

**Conference on Crisis Management and Information Technology**  
**“Security –the Common Denominator for Connectivity”**  
*Nice, 3-6 November 2004*



## **1. Background**

The first Crisis Management and Information Technology conference was held in Helsinki in September-October 2002. It was initiated by the Crisis Management Initiative (CMI), a non-governmental project that aims to improve the capacity of the international community to deal with crisis situations and post-conflict rehabilitation through practical and innovative joint projects. This first conference was co-organised by the Object Management Group (OMG), a non-profit consortium that produces and maintains computer industry specifications for interoperable enterprise applications.

In September 2003, the second conference was held in Helsinki, this time with the United States Institute of Peace (USIP) as co-organisers with CMI. USIP had previously established its Virtual Diplomacy Initiative, a project to follow the effects of new Information and Communication Technologies (ICTs) on the nature and conduct of international relations and to explore how to use new technologies (such as remote sensing, GIS, and internet-based solutions) to respond more effectively to humanitarian crises and conflicts with an international aspect.

During the second conference, security emerged as a critical issue for the application of new technologies to crisis management in the field<sup>1</sup>. As a shared interest of the diverse actors in crisis management – UN, intergovernmental organisations, NGOs, local government – security management offers opportunities to develop working relationships that form the basis for further cooperation and coordination. At the same time, however, security can constrain the successful deployment of ICTs, and is therefore a key concern in the development of new technologies.

These issues had already been noted by the Brahimi Report on peace operations in 2000<sup>2</sup>, but they have become of greater concern since the events of 11<sup>th</sup> September 2001, particularly given experiences in Iraq. However, discussions around security are wider than the war on terror, and security is therefore the subject of the third conference in the series, to be held in Nice, France, in November 2004. CMI and USIP will again co-organise this third conference, which will be hosted by UNISYS, the multinational IT company.

The objective of this conference is to explore the potential that connectivity – both technical and organisational – has to improve security mechanisms, and also to discuss the impact of insecurity on connectivity in the field during and after a crisis. The key question is how does security – as a common concern of the crisis management community – catalyse information sharing – and consequently, how can ICTs facilitate that sharing process? This question must be approached from the perspective of the ultimate goal of any such efforts – saving the lives of both those working in the field and the communities they are working for.

The conference will also continue to explore the theme of the previous meetings, that of interoperability at the political, organisational, field, and technical levels. Of particular importance is the role of these conferences in bringing together representatives from the crisis management community to discuss their ICT needs with private sector vendors in information systems and technology. The 2004 conference aims to build on the co-operation expressed at the previous conferences with the specific goal of increasing both security and connectivity in the field.

---

<sup>1</sup>Crisis Management Initiative (2004) “Towards Interoperability in Crisis Management”, Final Conference Report

<sup>2</sup>Brahimi et al. (2000) “Report of the Panel on United Nations Peace Operations”

**Conference on Crisis Management and Information Technology**  
**“Security –the Common Denominator for Connectivity”**  
*Nice, 3-6 November 2004*

This Paper explores some key issues in security and security management in crisis situations, providing a framework for conference discussions on how ICTs can support organisations in this important aspect of their work.

## **2. Defining the Secure Environment**

Security management has become one of the key issues in crisis management, both during and after conflicts. A number of trends that have emerged following the end of the Cold War – the targeting of aid workers and journalist, an increased prominence for human rights law, the specific needs of large-scale nation-building, a new focus on the rule of law – have been brought into sharp relief by events since 9/11. In particular, a tension has emerged between the legitimate security needs of states in combatting criminal and terrorist activities and the broader needs of what has become known as “human security.”

The human security approach is a deliberate attempt to move beyond state-centred notions of security, since it views measures taken to protect state security as valid only insofar as they promote the security of the individual. Tension arises because the human security concept requires a holistic approach to security, ensuring that activities aimed at improving security do so with the clear intention of improving the security of the individual – rather than simply the security of the state.

For some policy-makers, this represents a potential conflict with national security needs, particularly in the context of the war on terror. Despite these concerns, this new security paradigm has been welcomed by many, and it seems likely that human security will become a normative idea in international relations in the future. For our purposes, human security will be defined as by the International Commission on Intervention and State Sovereignty, as “the security of people, their physical safety, their economic and social well-being, respect for their dignity and worth as human beings, and the protection of their human rights and fundamental freedom”<sup>3</sup>.

This formulation may sound vague when applied to the specific requirements of crisis and post-crisis situations, but in fact it offers an increasingly solid framework for discussion of the sometimes conflicting needs of relief and development work on the one hand, and peacekeeping and reconstruction on the other. The question for crisis management organisations is how to translate this into practical measures that can increase the effectiveness of their work while maintaining a clear focus on the end goal – the assistance of people in need. It is in this context that this conference will examine two layers of the current security debate.

The first, **organisational security**, is the question of security during conflict, including the security of relief deliveries and other humanitarian work (including codes of conduct), civil-military co-operation, the privatisation of security functions, information security, and the role of media. The second is **state security**, defined as the process of building the capacity of a post-crisis state to manage its own security, while ensuring that any international presence retains a basic minimum standard of security. State security includes handover from international military and police forces to national counterparts, the role of international police forces (particularly the question of executive vs advisory roles), and the role of a functioning judicial system for public security.

### **2.1 Organisational Security**

While insecurity has always been an unavoidable part of working in crisis situations, recent developments have raised some critical questions about striking the right balance. A white paper prepared earlier this year by the Humanitarian Information Unit of the US government stated that “aid workers experienced more fatal attacks in 2003 than in any prior year,” coinciding with “an increase in terrorist tactics targeting UN and non-governmental organization (NGO) activities”<sup>4</sup>.

It is not just humanitarian organisations that are affected by these problems - diplomatic missions in Iraq

---

3ICISS (2001) “The Responsibility to Protect”, Report of the International Commission on Intervention and State Sovereignty

4King, D. (2004) “The Year of Living Dangerously: Attacks on Humanitarian Aid Workers in 2003”, Humanitarian Information Unit, White Paper

**Conference on Crisis Management and Information Technology**  
**"Security –the Common Denominator for Connectivity"**  
*Nice, 3-6 November 2004*

have also had problems identifying staff prepared to work in these conditions. The deliberate targeting of aid workers, journalists, contractors and diplomats was a worrying trend even before September 11, particularly for the first two groups, who have traditionally relied on perceptions of their neutrality to protect them. And it is not just international staff that are in danger; national staff are often more at risk, while at the same time frequently excluded from many of the basic security measures that international staff take for granted.

The capacity of organisations to carry out their work is proportionately reduced by deterioration in the security situation. The situation in Iraq is exceptional, but provides a useful illustration. The withdrawal of large numbers of NGOs from Iraq and the unwillingness of the UN to return following the Canal Hotel bombing demonstrate a welcome new awareness of security issues within the humanitarian community – but they also show a new caution that potentially constrains humanitarian activities.

While improvements in security procedures are to be welcomed, will this new security environment prevent organisations from delivering the assistance needed by populations in need? This issue was recently highlighted by the French NGO Medecins Sans Frontieres (MSF), who have withdrawn from Afghanistan after 24 years, citing rising insecurity in the areas in which they work. Their withdrawal reminds us that of course it is beneficiary populations that suffer the most, continuing the trend begun in the twentieth century of civilians being the main victims of war. As the United Nations' work on the the protection of civilians in armed conflict has pointed out, "[w]ith the upsurge of global terrorism, a new kind of threat to civilians has emerged, one that may significantly increase the scale of suffering in the future and severely impact on the efforts of the international community to protect civilians, particularly the need to separate civilians from combatants"<sup>5</sup>.

The behaviour of the US military was cited by MSF as a factor in their decision to withdraw. The wars in Afghanistan and Iraq have opened up the debate about civil-military relations that has been simmering since the end of the Cold War, frequently accompanied by accusations of incompetence, deception and malicious intent on both sides. NGOs are still working through how to approach their interaction with the military, but are gradually moving towards a more defined collective position<sup>6</sup>. Meanwhile, the United Nations system has responded by developing guidelines on relations with the military and the use of military assets, both in the context of Security Council-approved peace operations and outside.

While many of the political questions around civil-military relations still require discussion, this should not be at the expense of developing guidelines to ensure that essential information is shared in appropriate and timely ways, while allowing both sides can meet their minimum requirements for sensitivity and confidentiality of that information. Technical agreements on measures for improving security management can be made in areas such as shared communications resources, procedures for incident reporting, and ensuring that civilian actors are aware of military operations in the areas where they work. By laying out parameters for co-operation with government, civilian and military agencies based on clear humanitarian principles and good practice, such guidelines can act as standard operating procedures for both sides and consequently help build better working relations.

A security assessment carried out earlier this year in Liberia by the NGO community found that "the ability of agencies to communicate emergency related information, particularly in areas outside Monrovia, emerged as a central issue." In the operational environment, the question of information-sharing dominates the security debate – how information should be shared, who should it be shared with, how sensitive information should be handled – to the extent that NGOs have now begun to establish their own security focal points in some countries, notably Afghanistan and Iraq.

The assessment continued, "[i]n planning for expanded operations around the country, NGOs are understandably concerned about how their operations in up country locations can best communicate with UN agencies and/or UNMIL forces in the event of an emergency"<sup>7</sup>. The single weakest link in the security

---

5UN (2002) "Report of the Secretary-General to the Security Council on the protection of civilians in armed conflict", United Nations Security Council Report S/2002/1300

6Barry, J., with Jefferys, A. (2002) "A bridge too far: aid agencies and the military in humanitarian response", Humanitarian Practice Network, Network Paper 37

7InterAction (2004) "NGO Security Assessment Mission to Liberia", Final Report

**Conference on Crisis Management and Information Technology**  
**“Security –the Common Denominator for Connectivity”**  
*Nice, 3-6 November 2004*

environment is this interface between UN and non-UN bodies, and even within the UN there are frequently problems communicating between different offices.

This has been a consistent theme in peace operations: a 2003 study of the UN Mission in Kosovo (UNMIK) found that “uncoordinated media of communication reduced the degree of responsiveness of the network”, citing an example of a traffic accident encountered by the researcher; the lack of a direct link to the Kosovo Police Service meant that “the delay due to the circuitous route to the police could potentially have serious consequences in a security situation, for instance, in a riot or potential riot-producing situation, neither of which was uncommon”<sup>8</sup>.

## **2.2 State Security**

The bombing of the UN Baghdad headquarters in August 2003 – a key event in defining the new security environment – has led to some improvements in UN systems, but there is still a lot of work to be done to ensure that any systems that are established successfully integrate all mission agencies, and can be extended to non-UN actors as well. Perhaps the most important examples of the importance of an inclusive approach to security management have been in the Balkans, where there has been greater regional involvement from organisations such as the OSCE, NATO and the European Union.

Missions such as Kosovo and Afghanistan demonstrate that there is no clear division between organisational and state security. The factors that led MSF to withdraw their humanitarian mission from Afghanistan are the same factors that are placing the impending elections in jeopardy. On 21 August, the UN staff association in New York requested that all UN staff should be withdrawn from the country until new security procedures are in place. This call was rejected firmly on 22 August by the UN mission in Afghanistan, but there are still concerns that the October elections will be disrupted by attacks from revived Taliban forces. In Afghanistan, organisational security issues have an immediate effect on state security initiatives.

It is impossible to identify a clear cut-off point between 'crisis' response and longer-term projects. The idea of a 'continuum' from relief to development is increasingly discussed as a 'contiguum' in which different stages may be present in the same country at the same time. Despite this problem of definition, state security issues need to be discussed separately from security during the crisis period, since state security encompasses issues other than simply organisational security. Sudan is an excellent example of this; the needs of different parts of the country differ greatly, from the humanitarian crisis in the West, to the return and reconstruction processes of the South, to the development needs of the central areas. Each region requires very different approaches from the international community – but always within a coherent and coordinated framework.

Sudan also offers a good example of the need for the human security approach mentioned above. /For whatever reason, the Sudanese government is unable to meet the basic security needs of the people of the Darfur region, whether in dealing with rebel attacks on one side or controlling the activities of the Janjaweed militias on the other. The question of security is not just a matter of providing protection for the refugee camps, food security for the displaced or peacekeepers to enforce a ceasefire. It also requires constructive (and more complex) engagement with the government to strengthen the capacity and willingness of the state to extend their shelter to all the citizens of Sudan.

In states requiring comprehensive rebuilding after conflict (frequently, but not always, 'failed' states), the reconstruction process requires that the civil and military security apparatus function effectively. In Iraq, it was a priority for the Coalition Provisional Authority to stand up the Iraqi police force as soon as possible, in order to hand over responsibility for law and order as quickly as possible – a process which is still ongoing, even after the formal end of the occupation. The attachment of international police forces has been a recurring feature of larger UN missions in the last 5 years, raising many new questions around their role – whether operational, developmental or advisory – and how that role can be successfully handed over when the mission comes to an end.

---

<sup>8</sup>Holohan, A. (2003) “Cooperation and Coordination in an International Intervention: The Use of Information and Communication Technologies in Kosovo”, Information Technologies and International Development, Vol 1, Number 1

**Conference on Crisis Management and Information Technology**  
**“Security –the Common Denominator for Connectivity”**  
*Nice, 3-6 November 2004*

Information sharing becomes a much more sensitive issue when viewed across the gaps between organisational mandates. In a peacekeeping operation, the security goals of the military may not be synchronised with the aims of the legal department – for instance, in the need to maintain civil order versus the need to bring war criminals to justice. The security goals of a political mission will frequently clash with the goals of humanitarian agencies. And, most vitally of all, the aims of the international component may not be entirely in the interests of local actors.

As reconstruction processes move forward, security becomes increasingly focused on state security and rule of law. Lines of communication and authority become more complicated as local government bodies take on more of their responsibilities, but the ability of the government to provide security for its citizens is a basic indicator of progress for both government and citizens alike. Essential nation-building functions, such as elections, require secure environments that can only be provided on a long-term basis by national institutions (including civil society organisations) that provide for the rule of law.

As well as ensuring that individual institutions (such as the police or judiciary) are well-supported, it is also essential to make certain that these institutions are well-coordinated – and that depends on good inter-agency communication. The National Commission on Terrorist Attacks Upon the United States recently found that intelligence and law enforcement agencies were not effectively sharing information, and steps are now being taken to address this<sup>9</sup>. The same needs for inter-agency information-sharing channels apply no less in countries such as Bosnia and Herzegovina, but perhaps with greater urgency, since the viability of the entire state relies on the effective functioning of these institutions during the long, slow reconstruction process.

However, in essentially failed states, police and military forces may have become criminalised through involvement in illegal activities or complicity with political groups. In such cases, state institutions can be a source of insecurity, particularly for local populations, and co-operation at all levels – including sharing information – becomes more problematic. It is essential that government agencies are brought into both formal and informal information-sharing processes, and are given access to the technology necessary to make them effective and viable long-term partners. At the same time, any such partnership must be part of wider efforts to decriminalise state institutions and prevent both information and technology reinforcing existing disruptive power structures.

### **3. Delivering Connectivity in Insecure Environments**

If we define connectivity broadly as *access to information via appropriate ICTs*, it is clear that, in the context of crisis management, security is a prerequisite for improving connectivity in operations – and that, increasingly, connectivity is a prerequisite for improving security. But what does this mean in practice?

The most clearly expressed need in the field is the sharing of security information during crisis situations. Effective communication to gather and share information is a basic prerequisite for security management. While new information and communications technologies make it possible for crisis response organisations to establish new and more effective security mechanisms, those organisations also face challenges to successfully apply those technologies.

Speaking via a videolink from Kabul at the 2003 conference, CARE explained how their vehicles were sent out in southern Afghanistan without any radio communication, simply because a radio antenna on the car would make them a target for criminal and terror attacks<sup>10</sup>. Basic radio communications can become a security risk in certain environments, effectively negating any of the gains that might be had from other improvements.

Connectivity in insecure environments must be approached from two directions: firstly, the technical specifications of building the physical infrastructure to ensure connectivity; and secondly, the organisational and inter-organisational structures to make sure that any infrastructure is used effectively and appropriately. Both of these rely on establishing standards and policies that create a common platform for connectivity, as underlined by a recent UN OCHA report. The report, reviewing requirements

---

<sup>9</sup>National Commission on Terrorist Attacks Upon the United States (2004), Final Report

<sup>10</sup>Crisis Management Initiative (2004) “Towards Interoperability in Crisis Management”, Final Conference Report

**Conference on Crisis Management and Information Technology**  
**“Security –the Common Denominator for Connectivity”**  
*Nice, 3-6 November 2004*

for maintaining a UN presence in insecure situations, recommended that “[a]ccountability for compliance with standards and rules is an essential element of security management. These, and the [technical] support provided, should be appropriate for the specific context and requirements of the humanitarian operation”<sup>11</sup>.

The problem of interoperability – both technical and organisational – is central to this discussion. There are significant differences in the resources available to organisations, making it difficult to establish a common platform. Even when a common network exists, systems still need to be agreed to ensure that it is used appropriately and effectively. For example, when e-mail is used to the exclusion of other forms of communication – for announcing meetings, or circulating minutes afterwards – it excludes organisations with poor access, particularly local organisations who may have no access at all. This is a minor inconvenience during quieter times, but it becomes a security risk if the situation deteriorates, when over-reliance on a single means of communication becomes a weakness that can affect the entire mission.

Some technologies act as disruptive influences, as well as enabling factors; mobile phones, for example, have become a very common technology in crisis situations in the last 5 years. Undoubtedly mobile telephony has made communications in the field much easier and more productive; last year’s ITCM conference heard how WFP and the Ericsson Response Team were able to establish a mobile phone network in Kabul for the aid community and Afghan government. The role of the private sector in providing ICT support in this way needs to be developed further, particularly in the pre-deployment stages.

With reference to the example above, however, it is worth noting that the head of UN security in Afghanistan expressed his concern that the reliance on mobile phones was eroding the use of the radio network, which has traditionally enabled far more secure communication. In the event of a major security alert, the mobile telephone network could collapse due to the number of users, stranding staff members without useable communications in an insecure situation. This does not mean that there is no place for mobile telephony; but it must be considered as part of a wider system that uses the most appropriate tools for the most essential tasks.

A common but simple example of this is the phone tree used in many insecure situations, in which organisations sign up to an agreed hierarchy that facilitates the rapid dissemination of critical information. Previously this would have been done by radio; recently, mobile phones have taken the place of radio handsets. The strength of the system is that it does not rely on a single technology, and can be used with any method of communication as appropriate.

The phone tree is an example of a distributed network approach to communication requirements; the alternative is a centralised system, such as the Humanitarian Operations Centre (HOC) in Liberia. The HOC has acted as a clearing house for logistics-related issues, with staff that organisations can contact either by radio, phone or in person. With civil-military liaison, logistics experts and clear access to the UN security co-ordinator in place, it was invaluable for planning assessments, requesting military assets for deliveries, and getting the latest information<sup>12</sup>.

The distributed network approach and the centralised “common services” approach have their own advantages and disadvantages. One example of this is access to the internet, the other major connectivity tool available to organisations working in the field. In some cases, a “common service” can be established – for instance, by the WFP Fast IT and Telecommunications Emergency and Support Team (FITTEST) – to provide connectivity. However, this approach leaves the community vulnerable – for instance, if the sole provider leaves because its funding runs out. On the other hand, a consortium – such as the US NGO group NetHope – can introduce its own internet solution, but this will necessarily be limited to the members of the consortium. The barrier to entry for internet access is high for smaller organisations, who often end up relying on the generosity of their colleagues or commercial providers (who may in fact be more reliable).

---

11UN OCHA (2004) “Maintaining a UN humanitarian presence in periods of high insecurity: learning from others”

12WFP (2004) “Review of the UNJLC Operation in Liberia: Summary Report - Final”

**Conference on Crisis Management and Information Technology**  
**“Security –the Common Denominator for Connectivity”**  
*Nice, 3-6 November 2004*

The centralised and the distributed approaches can be seen as points at opposite ends of a continuum, but whichever approach is taken must be based on collective agreement. Such agreement needs to be made prior to deployment, and not during the deployment itself, as has often been the case in the past. Agreements such as these need to cover a range of issues, including the question of ownership and control of communications infrastructure.

This last is of particular importance in state security development, when there will be increased local government involvement. Although in many failed states government involvement is weak, eventually the responsibility for regulating any large-scale ICT infrastructure usually lies with the national government. This is an issue of key importance to the private sector, who need such a regulatory framework in order to secure investment and establish their own operations. It is therefore critical to involve government in this aspect of the reconstruction process and ensure that, wherever possible, any developments are appropriate to that country and can be handed over as part of the transition.

#### **4. Next Steps for the ITCM Conference**

The ITCM conference will create the space to discuss many of the issues outlined above, and perhaps the opportunity to reach agreement on how to resolve some of those. Conference participants should aim to arrive at practical steps that can be developed to lay the foundations for a comprehensive solution to common ICT problems faced in the field for both the organisational and state security aspects of crisis management.

Of particular concern to the conference organisers is the importance of developing common standards and policies for ICTs. This is one area where it is possible to reach agreement on interoperable technical solutions and their deployment in the field. The best example of this is in the field of emergency telecommunications, where there is consensus that appropriate communications technology is central to effective crisis response. As a result, the Tampere Convention on emergency telecommunications (discussed at the previous two ITCM conferences) was developed to create a common platform, and is now close to being ratified. There are many other areas where this approach could be explored, such as wireless connectivity and security tracking databases.

As well as technical standards, there is great potential in the development of inter-organisational agreements, drawing on examples of good practice from the participants' own experiences. Protocols for sharing information are being developed in some countries, but without much detail about the type of information or the methods that should be used. Security information must be shared as a prerequisite for successful operations for all parties, but a number of important questions must be answered. What sort of information? How will it be used? Who will make best use of it? What are the appropriate mechanisms for sharing?

There needs to be a more systematic approach to using ICT to support security management, firmly grounded in a clear vision of the objectives and parameters of the different actors involved. Such an approach requires the involvement of the private sector, to help the public sector to articulate their requirements and then work to develop the appropriate solutions. Conference participants should therefore also discuss the best way to build the partnerships between public and private sectors to achieve these goals, with the aim of taking any such recommendations forward independently of the conference itself.