

Crisis Management and Information Technology

“Towards Interoperability in Crisis Management”

Helsinki, 11 – 14 September 2003

BACKGROUND PAPER

CONTENTS

Background	2
Perspectives on Interoperability.....	3
The Political Agenda.....	4
Organisational Commitment.....	5
Partnership with business	5
The Field Perspective	6
Factors for Success.....	7
Technical Standardisation	7
Further Reading	9
Relevant Websites	9

Background

In September-October 2002, the first Crisis Management and Information Technology Seminar was held in Helsinki. It was initiated as part of the Crisis Management Capabilities Programme of the Crisis Management Initiative (CMI), a non-governmental initiative designed to improve the capacity of the international community to deal with crisis situations and post-conflict rehabilitation through practical and innovative joint projects. The seminar was co-organised by the Object Management Group (OMG), an open membership, non-profit consortium that produces and maintains computer industry specifications for interoperable enterprise applications.

This co-organisation between public and private actors was critical to the basic premise of the seminar: to bring together key representatives from the international humanitarian and crisis management community to discuss their Information and Communication Technology (ICT) needs and requirements with private sector vendors in software and information systems. It established a permanent dialogue and cooperation process between these two groups to help to deliver interoperability solutions and standards for crisis management, setting up the Crisis Response Executive Advisory Team (CREATE) to facilitate partnership between actors from both sides.

The United States Institute of Peace (USIP) had previously established its Virtual Diplomacy Initiative, a project to follow the effects of new 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. In order to explore practical next steps toward improving cooperation in this sector between different levels within organisations – from headquarters to the field – and between different organisations responding to crises, the CMI and USIP are co-hosting a second conference, entitled “Towards Interoperability in Crisis Management”.

The objective of this conference, to be held in September 2003, is to affirm the commitment of organisations operating in the field of crisis management to work towards interoperability at the political, organisational, field, and technical levels. Such a commitment at the highest political leadership of the agencies is indispensable for achieving interoperability, and conference participants will therefore include high-level representatives of international organisations, experienced practitioners in humanitarian assistance and crisis management, and technical experts who understand the nature of field operations.

The issues that the September conference will discuss are applicable in all types of service organisations and at all levels within those organisations. The conference will identify concrete measures that can enhance effective crisis management within and across responding organisations. In particular, the intention is to contribute to the drive towards ICT standards for

crisis management, including the policies and structures necessary for the implementation of those standards.

This Discussion Paper is intended to act as a guide to some of the key issues at each of these levels to help you to prepare for the conference. While the focus of the Paper is on international actors, much of what is contained in it is equally applicable at every level of crisis response. Most if not all of the issues addressed in this document apply to all levels and participants of the crisis response community, from "first responders" (emergency services, law enforcement, etc) and local government officials, all the way up through national civilian and military organisations, to national governments and international bodies. This document should act as a basis for discussions at the conference, and as a contribution to the wider dialogue within the crisis response community in its many forms.

Perspectives on Interoperability

Over the past decade, the international community has responded to an increasing number of major political conflicts. Crisis management refers to both the types of response offered – ranging from peace-enforcement to peace-keeping, from policing to nation-building, from humanitarian relief to reconstruction and development – and the range of activities that these interventions comprise, including military intervention, diplomatic initiatives and humanitarian and reconstruction assistance. The final objectives of crisis management are to restore and enhance local capacities in support of stable and sustainable societies.

In order to achieve these objectives, the international response to conflicts has become more complex and sophisticated, and most interventions can no longer be easily classified, consisting of a combination of the elements outlined above that changes over time. The current environment also includes increasing challenges created by intrastate conflicts and supranational security threats (such as organised crime and terrorist activities). The increase in the number and complexity of interventions requires greater levels of resources – and more cost-effectiveness in how and where those resources are applied.

In October 2000, the Report of the Secretary-General on the implementation of the report of the Panel on United Nations peace operations identified information technology and knowledge management as key to the success of future operations. Interoperability refers to the requirement that, at every level, organisations and individuals in this sector require a strong basis for co-operation and co-ordination. A vital component of effective crisis management is the implementation of information and communications technologies (ICTs) that can improve co-operation within and between responding organisations acting at different levels.

There are three major barriers to establishing interoperability in this sense. The first is that between the different levels of crisis management – whether political, organisational, operational or technical – there are genuine issues of coherence in policy and practice, even within organisations. The second is that, within each of those different levels, for a number of reasons, there is frequently competition rather than co-operation. Crisis management is seen as a zero-sum game, where one actor's loss is another's gain – as opposed to an environment in which the value of resources can be multiplied by combining them.

The third and final barrier is simply that the operational environment for organisations involved in crisis management works against longer-term partnership and planning. During crises there is little time to allocate resources to these types of development; between crises there is plenty of time but few resources to invest in such preparation. This conference offers the space to discuss and develop such partnerships, to identify and address the underlying causes of this lack of coherence and co-operation, and move towards concrete recommendations that will address these problems in the key sector of ICT.

The Political Agenda

The number and diversity of actors and networks involved in crisis management creates multiple challenges. Organisations working in crisis management at any level, whether governmental, intergovernmental or nongovernmental, are competing for resources. One implication of this state of affairs is that organisations will not invest in initiatives that do not deliver concrete returns to them.

Each of these institutions is governed by specific information sharing policies and operates a range of technologies to implement those policies. In the absence of investment in interoperability, many such systems are likely to be incompatible between (and sometimes within) organisations. This can become a particular obstacle for the effective coordination of crisis management within national governments – for example, in the area of response to flooding, which may require the mobilisation of resources from the military, civilian emergency services, government agencies responsible for preparedness, response and reconstruction, as well as non-governmental community groups and charity organisations.

In such instances, interoperability and information sharing ‘problems’ are often rooted in political, management and resource issues, rather than in significant technical obstacles. Organisational behaviour based on these issues tends to subscribe to more traditional ways of thinking about information. Such attitudes reinforce the position that information is more valuable if it is restricted rather than shared – rather than recognising it as an asset whose value increases in direct relation to its distribution – and fails to realise the potential of information sharing as a route to building the organisation.

In many organisations, however, the recognition of information as a key organisational resource has begun to change this type of approach. The result is that more attention is paid to developing that asset, particularly in enabling organisations to learn from their experience more easily – a need that is repeatedly felt by those involved in crisis management. This shift in attitude also means that organisations are more prepared to share information strategically to gain real returns.

It is actually in the self-interest of organisations to share information and to create systems that facilitate that sharing – for instance, for governments to ensure that their systems are in step with those of their regional neighbours and international partners. In this case, information sharing adds value to their existing resources (by combination with the information resources of other organisations) and thus increases their status as a key information resource for others. The value of sharing and combining information resources outweighs the transaction costs involved in working with other organisations.

Proper management of information and the resulting analysis of crisis situations are crucial for informed decision-making and the effective use of resources. In many cases, organisational relations and responsibilities are not necessarily clearly delineated – such as in the relations between military and civilian operators in both national and international emergencies. Yet even where working relationships are clearly defined – for example, during UNDAC deployments for international responses to national disasters – each of these organisations has its own information systems, data standards, operating procedures and the like. There is a need for a more coherent approach to strategic information sharing that will allow accurate and in-depth analysis to be made at the strategic level in a crisis situation. There is also a clear need for the creation of the tools necessary to enable information sharing to take place, and the political will to support that sharing.

At the political level, clearly understood frameworks for co-operation need to be put in place in order both to agree on policies for information-sharing and implement ICT standards to ensure that those policies can be acted on. The NATO Partnership for Peace programme has established an Information Management System (PIMS) as an attempt to create such a framework for information-sharing between NATO and non-NATO countries within Europe, as part of the process of incorporating these partners into NATO initiatives. The gain on both sides is significant, both in

political terms and with regards to the mobilisation of information resources for common and individual goals.

Organisational Commitment

While their underlying mandates may be very different, management processes are similar across organisations working in crisis management. Despite the different structures and cultures within these organisations, there are common needs in areas as diverse as human resources, procurement and logistics, communications and security management. Organisations need to articulate and understand their aims and objectives, clarify and communicate what their management processes are, and look at the environment in which they are going to be implementing ICT solutions. Only then will they be able to review the tools that are available and judge how they might use them most effectively to add value to their programmes.

Once shared processes are in place, standards for ICT can be identified and shared on the basis of common practices amongst organisations. The result will be that vendors will increasingly participate once they see a market for ICT solutions in more than one organisation. One clear example of this is supply chain information to support logistics activities; the IFRC is currently rolling out a logistics software package developed by the US-based Fritz Institute, based on the same processes and tools now used by UPS. The same basic processes underlie procurement for both the manufacture of automobiles and the response to a refugee crisis; many of the same problems of information flow affect both types of activity; and the same needs exist for real-time connection with sources of supply information.

A number of other significant non-technical barriers impede implementation of solutions, including organisational structures (preventing horizontal coordination of ICT initiatives), organisational cultures (including resistance to sharing data), lack of overall system architectures, the absence of applicable standards and non-adherence to existing standards. Standards for ICT use in crisis management environments must build on existing achievements in other standardisation contexts – for instance, the work of OMG and other ISO-related groups. It is also essential that advances in ICT are accompanied by changes within organisations addressing issues such as management structures, policy development, staff capacity and resource allocation.

The most important factor in the success of ICT implementation within organisations, however, is investment – not just financial and human resources, but also in terms of management support based on recognition of the strategic importance of it. This support also needs to be tempered by awareness of both the potential and limitations of ICT to solve specific problems. The introduction of many new technologies most often founders on these obstacles, rather than any fault in the technology itself. Management of information systems requires specific structures and skills to succeed, and this is perhaps one of the greatest opportunities open to the crisis management community – strategic partnership with private enterprise.

Partnership with business

It is clear that many of the organisations involved in crisis management – whether within national governments, intergovernmental bodies or non-governmental organisations – have not yet integrated ICT successfully into many of their key functions. Despite rapid developments in ICT in recent years, its potential remains largely under-utilised in crisis management; and, where technology is utilised, it tends to be without coordination with partner organisations.

One key aspect of introducing ICT to crisis management is building relations with the private sector. Many international organisations still have an approach to working in partnership with business that is characterized more by distrust than by dialogue. Furthermore, bureaucratic administrative systems often interfere with the potential exploitation of opportunities offered by advances in ICT. On the side of the private sector, there is frequently a lack of comprehension of the specific needs and constraints on organisations involved in crisis management.

This is partly due to the focus of the crisis management community primarily on integrated solutions using existing technology as part of short-term responses. ICT researchers and vendors, on the other hand, are interested in developing and testing longer-term, leading-edge technology with wider applicability. There is also the more general problem of interoperability that comes from the attempts by diverse vendors to develop products based on diverse end user requirements in an open market place.

The obvious need is for more structured dialogue between the two sides to build constructive and cost-effective approaches to basic problems. Once information and communication needs have been identified at the strategic and organisational levels, these requirements need to be articulated at key points of institutional and commercial interface. This in turn should lead to more structured dialogue between ICT vendors and users in advancing ICT's contribution to the management of crisis situations.

A good example can be seen in the agreement between WFP and Sony Ericsson to establish a short-term cellular network for the international community and Afghan Interim Administration. This arrangement made it possible for both parties to work more effectively – yet it could have been improved, particularly in the involvement of stakeholder organisations in the implementation of the agreement and in the transition to commercial providers such as the Afghan Wireless Communications Company (AWCC).

The Field Perspective

The example given above raises one of the key factors that often creates distance between headquarters (which set policies and introduce tools) and field offices (who actually have to implement these systems). The disconnect between global solutions and local operational environments exposes the weakness of approaches based on the principle that 'one size fits all'. ICT solutions must be appropriate to the needs of the field – the clear implication being that the development of those solutions must involve those working in the field.

The question of what ICT needs are experienced in the field is perhaps the most difficult to answer. Field operations are characterised by rapidly changing environments (often accompanied by unreliable power supply and communications), multiple international and local perspectives and different outcome orientations. Compare the experiences of the large missions of the last 5 years – Kosovo, East Timor, Afghanistan, Iraq – and it becomes clear that, with each new mission, old challenges are recast and new challenges arise. ICT initiatives need to look at the commonalities between previous operations to predict what shape future demands might take and develop appropriate solutions based on those predictions.

One response to this has been the development of Humanitarian Information Centres (HICs) by the UN Office for the Coordination of Humanitarian Affairs (UN OCHA). These flexible, field-based units aim to respond to actual needs in the field, collaborating with partner organisations to develop a range of services and products. Yet projects like these HICs cannot answer every need of every response organisation, and it is still the responsibility of each organisation to develop its own capacity (and the capacities of its partners) to deal with its ICT and information management needs.

Those working in the field are perhaps least well-positioned to actually address their needs. Always under pressure, and frequently under-resourced, it is clear that the key factor in the success of introducing new ICT initiatives to crisis management rests on ensuring that field practitioners are more closely linked both to headquarters level activity and to ICT providers that can meet their needs. In addition field offices themselves will require additional investment in the form of training and technical support if they are to fully realise the benefits of ICT, particularly in situations characterised by a high turnover of staff. Before headquarters or external providers will invest, however, they need to see how the outputs of such initiatives will be used, which in turn requires a careful review of the applicability of these products in the field.

Factors for Success

There are a number of key factors that will contribute to the successful introduction of ICT into the field. Amongst them are the following:

- Portability. Mobility is frequently vital for aid workers in the field, who cannot afford to be tied to an office-based system, and so ICT must be easy to transfer between locations. One obvious example is the development of PDAs and PDA-based data gathering tools represents a major opportunity to meet the needs of field workers.
- Durability. The rigours of a harsh working environment – during a natural disaster, or a conflict situation – mean that standard products may not be suitable. Mobile phones are now standard communications tools – but not many organisations invest in upgrading the phones themselves to make them more rugged and resistant.
- Flexibility. Proprietary software represents a dilemma to many organisations. Off-the shelf packages meet most of the needs of most organisations, but are limited when used by non-technical staff. Dedicated solutions may be easier to train staff in – but are frequently not as flexible when faced with novel situations. Solutions must strike a balance between meeting current needs and facing future challenges.
- Simplicity. Products and services cannot afford to place additional learning burdens on field workers, and should minimise the need for training and support. The constant trade-off between simplicity and flexibility must be taken into account.
- Affordability. Funding constraints are a constant in field operations, and interventions must be low cost. Economies of scale would go some way towards addressing this issue – if organisations could collaborate on joint procurement exercises!

Technical Standardisation

Interoperability at the levels outlined above will never be a reality unless there are tools available to enable this development. Crisis management activities are information- and communication-intensive efforts that impose great demands on underlying technologies. No overall system plan exists that would facilitate integration of individual software systems into a single system. The resulting multiplicity of systems may not effectively interoperate or support upgrades. In addition, when underlying infrastructure such as the operating system changes, many parts of the whole system may have to be replaced or upgraded.

This issue is a common one in many areas of systems integration, in sectors as diverse as manufacturing, finance and healthcare. Given that crisis management depends on the integration of information coming from multiple organisations and government agencies, each of which may have policy constraints regarding security of information, it is a significant challenge to develop techniques that permit integration for the purpose of crisis management consistent with maintaining those constraints. The first step in reaching solutions to these problems is open dialogue regarding these concerns – yet even this first step is sometimes difficult to take, due to those same security concerns!

There is also a tendency to reinvent the same solutions within each organisation, because sharing ICT experience can be difficult for agencies, with the result that they tend to seek their own individual solutions using their own contractors. Identifying which ICT standards to adopt poses a challenge for managers in these organisations purchasing new hardware or implementing new software. One starting point should be agreement on hardware and software standards within political groupings (such as NATO member countries) or familial groupings (such as the UN) – which could then form the basis for negotiating package deals with suppliers, or even schemes to enable less well-resourced actors to benefit from the generosity of larger partners.

Information systems depend on standards – not just in terms of hardware and software, but also in terms of staff capacity – and the international community needs to move towards standardisation if it is to take advantage of ICT. Only standardisation at every stage in the information cycle will allow information to be integrated and compared across different organisations. The work of consortia (such as the OMG or the Open GIS Consortium), the support of private sector organisations (such as ESRI in the specialised field of GIS), the successful creation and adoption of standards (such as those used by the Tampere Convention, creating an interagency standard for telecommunications), the example of interagency groups (such as the Geographic Information Support Team) – all of these suggest that we are on the right track.

However, in order to satisfactorily design and market ICT capabilities to support crisis response, it will be necessary for the entire community to undertake system-wide planning that includes ICT as a key factor in their operations and takes into account the widely differing capabilities of different actors. We hope that this Conference will create the opportunity to begin that process.

Further Reading

Seminar Report

Seminar on Crisis Management and Information Technology

Helsinki, 29 September – 1 October 2002

(December 2002, Helsinki, ITCM)

http://www.itcm.org/pdf/ITCM_seminar_report.pdf

Taking it to the Next Level: Civilian-Military Cooperation in Emergencies

(August 2000, Washington, USIP)

<http://www.usip.org/virtualdiplomacy/publications/reports/NextLevel.pdf>

Good Practices: Information Sharing in Complex Emergencies

Report from a Roundtable on Humanitarian-Military Sharing

Worldwide Civil Affairs Conference

New York, 28-30 June 2001

(March 2002, Washington, USIP)

<http://www.usip.org/virtualdiplomacy/publications/reports/11.html>

Final Report

Symposium on Best Practices in Humanitarian Information Exchange

Geneva, 5 - 8 February 2002

(July 2002, Geneva, UN OCHA)

<http://www.reliefweb.int/symposium/Symposium%20Final%20Report.pdf>

Relevant Websites

Information Technology and Crisis Management

Seminar Page

<http://www.itcm.org/seminar/index.html>

US Institute of Peace

Virtual Diplomacy Initiative

<http://www.usip.org/virtualdiplomacy/>

OCHA Reliefweb

Humanitarian Information Network

www.reliefweb.int/hin

Object Management Group

www.omg.org