing political objectives, on the other hand. For example, in Afghanistan, coalition military forces can, on any given day, be involved in both relief-type activities and launching military raids – perhaps in villages right next to each other. So it is essential that civilian and humanitarian workers are recognised by the locals as non-combatants. Otherwise we may end up putting their lives at risk.

That message seems to be sinking in. In the early days of the Afghan war, military forces - primarily special operations forces - were conducting relief-like activities while wearing civilian clothes and driving civilian vehicles. The only difference between their appearance and that of humanitarian workers was the bulge under their shirts or the weapon barrels pointing out of the land cruiser's window. Following intense pressure from humanitarian agencies, the US military has sought to ensure that all troops engaged in "humanitarian-like" activities now do so in uniform. To be clear: whether or not military forces engaged in combat choose to wear uniforms is a different question and isn't really any of our business. But it becomes our business when military forces go into the same villages, meet the same people that we do, dress like us, drive vehicles like ours and are less than clear about what their interests are.

The greatest contribution that military forces engaged in crisis response operations can make is to provide a secure environment in which the various other actors, not least of which the locals, can rebuild and do the work that needs to be done. In exceptional circumstances, usually due to questions of security or particularly tough logistical challenges, the military is sometimes in a unique position to provide aid to communities at risk. In such cases, there is more or less unanimous support among the NGO community for military intervention, so long as it is coordinated with humanitarian agencies.

The military and humanitarian communities have different jobs; we both need to be good at them in our own way. There will be situations where we do bump into one another in crisis situations, and in those instances we need to build greater mutual understanding, communication, and cooperation to help ensure that we can both accomplish our respective missions.

ANSO ON THE RISKS AND CHALLENGES IN AFGHANISTAN

Interview with Christian Willach and Christopher Finucane

Short Introduction of Afghanistan NGO Safety Office (ANSO)

The ANSO programme has been running in Afghanistan since 2002. It is entirely devoted to providing security coordination and services to NGOs. It is the only actor in Afghanistan that has the sole mandate to provide security assistance to NGOs and to assist NGOs in developing their security management capacity. In addition, ANSO acts as the security advocate on behalf of NGOs, working closely with NATO/International Security Assistance Force (ISAF), UN Department of Safety and Security (UNDSS), the Afghan government and foreign missions.

ANSO has a staff of almost 50 people, located in five offices around the country. The office in Kabul acts as an information centre, collecting information from the Regional Security Advisors in each of the five operational regions corresponding roughly to the north, south, east, west and central portions of Afghanistan. ANSO's national and international staff are tasked with collecting reports of security incidents; disseminating news of those incidents; and attempting to investigate the underlying reasons for those incidents. At the end of each week ANSO creates a weekly brief that summarises incidents that have happened during the previous week; follows up on incidents reported during that week; provides a brief analysis of the situation; and then produces a colour-coded threat level map of each of its five regions. ANSO is rated highly among beneficiaries for being the first to report incidents and get information out quickly.

What is ANSO's main role in Afghanistan?

CW: We provide timely and accurate information on security issues to the NGO community across the country. Our information and analysis helps them decide how to deploy their staff and what they need to do to keep their staff safe. We aim to help them continue to deliver the work that donors pay them to do.

What are the main security threats and risks facing the NGO community?

CW: It's hard to generalise. Afghanistan is such a huge country and it depends where you are. In the northern and western regions the largest threat is road banditry and organised crime, whereas in the south and eastern part of the country political motivated violence is a real concern. In those regions, insurgents are directly targeting the international military forces and the UN.. Some NGOs get targeted too - insurgents fail to make a distinction.

CF: Even in the northern region we're seeing a shift towards more political violence since the elections in 2004. An NGO worker was recently killed in the region. It may have been a case of mistaken identity as a UN worker was killed in the same location some two days earlier.

CW: At last count some 24 NGO workers have been killed since the beginning of 2005 – the same number as for the whole of 2004.. Afghanistan has the highest NGO death toll rate worldwide.

How does this affect the NGOs ability to recruit staff & carry out their work?

CW: Of course, the country directors I talk to tell me that recruiting for Afghanistan is very hard. Many of the people with experience, who stayed for decades during the Taliban time, do not want to work there in the current environment. It's not often mentioned – especially by the US Government – but in fact during the Taliban time there were about 40-45 international NGOs working in Afghanistan with very little hassle. The Taliban restricted them, watched them very carefully and, if they overstepped certain cultural barriers, they were very politely but forcefully asked to leave the country. But they were not attacked. That started after the Taliban regime was ousted.

As a result NGOs today tend to have many young staff and, one of the things I think is absolutely critical, is that these staff are adequately trained before being deployed. Even experienced NGO workers often do not understand what they're getting into in Afghanistan – it's a whole different ball game. If you don't follow the rules, you risk being shot. It's considered acceptable to use deadly force to settle an argument – even arguments that may be trivial to us.

But there are still some 2500-3000 international aid workers in Afghanistan and approximately 800 NGOs. A large majority of those are

***Christian Willach**: is security coordinator for the Afghanistan NGO Safety Office (ANSO), Christopher Finucane: works in one of ANSO's five regional offices in the northern region of Afghanistan.*

national NGOs - the big international NGOs are mainly involved in capacity building among the local civil society. In 2004, Médecins Sans Frontières pulled out of Afghanistan - they had lost five staff members during the year.

How do you cooperate with the international institutions and the military?

CW: Our relationship with the humanitarian aid office of the EU – based in Kabul – is excellent. The EU pays an important share of our budget, but aside from that, the staff in ECHO are excellent to work with – very down to earth and professional.

There are two military presences in the country – the NATO-led International Security Assistance Force (ISAF) and the coalition forces. Both operate in totally different ways. At the moment our cooperation with ISAF in terms of information sharing is relatively good – while it is less good with the coalition forces. But this reflects the fact that there are no institutionalised procedures of cooperation between the NGOs and the international military forces. It depends wholly on the personnel involved. When I started, the cooperation with ISAF was virtually non-existent, but there was good information sharing with the coalition forces. This reversed with the staff changes and it will no doubt change again.

There are of course cooperation agreements between the UN and the military forces but NGOs are not included – which is why we come in as a buffer. NGOs in Afghanistan are very reluctant to work directly, or even communicate directly, with the military because it could make them a target. That's why they come to us with any requests for military assistance – mostly medical assistance - and we then contact the military.

To give a concrete example: I was called at 7 o'clock in the morning with news of a crash in a remote region involving two internationals and one national NGO staff. The car had fallen down a 50-metre ravine and one of the international members of staff had suffered a severe neck injury. We were able to locate him via the Global Positioning System (GPS) scan from his cell phone and contacted the military forces responsible for that area. Thankfully they responded very quickly and flew him by helicopter to the next big city where he was stabilised. Later the same day he was flown to Dubai and he survived. That's the kind of thing that happens, not every day, but too frequently for my taste.

How has your programme been received by the NGOs?

CW: I think the ANSO programme is very successful and conceptually works very well. But it is not without its problems. We still have resource limitations and the budget is seemingly never enough, particularly for a good IT and communications infrastructure and vehicles. But even with those shortfalls and a very high turnover of international staff, we are able to meet the primary responsibilities of our mandate, which is to continually inform the humanitarian community of what's happening around them.

We have around 1,800 people on our e-mail distribution list. I get about 300 e-mails per day from the beneficiaries the NGO community – asking for assistance, giving information. And I get called around the clock by people wanting information, inviting us to meetings, and so on. So the interaction exists and given that beneficiaries' participation is entirely voluntary, this would indicate that the service works pretty well.

In fact we're reliant on the NGOs to provide us with information on the ground.

With just five regional offices and the HQ, and with just 6-7 national staff, we can never hope to cover the whole of Afghanistan. By contrast, there's at least one national or international NGO working in every district in Afghanistan so they have to be our principal information source. We then analyse the information, work with it and disseminate it.

What are some of the personal risks and challenges you face working in Afghanistan?

CF: Well, to illustrate the environment we're working in, I had an incident just before coming here where a staff member burnt my office down. I don't know if it was due to a personal vendetta or whether he just didn't like his job anymore. The issue is that alliances and allegiances can change overnight for seemingly no reason. That has been the culture over there for as long as anyone can remember.

CW: On a personal level, the accommodation is extremely basic – that's OK for a while but it is difficult for extended stays – and basically we have no social life. Even if we just want a walk around the block there's a high risk of kidnapping. Insurgents seem to have got wise to the fact that kidnapping internationals for ransom may pay off.

And professionally, the frustration is not to have sufficient resources to run a better service. With the donor funds we have, we can run a basic service but we lack several things in our infrastructure that would enable us to meet more of the needs of our beneficiaries. Right now we simply don't have the manpower or resources.

CF: Yes, to give an example of how thinly our resources are stretched. In the northern region I'm dealing with around 200 people from almost 60 organisations – and they are the ones I have a formal relationship with. There must be the same number again of people and organisations with whom I have no formal relationship. It's a real challenge to know who's out there, where they are and what they're doing. Ultimately it's voluntary participation, so it's difficult for us to continually update our records and to know what the NGOs need from a safety point of view.

And how do you see ANSO's role evolving in Afghanistan?

CW: It would be great to say that ANSO's services would no longer be needed in the next few years. That would mean that NGO staff are no longer being killed. But to be honest I don't see any imminent improvement to the situation.

Chapter 35: The role of ICT in crisis management

Summary

Sharing of relevant and reliable information between the main actors of the international crisis response community is a key to sustainable results in promotion of peace worldwide. This article identifies ways information and communication technology (ICT) can be used to facilitate peace-building and humanitarian activities ranging throughout the conflict cycle - from early warning to post-conflict reconstruction. Main ICT initiatives, challenges and solutions are identified.

***Paul Currion**: consults on information management and advises the ICT4Peace Foundation[1]. He is currently working with an NGO consortium to improve ICT use in emergency response. Julia Steinberger: has worked on the ICT4Peace aspects of the World Summit on Information Society in 2005 and is now Project Officer for the ICT4Peace Foundation.*

The importance of ICT for crisis management

ICT is crucial to crisis management, yet there is surprisingly little research into its use. To address this gap, the Swiss Government established the ICT4Peace Project to make a preliminary overview of the many uses of ICT before, during and after conflict.[2]

Since the end of the Cold War, crisis management – the responses available to the international community in the different stages of the conflict cycle – has involved a wide range of agencies: governmental, non-governmental, national, international, civilian and military organisations. Sometimes they share objectives, but often they have conflicting priorities. Agencies may not be willing or able to share information for reasons of capacity limitations, technical barriers or political sensitivity – and it is worth noting that these barriers can apply equally *within* a given organisation, as much as between organisations.

Inaccurate, misleading or inadequate information leads to inefficient programmes that fail to achieve their objectives, the continued suffering of local populations, or even the loss of life of agency staff. New technology has the potential to improve the effectiveness of our work in responding to crises and conflicts – as long as, at the same time, we generate the political will to implement the necessary changes within our institutions and across historically separate sectors.

Early warning, conflict prevention and early responses

While it is accepted that conflict prevention is less costly in human and financial terms than intervention during a conflict, there are significant political and practical obstacles to prevention. Satellite communications and the internet have increased the speed with which we learn of conflicts, and provided the basis for greater understanding of conflict. Yet often the political will to prevent conflict is lacking, with a key issue being lack of accurate, timely information about the likelihood of conflict. Early warning systems offer one answer, yet early warning may not translate into early action; for example, in the case of Rwanda there were relatively unambiguous warning signs, and yet the international community failed to act. While there are understandable concerns about the practice, these do not constitute a solid case against the principle of early warning.

1. *Based in Geneva, the ICT4Peace Foundation works to promote the role of ICT in conflict management, emerging from research carried out by the ICT4Peace Project during 2004-2005.*
2. *ICT4Peace: the Role of ICT in Preventing, Responding to, and Recovering from Conflict, Stauffacher D., Drake W., Currion P., Steinberger J. 2005, United Nations ICT Task Force. The Report contains extensive references on all topics discussed in this article, as well as other case studies in this field www.ict4peace.org.*

ICT and Early Warning

Within the UN, the Office for the Coordination of Humanitarian Affairs (OCHA)[3] provides ReliefWeb[4] and IRIN[5] as information services that offer information that can be drawn on in identifying and profiling emergencies. ICT-enabled early warning initiatives are also seen in the European Commission, with the Tarîqa system developed for the external relations directorate (DG-RELEX) enabling EC delegations around the world to follow global developments relevant to their work through one portal. Tarîqa integrates multiple public information sources, filtering news from thousands print, radio, and television channels and building a customized portal for different geographical desks in the Commission.

The Frühanalyse von Spannungen und Tatsachenermittlung (FAST) System[6] created by SwissPeace is considered to be a major advance, employing both qualitative and quantitative methods by blending data analysis with interpretation by country experts. Another interesting project is Stockholm International Peace Research Institute's (SIPRI)[7] "Early Warning Indicators for Preventive Policy", which provides statistical analysis of a database comprising more than 1,200 structural and event indicators from a range of sources.

The ICT revolution has created the opportunity to develop tools to manage a wider range of data more systematically, applying statistical techniques to predict and analyse conflicts. While such systems continue to develop, they are only the starting point. It is still unclear what role ICT can play in preventing conflict, but the best examples can be found in the ways in which improved communications technology can build bridges between groups in conflict. This can be at the diplomatic level, but also at the community level, where social reconciliation may play a role at least as important as that of diplomatic initiatives. Examples of this can be found in the work of organisations such as War Torn Societies Project International, which promotes links between communities using media, such as video exchanges, providing communities in conflict with a better understanding of each other – very often the first, vital step towards peace.

Humanitarian interventions, peace operations and post-conflict reconstruction

While inter-agency coordination in field operations is a priority, it is also extremely difficult, hindered by differences in mandates, resources and capacities. Ironically, in conflict-related emergencies, this very complexity increases the need for effective coordination. More widespread use of ICT has become essential to manage these operations, although ironically the adoption of new technologies itself has not been co-ordinated effectively.

One widely-known concept is the Humanitarian Information Centers (HICs) operated by OCHA. HICs are service providers established in post-conflict and post-disaster zones to support humanitarian interventions through provision of information resources (that would otherwise be unavailable) to UN, NGO and sometimes governmental actors. Other examples are the creation of the WFP Fast IT & Telecommunications Emergency and Support Team, which sets up telecommunications for the UN system; on the NGO side, Télécoms Sans Frontières which plays a similar role in setting up emergency telecommunication systems; and from the private sector, the Ericsson Response Team which assists both sides in setting up field operations and reconstruction. Online, several initiatives have begun to create online humanitarian response clearing houses, such as Reliefguide, GlobalHand and AidMatrix, attempting to match needs with suppliers, potentially changing the way in which relief itself is delivered.

The impact of Geographic Information Systems (GIS)

GIS technology in particular has made an impact, providing map products that are more up-to-date, thematically relevant and more

3. *http://ochaonline.un.org/*
4. *www.reliefweb.int*
5. *www.irinnews.org*
6. *www.swisspeace.org/fast/*
7. *www.sipri.org*

widely disseminated than ever before, helping to guide interventions more effectively. The best example of this is the IMSMA system (provided by the Geneva Centre for Humanitarian Demining), which develops and disseminates data on issues related to mine action. GIS has spread rapidly, with actors such as the Joint Research Centre of the European Commission joining established actors such as the HIC. On the ground NGOs, such as the UK-based MapAction , specialize in satellite earth imaging matched with locally deployed teams to create real-time maps of disaster areas; at the policy level, agencies (such as UNOSAT) and interagency groups (such as the Geographic Information Support Team, or GIST) work to improve the use of geographic information.

In post-conflict environments – which often exist in close proximity to ongoing conflicts, and may be at risk of relapsing into conflict – reconstruction requires basic security, the rule of law and an evolution towards stability and reconciliation. In such an environment, ICT can be used creatively to quickly install government infrastructure, along the lines of the Government-out-of-a-Box (GooB) proposal supported by the Crisis Management Initiative of Finland, which envisions an ICT toolkit for governments rebuilding after conflict. Furthermore, the process of post-conflict reconciliation rests largely on sharing critical information, both between agencies and with affected populations, and ICT can provide the basis for this through more access to a variety of media sources.

The future of ICT4Peace

The ICT4Peace Report arrived at a range of conclusions, yet these conclusions are only the starting point for the crisis management community. Changes need to be made at every level of operations, and better links must be created both between different levels within organisations, and between different organisations. In particular, we need to move beyond the traditional view that knowledge is power when it is held by an individual or organisation; and accept that, in the new knowledge economy, information is more valuable when it is shared, providing the information provider with credibility and influence through their position as an information provider.

At the strategic level, information systems need to be developed that enable our various organisations to develop a shared understanding of the emergency environments in which we work; without that shared understanding, we will never be able to pursue coherent policies that lead to the outcomes we hope for in terms of peace, security and the relief of human suffering. At the operational level, we need to ensure that staff have access to the information resources that they require to work effectively, but also the mechanisms for sharing those resources with their partners. These tools will become increasingly vital for ensuring that individual activities on the ground truly meet the needs of affected communities.

In practical terms, the obstacles to sharing are often found in the disparities between different organisations' access to ICT resources, both technological and human. This is felt most acutely in the divide between civilian and military actors, headquarters and field levels, and international and local organisations. There are ways of addressing this, for example through provision of "common services" that are available to the entire community (such as the UN Joint Logistics Centre, which works in the field to provide services and products to the humanitarian community); or through investment in public infrastructure, ensuring better access to key technologies such as mobile telephony and the internet.

Inter-agency information sharing in the field

It has become increasingly clear that common standards and policy support are critical for successful ICT use in emergency operations. The 2002 Symposium on Best Practices in Humanitarian Information Exchange[16] presented guidelines for practitioners, as well as identifying challenges faced in the field. The best example of policy development is the *Tampere Convention*[17] which came into force in January 2005, and facilitates the international transportation and installation of telecommunications services for disaster relief operations. OCHA and the International Telecommunications Union are responsible for promoting implementation of the Convention; OCHA also convenes the Working Group on Emergency Telecommunications, to work on issues of deployment and interoperability. Meanwhile, groups such as the UN Geographic Information Working Group focus their efforts on data standards, which are key to sharing information more easily between agencies.

16. www.reliefweb.int/symposium/
17. www.reliefweb.int/telecoms/tampere/

There are a number of obstacles that must be overcome in order to realise fully the potential of ICT for crisis management, and the greatest obstacles are undoubtedly institutional rather than technological. Interoperability is key in this regard; ICT managers have strong incentives to build their own internal information infrastructures, and much weaker incentives to focus on inter-organisational information sharing. In practical terms this means that, although hardware and software need to be based on common technical standards to connect organisations, those organisations often procure technology from different vendors that are not interoperable. In the absence of frameworks that significantly alter these incentive structures, it is hard to build the necessary tools to overcome those institutional barriers.

Data also needs to be in common formats so that it can be shared between organisations; organisations, however, tend to become very attached to their own formats and are unwilling to change in order to share with others. Of course, when considering whether to share sensitive information, individuals and organisations need to have confidence that the security of information is not compromised. Obviously this is particularly difficult in a conflict setting, and may appear to be impossible between actors with differing interests – such as between civilian and military actors.

Inaccurate or misleading information can have serious consequences during a conflict, and even basic issues around quality of information can make people feel that sharing that information poses an unnecessary risk to their own credibility or security. However, while the question of security cannot be overlooked, ICTs can play a key role in facilitating trust relationships. The principles of Open Source Information – seen in the development of the Tarîqa information system by the EU – offer a new way of dealing with information that can avoid the traditional problems of classification and declassification.

Conclusion

Our agencies need to look beyond our traditional partnerships, to the full range of actors we work with in today's crisis management operations. It means building wider and stronger networks, based not around institutional affiliations but around communities of practice in fields such as conflict prevention, humanitarian operations and reconstruction. ICT offers both the opportunities to create and sustain these networks as never before, and also the tools to make all of our work more effective.

All of these issues must be addressed in a transparent and open manner, in a framework of trust between different stakeholders, realising that technology is a means to an end – and not an end in itself. It is only through this approach that organisations can work towards the same end goal – broadly speaking, to minimise human suffering, and enable people and communities to live with dignity – and can overcome the institutional barriers that still hold us back today.

FITTEST
Delivering critical information tools to save lives

What is FITTEST?

FITTEST is the World Food Programme's (WFP) ***Fast IT & Telecommunications Emergency and Support Team*** launched in the Great Lakes region of Africa in 1999. It provides rapid intervention in emergencies and support to WFP operations in ICT (Information and Communications Technology). Today, the response team handles numerous projects related to IT networks, electricity systems and telecommunications both for WFP and interagency projects.

How can FITTEST help?

- ***Emergency preparedness and response***
  FITTEST upgrades all aspects of IT, electricity and telecommunications infrastructures including computer hardware and software, networking equipment, radios, telephones and satellite connections, and electrical utilities. It supports ICT operations in the most demanding situations with the primary goal of improving field staff security.

- ***Standardisation and training***
  FITTEST enhances the existing ICT environment up to WFP and UN Department of Safety and Security (UNDSS) standards and helps local ICT support staff to become more efficient through on-site training.

- ***Supporting large-scale and special projects***
  FITTEST offers valuable support for a range of activities – such as office moves, interagency ICT projects and deployment of nationwide data and radio networks.

In summary, FITTEST delivers comprehensive ICT services in the fields of telecommunications (radio, telephone, satellite), IT (hardware, software, computer networks, Lotus Notes, WINGS, Internet, E-mail) and electricity (including wiring, power rectification equipment, solar power and generators). It rapidly implements integrated and sustainable ICT systems that support priority needs such as staff security.

Examples of FITTEST missions:

- At the request of the Humanitarian Coordinator, FITTEST acted as telecommunications coordinating unit for the Darfur and Sudan emergency. Enhancing the system to a level never experienced in Sudan before, with sustainable operation handed over to UNDSS in country.

- At the request of the Humanitarian Coordinator, FITTEST acted as telecommunications coordinating unit for the post-conflict Iraq re-entry, supporting the UN and NGO community by setting up the common security communications network covering the whole of Iraq, Internet cafes and radio rooms at all operational centres, including deployment and support staffing.

- At the request of OCHA and the Security Management Teams, FITTEST redesigned and upgraded the interagency security communications systems for all UN agencies in Iran, Pakistan and Afghanistan during the crisis in Central Asia.

- Assessed the common UN security telecommunications systems in Nepal, Chechnya, Iran, Bhutan, Laos, Eritrea and Honduras.

- Installed the WFP ICT and electricity systems in support of all recent emergency operations including Kosovo, Angola, East Timor, Mozambique, India, DRC, Central Asia, Iraq, Sudan, Liberia, Tsunami areas, Chad and at present Niger.

- Assessed and upgraded all WFP field operations to full UN Minimum Operational Security Standard (MOSS) compliancy for security communications.

- Provided staff training on WFP ICT systems in Kampala, Nairobi, Dakar, Panama, Islamabad and Skopje.

- Provides regular training for WFP Security officers in the usage and security management of telecommunications tools and systems.

- Coordinated/assisted in the WFP office move in Bangkok, Khartoum, Dar as Salaam and Conakry.

- Defined and documented the new WFP HF and VHF radio standards and provided training-of-trainers.

FITTEST operations

In 2002, FITTEST consolidated all its stocks and staff in the new WFP support base in Dubai. This enables the unit to respond to emergencies within 48 hours with engineers and equipment. Currently the unit has a technical stock worth USD 2.8 million enough to cater for over 23 emergency field offices. The Dubai Support Office is also providing procurement and logistics contingency services to WFP operations.

FITTEST staffing

FITTEST is a team of about 20 highly qualified engineers supported by administrative and stock maintenance staff. The team expands and shrinks following or anticipating corporate demands. The team is a core component of WFP's ICT rapid response capacity.

Who requests support from FITTEST?

- The WFP Regional/Country Office management through the Regional ICT Officer.
- WFP Headquarters in Rome.
- Humanitarian coordinator through WFP Headquarters.
- FITTEST independently identifies a priority intervention.
- In exceptional cases other UN agencies request for support, which are considered on a case by case basis.

How does FITTEST operate?

FITTEST has developed Standard Operating Procedures (SOPs) to maximise its effectiveness in the field. This includes close cooperation with local and/or regional ICT structures. In most interventions, the FITTEST team becomes an integrated part of the local set-up and reports directly to the ICT management in the designated location.

Who approves a FITTEST mission?

Initially, FITTEST develops mission-specific Terms of Reference, including a cost estimate which is approved by the Chief FITTEST. Once approved by the client and funding is identified, security clearances and travel authorizations are requested. Upon receipt of the clearances, the Chief FITTEST gives final clearance for the mission and deploys the required staff and resources to the field.

Who pays for FITTEST services and equipment?

Services and equipment are provided to the beneficiary Country/Regional Office or Interagency operation on a cost-recovery basis. FITTEST has no fixed budget that covers the team's regular operating costs, such as tools and administrative staff, but recovers its fixed costs by charging a small overhead fee for the services rendered.

FITTEST contacts:

Chief FITTEST: Mats.Persson@WFP.ORG
Technical Advisor: Martin.Kristensson@WFP.ORG
General address: wfp.dubai@wfp.org
Website: www.wfp.org/operations/Dubai_support_office

Safety Information Reporting Service

The safety and security of aid workers is essential for the effective delivery of relief and development assistance. The ability to deliver aid to populations in need depends on logistical and security considerations. The international relief community has developed very sophisticated, multifaceted logistical support mechanisms, but has only recently begun to address the security considerations of relief and development operations.

Recent events have dramatised and highlighted the critical nature of allowing aid workers to operate safely. The bombing of the Canal Hotel in Baghdad in 2003 led to temporary paralysis of UN work in Iraq; killings of camp workers in Sudan led to the withdrawal of agencies from areas of Darfur province and southern Sudan. Killings of staff in Afghanistan led to the withdrawal of Médecins Sans Frontières (MSF) from that country. The kidnapping of a CARE worker in Kabul led to a pause in development programmes in Afghanistan while negotiations were underway for her release; the threat of street violence, kidnappings, and killings continue to dramatically hamper relief efforts in Chechnya.

The Safety Information Reporting Service (SIRS) works together with lead civilian agencies to provide aid workers with information that will enhance their awareness of safety and security issues in the field.

The service's **mission** is to support lead civilian agencies in responding to an emergency. Its primary goal is to collect and provide data in a neutral, systematic, and structured manner in order to support decision-making in the field. Its primary **functions** are to collect safety and security data from participating organisations, synthesise it into an overall picture of the security situation, and present the information in a variety of formats to promote a common situational awareness.

SIRS is envisioned as an operation that coordinates support activities to NGO "security focal point" operations in the field. These kinds of operations exist in a variety of forms, sponsored by a variety of institutions, in Afghanistan, Iraq, Indonesia, Haiti, Sudan and are emerging in Kashmir, Nepal and northern Uganda. SIRS provides a variety of technical and operational assistance packages to local and regional safety information operations. Such assistance helps to improve safety of aid workers, as well as raise their awareness of the risks in their area. It also provides a better operational context for organisations considering relief and development activities.

Specifically, SIRS will aggregate and promote best practices and standard operating procedures related to creating and compiling safety assessments, developing safety communications systems, and deploying incident mapping and management systems. But more than just acting as a repository for best and current practice, SIRS acts as an agent to seek funding for local NGO security efforts and to assist with the local and regional implementation of such best practices by providing training, consulting and operational services. A result of such activities, SIRS collects safety incident data and identifies the critical needs, which can then be addressed at the local, regional and global levels. The SIRS concept grew out of a series of Information Technology and Crisis Management (ITCM) conferences begun in 2002, hosted by the Crisis Management Initiative (CMI) in collaboration with the US Institute of Peace (USIP). The 2004 conference focused on security issues as a catalyst for technical and organisational collaboration to improve security management. Participants in this conference identified the need for better tools for sharing security-related information between different actors in the field. They called for the development of a prototype of a suite of tools and services focusing on field security.

As a result of the conference, CMI and USIP pursued a project to develop a **comprehensive incident mapping, reporting and threat-monitoring service** to be used in any environment by a range of actors to share information related to the safety and security of civilian personnel.

In the summer of 2005, a joint team of CMI and USIP personnel began a stakeholder **consultation process** that led to a fact-finding trip to Kabul and Banda Aceh. This in turn led to two formal consultative meetings with stakeholders in the autumn and winter of 2005. The recommendations resulting from the field trip, plus a more formal proposal of the SIRS concept, were presented to key stakeholders at the European Union headquarters in Brussels on 13 November

2005. The participants had useful and positive feedback, and encouraged the team to proceed to vet the idea with a larger group of potential collaborators. In December, CMI and USIP hosted a meeting in Saint-Paul-de-Vence, France with 44 people from 39 organisations participating, including representatives from national governments, international organisations, non-governmental organisations and corporations.

The SIRS concept was proposed and vetted in a series of workshops held over three days that investigated and discussed aspects of moving the concept forward. Specific discussions included investigations into the concept; the security environment for aid workers; existing initiatives; potential governance structures; operational considerations; and external relationships with other types of actors including national and local government agencies; international organisations; the NGO community; military organisations; commercial enterprises; and local populations. The participants worked together to craft a provisional mission statement, goals and objectives, and brainstormed on how to move the concept to reality. Participants agreed that SIRS should become an independent organisation that represents a security focal point for the crisis management community. Until SIRS is a fully developed field service, however, CMI and its partner organisations will act as incubators for its development.

THALES ON CHALLENGES TO EUROPEAN SECURITY

Interview with Edgar Buckley

***Edgar Buckley**: joined Thales as Senior Vice President, European Business Development, in September 2003 following a career in British government and international organisation service. From 1999 until 2003 he was NATO Assistant Secretary General for Defence Planning and Operations, responsible for NATO defence policy and operational issues. From 1996 until 1999 he was the Assistant Under Secretary of State in the UK Ministry of Defence responsible for policy on military operations.*

What are the most important security challenges facing the EU at the moment and in the foreseeable future?

In its 2003 Security Strategy, the EU identified five main threats facing Europe: terrorism, proliferation of weapons of mass destruction, regional conflicts, state failure and organised crime. All of these can combine to pose even greater threats. Undoubtedly, the combination of terrorism with proliferation of nuclear, chemical and biological weapons would be the most frightening eventuality. Even without WMD, terrorism is a clear threat to our lives, our freedoms and our values. We must oppose it in every way possible, while at the same time looking to address the underlying reasons for its support by others.

In parallel, the EU must prepare to play its part in external security operations, such as the one it is currently leading in Bosnia-Herzegovina. The EU has a unique capability to combine military operations with civil support actions and to back these up with real political and economic incentives to achieve peace. It also has a unique moral authority in its region, linked to the transparency of its strategy for peace.

The EU cannot know when it will be called upon to act in a future crisis but it can be certain that such calls will come, and when they do it will have to act quickly and succeed in what it undertakes. Preparation for future crisis operations is therefore an urgent political obligation. But the EU is severely challenged by the fragmentation of authority for civil and military actions, and by problems of interoperability among the services and forces of its Member States. Technical solutions exist to enable joint, civil-military, multinational forces to come together and be deployed quickly and effectively, but political consensus to implement them is not easy to achieve.

How can the European industry contribute to the successful achievement of the objectives set in the European Security Strategy and of the build-up of a genuine European capacity?

Industry's role is vital. In the defence domain, this has long been understood and accepted. But in Europe that realisation has been slower to become established where homeland security threats are concerned. There was no mention of industry, for example, in the EU's security strategy document. By contrast, the US was quick to see that industry would have a key partner role in this sphere. Its homeland security strategy, published shortly after the September 11 attacks, gave prominence to the private sector's role.

Europe too now recognises industry's role, in particular that we need to support industrial research in the security domain in order to develop the solutions we need and to ensure that Europe maintains its appropriate influence as security standards are prepared. As evidence of this, a Group of Personalities, with strong industry representation, prepared a report for the EU Commission, which led to a Preparatory Action for Security Research and Technology. The research studies carried out under this relatively small-scale preparatory programme are already providing essential reflections and solutions. Two of them in particular - ESSTRT and SeNTRE - are aimed at guiding the EU's security research activity towards the most important new security needs as seen by the customer governments. All those involved in this work are convinced that the follow-on European Security Research Programme can significantly assist Europe to respond appropriately to current and future threats. The creation of the European Defence Agency is another indication that the importance of the supply side is now better recognised at the political level.

Industry for its part is preparing to launch a new European public-private forum in the homeland security field to deepen the dialogue and ensure that Europe's voice is heard. This forum, which will promote active participation by all sectors involved in this domain, is intended to be established early in 2006.

Looking to the three specific strategic security objectives of the Union, industry has much to contribute. So far as addressing direct threats is concerned, industry will provide new and better ways to support security monitoring and responding to attacks. This will enable European political leaders to help frame global approaches to these issues, so that they are not simply asked to accept solutions proposed from the outside. To help build security in the EU's neighbourhood, industry can act both with the Member States themselves and with neighbouring countries to deliver consistent and interoperable approaches. Finally, to assist in the creation of an effective international order, industry will play its part both by directly supporting international organisations such

as the UN, the OSCE and NATO, and by supporting international agreements such as those relating to the supply of weapons and transfer of defence technology.

In what ways can industry contribute to more effective civilian ESDP capacity and more generally to the civilian crisis response capacity of the international community?

The main challenge is to support a unified civil-military approach to deployments and operations in the field. Typically, in complex peace support operations, there are difficulties in communicating with and coordinating the efforts of all those involved. The military side, if well-organised, can effectively communicate with itself, but that is not sufficient because often it is the civil contribution which is critical: new approaches to communications and command and control are needed, to allow a more "plug and play" approach so that all those involved can share information when they want to.

There are of course other challenges. For example, assisting in establishing or re-establishing public communications facilities, public utilities and secure ground and air transport, rebuilding energy infrastructure, and ensuring minimum standards of law and order. In all of these areas and others, industry has a key role to play.

But the most important point to keep in mind is that we need to prepare for these tasks multinationally. Industry can assist in defining multinational standards to support these preparations, including in the important domain of network centric operations where work is already underway through the Network Centric Operations Industry Consortium.

What are the opportunities and challenges in developing solutions for civilian crisis response operations? How can the identified obstacles be overcome? How can we improve collaboration between stakeholders?

The main obstacles to better civilian crisis response are lack of resources, slowness of deployment, problems of communication and coordination, and mutual misunderstanding and distrust. From the EU standpoint, what is needed is that the Union and its Member States should develop rapid deployment capabilities on the civil side to complement those of their military forces, and that they should pre-plan as much as possible their working cooperation approaches to NGOs and other international organisations whom they will probably be working alongside.

We should also keep in mind the trend in government to outsource services to industry as a way of providing cheaper or better outcomes for the consumer. Outsourcing can play a role in civil crisis response operations too, for example to provide air traffic control, security or telecommunications services. Industry needs to be consulted early to be ready to provide such contributions.

The EU is already taking the lead in this domain through its civil/military planning unit. Industry can assist by contributing to standardisation and interoperability discussions. We can also support a better public-private dialogue, which may go some way towards helping build trust and support calls for increased resources. Industry sees itself as one of the stakeholders in this domain and wants to play its part in improving overall capabilities.

What is the role of the European security research programme in this development?

The European Security Research Programme (ESRP) is a key step to ensure that European industry is able to marry developing technologies to real operational requirements and with an increased tempo. The ESRP therefore needs to be established at the appropriate high level, bearing in mind that much greater sums are being devoted to this sort of research in the United States. The ESRP also offers a real dialogue between industry and the EU on the priorities for technological investment. This is a particularly important aspect since industry also needs to invest its own resources in these efforts. We are willing to do so but we need to have reasonable confidence that there will be a market for what we produce as a result. The EU has established the European Security Research Advisory Board (ESRAB) with industry to assist dialogue and help guide priorities in the ESRP. Other partners need to be heard as well, which is where a new public-private forum can play a key role.

In concrete terms, industry looks to the ESRP to assist in developing new approaches in three fields: supplying immediate operational needs (e.g. ICT systems, surveillance systems, command and control facilities); developing new technologies and applications to address security needs (e.g. early warning/detection systems, secure interoperable radios, border security systems, open-source intelligence systems – data mining); and ensuring civil-military and multinational interoperability (e.g. through developing new open standards for network centric operations). The ESRP will be a key enabler for much of this work.

Satellite solutions for disaster relief and humanitarian operations

Eutelsat Communications is the holding company of Eutelsat S.A. The Group is a leading satellite operator with capacity commercialised on 22 satellites providing coverage over Europe, the Middle East, Africa, India and significant parts of Asia and the Americas. The Group's satellites are used for broadcasting TV and radio, for TV contribution services, corporate networks, mobile positioning and communications, Internet backbone connectivity and broadband access for terrestrial, maritime and in-flight applications. Eutelsat Communications is headquartered in Paris and its workforce comprises over 450 experts from 25 countries.

Objectives

Satellite communications are particularly well suited to relief and humanitarian operations in the field, as a result of five unique features:

- coverage of very large geographical areas;
- independence from terrestrial infrastructure and natural terrain conditions;
- sharing of transmission bandwidth between all points of the network;
- instant transmission of signals to all points located in the coverage (cost is independent from the number of points); and
- complete transparency to all formats of information sent.

Eutelsat offers Disaster Recovery solutions via satellite designed to swiftly restore voice and data communications between all types of locations in emergency situations and for all types of activity for example, businesses, governmental services and NGO's.

The frequencies of Eutelsat satellites (Ku band) make them particularly attractive for the implementation of emergency systems through the use of small, low-cost and easily transportable ground terminals.

Experiences in the field

Eutelsat systems have already been used in several emergency situations, both inside and outside Europe.

Following the December 2004 tsunami in South-East Asia, the Italian Civil Protection Agency needed a solution that would help its field agents working in different location in Sri Lanka to communicate between themselves as well as with their headquarters in Rome. The solution had to combine independence from a largely destroyed terrestrial infrastructure, portability and user-friendliness, while allowing voice communications as well as e-mail, instant messaging services and Internet access for reporting on the relief effort. Implementation of the network was carried out in four days, but this period can be substantially reduced if a cell for emergency satellite communications is created either in Eutelsat or in the entities devoted to crisis management.

Another solution has been developed for NetHope, which is responsible for maintaining and operating the voice and data communications infrastructure of member humanitarian organisations in over 40 countries, from Paraguay to Nepal. NetHope was seeking a common voice and data communications solution for all its member organisations, present and future. The system had to be universal, provide coverage all over the world, including the most remote areas, be easy to use and maintain, enabling humanitarian staff to connect anywhere, anytime, while remaining affordable.

Description of the systems

Eutelsat's Disaster Recovery solutions are based on three main components:

- The satellite terminal: this equipment enables the communication via satellite and can be connected to WiFi access points to guarantee acces to satellite links by field teams working remotely from the satellite terminal. For greater ease of use in emergency situations, the satellite terminals are available in a light, portable

"Flyaway" version, and include an integrated GPS receiver, satellite modem, and Voice-over-IP adaptor, as well as a lightweight, foldable antenna.

- The broadband link Eutelsat offers two types of broadband services: dedicated (IP Connect) and shared (IP Access), depending on actual communications requirements. For the needs of humanitarian operations, the best solution has been proven to be the use of a dedicated frequency band shared among all the terminals involoved in the operations.

- The Network Operation Control (NOC) Center located in the Turin teleport that automatically provides the frequencies required by the network, continuously monitors the network status and guarantees assistance to remote terminals in the event of on-site problems.

The application in Sri Lanka comprised PCs, WiFi access points and internet connections operating through D-STAR satellite broadband terminals. The network also provided VoIP telephone and videoconferencing services between Sri Lanka and Rome. Connections were established through capacity on Eutelsat's W6 satellite, which is equipped with a steerable beam that was pointed over the region, and the Skylogic teleport in Turin.

The NetHope solution called upon Eutelsat's 2-way satellite broadband connectivity D-STAR system. This provides NetHope a one-stop, one price solution for all its member organisations around the world. The network uses capacity on four satellites, including the African beam on Eutelsat's recent W3A satellite. Communications with humanitarian staff in remote areas around the globe has been improved, and Internet access and other basic communications means have been made available to local populations.

Security

Security has to be dealt with from different perspectives. In particular:

- From the point of view of information security, Eutelsat systems enable the transmission of encrypted messages and data and the creation of Virtual Private Networks inaccessible by unauthorised persons;

- From the point of view of equipment reliability and network availability, the satellite terminals are designed and manufactured to achieve very high reliability. The same applies to the NOC, which features redundant equipment. Moreover NOC staff ensures 24/24 and 7/7 network control and assistance to remote users.

- From the point of view of on-site intervention speed, Eutelsat has an extensive network of installers, able to intervene swiftly in the different regions of the world.

Increased situational awareness in a crisis arena saves lives

Insta DefSec provides services and products for crisis management environments. Insta iCM – Inter-organisational Crisis Manager – is a solution for situational awareness and crisis management. Insta iCM is designed to facilitate decision-making and coordinating operations between crisis management organisations both in international and domestic crisis situations.

Objectives

The objective of using Insta iCM is to improve the **safety** and **security** of field personnel by improving access to relevant security-related information. Insta iCM has been developed and demonstrated together with end user organisations with the aim of developing it into an internationally interoperable management and information-sharing system for civilian crisis management organisations.

Experiences in the field

Insta iCM has been widely tested in different kinds of international and domestic crisis environments. In the Insta iCM exercise (hosted by OSCE) in Sarajevo in October 2004, all the security officers of the international organisations working in Sarajevo found the exchange of information with other organisations with the help of Insta iCM easy and beneficial for their operations. The following organisations participated in the exercise: CAFAO, EC, EUPM, EUMM, OHR, OSCE, UNRFSO and SFOR.

In September 2005 Insta iCM was used by Finnish officials in the international Barents Rescue 2005 exercise in North Norway close to the North Cape. With the help of Insta iCM the people in the field shared their situational awareness with other Finnish officials both in the exercise area and offices in Finland. Barents Rescue is a series of exercises in which Norwegian, Swedish, Finnish and Russian search and rescue officials explore their capabilities and train for joint search and rescue operations. Barents Rescue 2005 included a realistic exercise of the evacuation of more than 500 people from a passenger ship and an oil tanker that "had collided". The northern location guaranteed that the whole exercise was conducted under extreme arctic conditions.

Another concrete case where Insta iCM has been used was the CITY04 joint exercise where Finnish Search and Rescue officials cooperated in realistic training for domestic crisis scenarios in southern Finland.

Description of the solution

Insta iCM operates on modern PCs and laptops. The system is browser-based, which makes it easy to access anywhere in the world.

The ease of use and versatility of Insta iCM enable it to be quickly deployed in all kinds of crisis situation and environment. The flexible technology platform enables scenarios to be created varying from complex homeland security or international crisis environments where numerous systems and data sources are integrated to straightforward catastrophe scenarios where fast deployment and simple ease of use are essential.

Insta iCM is not dependent on any network technology, but it can be accessed over any available existing or newly deployed data network, such as GPRS, WLAN, satellite networks or TETRA.

Security

The solution supports different security levels and data confidentiality requirements. Role-based access control using PKI-based smart card authentication and encrypted information distribution is recommended for high security requirement environments. For uses where transparency is essential, the system can be configured to have low-level access control or none at all.

Insta DefSec's Security Systems provide a wide range of products, services and expertise for high-security environments. Solutions enable secure interoperability between different organisations, networks and systems.

ANNEX 1: EXTRACTS FROM THE REPORT ENTITLED:

"For a European civil protection force: Europe Aid" by Michel Barnier

Introduction

In January 2006 Wolfgang Schüssel and José Manuel Barroso, Presidents of the Council of the European Union and of the European Commission respectively, asked me to draw up a report on the EU's response to major cross-border emergencies for the June European Council.

Since the tsunami of 26 December 2004, the EU and other players, in particular the United Nations, have been eager to improve their response to emergencies. Since January 2005 the EU has been working on the basis of an action plan. Successive EU Presidencies have since shown their resolve to boost the EU's capacity to show solidarity at home and abroad.

As the tsunami so tragically bears out, **the price of non-Europe in crisis management** is too high. First and foremost, a series of hastily organised individual responses is no match for an EU response that has been planned, organised and tested against specific scenarios. Secondly, multiplying responses results in a lack of coordination that diminishes the EU's impact and visibility on the ground. The EU response can only be made more cost-effective by properly organising the Member States' civil protection capabilities and consular assistance on the basis of common scenarios, training programmes and exercises.

When drafting this outlook report, I naturally took account of the progress of the many projects under way at the Council (especially in the Permanent Representatives Committee) and the Commission. I had talks with a number of Member States, and I sounded out the Commission and the Council's General Secretariat.

When all is said and done, I wanted to place the work under way in a political context.

I have therefore taken the calculated risk of framing my proposals and the associated timetable in the medium term, and more specifically with an end date of 2010, by which time, one way or another, the countries of the EU will have created **the post of Union Minister for Foreign Affairs, provided for in the Constitution, which they wanted and accepted unanimously in Rome**. By 2010 the Council, the Commission and the Member States will be working together more effectively on the EU's external action. I therefore hope that the reader will make the same mental leap into the medium term. This is the only way in which we can get over the present hurdles and shortcomings. I also hope that no more disasters will be needed in the interim to set our thinking, resources and expertise on the right track.

My mission statement[1] poses the question of what the EU can do to improve its response, especially to major emergencies **outside the EU**.

External emergencies differ in a number of ways from emergencies inside the EU:

- They affect **sovereign states**, which are free to decide how to respond to an emergency and whether to request assistance from abroad.
- The **EU Presidency** coordinates the response politically in close cooperation with the **United Nations, national and local authorities in the country concerned and non-governmental organisations**. We need to find ways to increase the speed and effectiveness of their collective decisionmaking.
- There are **many tools at the EU's disposal**. Naturally, national or regional civil protection resources can be drawn on. At any rate, we have a presence on the ground through humanitarian aid, coordinated at international level by the United Nations and channelled at EU level through ECHO (European Commission Directorate-General for Humanitarian Aid). Last but not least, the EU implements reconstruction programmes. We need to work out how best to pool these resources and maximise synergies.
- Such emergencies, often in far-off places, affect more than one country and call for **capability projection**. This projection of men and resources is currently lacking.
- Lastly, such emergencies call for **consular assistance**, since EU citizens are naturally more vulnerable when they are far from their country of origin. In 2003 there were more than 30 million trips by Europeans outside Europe. The falling price of air travel will increase this number in the years ahead. In the Indian Ocean tsunami of 26 December 2004 about 200 000 people died and thousands disappeared. In Thai-

***Michel Barnier** is the Former French Minister for Foreign Affairs and former Member of the European Commission.*

1 ???

land alone, 2500 foreign tourists, many of them EU citizens, died. At issue is whether the Member States of the EU are willing and able to work together to improve their assistance to citizens in difficulty.

Obviously, if the Member States and the EU institutions take up the proposals outlined in this report and decide to improve our civil protection response considerably, **that will apply to emergencies in far-off places as well as to disasters within the territory of the EU**. In 1999 Turkey and Greece were hit by earthquakes at the same time. In the more distant past, some 100 000 people were killed by an earthquake and tidal wave that destroyed the Sicilian city of Messina in 1908. Exactly twenty years ago the Chernobyl disaster, just across the border from the EU, affected the whole of Europe. And the bombings in Madrid and London have shown that a European September 11 is possible.

The need for Europe

Our countries' citizens **need new proof of the EU's value added**. Voters in France and the Netherlands have told us this quite bluntly.

Whether it is the earthquakes or storms of 1999, the wrecks of the *Erika* and the *Prestige* off our shores, the floods that hit Central Europe in 2002 and again this year, whether it is the tsunami or the earthquake in Pakistan, **Europe is expected to show solidarity: the EU is called on to act and the Member States asked to help**.

Obviously, a better EU response to these emergencies reflects a real duty to help as well as responding to the citizens' political expectations. It has been at the very heart of the European project for fifty years now. **Since 1950 Europe's peoples have shown solidarity towards each other but also towards the other peoples of the world.**

It is not by chance that we find this demand for solidarity in two recent initiatives:

- The **European Union Solidarity Fund** set up in 2002 at the behest of the Prodi Commission in the wake of flooding in Germany, the Czech Republic and Austria can mobilise 1 billion a year for devastated regions of the EU.

- The **draft European Constitution**, for its part, contains a solidarity clause (Article urces, to protect democratic institutions and the civilian population in the event of terrorist attack or natural or man-made disaster.

The same needs are being expressed and the same proof asked for beyond our continent: international instability, new threats and environmental hazards oblige us to respond. The citizen has consistently asked for this: as recently as December 2005,[2] 77% of EU citizens expressed their backing for a common foreign and security policy and 68% for a common external policy.

Javier Solana has clearly identified the five main threats facing Europe:[3] terrorism, proliferation of weapons of mass destruction, regional conflicts, failed states and organised crime. The governments of each and every Member State have a duty to protect themselves and to respond to these new geopolitical threats. It is also in their interest to do this together.

The Treaties and the risks being what they are, **we can and must find the will and the resources to act together more effectively now**.

But one way or another, sooner or later, we will need the solutions offered by the draft Treaty establishing a Constitution for Europe, and in particular the following innovations:

1. a **Union Minister for Foreign Affairs** with authority over all services involved in external action (external relations, development assistance and humanitarian aid); a **European External Action Service** will help the Minister fulfil his or her mandate (Article III-296);

2. the **solidarity clause** (Article I-43) referred to above and its implementing procedures (Article III-329);

3. a **European policy on the prevention of natural disasters and on civil protection** (Article III284);

4. **EU action on humanitarian aid** in the context of the principles and objectives of the EU's external action (Article III321);

5. a **public health** policy covering, in particular, the fight against the major health scourges (Article III-278);

6. **enhanced cooperation** (Articles I-44 and III-416 to III-423) making it easier for those Member States that wish to take things further and faster to do so.

2 *Eurobarometer 64 – December 2005.*

3 *European Security Strategy, proposed by Secretary-General/High Representative Javier Solana and adopted by the Heads of State and Government at the Brussels European Council on 12 December 2003.*

What the EU is already doing

Since the early 1990s the EU has been able to respond to emergencies.[4] The Humanitarian Aid Office (ECHO) was set up in 1992. The Commission – like a number of Member States – is already a very active member of the Good Humanitarian Donorship Initiative and of the donor support groups set up by the International Committee of the Red Cross and the UN Office for the Coordination of Humanitarian Affairs.

In 2001 Margot Wallström, who was Environment Commissioner at the time, proposed a Community Civil Protection Mechanism, which triggers a movement of solidarity in the event of emergencies both inside and outside the EU. Depending on the circumstances, this solidarity currently involves pooling certain resources available in the Member States (transport, equipment, medical teams, etc.). It is designed to respond to the consequences of natural and man-made disasters (industrial and maritime accidents, terrorist attack, etc.).[5]

Lastly, the EU has worked to consolidate its emergency response and provide back-up over time.[6] Preparing reconstruction and stabilising fragile political situations are two key areas of EU action. Just as humanitarian aid and the rapid reaction mechanism[7] have their role to play, so do large-scale reconstruction programmes.

Moreover, since 2003, at the prompting of Javier Solana and the Council of the European Union, civilian crisis-management operations in the context of the European Security and Defence Policy (ESDP) have been added to this arsenal, helping respond effectively to emergencies with a common foreign and security policy dimension. Twelve such missions are currently under way in, for instance, Bosnia in the Balkans, Rafah in Palestine and Aceh in Indonesia.

Building on and learning from this, I have worked out 12 practical, operational solutions. They address **three concerns**:

1. **making humanitarian aid and civil protection more effective**,
2. **providing EU citizens with greater protection and assistance**,
3. **strengthening overall consistency**.

Twelve proposals for improving the European Union's crisis response capability

Our **twelve proposals** for improving the European Union's crisis response capability rest on the ideas developed in the second part of the report and on progress in the projects and discussions currently under way in the Council, the Commission, the European Parliament and the Member States.

In general they call for **voluntary participation by the Member States** and they are spread over a four-year time-frame.

We propose:

1. **A European civil protection force: "Europe Aid"**
2. **Support for the force from the seven outermost regions of the European Union**
3. **The setting-up of a Civil Security Council and a greater role for the General Affairs and External Relations Council**
4. **A one-stop shop for the European Union's humanitarian response**
5. **An integrated European approach to crisis anticipation**
6. **Six European Union delegations to specialise in crisis management**
7. **A clear information system for European Union citizens travelling outside the Union**
8. **The pooling of consular resources**
9. **The creation of consular flying squads**
10. **The setting-up of "European consulates" on an experimental basis in four geographical areas**
11. **The establishment of a European consular code**
12. **Laboratories specialising in bioterrorism and victim identification**

4 *See pages 43 to 46 of the technical report for further details.*

5 *Council Decision of 23 October 2001 establishing a Community civil protection mechanism.*

6 *See pages 47 to 49 of the technical report.*

7 *Council Regulation (EC) No 381/2001 of 26 February 2001 creating a rapid-reaction mechanism.*

Proposed timetable

1 July 2006 – 30 June 2007 (Finnish and German Presidencies)

- **Humanitarian aid/Civil protection**

1. **Establishment within a year of the following seven scenarios** - MIC in close cooperation with the Member States and the stakeholders (other Commission Directorates-General, the Council General Secretariat's Civil/Military Cell):
   - earthquakes and tsunamis
   - forest fires and other fires
   - flooding
   - industrial and nuclear accidents
   - terrorist attacks
   - disasters at sea
   - pandemics.

2. **Establishment of "menu" of needs for each scenario.**

3. **Those Member States that wish to do so start taking account of the "menu" in their organisation.**

4. **Alignment of MIC and ECHO emergency structures for external relations.**

5. **Reinforcement of MIC** with Member State experts to form the basis of the operations centre.

6. **European Council decision to establish a EuropeAid civil protection force**.

- **External relations**

1. Study into possibility of "common" financing from the CFSP budget for **operations to evacuate** EU citizens abroad.

2. **Empowerment of heads of delegation** to act in emergencies in liaison with Member States' diplomatic and consular services and establishment of contingency fund for heads of delegation.

3. **Identification of six regional delegations** and preparation of organisational set-up for three of them.

4. Establishment of structure for the two "emergency" and "consolidation" databases.

- **Assistance to EU citizens in the event of a crisis/Consular matters**

1. **Assessment of the Member States' consular capacities,** in order to anticipate needs in the event of a crisis, and identification of best assistance and evacuation practices at national consulates abroad.

2. Preparation of Commission proposal on the four pilot areas for establishing EU consulates.

3. Start of work on EU consular code.

1 July 2007 – 30 June 2008 (Portuguese and Slovenian Presidencies)

- **Humanitarian aid/Civil protection**

1. In follow-up to the Berend Report, the Council, Commission and Parliament hold a tripartite meeting to adapt the EU Solidarity Fund Regulation to finance civil protection training and the purchase of certain types of equipment.

2. Preparation of operations protocols by the "enhanced MIC" (future operations centre) assisted by the Member States and the Council General Secretariat.

3. Feasibility study on legal cover necessary for civil protection missions within the EU.

4. Stepping-up of joint training and implementation of an annual exercise open to all Member States and organised by the future operations centre.

5. Commission proposal for setting up a European civil protection force (EuropeAid). Adjustment of visibility factors for external aid.

6. Setting-up of "Civil Security" Council by Heads of State and Government.

7. Launch of feasibility study for foundation or specialisation of a European victim-identification laboratory and one or more laboratories specialising in bioterrorism.

- **External relations**

1. Entry into service of the three regional delegations specialising in crisis management after finalisation of organisational setup.

2. Introduction of new administrative and financial framework for heads of delegation.

3. Creation of the two "emergency" and "consolidation" databases.

4. Training of first joint assessment teams for "emergency" and "consolidation".

5. Application of institutional provisions on external action and civil protection.

- **Assistance to EU citizens in the event of a crisis/Consular matters**

1. Identification and training of consular flying squads of volunteer diplomats.

2. Presentation and adoption of the Commission proposal on the four experimental regions for setting up EU consulates. Failing that, enhanced cooperation for those wishing to press ahead.

3. Presentation of Commission proposal for **an EU consular code.**

1 July 2008 – 30 June 2009 (French and Czech Presidencies)

- **Humanitarian aid/Civil protection**

1. Discussion in Council of act creating the EuropeAid European civil protection force.

2. At end of period, adoption of act creating the EuropeAid European civil protection force or, failing that, start of enhanced cooperation between those countries wishing to press ahead under Article 43 (Title VII of Treaty on European Union).

3. Setting-up of the force's operations centre and training college. Choice of college's location by Council.

4. Proposal for EU regulation on the legal cover necessary for civil protection operations within the EU.

5. Initial application of scenarios and their testing during the annual exercise.

- **External relations**

1. Evaluation of first three regional delegations specialising in crisis response.

- **Assistance to EU citizens in the event of a crisis/Consular matters**

1. Introduction of consular flying squads and first joint training courses.

2. Evaluation of working of four experimental regions and extension to other areas.

1 July 2009 – 30 June 2010 (Swedish and Spanish Presidencies)

- **Humanitarian aid/Civil protection**

1. Launch of initial approval procedures for units of the "EuropeAid" force. The Member States choose items from the proposed "menu" that they undertake to make available to the force.

2. Grouping of humanitarian action and civil protection under the authority of a single European Commissioner.

3. First integrated operation involving humanitarian aid and the resources of the European civil protection force.

- **External relations**

1. Extension of organisational set-up of first three regional delegations to another three.

- **Assistance to EU citizens in the event of a crisis/consular matters**

1. Drafting of an EU consular code.

2. Foundation or specialisation of a European victim-identification laboratory and laboratories specialising in bio-terrorism.

3. Adoption of EU consular code. Failing that, enhanced cooperation between those countries wishing to press ahead.

European Commission

Faster and more united? – The debate about Europe's crisis responses capacity

Luxembourg: Office for Official Publications of the European Communities

2006 — pp. 411 — 29.7 x 21 cm

ISBN 92-894-9952-4