

SPECIAL COMMENT

The last century has been characterized by dramatic changes with regard to scientific and technological developments. The multiplier effect and positive aspects of inventions in the area of information and communication technologies (ICTs) have become increasingly evident. ICTs facilitate communication, open new markets, attract investments and accelerate economic and social development. In an age of globalization, it is hard to imagine a country achieving economic prosperity without a well developed ICT infrastructure. The power of the ICT revolution rests with the fact that ICTs are embedded in every aspect of our lives—from communicating by e-mail and mobile phone to the command and control systems of our militaries.

However, while the benefits are innumerable, ICTs can also be used for malevolent or malicious purposes. There is increasing concern from many quarters about privacy issues, cybercrime, cyberterrorism and military use of information technologies.

While international debate and cooperation has moved forward on the first of these three areas to varying degrees, international understanding of ICTs and warfare is less developed. The Revolution in Military Affairs is founded on developments in ICTs, developments which have enabled military forces to assume new methods of command and control of personnel and equipment at the strategic and tactical levels. However, the evolution of ICTs also serves as a basis for cyberweapons and permits the possibility of electronic warfare. This has implications not only for changing forms and methods of conducting military operations, but could ultimately transform the traditional warfare paradigm, from physical battles between belligerents to information attacks in a virtual space that have all too real consequences in the physical world. As states come to terms with the capabilities—and dangers—of information warfare, it is not implausible that a cyberspace arms race could erupt. Such a race would not only be immensely destabilizing, but would also ultimately divert enormous resources from peaceful and sustainable development.

The potential threats posed by abuse of ICTs are of a universal and transnational character and touch upon all facets of the existence of states, societies, the private sector and individuals. However, despite the fact that these issues concern all of humanity, there are two major issues inhibiting international cooperation in this field. First, the terms used in discussion—such as information warfare, cybercrime, cyberterrorism, information weapons, information security, to name a few—lack agreed definitions. Second, there is a fundamental question about whether existing international law adequately covers security-related aspects of ICTs.

The international community has the responsibility not to allow this potential new area of confrontation among states to emerge. The United Nations has risen to the challenge through consideration by the General Assembly of the annual resolution on "Developments in the Field of Information and Telecommunications in the Context of International Security" initiated by the Russian

Federation in 1998 (resolution 53/70 of 4 December 1998). The resolution was adopted by consensus annually until 2005; for the past two years one state has voted against it.

The resolution stresses that ICTs and their means "can potentially be used for purposes that are inconsistent with the objectives of maintaining international stability and security" and may adversely affect the integrity of the infrastructure of States to the detriment of their security in both civil and military fields. The resolution also notes the necessity to "prevent the misuse or exploitation of information resources or technologies for criminal or terrorist purposes".

The resolution promotes consideration of existing and potential threats in the sphere of information security. It also encourages possible cooperative measures to address these threats and relevant international concepts aimed at strengthening the security of global information and telecommunication systems.

One of the first attempts to describe the spectrum of information security issues that are of primary importance for international community was made by the UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, which met in 2004 and 2005.

Continued interest in this topic was confirmed by resolution 60/45, which recommends the establishment in 2009 of "a group of governmental experts ... to continue to study existing and potential threats in the sphere of information security and possible cooperative measures to address them", as well as the concepts aimed at strengthening the security of global information and telecommunications systems.

I deeply appreciate UNIDIR's consistent support for international study and discussion of disarmament issues. Its interest in ICT security is long-standing, dating to its practical and positive initiative in convening an international meeting of experts in Geneva in August 1999 on developments in the field of ICT in the context of international security. This meeting helped to develop a better understanding of the substance of international information security issues and related concepts.

It is commendable that this issue of *Disarmament Forum* is dedicated to the subject of information security. This particular contribution will be a useful tool for diplomats, scientists, business, civil society and international organizations, as well as to the work of the 2009 Group of Governmental Experts on international information security.

Andrey Krutskikh

Chairman, United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, 2004–2005