INSTITUT DES NATIONS UNIES POUR
LA RECHERCHE SUR LE DÉSARMEMENT

UNITED NATIONS INSTITUTE
FOR DISARMAMENT RESEARCH

DEVELOPMENTS IN THE FIELD OF INFORMATION AND TELECOMMUNICATIONS IN THE CONTEXT OF INTERNATIONAL SECURITY
Geneva - 25-26 August 1999

PRIVATE DISCUSSION MEETING
HOSTED BY DDA and UNIDIR

Discussion Summary

As part of the response to the General Assembly resolution (53/70) on "Developments in the field of information and telecommunications in the context of international security", the Department of Disarmament Affairs and the United Nations Institute for Disarmament Research held a discussion meeting in Geneva on the 25th and 26th August 1999. The meeting was attended by over 60 participants from over 40 countries.

The aims of the meeting were both to raise awareness among United Nations member states of the security issues relating to developments in Information and Communications Technologies (ICT) and to initiate multilateral discussions so that the international community can engage in better-informed discussions of the problem.

The workshop ran in parallel to a bilateral consultation exercise in which interested states are submitting responses directly to the United Nations Secretary General and provided the first forum of its kind at this level for governmental and non-governmental experts to discuss these issues.

A - BACKGROUND

The discussions were held against the background of a number of developments in the international arena that stem in large part from rapid technological and commercial developments in information and communications technology (ICT) that have ushered in an "Information Age" (or a "Networking Age"). Although political and strategic factors have also had an impact, the information revolution has a number of security implications:

1. States, economies and citizens are becoming ever more reliant on Networked Information Systems (NIS) that are inherently vulnerable to electronic attack. As

dependence increases, so the results of attacks become potentially more disruptive. The nature of these systems and of possible modes of electronic attack means that the capability of carrying out attacks is inevitably enhanced. It is difficult to identify attackers and to distinguish between electronic vandals at one end of the spectrum and State aggressors at the other.

2. Economic globalisation, the spread of information technologies and developments in the global media mean that, on the one hand, it is increasingly hard for states to impose controls on the media to which their citizens are exposed. On the other, arguably, it is increasingly easy for states or groups to use propaganda, disinformation or psychological operations in order to achieve their strategic, political or economic goals.

3. The information revolution (and other strategic pressures within Western armed forces and defence policies) is leading to a phenomenon often described as a Revolution in Military Affairs (RMA). This involves the exploitation of advanced technologies to develop new doctrines, organisations and modes of war that allow conventional armed forces to be smaller, more lethal, operate at a higher tempo and to react more rapidly over long distances.

B - DEFINING THE PROBLEM

There was agreement that the problem involves a number of discrete but inter-related activities. Whether it is useful to treat the problem holistically or to break it up into its component parts will continue to be a subject for debate. Various approaches were proposed to help categorize the problem. One approach is to define three categories:

1. RMA - issues relating to conventional conflict arising from the advent of new military technologies and doctrines;

2. Information Operations/propaganda - issues relating to attempts to manage popular or elite perceptions across international boundaries through overt and covert means of persuasion;

3. Critical Infrastructure Protection and Information Assurance - the development of trustworthy network information systems (NIS) and the development of technologies, policies, collaborative mechanisms to ensure a secure environment for the growth of the global information infrastructure (GII). This category focuses on two areas. First, standards for the development of trustworthy systems. One concern expressed, for example, was the inability of most organisations today to check the source code of commercial off-the-shelf software to ensure it is free of computer malicious codes (CMC). Second, efforts to curtail computer crime and information terrorism. The focus here was on issues such as international legal co-operation and investigation.

However, although technology is advancing, there can still be difficulty in untangling categories of malicious activities from one another in a short time frame. The distinctions between war, inter-state conflict, peacetime diplomacy, economic competition and the activities of sub-state groups can be blurred. Furthermore, the impact of RMA and Information Operations doctrines is not confined to periods of conventional conflict. If, as some military theorists speculate, information operations could be used to achieve strategic coercion without resort to conventional force, then the impact of the RMA is much broader than merely war fighting.

In addition, some States see computer crime and information terrorism as being their primary concern and are keen to focus discussion on means of improving international co-operation in this field. Other states see the development of RMA or information operation capabilities, particularly by the more advanced military powers as being the key security issue.

This reflects the geostrategic context of the current debate. Information operations and information assurance have come to the fore in recent years because a small number of major powers have vertically proliferated information operations capabilities. Understandably, they object to attempts to constrain vertical proliferation, recognise that it is impractical to control horizontal proliferation and are concerned to maintain the freedom to use these capabilities while at the same time ensuring they are not themselves vulnerable to information attacks. States that feel vulnerable to information operations, meanwhile, are keen to use multilateral mechanisms to restrain this vertical proliferation.

C - SPECTRUM OF DEBATE

Participants at the seminar agreed on a set of baseline concerns and were able to define remaining areas for debate.

There was agreement that:

· The information infrastructures on which all states are coming to rely for civil, economic and military purposes are becoming more vulnerable and states need to make greater efforts domestically (in cooperation with the private sector) to improve information assurance.

· Due to the transnational nature of the problem, states need to improve dialogue and co-operation in promoting more trustworthy systems and in securing their information infrastructures against vandalism, crime and terrorism. Discussion centred round two categories of issues:

1. Structure of the dialogue and of international co-operation

It was agreed that a variety of bilateral and multilateral forums need to be used (including the G-8, regional organisations such as the Council of Europe, policing

organisations such as Interpol, standards organisations such as ITU, Common Criteria, OECD)

There was discussion on whether the United Nations General Assembly was a suitable forum for broad-based multilateral discussion (and which Committee to work through) and to what extent arms control arenas had any relevance

2. Content of the dialogue

There was agreement that the process of multilateral dialogue is important and should proceed in parallel to bilateral dialogues. The dynamic nature of the ICT field means that definitions of the problem and responses need to constantly evolve. Discussions on taking forward security technologies and security standards on improving international co-operation on law enforcement responses (national legislation, international detection and trace-back) are also necessary and issue of crime and terrorism should be included. Practical steps towards implementation of enhanced cooperation will need to be taken in the near future.

Debate centred on whether to focus on cyberspace or the broader infosphere - i.e. to what extent should the dialogue cover the content of transborder information flows as opposed to the infrastructures underpinning these flows. The question of whether the dialogue should encompass military affairs as well as trustworthiness, crime and terrorism was raised as was whether existing international organisations, conventions and legal instruments merely need to be evolved to deal with this problem area or whether new conventions are required.

D - KEY FINDINGS AND QUESTIONS

1. Offensive information operations and military applications of RMA/ICT

Should consideration be given to how information operations can be used offensively under international legal auspices for sanctions or enforcement operations?

Should there be efforts to either control the proliferation of RMA/information operations capabilities or to restrict their use using the Laws of Armed Conflict? A common, though not universal view, was that the existing Laws of Armed Conflict can, with adaptation, cope with the problem of information operations and RMA-era conflict.

Existing approaches to arms control are unlikely to be effective in limiting state development of information operations capabilities or the proliferation of capabilities to non-state actors.

2. Defensive IW/information assurance/critical infrastructure protection

There are clear practical measures that can be implemented to improve the security of the Global Information Infrastructure. These could be pursued in national, bilateral and multilateral arenas.

Key measures include: i) building more trustworthy systems using new technologies and improved standards; ii) passing and enforcing improved legislation on information crime - though with due regard for civil liberties and cultural differences; iii) improving international co-operation in network anomaly monitoring, trace back and investigation of computer intrusions; iv) improving education and ethics of users of ICT in order to make information assurance a societal responsibility.

Existing conventions and legal instruments on crime and terrorism (as well as standards, telecommunications procedures, etc) provide a basis from which to work; existing multilateral forums provide mechanisms that can be built upon. New mechanisms may need to be created, or evolved from existing mechanisms, to take forward necessary steps, notably intrusion monitoring and investigation

E - NEXT STEPS

On a pragmatic and ad hoc basis, states and corporate/NGO entities, which are concerned about their vulnerabilities to electronic, and information attack will improve their defences and pursue bilateral and multilateral initiatives.

Potential Steps Forward:

In the network age solutions will not be top down and not mediated through one single authority. Nor will solutions come primarily from governments. Rather, action needs to be taken on a variety of levels, by a variety of actors:

- Continue dialogue on the impact of the RMA in the context of arms control/Laws of Armed Conflict;
- Use United Nations framework to raise awareness of information assurance/critical infrastructure protection in international community (United Nations General Assembly since this involves all nations?). Use this broad framework to define problem and to agree a segmentation on which practical measures can be taken in the short and medium term;
- Segment the problem into manageable components on which practical action can be initiated. Use existing international structures (e.g. 1st, 2nd and 6th Committee plus other non-United Nations bodies) to take forward practical information assurance/critical infrastructure protection steps

Potential Immediate Next Steps:

- Collate and categorise national approaches to the problem (use responses to the Russian resolution as a baseline). This will help establish common definitions and categories and identify areas of disagreement.
- Identify conceptual and practical measures that will promote security of the GII and problems with implementing these solutions (e.g. privacy and data protection laws).
- Survey national approaches and multilateral mechanisms relating to information assurance/ critical infrastructure protection to identify the current "best practices." Compare this with the "ideal" solutions outlined at ii) in order to identify requirements for further work.
- Identify short, medium and long-term measures for information assurance/critical infrastructure protection that nations can take individually and those that require multilateral action; provide information and advice for nations, international bodies and the private sector to assist in the improvement of system trustworthiness.
- Various specific initiatives should be discussed further. For example, the establishment of warning and anomaly centres allowing exchanges of data in appropriate international structures on threats, intrusions, and facilitating trace-back and investigation should be examined.

All participants shared the view that current and future developments in information technologies raise legitimate and important concerns from the perspective of international security broadly defined. While perspectives diverged on priorities and approaches, all were aware that the discussion broached in Geneva is only in its very initial phases. Appropriate approaches and measures will require further exploratory discussion, and are likely to involve a variety of international actors to deal with the national, international, or transnational dimension of the problem.