

Seminar on Crisis Management and Information Technology
Helsinki, 29 September – 1 October 2002

Seminar Report

About the Crisis Management Initiative

The Crisis Management Initiative (CMI) is an independent non-governmental actor whose aim is to respond to new security challenges by enhancing the conflict prevention and crisis management capacity of the international community.

CMI's founder, President Martti Ahtisaari, is the Chairman of the Board and Ambassador Jaakko Iloniemi the President of CMI. CMI's strength is its unusual network of political decision-makers, international organisations, research institutes and individuals. CMI sees its mission as mobilising and bringing together the resources of these actors for crisis prevention, crisis management and post-conflict rehabilitation.

The Crisis Management and Information Technology Seminar organised in Helsinki 29 September – 1 October 2002 was part of the CMI's Crisis Management Capabilities Programme, designed to improve the capacity of the international community to deal with crisis situations and post-conflict rehabilitation through practical and innovative joint projects.

Acknowledgements

Crisis Management Initiative would like to thank the Object Management Group, the co-organiser of the seminar. CMI thanks also David Stewart Howitt, Bayard Limited and Adam Austerfield, Enterprise LSE Ltd for producing this seminar report.

The CMI is grateful to IBM Finland, Hypermedia Laboratory of the University of Tampere, the Ministry for Foreign Affairs of Finland and eTampere for the support of the seminar and this report.

Crisis management and Information Technology Seminar
Helsinki 29 September – 1 October 2002

CONTENT

1	Introduction	4
1.1	Conference Organisation	4
1.2	Context for the Conference	4
2	Executive Summary	5
3	International Crisis Management Environment	6
4	Examples of diversity and need for inter-operability	8
4.1	The Office for the Co-ordination of Humanitarian Affairs of the UN	8
4.2	World Food Programme: Afghanistan	9
4.3	The Lessons Learned and Analysis unit in Kosovo	9
4.4	The Property Law Implementation Plan	9
4.5	National Disaster Management in the US	10
5	The Institutional Perspective: ICT as a tool in crisis management and information management	10
5.1	The United Nations perspective	11
5.2	The EU Perspective	12
5.3	NATO Perspective	12
5.4	OSCE Perspective	13
5.5	Vendor perspectives	15
5.5.1	IBM and The Role of Technology in Global Disasters	15
5.5.2	ITCM project's implementation of a C4I system	16
6	Conclusions and recommendations	16
	ANNEX I	19
	ANNEX II	22
	ANNEX III	25
	ANNEX IV	30
	ANNEX V	32

Crisis management and Information Technology Seminar Helsinki 29 September – 1 October 2002

Objective of the Conference

“To find ways to enhance the tools that our organisations have available for crisis response and management.”

1 Introduction

The conference gathered a diverse group of experts on humanitarian emergencies and peace support operations. Some were specialised in utilising information and communication technology for varied and complex crisis situations. Others were members of the business community; communications and information technology (ICT) developers and vendors. The seminar aimed to find practical means to improve coordination and information sharing between different organisations, including the interoperability of communication and IT-systems. Meeting user requirements in a globalising and highly complex crisis management environment can be facilitated through an effective liaison between the crisis management community and the business community.

1.1 Conference Organisation

The conference was organised jointly by the Crisis Management Initiative (CMI) and Object Management Group (OMG). CMI is an independent non-governmental actor whose aim is to respond to new security challenges. OMG is an open membership, non-profit consortium that produces and maintains computer industry specifications for interoperable enterprise applications.

1.2 Context for the Conference

Integrated ICT systems, designed to support decision-making and communication in multilateral peace support operations, are an important tool. Crisis management involves the activities of a great number of agents confronting the same problems but lacking shared or consistent knowledge, coordination or communications technology or a common user culture. As a consequence, different organisations work wastefully on the same problems, plan and take decisions without consulting other organisations and without access to up-to-date or adequate knowledge. Although competition between organisations is a normal part of life, the real challenge is to overcome these difficulties by understanding the requirements of each stakeholder. To do this a thorough understanding of the behavioural tendencies of collaborative crisis management responses and the political constraints is essential to identifying the means by which improved ICT standardisation can strengthen collaborative crisis management action.

2 Executive Summary

The conference was organised in four parts:

- Session One: What is the current state of crisis management and what are the challenges for organisations involved?
- Session Two: Managerial questions in field operations.
- Session Three: A review of examples of the use of ICT-systems and tools in different crisis situations.
- Session Four: Working groups to propose practical steps to improve civil-military coordination and to discuss organisations' IT needs and requirements.

Today's crisis management environment is complex and diverse. Many recent examples of this have demonstrated the requirement for facilitative and adaptive mechanisms, which can be used by a wide range of actors. To prescribe ICT architecture prematurely is to limit the effectiveness of coordinated operational response and hinder the desired objective of a sustainable and stable end state. The case studies presented in the seminar illustrated the wide range of needs, and the necessity to take a view from a neutral perspective that identifies the management response and requirements from the beginning of a crisis. The key question is: who needs to talk to whom, and why?

The aim of the conference and sessions was to break down the artificial borders between governmental and non-governmental sectors, civilian and military organisations and public and private sectors, and forge co-operation between them in developing the use of ICT in crisis response and management.

Significant efforts have been mounted by various organisations to make their crisis response capability more timely and effective. The use of the latest information technology has expanded rapidly within organisations. Crisis management organisations already have a number of commercially available groupware systems at their disposal. Naturally, these organisations use these systems in field operations. Collectively, however, this has resulted in inter-operability problems.

The solution is to harness the same integration technologies used by commercial organisations worldwide. From this point the appropriate "off the shelf" equipment is relatively straightforward to configure and deliver.

This solution must come from an international partnership, and needs to focus on:

- Requirements process to scope and define needs and priorities for IT integration for coalition partners in international crisis response and management situations;
- An international organisation to support rapid prototyping and trial systems to provide IT integration techniques for coalition partner IT support organisations;
- An International standards process to define norms for IT interoperability in crisis management situations, driven by both users (NGOs, national- and international-bodies, IT organisations) and vendors to those users.

Such a partnership would result in standardisation around technology specifications that are available in commercial solutions and have been proven in the field, resulting in much higher interoperability between coalition partners.

The Information Technology and Crisis Management, (ITCM) programme and OMG's C4I Task Force provide this solution; however, an International Executive Advisory Board, dedicated to the fostering of both the ITCM programme and OMG's C4I Task Force, is necessary to ensure that needs and priorities are set correctly for both organisations.

3 International Crisis Management Environment

After the end of the Cold War the nature of peacekeeping and the means of managing crisis situations have been profoundly transformed. The conflict resolution capabilities of international organizations such as the UN, the OSCE and the EU, as well as of relevant NGOs, have been challenged by the proliferation and complexity of contemporary conflicts. A majority of these are of an intra-state rather than international nature, and involve systematic violations of human rights and of international humanitarian law, collapsed state structures, and political mobilisation based on ethnic and religious identities. These developments have fundamentally changed the role of the international community. Previously core tasks of monitoring and advising have been largely supplanted by executive mandates, such as in East Timor and Kosovo.

The 'classical' form of UN peacekeeping mission arguably helped only to freeze a situation. In new paradigms however, for example in Namibia, the UN operation was deeply involved in the process of change, peace-building and national reconciliation. In such examples, peacemaking and peacekeeping were in the same hands. Complex international peace support operations with active UN mandates have taken place in locations such as Mozambique, Macedonia, Croatia and East Timor. These have been the test of the new political environment and mandates to secure peace within them.

Increased role of regional organisations

During the last decade the involvement of regional organisations in conflict prevention, crisis response and post conflict reconstruction has increased considerably, particularly in Europe. NATO has begun crisis management operations in Bosnia and Herzegovina and elsewhere in SE Europe. The Organization for Security and Co-operation in Europe (OSCE) has established over twenty field missions and presences in the Balkans, Central Asia and Caucasus. The European Union will deploy its first field mission and replace the UN's International Police Task Force (IPTF) by the EU Police Mission in Bosnia and Herzegovina in January 2003. African regional organisations, such as ECOWAS and OAU are involved in solving some crisis in their regions.

There has been a growth of understanding among organisations of each other's mandate and activities. The critical output has been the comprehension of the need to co-operate to achieve optimal results. However, there are still far too many examples of inter-agency and inter-entity rivalry in the field impeding progress and exacerbating what is often an already negative perception of the international operation on the part of the local population. Overlapping mandates often result in tensions and the ability of a multi-faceted operation to function on the ground is frequently determined by the quality of the personnel and the leadership on the ground, rather than by contingency plans or formulae for cooperation. This is equally the case for the different specialised agencies as it is for the military and civilian components of an operation.

Increased demand for civil military co-operation and interoperability

Crisis management can include both military and civilian tasks and the corresponding actors. Often two or more fundamentally different operations must be carried out in parallel. Military crisis management is usually necessary in order to end hostilities and to restore peace and security on the ground. The primary aim of peacekeeping operations is to prevent violence and to create basic conditions for communities to function properly again. In recent crises, peacekeeping operations have focused particularly on the protection of civilians. They are also often designed to ensure that humanitarian aid intended for civilians reaches its target.

At the same time, the demand for civilian crisis management has increased. A central task is to support democracy and strengthen the rule of law. In many cases, this involves down-to-earth practical work on the ground. For instance, a stable society needs a well-functioning local police force. Without the concrete help of international civilian police officers this is often impossible. A solid local government is essential for the society to recover.

This mixture of civilian and military, preventive and conflict and post-conflict crisis management tasks presents a multifaceted and complex task challenge. There can be a tendency by the military component of an operation to see peace support operations as war scaled down, with consequences, which may include excessive focus on domination through superior force to minimise risks to troops, limit tasks and shape a subsequent exit strategy. Equally, when civilian organisations are involved, this kind of operation can be perceived as foreign and security policy scaled up, or

process bureaucracy extended into a new field. This can exacerbate the difficulty in meeting the minimum standards of rapid reaction, rapid resource flow.

One of the key challenges in the field is the fact that so many different players are necessarily involved - the UN, its specialised agencies, regional organisations, NGOs and so on. The imperative of coherent action in the civilian world is often much more difficult to achieve than that in peacekeeping operations which operate under a unified command. Modern information technology, common standards and interoperability could usefully be applied here in order to facilitate communication and co-ordination for optimal results.

New security threats

The processes of globalisation and interdependence are multiplying both the numbers of participants and permutations of the crisis management constituency. This is altering notions of accountability, transparency and responsibility. Current day crisis management response must adapt to these ever more complex demands whilst recognising the shifting realities in a globalising world that is faltering in the shadow of September 11. Recent events urge us to acknowledge that new threats to international peace and security such as in the form of trans-national terrorism, destabilizing cross-border refugee flows, organised crime and narco-trafficking cannot be seen in isolation from some of the "old types" of conflict that have been left to fester.

There are many examples in the contemporary global crisis management environment that highlight the inadequacy of responding to the symptoms without addressing the substance. Every crisis situation demands its own particular remedy, which takes account of all the relevant circumstances. There is no 'one size fits all' in peacekeeping or international crisis management.

Basic preconditions for an effective response

Conflict prevention and crisis management are crucial elements in enhancing international security, in an appropriate legal framework to act. The crisis management capability of the international community should be of such quality and effectiveness that evolving crises can be resolved quickly and prevented from spreading. The aim must be to minimize human suffering and economic loss.

In order to be effective, crisis management requires quick decisions and coherent action at all levels. The situations on the ground are often extremely complex and volatile and can change rapidly without warning. A coherent and co-ordinated reaction can only be based on accurate information that must be produced and transmitted with speed and precision. Innovative ways and means to respond to crisis situations as well as appropriate technological tools are essential.

The essence of international collaboration lies in the principle that in response to crises, each country should contribute according to its capabilities and fields of competence. The key to policy at present is to combine two areas: firstly, the need for multinational cooperation in the crisis management; and secondly, the need to focus on areas of specialisation. Additionally, establishing interaction to encourage political leadership through the exchange of information is also a crucial aspect - permanent interaction between theory and practice.

Experience from recent crisis situations dictates the need to adopt a fairly broad overall concept when preparing for crisis prevention and management. Crises occur not only *between* but also *within* individual countries, often involving an ethnic dimension. A wide range of means must be available to put an end to hostilities and restore conditions of peace, but also to create trust between parties and to begin the rebuilding of a functioning society.

In the contemporary arena it should be noted that all stakeholders dealing with crisis management situations, and pre-empting future crises, are better equipped than ever to deal with such situations, but coordination can still improve greatly. The pre-emptive UN peacekeeping force in 1993 in Macedonia was noted in this regard as an example of the international community acting in cohesion. However, more generically, there is deep concern that there is more attention given to the symptoms of crisis at the expense of their substance. The cycle of poverty, dictatorship, hopelessness, alienation and terrorism in much of the world remains the responsibility of the international community to pre-empt, by deeper understanding of the circumstances in which they arise.

4 Examples of diversity and need for inter-operability

The seminar discussed several examples of the differing requirements for the crisis management environment. Each case highlighted different perspectives and priorities according to circumstances and mandate. The examples demonstrated clearly that the effectiveness of crisis response operations is largely dependent on interoperability between organisations, processes, and technologies in the field. Interestingly they all highlighted the issue that there is plenty of information and the technology exists to transmit, but the central function lies in communication. Development of capabilities requires (1) harmonisation of requirements, (2) readiness to compromise and (3) active participation of all actors. Mechanisms to do this already exist in the military. As to civilian crisis management, mechanisms are in the process of being created.

The following case studies were presented:

- Office for the Co-ordination of Humanitarian Affairs of the United Nations
- An operational deployment (FITTEST)
- A policy analysis and advisory function (LLA)
- A complex post-conflict implementation process (PLIP)
- National Disaster Management in the US

Perhaps the best example of the complexity and diversity of today's crisis management environment could be seen in the recent earthquake in Afghanistan where the crisis response teams and emergency services (national and international) had to undertake the response in challenging topographical circumstances, in winter and in a country with a collapsed infrastructure and in a hostile political and security environment.

4.1 The Office for the Co-ordination of Humanitarian Affairs of the UN

The United Nations Office for the Co-ordination of Humanitarian Affairs (OCHA) has the mandate to facilitate co-operation between the many partners working on the alleviation of human suffering.

The priority for crisis management situations, whatever the sophistication of the ICT, was to be able to communicate as quickly, accurately and securely as possible. Communications should not be entirely reliant on ICT but should be the primary driver in operations of humanitarian assistance and be simply able to supply the right information to the right place at the right time.

Communications depend on co-operation, on compatibility through common standards. Without agreement on common language and terminology, even inter-personal, verbal inter-action cannot work, not to mention the intricacies resulting from the need to share resources such as a frequency spectrum or public networks. In increasingly complex humanitarian operations, such as Afghanistan and Central Asia, the success of such operations depends on the teamwork of many institutions. This, in turn, stems from a joint position concerning the environment in which communications in the service of humanitarian assistance take place.

Standardisation is a critical area for ITCM. This depends not only on the good intentions of the creators of new and advanced technologies, but on the appropriateness and, most of all, the affordability of the latter. The inter-operability by application of common standards depends not only on agreement among telecommunications experts and managers, but often requires administrative, financial management decisions. The creation of more awareness of the role of IT in crisis management, and thus also for the need to allocate sufficient resources to the respective units in each institution is a priority of the common work in the Working Group on Emergency Telecommunications (WGET) and related inter-agency mechanisms. The recognition of the needs of the "humanitarian community" in respect to the *un-hindered* use of appropriate communication tools will greatly benefit from the entry into force of the Tampere Convention, but this entry into force requires 16 more ratifications from among the 54 signatories or other States before 21 June 2003.

4.2 World Food Programme: Afghanistan

WFP has 2600 staff feeding 77 million people a year in 82 countries, using 4.2 million tons of food with massive logistical requirements. WFP has a global technical team, FITTEST, utilised as an intervention team. It is on 24 hours notice to move. They have about 3 million dollars of ICT equipment that can deploy anywhere in the world for large-scale complex projects or emergencies. In Afghanistan, the first plane carried the security officer who did the two-hour assessment before the agency representatives flew in on the second plane, three days after the fall of Kabul. The plane with the ICT equipment was the fourth to arrive. The situation was a typical post-conflict situation, destroyed infrastructure, remains of all kinds of military, remains of all kinds of generations of war and the UN in-between.

The mandate was to both support the peace operation itself, *and coordinate ICT and humanitarian agencies*. In order of priority, the first was to ensure communications within one operational area, in this case the boundaries of the town, using handset communications. They used low-tech, long-range communication means through HF radio. They also provided data via HF communications and developed an e-mail system run over the HF radio at 10 kilobytes per minute. This was the main data communication system in Afghanistan and was the first time portable satellite communications were used. Overall, the implementation was low-tech and low-cost. For inter-agency coordination the HF radio systems were redesigned but different call signs, calling systems and different frequencies made this difficult.

The lessons from Afghanistan were that 'fast is good'. Fast deployment means that much more can be realized. In an emergency, communication teams have to be the first deployed because they must secure the sites immediately. In a crisis environment, the ability to get such things as licences is easier as governments will quite often provide anything at their disposal at the early stages. The main needs of ICT in these kinds of environments are very simple and really come down to needing handheld HF radios, but technical knowledge is very important. Most of the agencies do not have e-mail to communicate. Most of them do not have satellite phones to communicate. Thus what is needed is a common denominator, and radios with appropriate structures can help provide that before anything else occurs. The real requirement for inter-operability is at the deep field level, neither at the headquarters level, nor at a European or US level.

4.3 The Lessons Learned and Analysis unit in Kosovo

The UN Interim Administration Mission in Kosovo (UNMIK) is engaged in an ambitious, comprehensive and, for the time being, open-ended mission which entails both the interim governance of Kosovo and the development of domestic institutions to take progressive responsibility for the functions of government. There are no recent precedents for an institution-building mission of this scale and complexity. The Lessons Learned and Analysis Unit is an innovation of the EU Pillar of UNMIK in Kosovo in cooperation with the European Stability Initiative (ESI), the South Eastern Europe think-tank. Its goals are to carry out research and analysis of the challenges of institution-building and development in Kosovo, to gather best practices from around the world for use in Kosovo, to capture the lessons of Kosovo for use in other contexts, and to contribute to the development of international expertise in this vital area of international endeavours.

The particular role and function that the LLA fulfils is one that is becoming increasingly important; that of critical policy input and analysis. For these purposes this ad hoc operation should be fully integrated into the institutional and operational structures of the crisis response structures. The temptation is to see inter-operability only in terms of management of operational units (humanitarian, medical, etc) however the LLA illustrates the need for policy functions to be integrated and fully inter-operable so that key decision makers at all levels are apprised of the necessary information.

4.4 The Property Law Implementation Plan

The Property Law Implementation Plan (PLIP) represents an example of a highly complex property return process aimed to overcome the obstacles, both political and practical, impeding the return of Displaced Persons and Refugees throughout Bosnia Herzegovina. This entailed the systematic return of all property to pre-war owner and occupancy right holders, through collaborative policy implementation between the OSCE, UNHCR, UNMIBH, OHR and CRPC throughout BiH. To aid this process a highly complex transfer of information was required between domestic administrative organs, with assistance from the international community. This facilitated the significant reduction of what became known as double occupancy, thus freeing up housing space to be returned to rightful owners/occupancy right holders.

Critical to the success of PLIP was the ability of the respective agencies of the PLIP to benchmark progress through the monitoring of developments in the claims and repossession processes. This was done through the standardisation of statistics measuring claims against repossessions, involving intensive inter-agency co-ordination of information flows. The successful achievement of this collaborative effort was critical to the successful standardisation of procedures and consequent de-politicalisation of the property return process. The model offers insights into how successful collaborative International Community crisis responses can operate. The importance of the definition of a common objective was critical to reducing the inter-agency pressures resulting from mandatory overlap and competing justifications for budgets between organisations. Additionally it assisted substantially in the division of labour and responsibilities therefore clarifying user requirements. Whilst not wholly resolving the refugee return process in BiH it removed what was probably the single most serious obstacle. It may yet be seen to be the single most effective international intervention in post-Dayton BiH. It illustrates the nature of future International interventions that must continue to improve in their effectiveness.

4.5. National Disaster Management in the US

In the US, there is a belief that there is little different in the functionality required to respond to natural disasters and man-made disasters, although there may be some differences during the consequence management stages. In examining the needs of crisis response organizations at the local level, it can be seen that much of what is learned there is applicable to peace support operations as well. Additionally, many of the challenges between the organisations involved in local response and peace support operations are similar and we can all benefit by working together to address these common interoperability problems faced in national emergencies and crisis management field operations. The functionality and the opportunities for standardisation are identical, the differences lie in the different levels of aggregation of the data and the scale of the operations. There are the everyday emergency management problems faced by fire departments/brigades, police, emergency medical personnel, etc. (commonly referred to as "first responders" in the USA). The functional differences among these organisations differ little from country to country and event to event. A police force trying to reestablish control in a village in Kosovo is no different functionally from a police force in Japan trying to reestablish control after an earthquake, a major city anywhere in the world after a major civil disturbance, such as a riot, or the simple country gendarm that relies on his ability to get help from neighboring jurisdictions when there is trouble.

In United States the Homeland Security programme aims to improve the information systems used for crisis planning, prevention, response, and recovery in national emergencies. A key obstacle is that sharing of information about the effected area is rarely possible among jurisdictions at any level, and particularly between levels of jurisdiction. However, response operations assets and recovery aid to disasters (man-made or natural) may come from far outside the effected jurisdiction. Therefore, the Homeland Security programme will need to focus on improving security interoperability in a multi-enclave environment, cross-jurisdictional collaborative planning tools, situation awareness along jurisdictional boundaries and incident management for cross-jurisdictional operations as well as modeling, simulation and planning collaboration for cross-jurisdictional operations. Furthermore, new knowledge-based tools to broker services and integrate responses and virtually integrate information resources will need to be developed. These will be based on standardised metadata for services and information resources.

The aim is a "digital nervous system" for a unified Homeland Security system linking national governments to local/municipal governments, NGOs and international actors. The system will support collaboration and sharing of information resources among and within all echelons, as well as sharing of information services.

5 The Institutional Perspective: ICT as a tool in crisis management and information management

In any crisis management situation, the critical factor in making timely, appropriate decisions is to have the benefit of the optimum amount of quality information. This information may come from a variety of sources that need to be integrated in an information system that is appropriate for the environment in which it is operating.

Investment in information technology developments in the last decade have radically transformed the way organisations operate. The challenges of technology now are related less to capacity than to the effective management of technology and its appropriate application, including:

- 24/7 operational capability
- design, securing and implementation in reliable operational environments
- ensuring business continuity
- ease of understanding and application

There is already more than enough capacity, and infrastructure is relatively inexpensive, at least compared to the industrial world. However institutions still operate through business processes established before the information age. Vast amounts of information are stored on electronic media and exchanged over the Internet or intranets. But the main point is that the processes which allow this to be turned into useful information and intelligence are still very much in their infancy – most organisations do not know what they know. The technology to share information is there, but business drivers of knowledge sharing are still immature.

Purchasing goods or paying people is relatively easy these days, but transforming data into intelligence is a business function that is much more complex, qualitative and requiring a high degree of sophisticated human thinking. The challenge is of information management, not of technology. The trust and drive for this must come from information owners and information users.

5.1 The United Nations perspective

The political context for international action determines the nature of the UN's response to conflicts, just as much, if not more so, than the nature of the conflicts themselves. Ethnic strife, confessional politics, religious division, greed and grievance, bad governance, inequities in the allocation of scarce resources, corruption and/or the quest for power will continue to fan the fires of the third millennium's conflicts.

In the last year the United Nations has been involved in trying to help mitigate or resolve more than 30 different conflicts worldwide. In a number of these cases, the UN's conflict management role has been primarily restricted to discrete diplomatic efforts by the Secretary-General himself, whilst in others, he has dispatched Special Envoys to support regional and sub-regional efforts to resolve civil conflicts. The most visible and high profile form of UN involvement is evidenced in the deployment of 15 peacekeeping operations around the world, with total annual budgets hovering between \$2 - 3 billion.

The key question is: does the nature of the conflict dictate the response? The end of the Cold War afforded the international community the opportunity to bring peacekeeping treatment to bear on a number of proxy wars. The internal conflicts in Cambodia, El Salvador and Mozambique were not new. What was new was the ability of former Cold War adversaries to forge consensus in the Security Council on the need to end those wars - the opportunity for peace. What was also new was their unity of vision that the UN should create that avenue for peace.

The Security Council is now more ready to enlarge the scale and scope of the operations' mandated tasks, and Member States' willingness to provide them with the political, financial, material and personnel support to do so. The new generation of peacekeepers thus facilitated the disarmament, demobilization and reintegration of former combatants into civilian life, conducted elections, monitored human rights and developed national human rights institutions. They engaged in monitoring and restructuring of police forces, and were given a prominent role in fostering good governance and economic recovery.

The challenge for the UN is twofold: firstly to retain the requisite commitment and support of governments; and secondly and in parallel, to be able to turn to the private sector to help sustain a rapid deployment capacity and to maximize the output of limited resources by leveraging them with modern technology.

The challenge is compounded by the fact that establishing the proper security environment quickly is of no use, unless it is capitalised upon, with the urgent delivery of the requisite humanitarian, developmental, human rights and economic assistance. For example, social services may need to be restored, rule of law institutions might need to be strengthened, agricultural production may need to be rejuvenated, and water and electric-supply restored. Jobs will need to be created to provide a viable economic alternative to crime or war. The need is often urgent to re-establish methods of

disseminating information to war-affected populations. Governmental structures at the local, regional and national level need to be repaired, and sometimes created afresh to sustain genuine national peace.

The entire family of United Nations departments, agencies, funds and programmes need to be able to work together. It means cooperating with regional and sub-regional organisations to identify tasks for which they might be better suited. It entails cooperating with non-governmental organisations and International Financial Institutions on both short-term recovery and the initiation of long-term reconstruction. When the UN is given a central role for stewarding the transition from war to peace, the burden of effective coordination is immense. There is tremendous scope for the UN to better coordinate its efforts within itself and external partners - as well as to enhance its rapid deployment capacities - by making maximum use of modern technology and information systems.

5.2 The EU Perspective

In today's complex and globalised world it is more vital than ever for the European Union to create tools able to meet the information need in the field of security and environment. The EU is increasingly confronted with the challenge of international field operations and the need for efficient IT and communications. The EU has perceived a 'clash' of crisis management paradigms in that crisis management can often be configured as 'normal curve' military operations focussing on conflict prevention. As an example of this proliferation, there exists the Joint Situation Centre in the Council, the DG Relex Crisis Room, Civil Protection alert system, Euratom controls and ECHO. This amply illustrates the requirement for interoperability, and the EU has identified short-term tools for HQ and the field to handle the immediate requirements whilst at the same time is investing in the development of medium-term and long-term tools.

In addition, there is the understanding that Crisis Management can focus on conflict prevention, counter-terrorism situations and as a generic Common Foreign and Security Policy (CFSP) function. There are different yet similar technological requirements, such as information software, means of communications and orientation, and critical to going forward, interoperability.

The EU has introduced the Global Monitoring for Environment and Security (GMES) programme. The development of GMES was in direct response to growing concern among policy-makers that access to environmental information was critical to many crisis management situations at regional, national, but also at the global level, such as 'A Sustainable Europe for Better World'. One of its key aspects is to assess and identify risk, and then apply mitigation strategies, add and develop early warning systems. Simulation models are useful and being tested in five places, and can help with multi-hazard situations. Attempts are being made to integrate into one Geographical Information System, GIS for servicing the whole community affected. GMES is also related to common defence and security policies, but mainly in the field of communication and for conflict prevention.

A key aspect of ICT in crisis management is to keep it simple. Technologies have to work across lines and boundaries that are often not standardised. Complex technologies that cannot communicate with each other can often be more problematic than basic systems. Planning and preparation in downtime is essential. Communications en route are critical as well as on the ground. The earlier connectivity can be established the better, and additionally assessment of where support will come from. Unsophisticated knowledge management tools need to be developed so key people with low ICT skills but critical information can contribute, this may be through an information broker.

Incident command centres are also critical, to link the right user to the right information to make and implement decisions. One huge database will not happen, but the interoperability of each one is critical. Security and levels of access are also of key importance. For this to be successfully achieved, standardisation is key.

5.3 NATO Perspective

The key issue addressing military organisations is the change since the end of the Cold War, and understanding the complex needs from a civil as well as a military perspective. NATO is still a military organisation but has new relationships. Clear and significant challenges and opportunities have arisen, not least in the area of interoperability of IT-systems and C4I. It is critical to speak to non-NATO countries and other organisations in order to prevent conflict and crisis but to contribute its effective management consistent with international law.

The new security environment is clearly important and command and control is essential to enable forces from different countries and from different organisations to work effectively together. Intelligence, surveillance and reconnaissance (ISR) is needed that really relates to in-depth understanding of the situation or the entity. A high degree of ISR information sharing among military and civilian organisations is a must.

Interoperability is the ability of alliance forces and, when appropriate, of partner and other nations to train, exercise and operate effectively together in the execution of an assigned mission and task. It is not simply technology and data but includes the use of common languages and agreed operational systems. This is not easily achievable in a multi-national and a multi-cultural environment and requires a significant amount of training, especially in IT. There are a large number of systems that provide ISR information and various qualified resolutions. Most of these systems are owned by nations and not by NATO, and many of them are commercial systems. To meet all the needs and requirements of an operation it is required to employ a mix of systems in a 'system of systems' or, better, a federation of systems.

The key is the sharing of information in a particular environment, and the management of those systems where several stakeholders can deliver their objectives using the same technology and information sharing. This kind of data can be used now in criminal trials, and should interact with the judicial and NGO community to press for outcomes from human rights abuses. These interactions are symptomatic of the context of the new global crisis management environment.

Key lessons learned for NATO are the interoperability and connectivity of ISR information from national sources, and on a secure basis. Political and sensitive issues must be overcome for the greater efficiency of operational activity. Information is a matter of trust; not just trust in the people handling it but also trust in the system and processes. The key is for standards and people to specify the classification levels immediately. The process should be building partnerships with a core group, demonstrate its effectiveness and convince others of its benefits, not try and convince everyone at the same time. And the system must be secure. It is important to be inclusive nonetheless, since non-NATO partners are critical to this kind of success.

5.4 OSCE Perspective

The OSCE allocates about eighty five percent of its resources to field operations, which cover a wide range of activities including local election support, creation of ombudsmen offices, confidence-building measures, the training of multi-ethnic policing and border monitoring. These are complex operations that have to be built up within weeks, if not in days, after the political decision has been taken by participating States. Many field operations are time-limited interventions that have to be wound down as quickly as they have been started. Flexibility, speed and transparency are hence key for the work of the OSCE.

In its operations the OSCE works with many partners such as the United Nations, the European Union, NATO, the Council of Europe, and the International Financial Institutions as well as with international and local civil societies. The success of their work very much depends on the quality of information and communication with their partners. There are dangers, and three in particular which affect improving international crisis management through unifying IT systems.

First, it is the administrative and management systems that allow international organisations to mobilise crisis operations. It is their ability to identify and recruit qualified staff in time, to procure efficiently the equipment needed, to set up functioning offices, to ensure logistic support, to transfer resources from one operation to the next and to account for funds and in-kind contributions that make or break a crisis operation.

Second, the risk for any new unified IT-system for crisis management is the fragmentation within the humanitarian and reconstruction aid communities. UN agencies, bilateral aid agencies, the development banks and the NGO community have too many overlapping mandates and have too many conflicting interests to allow rational decision-taking – irrespective of the availability of a common information system. They compete for the same funds, for the same donors and the same media attention. This is built into the system, as the survival of many of the players will depend on the market share they are able to secure. Lots of funding attracts also lots of players, all with their own management culture, their own systems and their own priorities. All this makes coordination impossible. A win-win scenario under these circumstances is difficult to imagine and if it would happen, it would be the exception rather than the rule.

Third, the need to build up local capacities in crisis management situations should be prioritised before developing complex ICT systems that cannot be used in the appropriate environment. More information and research is needed to properly assess what is needed to restore a stable, secure, sustainable environment for rebuilding societies to prevent future disasters. The danger of widening the gap between international efforts and local capacity building by expensive ICT efforts should remain at the forefront of drives in this situation.

It was suggested that building basic administrative systems for failed states such as Afghanistan and putting them onto IT systems could be a way forward for dealing with crisis situations. This should allow procuring and recruiting while maintaining basic budgetary controls, and being pre-arranged, such system could provide at least a rudimentary first administrative local capacity within a relatively short time.

In general however, from an IT perspective the environment is rather fractured. Many factors have contributed to this: the rapid expansion of OSCE as a whole, geographical spread, the need for rapid deployment, the level of communication capabilities and services in post war areas as well as the lack of organizational standards and guidelines. Today OSCE has developed into a menagerie of communications avenues; a patchwork of centralised and decentralised systems, various hardware platforms, email systems, document management mechanisms and local intranets.

The Secretary General introduced the OSCE Management Agenda to move the OSCE forward. The Management Agenda presents a comprehensive and coherent approach for reforming resource-management of the OSCE while defining roles, processes, and accountability. They are also identifying areas for streamlining, elimination, and/or rationalisation. The management agenda touches upon human resource management, management of OSCE documents, information and data as well as the improvement of IT/communications. Core to the Management Agenda is the development and implementation of an Integrated Resource Management (IRMA) System. This system will be delivered through an integrated IT based platform. It will create a professional, cost efficient, budget based management structure that will ensure our future operational activities conducted in the most effective and transparent manner. When linked to strong leadership and clear political direction, IRMA will give the OSCE the capability to respond positively to new challenges whilst ensuring that all stakeholders can fully understand the resource implications of their aims and objectives. OSCE needs to focus on its core business, in which IT is an important tool used to enhance accountability and transparency in OSCE operations. Management has recognised that IT can support integration and simplification (demystification) of day-to-day processes.

As an example of how commercial ICT and software providers need to work with institutional clients in this field, and vice versa, OSCE had initial problems with the marketplace when describing their requirements and expectations of a potential outsourcing partner. The vendors' concerns focused around:

- the extremely short planning period available to OSCE in response to political mandates
- the legal and logistics issues for operating in post war areas and
- the need for being onsite where neither communication nor networks could be considered reliable.

The bidders asked whether a workshop in one of the OSCE mission could be conducted prior to the bidders providing their proposals. They wanted to experience the "real environment".

The OSCE expect this reform, streamlining and process simplification/elimination will create a lot of anxiousness and uncertainty in the organisation and will need to be supported from external partners. This experience highlights the issues that multi-million dollar investments must be supported by a business incentive, and that future ITCM building will need to have a hard commercial edge for appropriate corporate resources to be invested in R&D and application.

OSCE wishes to benefit from best industry practices in the IT market and to be able to use off-the-shelf solutions. Therefore, both management and the OSCE Permanent Council are aware of the need to make decisions on an ad-hoc basis. This is necessary to avoid OSCE specific or customised solutions of commercial packages and to improve the way the organisation is conducting its business instead.

5.5 Vendor perspectives

5.5.1 IBM and The Role of Technology in Global Disasters

Experience is the best teacher in the use of IT in crisis situations. The major ICT corporations used to give out cheques before they realised it often ended up in the wrong hands and nothing got to the victims. Therefore the crisis response team was formed with a remit to go directly into situations, no matter how bad, and help directly with particular skill sets. Different disasters require different responses:

- Earthquakes in Turkey: mainly medical challenges which required a complex and timely emergency supply chain and identification methodologies.
- Volcano in Ecuador: geophysical constraints, characterised by difficulties with evacuation and medical help at high altitude in mountainous terrain.
- Earthquake in El Salvador: here the issue was financial – the budget for emergency agency was \$50,000 per annum.
- India: massive devastation in Gujarat, cities completely flattened. Total annihilation leaving no infrastructure at all.

When responding to crises all the issues have to be addressed – the political, environmental, social and economic impact of disasters. Cultural awareness and understanding are key to the delivery capability, particularly when communication issues can be of the highest priority and essential to successful disaster recovery. Mostly the technology used in these situations is very low tech – occasional faxes but mostly handwritten notes passed around, and the system has to be able to incorporate whichever communications system works best – very little or no time for training. Timing is critical, with expired drugs and food being one of the worst problems.

How can technology help? It should provide access to critical, real-time decision-making information – getting information to people in a timely manner to save lives, limit damage and accelerate recovery. It should facilitate sharing of information and communication amongst multiple organisations and agencies. It should identify and reduce redundant efforts quickly. There are many examples of duplicate efforts going on in parallel, usually with the best of intentions. It is often required to develop manual systems in the first instance – simpler is better in most cases, especially in real-time situations. It should be recognised that nothing can be relied upon to work in pre-emergency situations – what if there is no power, no Internet and so on. If there is power and water and other supplies, it may be possible to use ICT but in a non-connected manner.

The use of a unified command and control system, and a unified incident command system, is critical. This should apply in both military and civilian circumstances and needs to be incorporated into the design of any system. A methodology of managing disasters would also be a useful output into which ICT can be built. It should be able to manage small and large events, and when ICT is deployed, teams of programmers in the field are also of great use to adapt systems on location to support networks. Any ICT developed must be flexible. It must have the ability to adapt, and to add and subtract components. Handheld communications devices, if they work in the context, are ideal. The key lesson learnt is to not overbuild the system – build it for the requirements to recover in an accelerated manner by designing an implemented targeted real-time decision support system to supply information.

Also of high priority in decision making and building systems is to leave a sustainable system in place so the local community can continue to service the requirements of the disaster, most of which last for months or years – and in many cases recur. The use of training is highly recommended to ensure systems function in local languages and simple programmes using mostly point and click user interface design.

5.5.2 ITCM project's implementation of a C4I system

The ITCM project aims to enhance the interoperability of ICT-systems between organisations involved in crisis response, humanitarian emergencies and peace support operations. A common distributed C4I (Consultation, Command, Control, Communications, and Intelligence) system will support advanced planning and cooperative execution of tasks and rapid, secure and reliable exchange of information between peacekeeping forces and international organisations involved in the operations.

The Information Technology and Crisis Management (ITCM) programme is a joint venture of Tampere University, The Finnish Defence Forces, Ministry of Defence of Finland, Ministry for Foreign Affairs of Finland, and Crisis Management Initiative. The Information Technology and Crisis Management programme will develop and deploy a decision-making support and knowledge management system for crisis response and peace support operations in cooperation with crisis management organisations. The product will unify information and communications technology system interfaces used in a field operation into a single, standardised entity. The system will be based on open, commercially available components.

The ITCM system aims to enhance security and efficiency of the field operations. Therefore all communications within the system are encrypted and access to different functions and data can be flexibly controlled. An enhanced document management system will build institutional memory in side organisations and in the whole operation. The project will emphasize increased situation awareness and better flow of information. Information sharing enables more effective use of resources and enhanced management of overall operations. This may eventually lead to a shortened need for international presence in the crisis area implying significant cost-savings.

The programme is divided into four tracks: 1) System Development, 2) Turnkey Delivery Capability, 3) International Dialogue and 4) Research. System development is a core part of the programme. Commercially available products such as document management applications will be integrated into a single component based standardised information system. The integration will be based on the Object Management Group (OMG) C4I standards. The system development started in the beginning of 2002 and is proceeding according to schedule. A fully functional and tested system will be demonstrated within the Nordic Peace and Co-operative Knowledge Partnership for Peace (PfP) exercises in September 2003 in Finland.

The importance of a turnkey delivery capability has become clear during initial discussions with crisis management organisations. The prospective clients for the system should be able to order an up-and-running system with comprehensive support, training and maintenance services from one place. During the year 2002 the partners in the ITCM program have started the planning of the organisational structure and business processes of the ITCM company. Currently the ITCM programme is conducting a feasibility study on setting up an international telecommunications operator that could provide a communication and data transmission infrastructure on the crisis area from day one.

6 Conclusions and recommendations

The discussions on the current crisis management environment highlighted the increasing challenges for crisis response and management created by intrastate conflicts and supranational new security threats, such as terrorism and organised crime. Many of the requirements for interoperability, information sharing and co-operation stem from this new multi-institutional setting.

While the orientation of the participants in the seminar was towards international crises as found in the Balkans and Afghanistan, the issues addressed, the conclusions arrived at, and the recommendations made are equally applicable at all levels: local, national, regional, international and all organisational types. This includes police departments, fire departments/brigades, emergency medical providers, and others as well as international humanitarian relief organisations and military organisations involved in crisis management operations. However, there should be a recognition of the differences in scale and response times required, which tend to be inversely proportional.

Modern peace operations and crisis management operations can be extremely difficult in military technical terms. They differ from traditional uses of armed forces or traditional types of intervention. The management and the style of the intervention must have some logical connection to the type of peace desired afterwards. Operations cannot be

conducted with complete disregard for human rights if the post-crisis peace is to be based on a foundation of respect for human rights.

The main organisations involved, UN, NATO, EU, OSCE and local and national governments are currently not using IT appropriately in their everyday functions. Despite rapid developments in IT and communications in recent years the potential of ICT remains largely untapped and under-utilised in crisis management. Where technology is utilised it tends to be done without coordination with partner organisations. Large bureaucratic institutions can be amongst the least well-equipped organisations in the world for correctly assessing what the private sector can offer.

The diversity of organisations, NGOs and other independent actors can also lead to misunderstanding desired outcomes, especially in stressful and challenging environments. A clear definition of objectives and division of labour between organisations in the field would allow the best use of ICT. Several participants stressed the need to have some kind of “pre-planning framework” in which these issues are addressed.

Consensus on the need to define technical requirements according to needs of the different crisis environments was achieved. In order to satisfactorily design ICT capabilities to support responses to crises scenarios, it will be necessary to identify who is doing what to whom, and why. Only once this has been established can the architecture be conceived to support these information processes.

It was noted that it is better to start from information sharing instead of coordination. In nearly every international emergency, information assets must be shared between partners in crisis response. Examples of failed cooperation caused not by national or personal considerations, but by IT systems failure, are rife in crisis response settings, from lack of supply-chain integration for parts replacement between KFOR forces to failed intelligence communications between allied forces.

Participants had the common view that the final objectives in peace support operations and in crisis management are to restore and enhance local capacities and build sustainable and democratic societies. ICT used in international field operations could be transferred to the local authorities of the host country. The use of information technology is a feature of all societies, and a peaceful, modern, open and democratic society certainly should include constructive use of the potential of ICT both by the government and by civil society for the process of construction as part of good governance.

It is impossible to automate ad hoc processes. Political leadership and proper management processes need to be put in place in the organisations before ICT can bring added value. Organisations have to understand their business, put down on paper what their business processes are, and look at the environment in which they are going to be using automation. Only then can organisations look at the tools that are available and how they might best use them.

Business processes are similar across organisations working in the international environment. Real time connection between sources of supply information, whether it is military or crisis response or inventorial parts from automobile manufacturers, are in essence the same thing. They face the same type of real time information flow problems that are faced by the stakeholder organisations. Business processes can be implemented even if the intent of the organisation is different. Once processes are shared, standards for ICT can be shared and it can be expected that vendors will also participate once they see markets in more than one organisation to develop software and hardware communication solutions that they can sell.

The seminar was seen as a first step in building dialogue between crisis response organisations and ICT vendors. The establishment of the Advisory Team was seen as a means of institutionalising this network and to get the right people together. It was proposed to include the WGET in the advisory body in order to ensure that the lessons learned in emergency telecommunications would be included in the future work.

The following recommendations were made:

- There is a need for a framework document defining norms for ICT interoperability in crisis management situations. This would need to include conceptual definitions of generic requirements.

- There is a need for a thorough assessment of multi-institutional requirements for critical information and communications needs, particularly at the deep field level, on who needs to communicate what to whom, and why. A methodology is required to structure prioritised communications needs.
- Once communications/information needs have been identified at operational and strategic levels, these requirements need to be articulated at the key points of commercial and institutional 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.
- Standards for ICT use in crisis management environments must build on existing work in other standardisation contexts.
- Crises are often the consequence of the failure of systems of governance and representation and natural disasters. The resolution of a crisis often lies in restoring domestic governance capacity. This may include the capacity to organise elections or the ability to deliver humanitarian aid in the event of a natural disaster. The implementation of ICT solutions to crisis management situations should be inclusive in their design to enable a transfer of governance capacities to domestic authorities, delivering a governance and sustainability dividend.
- Thus far contributions to C4I have been confined mainly to the military. For effective ICT interoperability and the convergence of civilian stakeholder requirements there must be greater civilian inputs and participation.
- Civilian - Military interface must equally accommodate the immediate needs with the long-terms needs of sustainability and avoidance of repeat crisis situations.

ANNEX I

Report from the Workshops

Workshop 2: Civil-military interface and exchange of information in the field

The objective of the workshop was to discuss how civilian and military organisations' working cultures differ and how ICT-systems tailored to crisis management can improve and facilitate their day-to-day co-operation, information sharing and coordination. One of the key issues was to define when and how that divide between military and civilian organisations needs to be crossed. The workshop identified key requirements for a common IT-system and the potential benefits of such decision-making and knowledge management products in operational environments requiring joint military-civilian co-operation.

Because of the interdependence of the military and civilian organisations engaged in emergencies and peace operations, information sharing was deemed vital for achieving successful results. Information sharing can enhance operational efficiencies, thereby saving lives and resources. It was noted that military organisations are still unaccustomed to exchanging information with international organisations and NGOs, and vice versa. The group identified the problems of battles and rivalry between various organisations and the cultural gap that exists. There is a lot of room and possibilities on convergence in this area, particularly when it comes to safety and security, which are issues of fundamental, mutual concern that all the organisations in the field share. Therefore, security should be a common denominator for information sharing.

Information security was another key issue discussed. How to validate the accuracy of the information, on the one hand, and ensure its security, on the other? The military, might worry that civilians are less rigorous about information integrity, both protecting it and ensuring its accuracy. Classifications should not be an obstacle to information sharing but the reality has to be accepted. However, the workshop noted that actually a lot of information available is not classified and could be shared. It was noted that at the local level in the field the information sharing is much easier than trying to implicate the headquarter level or operational information sharing. In the beginning of a field operation the common interface that is needed is information exchange rather than co-operation. There should also be a distinction made between content, security-level etc. That leads to the need of certain standardisations in that field of information exchange.

Because of the complexity of the multi-institutional operations, a concept for co-operation and information sharing is needed to overcome the ad hoc nature of attempts to share information. The concept should be based on questions such as how integrated operations can work, in what kind of fashion, and what kind of information could be shared. Building trust is an important prerequisite for getting a more systematic approach of information exchange and involving various actors in the field.

Understanding how the various organisations operate in the field is an important result of information sharing. It was recommended to increase joint civil-military pre-mission exercises and training. If there is no preparation before going into the field, civil-military relations are already strained but also any kind of information sharing becomes very difficult. There already exists training modules which could be used. The EU has recently undertaken a number of exercises in the field of crisis management. They have brought in interagency co-operation and cross-stakeholder participation from actors such as the police, the military, the EU, the UN and humanitarian agencies. This could in the future be an important preparation for going into a complex emergency.

It was recommended to develop a kind of plug-and-play arrangement/system, which would allow interoperability between civilian organisations and military when needed but would not be automatic. Missions cannot be precisely planned and it is impossible to foresee what will happen but the plug-and-play system may help to be prepared for different emerging situations. This leads to standardisation requirements. Furthermore, it was suggested to the military to create a kind of parallel information system, which would be public or at least open to partners in a complex emergency situation.

It was concluded that it is important not to ignore the models, best practises and standards for information sharing that exist today. One standard is the Oslo Guidelines for natural disaster contingencies. There also exists draft guidelines on civil-military relations in peace operations including lessons learned practises published by NATO and the EAPC, the

Euro-Atlantic Partnership Council in the year 2000. It was pointed out that it should not be forgotten that there are already certain languages and software, which exist in the field, which is accepted by the UN, particularly for identifying land mines. It was suggested to take stock of a number of standards, which exist in the field of civil-military relations to facilitate the development of information-sharing mechanisms that support advance planning and coordinated implementation.

Discussion Points Made

- Linux is a possible key to future interoperability developments, and so systems are not dependent on one manufacturer.
- Local level cooperation rather than headquarter level should be encouraged and studied further on a practical basis.
- Testing on unclassified information initially would give system interoperability scenarios a better chance of success
- Plug-and-play, commercially-available systems should be examined for information sharing rather than designing brand new systems
- The need for ICT specialists to observe discussions and live situations involving civil and military actors.
- There is a danger of automating something that has yet to be defined; there is a clear need to look at the processes and requirements, and look at the concept again for consensus on definition.
- Possibility of forming working groups in specific areas of ICT (emergency telecoms, internet, GIS technology) sponsored by particular organisations; this raises the further question of suitable fora for future discussions. Some of these fora already exist, and should be built on.
- The key aspect of determining what different organisations are trying to achieve, and then and only then placing ICT in that context – and should be examined in the same context as businesses when assessing ICT requirements.
- A full assessment of existing best practice in the field should be made. The British Government has already done this to some extent at www.itil.org.uk
- There is a clear need to make headway in the sharing of maps. There is of course a number of systems, GIS and others which could be used specifically also with regard to common situational awareness and land-mind fields.
- The necessity of having results driven, practical outcomes of this conference which should incorporate a fundamental aspect and the very first priority of operations – safety – and another which should address logistics, involving data communications internally as well as interoperability requirements.

Workshop 3: Supporting management change in international organisations with ICT

The objective of this workshop was to examine best practices and common obstacles related to the adoption of information and communication technology in international organisations. Again the difficulty of bringing together different communities and backgrounds was expressed. The workshop was asked to propose practical guidelines as to how ICT systems could and realistically should, be deployed more successfully in the future.

The first issue was the importance of organisational management with understanding for the introduction and changing systems. The group concluded that these definitions were critical in defining requirements well before ICT was introduced. It was important then taking in the account the field needs in the context of objectives. It is critical to see how they relate to the objectives of the system. It is important to make sure that you make use of existing investment, and a need to respect the necessary independence of different groups providing and using ICT. It is vital to enable the distribution of responsibilities within the organisations, but without excessive centralisation. But the most important issue was to define the information to be shared and the purposes, a simple global statement that you need to operate. It's not adequate to provide effective definition of systems.

The second issue was to identify who needed to be involved. It's clearly important to involve the management of organisations to have an organisational architect who has an overview of what is required and then involve the users. But there was a need to look for specific well-established standards, which is not very difficult to identify, but they

possibly would be in specific information exchange standards that relate to the kind of information that these organisations are concerned with.

The workshop also looked at the issue of outsourcing and the feeling here was that there was some very clear advantages in this in particular area because of the difficulty in maintaining the adequate skills within the kind of organisations we are talking about. The main point in outsourcing is in maintaining the adequate technical skills. But this kind of outsourcing does place a premium on clear understanding shared between the organisation and the provider of outsourcing on the nature of this system and the roles they play within the organisation. So outsourcing needs to be looked at on a case-by-case basis.

And finally the group looked briefly at the issue of security. It was noted that there is a need here again for clear objectives for what it is you're protecting and why you're protecting it. And so clearly there is a need to balance the requirements of the individual with the need to share information within the organisations.

Workshop 4: Preconditions for the adoption of common ICT systems on international organisations' field operations

The objective of the workshop was to identify a list of preconditions that are needed for the adoption of a more integrated ICT system for a certain mission area. The workshop also aimed to identify the key drivers for, and obstacles of crisis management organisations, when adopting interoperable ICT systems, and how these key concerns could be translated into system requirements.

It was difficult to find mutual ground among the very heterogenous group, but there were some limited conclusions. The conclusions focused on the difficulties in defining the international community's requirements in a fashion that is manageable and workable for the development of a technical framework or standardisation model.

The operational priorities should be defined by the field organisations themselves. All crisis situations are different and no technical solution should be architecturally overly prescriptive. A framework within which all stakeholders are able to define their requirements and to find a common operational framework for information technology is required.

Security was seen as the number one driver for a more integrated ICT system. The order of priority is to first have the voice and other communications mechanisms deliverable in the field. The second priority for the field organisations is logistics - providing the facility to be able to operate so what one actually needs essentially to operate.

Needs analysis should be conducted on a number of case studies to identify a methodology for operational needs identification. This will need to be inter-operable with the policy structures that also vary with each individual crisis management circumstance but to a much lesser degree.

In conclusion, the Chair noted that there was after the conference an understanding of the requirements and communication amongst the stakeholders that meant real progress had been made, particularly in the area of civil-military interface for delivering mutual objectives. The real aim is to have an impact on real life situations. The values here are shared, and there is a real need for management solutions for practical aspects of the problems. A great deal more effort needs to be put into planning, training and preparation by the different actors. It was encouraging to see interface between operations people and technology providers. The cultural divide, which exists, can be overcome if there both sides know what they want and what they can offer. Their objectives will remain different, but can be complimentary in seeking optimal and mutually reinforcing outcomes.

ANNEX II

Seminar on Crisis Management and Information Technology

Helsinki, 29 September – 1 October 2002

At Hotel Strand Inter-Continental

Co-organised by
Crisis Management Initiative and Object Management Group

Agenda

Sunday 29 September 2002

- 19.00 Inaugural dinner in Hotel Strand Inter-Continental**
Speech by Mr. Jan-Erik Enestam, Minister of Defence, Minister for Nordic Cooperation and Matters Relating to Neighbouring Areas

Monday, September 30, 2002

- 09.30 Registration**

- 10.30 Welcoming address:**
Mr. Jaakko Laajava, Under-Secretary of State, Ministry for Foreign Affairs of Finland

- 10.45 First session: “*International organisations and the new challenges in crisis Management*”**
Chairs: President Martti Ahtisaari, Crisis Management Initiative
Dr. Richard Soley, Object Management Group

Keynote address: “*Co-operation between the UN and regional organisations in modern crisis management operations*”

Mr. Cedric Thornberry, Former Assistant Secretary-General of the UN

Panel Discussion:

“*EU’s challenge to guarantee civil military coordination in its future field operations*”

General Gustaf Hägglund, Chairman, European Union Military Committee

“*Supporting peace in new kind of conflicts*”

Mr. Luiz Da Costa, Principal Officer, Office of the Under-Secretary-General for Peacekeeping Operations, UN

“*NATO and crisis management*”

Ambassador Robert Serry, Director of Crisis Management and Operations, NATO

“*European Commission’s role in bringing technology to support crisis management*”

Mr. Lars-Erik Lundin, Head of Security Policy Unit, European Commission

“*Need for civilian capability in modern crisis management*”

Mr. Michael von der Schulenburg, Director of Management and Finance, Organization for Security and Co-operation in Europe (OSCE)

- 12.30 Lunch**

- 13.30 Second Session: “*Enhancing the international field operations*”**
Chair: Mr. Michael Matthiessen, Director, Civilian Crisis Management, General Secretariat, Council of the EU

Keynote address: “Decalibrating the international community’s presence in Bosnia-Herzegovina”

Dr. Nicholas Whyte, Balkans Program Director, International Crisis Group

Statements

“Using Commercial Technology in Crisis Management, Case: Finnish Battalion CIS-system in KFOR”

Admiral Juhani Kaskeala, Chief of Defence, Finnish Defence Forces

“Telecommunications and Emergencies”

Mr. Hans Zimmermann, Senior Humanitarian Affairs Officer, Office for the Coordination of Humanitarian Affairs (OCHA)

“Property Law Implementation Plan in BiH”

Mr. David Stewart Howitt, London School of Economics

“Afghanistan: Feeding 10 million people where there are no telephones”

Mr. Peter Casier, Director, UN World Food Programme

15.00 Coffee Break

15.30 Third Session: “Information technology as a tool in crisis management and information management”

Chair: Mr. Eduardo Blinder, Director, Department of Management, Information Technology Services Division, United Nations Secretariat

Keynote address: “The Role of Technology in Global Disasters”

Mr. Brent H. Woodworth, Manager of IBM’s Worldwide Crisis Response Team

Statements

“Use of geographical information systems and satellite data in evaluating the impact and spreading of crisis and catastrophes”

Mr. Guy Weets, Head of Sector “Risks and Crisis Management”, DG Information Society, European Commission

“Using information systems in national emergency situations “

Mr. Sheldon C. Sutton, MITRE

“Sharing of Intelligence, Surveillance and Reconnaissance Information in Multiorganisational Operations”

Dr. Gert Retzer, Director, NATO Consultation, Command, and Control Agency

“Reform of the Information Management System in the OSCE”

Mr. Anders Norsker, Head of IT services, OSCE

“ITCM – a step towards integrated IT-system for crisis management field operations”

Mr. Kari Laitinen, Project Manager, ITCM

19.15 Transportation by boat m/s Chapman to Suomenlinna. The boat leaves from the dock in front of Hotel Strand Inter-Continental.

20.00-22.30 Dinner, Panimoravintola, Suomenlinna

Tuesday, October 1, 2002

09.00 Fourth session: Workshops:

Introduced by Ms. Alyson Bailes, Director, SIPRI

Workshop 1: *Political leadership of an operation: lessons learned*

Chair: President Martti Ahtisaari

Workshop 2: *Civil-military interface and exchange of information in the field*

Chair: Professor Fred Tanner, Deputy Director, Geneva Centre for Security Policy

Workshop 3: *Supporting management change in international organisations with IT*

Chair: Mr. Michael von der Schulenburg, Director of Management and Finance, OSCE

Workshop 4: *Preconditions for adoption of a common IT system in international organisations' field operations*

Chair: Mr. David Stewart Howitt, London School of Economics

11.00 Plenary Session:

Report from the workshops

12.00 Concluding remarks:

President Martti Ahtisaari

Dr. Richard Soley

12.30 Lunch

15.00 Executive Advisory Symposium with OMG BoD

(Afternoon Session by invitation only)

ANNEX III

LIST OF PARTICIPANTS

Mr Aleksi Aaltonen

ITCM Expert
Crisis Management Initiative
Erottajankatu 11 A
00130 Helsinki, FINLAND
Tel. +358 9 698 7024
Fax: +358 9 612 7759
Email: aleksi.aaltonen@ehtisaari.fi

Mr Martti Ahtisaari

President, Chairman
Crisis Management Initiative
Erottajankatu 11 A
00130 Helsinki, FINLAND
Tel. +358 9 698 7024
Fax: +358 9 612 7759
Email: martti.ahtisaari@ehtisaari.fi

Mr Simo Alho

Inspector of Signals
Finnish Defence Forces
PO Box 919
00131 Helsinki, FINLAND
Tel. +358 9 181 23600
Fax: +358 9 181 22508
Email: simo.alho@mil.fi

Ms. Dock Allen

Principal Software Systems Engineer
The MITRE Corporation
202 Burlington Road, Mail Stop 2B-421
Bedford, MA 01730, USA
Tel: +1-781-271 8216
Fax: +1-782-271 4686
Email: dock@mitre.org

Mr Adam Austerfield

Director of Projects
Enterprise LSE
Houghton Street
London WC2A 2AE, UK
Tel. +44 207 955 7128
Fax: +44 207 955 7890
Email: a.austerfield@lse.ac.uk

Ms Alyson J.K. Bailes

Director
Stockholm International Peace Research Institute
Signalistgatan 9
S-16970 Solna, SWEDEN
Tel. +46 8 655 9750
Fax: +46 8 655 9733
Email: director@sipri.org

Lt.Col Gil Baldwin

British Army
QDG, Athlone Barracks
Catterick Garrison
North Yorkshire DL9 3P2, UK
Tel. +44 1748 873348
Fax: +44 1748 873339
Email: gtbaldwin@msn.com

Mr Arne Berre

Chief Scientist
SINTEF
Forskningsveien 1, Blindern
0314 Oslo, NORWAY
Tel. +47 2206 7452
Fax: +47 2206 7350
Email: arne.j.berre@sintef.no

Mr Eduardo Blinder

Director
Information Technology Services Division
S-1927 United Nations
New York, NY 10017, USA
Tel. +1 212 963 8194
Fax: +1 212 963 2006
Email: blinder@un.org

Mr Peter Casier

Director
WFP Support Office – Dubai
United Nations Food Programme
Bel Haza Building, Al Quoz Industrial Area
PO Box 37297, Dubai
UNITED ARAB EMIRATES
Tel. +971 4 347 1089
Fax: +971 4 347 0761
Email: peter.casier@wfp.org

Mr Luiz Carlos Da Costa

Principal Officer
Office of the USG
Dept of Peacekeeping Operations
United Nations
1st ave corner 42nd street, room s-2260
New York, NY 10017, USA
Tel. +1 212 963 5053
Fax: +1 212 963 0383
Email: da-costa@un.org

Mr Eelco Dykstra

Professor in International
Emergency Management
University of Kuopio
Dept of Health Policy & Management
PO Box 1627
70211 Kuopio, FINLAND
Tel. +31 55 360 4490
Fax: +358 17 162 999
Email: e.dykstra@wxs.nl

Mr Esa Einola

Vice President
Confidence to Net
Secwell Networks Oy / Selgo group
PI 174
33101 Tampere, FINLAND
Tel. +358 3 336 8111
Fax: +358 3 336 8500
Email: esa.einola@secwell.com

Mr Rune Froseth

Head, Information Technology Section
United Nations Office for Coordination for Humanitarian
Affairs
1 UN Plaza, Room DC1-1354
New York, NY 10017, USA
Tel: +1 212 963 0048
Fax: +1 917 367 0416
Email: froseth@un.org

Ms. Nicole Glazen

Director of Business Development
Object Management Group
First Needham Place
250 First Avenue, Suite 100
Needham, MA 02494, U.S.A
Tel: +1-781-444 0404
Fax: +1-781-444 0320
Email: glazen@omg.org

Mr Erik Hammer

Head of Signals and Electronics Branch
Norwegian Defence Logistics Organisation / Land
Boks 43
1306 Barum Postterminal, NORWAY
Tel: +47 230 96053
Fax: +47 2309 6671
Email: ehammer@mil.no

Mr. E. Kenneth Hong Fong

Chief Technology Officer
Office of the Secretary of Defense (OSD)
OUSD (AT&L)
3015 Defense Pentagon
Washington , DC 20301, USA
Tel: +1-703-695 0472
Fax: +1-703-614 4570
Email: ekenneth.hongfong@osd.mil

General Gustav Hägglund

Chairman of the EU Military Committee
European Union
Rue de la Loi 175
1048 Brussels, BELGIUM
Tel. +32 2 285 5986
Fax : +32 2 285 5928
Email : gustav.hagglund@consilium.eu.int

Mr Jorma Hämäläinen

Vice President
Sonera Ltd
PO Box 910
Helsinki, 00051 Sonera, FINLAND
Tel. +358 2040 58861
Fax : +358 2040 58882
Email : jorma.k.hamalainen@sonera.com

Mr Jaakko Iloniemi

President
Crisis Management Initiative
Erottajankatu 11 A
00130 Helsinki, FINLAND
Tel. +358 9 698 7024
Fax: +358 9 612 7759
Email: jaakko.iloniemi@ahtisaari.fi

Prof. Charles Johnson

Senior Analyst (CTR)
Cherokee Information Services
(Supporting US DOD)
3015 Defense Pentagon
Washington, DC 204301, USA
Tel: +1-714-695 0472
Fax: +1-703-614 4570
Email: chuck.johnson@osd.mil

Mr Risto Kalske

Director, Preseed-Finance
SITRA
Itämerentori 2
00180 Helsinki, FINLAND
Tel. +358 9 6189 9412
Fax: +358 9 6189 9277
Email: risto.kalske@sitra.fi

Mr Yuki N. Karakawa

Chairman
Karakawa Foundation
4-20-17-201 Takanawa, Minato-ku
Tokyo 108-0074, JAPAN
Tel. +81 3 3443 8385
Fax: +81 3 3443 8385
Email: ykarakawa.kfgate@ma.newweb.ne.jp

Admiral Juhani Kaskela

Commander of the Finnish Defence Forces
PO Box 919
00131 Helsinki, FINLAND
Tel. +358 181 0111
Email: juhani.kaskeala@mil.fi

Mr Ossi Kerminen

University of Tampere
Hypermedia Laboratory
33014 University of Tampere, FINLAND
Email: ossi.kerminen@uta.fi

Mr Markku Koli

Chief of C3
Finnish Defence Forces
Defence Staff
PO Box 919
00131 Helsinki, FINLAND
Tel. +358 9 1810 111
Email: markku.koli@mil.fi

Mr. Harri Kreus

Senior Consultant
HM&V Research Ltd
Piispanportti 9
02240 Espoo, FINLAND
Tel: +358-9-2532 0525
Fax: +358-9-2532 0501
Email: Harri.Kreus@HMV.fi, harri.kreus@hmv.fi

Ms. Tomomi Kurata

Senior Technology Officer
Toshiba of Europe Limited
Audrey House, Ely Place
London EC1N 6WSN, UK
Tel: +44-20-7421 7620
Fax: +44-20-7421 7626
Email: tm.kurata@toshiba.co.jp

Mr Jaakko Laajava

Under-Secretary of State
Ministry for Foreign Affairs of Finland
PO Box 176
00161 Helsinki, FINLAND
Tel. +358 9 1605 5030
Fax: +358 9 1605 5002
Email: jaakko.laajava@formin.fi

Mr Kari Laitinen

ITCM Project Manager, Assistant Professor
University of Tampere
Hypermedia Laboratory
33014 University of Tampere, FINLAND
Mobile: +358 41 448 1230
Email: kari.j.laitinen@uta.fi

Mr Ari Lampela

Client Manager for Finnish Defence Forces
IBM Public Sector
PL 265
00101 Helsinki, FINLAND
Tel. +358 9 459 5014
Email: lampela@fi.ibm.com

Francois-Xavier Lebas

System Architect
THALES Communications
66 rue du Fosse Blanc
92231 Gennevilliers, FRANCE
Tel: +33-1-46 13 25 71
Fax: +33-1-46 13 26 86
Email: francois-xavier.lebas@fr.thalesgroup.com

Mr Walter Legrand

Europe and NATO Manager
EADS-Telecom
Rue JP Timbaud – Montigny le Bretonneux
St Quentin Yvelines, FRANCE
Tel. +33 1 3460 8768
Fax: +33 1 3047 6003
Email: walter.legrand@eads-telecom.com

Mr Krister Ljungqvist

Solution Manager Emergency Response
Ericsson AB
Department KI/ERA/POB/R
16480 Stockholm, SWEDEN
Mobile: +46 70 519 4939
Fax: +46 8 751 2394
Email: krister.ljungqvist@era.ericsson.se

Mr Lars-Erik Lundin

Head of Security Policy Unit
European Commission
Rue de la Loi 200
1049 Brussels, BELGIUM
Tel. +32 2 296 5081
Fax: +32 2 295 0580
Email: lars.lundin@cec.eu.int

Mr. Sumeet Malhotra

Director, Global Industries
Unisys Corporation
B-306 Unisys Way
Blue Bell, PA 19424, USA
Tel: +1-215-986 2468
Fax: +1-215-986 7046
Email: sumeet.malhotra@unisys.com

Mr Michael Matthiessen

Director, Civilian Crisis Management and Coordination
General Secretariat of the Council of the European Union
Rue de la Loi 175
1048 Brussels, BELGIUM
Tel. +32 2 285 5321
Fax : +32 2 285 8558
Email : michael.matthiessen@consilium.eu.int

Dr Robert Mikelskas

Vice President
The MITRE Corporation
7515 Colshire Drive M/S N605
McLean, VA 22102, USA
Tel. +1 103 883 7989
Fax: +1 103 883 6442
Email: rmikelskas@mitre.org

Jarkko Moilanen

University of Tampere
Hypermedia Laboratory
33014 University of Tampere, FINLAND
Email: jarkko.moilanen@uta.fi

Mr Jari Mäkinen

Nokia Networks
Nokia Professional Mobile Radio
PL 325
00045 NOKIA GROUP, FINLAND
Email: jari.a.makinen@nokia.com

Mr Kari Möttölä

Special Adviser
Department for Political Affairs
Ministry for Foreign Affairs
PO Box 176
00161 Helsinki, FINLAND
Tel. +358 9 160 55023
Fax: +358 9 160 55009
Email: kari.mottola@formin.fi

Mr Anders Norsker

Head of IT Services
OSCE Secretariat
Kärntnerring 5-7
1010 Vienna, AUSTRIA
Tel. +43 1 514 36571
Fax: +43 1 514 36588
Email: anorsker@osce.org

Mr Hiroyuki Ohno

Group Leader
CRL Communications Research Laboratory
4-2-1 Nukui-Kitamachi, Koganei
Tokyo 184-8795, JAPAN
Tel. +42 327 5542
Fax: +42 327 7941
Email: hohno-sec@ohnolab.org

LtCdr Olli Peltonen

CIS Representative
Mission of Finland to NATO
Rue Joseph Baus 99
1970 Wezembeek-Oppem
BELGIUM
Tel. +32 2 706 2123
Fax: +32 2 706 2142
Email: olli.peltonen@formin.fi

Mr Juho Pitkänen

Versokuja 3 A 8
00710 Helsinki, FINLAND
Mobile: +358 40 831 1880
Email: juho.pitkanen@helsinki.fi

Ms Pia Posio

Software Account Manager
Oy International Business Machines Ab
Laajalahdentie 23
00300 Helsinki, FINLAND
Tel. +358 9 459 4832
Fax: +358 9 459 6901
Email: pia.posio@fi.ibm.com

Mr Ari Rahkonen

Country Manager Software Group
IBM Finland
P.O.Box 265
00101 Helsinki, FINLAND
Tel. +358 9 459 3712
Fax: +358 9 459 6901
Email: ari.rahkonen@fi.ibm.com

Dr Gert Retzer

Director
Command and Control Systems
NATO Consultation, Command, and Control Agency
P.O. Box 174
2501 CD The Hague, THE NETHERLANDS
Tel. +31 70 374 3070
Fax: +31 70 374 3079
Email: gert.retzer@nc3a.nato.int

Captain Tom Richardson

Seattle Fire Department
PO Box 339
La Conner, WA 98257, USA
Tel. +1 360 466 4086
Email: thomas.richardson@verizon.net

Ms Kristiina Rinkineva

Advisor
Crisis Management Initiative
Erottajankatu 11 A
00130 Helsinki, FINLAND
Tel. +358 9 6987024
Fax: +358 9 6127759
Email: kristiina.rinkineva@ehtisaari.fi

Lt.Col. Pasi Rikkinen

Finnish Defence Forces
P.O. Box 919
00131 Helsinki, FINLAND
Tel. +358 9 181 23606
Fax: +358 9 181 23645
Email: pasi.rikkinen@mil.fi

Mr Aappo Roos

Portfolio Manager
Finnish National Fund for Research and Development
SITRA
P.O.Box 160
00181 Helsinki, FINLAND
Tel. +358 9 6189 9286
Fax: +358 9 6189 9277
Email: aappo.roos@sitra.fi

Mr Leo Saes

Chief of Communication and Information Systems
CIMIC Group North
Randweg Oost 32
Budel, 6021 PB, NETHERLANDS
Tel. +31 495 557 170
Fax: +31 495 557 029
E-mail: cjb6-chlof@cimicgroupnorth.org

Ms Raija Sarajärvi

University of Tampere
Hypermedia Laboratory
33014 University of Tampere, FINLAND
Email: raija.sarajarvi@uta.fi

Colonel Jussi Saressalo

Military Adviser
International Peace Academy
777 United Nations Plaza
New York, NY 10017, USA
Tel. +1 212 687 4579
Fax: +1 212 983 8246
Email: saressalo@ipacademy.org

Mr Michael von der Schulenburg

Director for Management and
Finance
OSCE Secretariat
Kärntnerring 5-7
1010 Vienna, AUSTRIA
Tel. +431 5143 6113
Fax: +431 5143 694
Email: mschulenburg@osce.org

Ambassador Robert Serry

Director, Crisis Management and Operations
NATO
NATO HQ
1110 Brussels, BELGIUM
Tel. +32 2 707 4030
Fax: +32 2 707 4768
Email: cmo@hq.nato.int

Mr David Stewart Howitt

London School of Economics
Houghton Street
London WC2A 2AE, UK
Tel. +44 20 7852 3608
Fax: +44 20 7955 7980
Email: d.stewarthowitt@lse.ac.uk

Lt.Col Rolf Stroessner
AO 1, CIS Division, EUMS
European Union Military Staff
Rue de la Loi 175
1048 Brussels, BELGIUM
Tel. +32 2 285 5682
Fax: +32 2 285 5793
Email: rolf.stroessner@consilium.eu.int

Mr Sheldon Sutton
Principal Information Systems Engineer
MITRE Corporation
7515 Colshire Drive
MS W928
McLean, VA 22102, USA
Tel. +1 703 883 6677
Fax: +1 703 883 6801
Email: shel@mitre.org

Dr Fred Tanner
Deputy Director
GCSP – Geneva
7bis Avenue de la Paix
1211 Geneva 1, SWITZERLAND
Tel. +41 22 906 1673
Fax: +41 22 906 1649
Email: f.tanner@gcsp.ch

Mr Cedric Thornberry
Consultant
Former Assistant Secretary-General of the UN
Stari Grad
20260 Korcula
CROATIA
Tel./Fax: +385 20 716 159
Email: cedric@cytanet.com.cy

Mr Julian Wathen
Deputy Director
Force Development
Ministry of Defence, UK
Metropole Building
Northumberland Avenue
London WC2N 5BP, UK
Tel. +44 207 218 3140
Fax: +44 207 218 7956
Email: DDFD@mod.gsi.gov.uk

Mr Guy Weets
Project Officer
European Commission – DG Information Society
1049 Brussels
BELGIUM
Tel. +32 2 296 3505
Fax: +32 2 295 3608
Email: guy.weets@cec.eu.int

Major Antti Viiru
Chief S6 / FinBn
Finnish Battalion / MNB(C) / KFOR
HQ / FinBn / KFOR
PO Box 61
00231 Helsinki, FINLAND
Tel. +358 9 181 52060
Fax: +358 9 181 52700
Email: g6@finbnkfor.com

Ms Linda Vilakazi-Tselane
Programme Manager
CSIR-Defencetek
PO Box 395
Pretoria 0001, SOUTH AFRICA
Tel. +27 12 841 4194
Fax: +27 12 841 2090
E-mail: lvilakazi@csir.co.za

Mr Pertti Virtanen
Manager of Business Unit
Suomen Erillisverkot Oy
Niittyläntie 5
00620 Helsinki, FINLAND
Tel. +358 2040 65871
Fax: +358 2040 65801
E-mail: pertti.virtanen@everkot.fi

Mr. Bryan M. Wood
Chief Systems Architect
Open-IT, Ltd.
11 Wilton Court, Sheen Road
Richmond, Surrey TW9 1AH, UK
Tel: +44-20-8940 1397
Fax: +44-20-8940 1397
Email: bryan@open-it.co.uk, Bryan.Wood@Open-IT.co.uk

Mr Brent Woodworth
Worldwide Segment Manager
IBM Crisis Response Team
21241 Ventura Blvd Suite 151
Woodland Hills, CA 91364, USA
Tel. +1 818 702 9412
Fax: +1 818 702 6372
Email: bhwoodwo@us.ibm.com

Major Pasi Välimäki
Senior Staff Officer
C3 Division, Defence Staff
Finnish Defence Forces
PL 919
00131 Helsinki, FINLAND
Tel. +358 9 181 23161
Fax: +358 9 181 23645
Email: pasi.valimaki@mil.fi

Mr Markku Österman
Managing Director
Suomen Erillisverkot Oy
Niittyläntie 5
00620 Helsinki, FINLAND
Tel. +358 2040 65870
Fax: +358 2040 65801
Email: markku.osterman@everkot.fi

ANNEX IV

Report of the Consultative meeting of the Crisis Response Executive Advisory Team for the ITCM Project and the OMG C4I Task Force *Helsinki, 1 October 2002*

The consultative meeting was convened from the invitation of President Martti Ahtisaari and Dr. Richard Soley, CEO and Chairman of the OMG. The meeting was organised to explore the feasibility and the interest of invited international organisations (see the list of participants attached) in establishing and joining the Crisis Response Executive Advisory Team (CREATE) for the Information Technology and Crisis Management– Project (ITCM) and the Object Management Group C4I Domain Task Force (OMG C4I). The meeting was held immediately after the completion of the OMG Board of Directors meeting with OMG's Board in attendance as a direct display of support for the concept and execution of the formation of the CREATE group.

Objective

Dr. Soley opened the meeting noting that the objective of the proposed Executive Advisory Team would be the development of a more structured co-operation between international organisations and ICT-vendors. The Team would foster both the ITCM programme and OMG's C4I Task Force and ensure that needs and priorities are set correctly for both bodies. Dr. Soley referred to the conclusions of the Crisis Management and Information Technology seminar and noted that business processes are very similar across governmental and inter-governmental organisations, as well as other ICT end user organisations. When organisations do share processes they can actually share standards for ICT. When the vendors see that the market is large enough they are likely to develop software and hardware for communication solutions. This keeps the price of the ICT down and makes it a valuable marketplace for vendors. The Executive Advisory Team would give the political and commercial weight and momentum to this process.

Work and future plans of the OMG C4I DTF

Mr. Brian Wood presented the work and future plans of the OMG C4I DTF. The Object Management Group (OMG) is an open-membership, not-for-profit consortium that produces and maintains computer industry specifications for interoperable enterprise applications and the tools to develop them. OMG C4I (Consultation, Command, Control, Communications, and Intelligence) Domain Task Force works for the enhancement of collaboration and critical information sharing among multi-national and non-government organizations operating in response to crisis situations through the adoption of consensus-based interoperability standards. OMG C4I is also promoting the creation of the International Partnership for Collaborative Operations (IPCO) initiative, to allow, encourage and direct joint international prototype research & development (ITCM is in fact an example of a national body already carrying out IPCO-style prototype development).

ITCM-project's work plan and timetable

President Ahtisaari briefly presented the ITCM-project's work plan and timetable. The objective of the ITCM programme is to develop a decision-making support and knowledge management system tailored for the use of international crisis management missions. The ITCM product will unify information and communications technology (ICT) systems used in the field operation into a single, standardised solution. The system will be based on open, commercially available components. ITCM-project is a Finnish national laboratory for implementing agreed OMG C4I standards, along the lines of the envisaged IPCO program.

The ITCM programme comprises of a four main tracks: 1) Systems Development, 2) International Dialogue, 3) Turn-Key Delivery Capability, and 4) Research. The technological development is proceeding as planned. Based on an ethnographic study in Kosovo an initial system design and functional specification was developed during the latter part of 2001. The first prototype covering the Intranet services was completed in July 2002. The rest of the system, including the communication, command, and control services, will be developed during the remainder of 2002, and first part of 2003.

The objective is to have full delivery capability for the system, support services, and customer organisation in place during 2004. The importance of a turnkey delivery capability has become clear during initial discussions with crisis management organisations. The ITCM programme is studying ways and prerequisites for setting up an international crisis management telecom operator that could set up and run a dedicated wireless telecom network in the crisis area.

The programme is supported by field research to make sure that the solutions are relevant for the end users. ITCM is working together with the London School of Economics on a research project on the operational requirements, deployability and added value of the ITCM in different crisis environments.

Discussion on the terms of reference for the Executive Advisory Team

Dr. Soley presented the concept paper for the terms of reference for the Executive Advisory Team. The Team would give the input of international organisations to the development of the ITCM-system and to the work of the C4I DTF to ensure that they remain relevant that their priorities are set properly. Among other things the Team would advise on strategic vision for the coming years in developing ICT-systems and standards for crisis response. It would also create a forum to communicate the developments and changes in the needs and requirements of the crisis response and management organisations regarding the information and communications technology they use to vendors to help them to deliver interoperability solutions and standards suited to modern crisis management. Furthermore, the Team would advice in areas for research and standardisation.

In the discussion on the draft it was noted the need to amend the first paragraph of the draft with direct reference to communications specialists and communications technology. The draft should also recognize more clearly the role of the humanitarian organisations in crisis response. It was noted that the language used in the C4I Domain Task Force is heavily influenced by the military language. Mr. Wood noted that this is due to the fact that so far only military organisations have actively engaged themselves in the work of the Domain Task Force. One aim of the Executive Advisory Team is to get the civilian and humanitarian organisations involved and make sure that the vendors understand their requirements. It was pointed out that the responsibility of the Team to advice the ITCM and OMG C4I DTF in funding their operations should not endanger the tendering processes of international organisations.

Conclusions

The United Nations Department for Peacekeeping, the United Nations Secretariat, the Organization for Security and Co-operation in Europe (OSCE), NATO, the NATO C3A and the London School of Economics announced their willingness to join the Executive Advisory Team. The European Commission and the Office for the Coordination of Humanitarian Affairs (OCHA) representatives will recommend the joining to their organisations.

President Ahtisaari proposed to have the first meeting of the Executive Advisory Team in March or April in New York City. His office will circulate the revised draft terms of reference to all participants of the consultative meeting. Both the ITCM and OMG Board will elect three representatives for the Executive Advisory Team. ITCM and C4I Task Force members will attend the meetings ex officio. It was proposed to have the second meeting of the Team in the context of the demonstration of the ITCM system that will take place within the Co-operative Knowledge 2003 and Nordic Peace 2003 exercises in September 2003 in Finland.

ANNEX V

CREATE

Crisis Response Executive Advisory Team for the ITCM Project and the OMG C4I Task Force

Objective

The purpose of the Crisis Response Executive Advisory Team, in support of the Information Technology and Crisis Management (ITCM) Project and the Object Management Group's C4I Domain Task Force (OMG C4I), is to establish a more structured co-operation between international organisations and information and communication technology vendors in order to deliver interoperability solutions and standards suited to humanitarian emergencies and modern crisis response and management.

Composition

The Executive Advisory Team shall comprise:

- Three representatives of the Executive Board of the ITCM Project
- Three representatives of the OMG Board of Directors
- Representatives of major international organisations working in crisis response & management and humanitarian emergencies, and foundations & research institutes

The intent is for the Executive Advisory Team to represent a worldwide constituency with participation from all geographic regions of the world. The Executive Advisory Team shall elect its Chair amongst its members.

The Executive Advisory Team is open for new members. The Executive Advisory Team shall adopt its own criteria and procedures for admission and exclusion of its members as necessary.

Operations

The ongoing secretariat for operations (meetings, notices, minutes, etc.) of the Executive Advisory Team shall be managed jointly by ITCM and OMG. The Executive Advisory Team shall normally convene at least once a year at the invitation of its Chair. Invitations to Executive Advisory Team meetings shall be dispatched by the operations secretariat at least one month in advance communicating the proposed agenda. Meeting participation costs shall be borne by the participants.

Responsibilities

The Executive Advisory Team shall serve as a consultative body and shall assist the ITCM Project and the OMG in the implementation of their duties. In particular, the Executive Advisory Team shall have the following responsibilities:

- Advise on strategic vision for the coming years in developing ICT-systems and standards for crisis response and management
- Communicate the developments and changes in the needs and requirements of the humanitarian organisations and crisis response and management organisations regarding the ICT they use
- Recommend areas for further research to support the development and deployment of the ITCM-system and related international research programs
- Recommend areas and priorities for fruitful future standardisation for OMG C4I
- Periodically evaluate the continued relevance of OMG C4I and ITCM-project
- Support ITCM and OMG C4I in their promulgation of ICT research results and standards.