ADVANCED INFORMATION TECHNOLOGY AND TERRORISM

Advances in commercial information technology and the rising threat of global terrorism are two of the most important influences on nations and their economies. Computing and communications services offered commercially nowadays provide capabilities with global reach that formerly were available only to the most advanced military organizations. Mobile user services, including 3G mobile telephones and broadband wireless networks, provide for wide range of applications previously constrained to static networks and desktop computers. Any group of users with sufficient funding can purchase off-the-shelf capabilities for network enabled operations, including video teleconferencing, shared white boarding, image capture and dissemination, and robust information protection.

The result is an "information battlespace" as an essential playing field for nations and their terrorist opponents. Since governments, their military and commercial sectors are major players in the war on terrorism, it is essential that they understand how to make best use of the new and emerging technologies while denying critical capabilities to terrorist organizations. Cooperation among the military and commercial sectors and across the nations will be necessary to reach this understanding so that appropriate actions can be taken in the commercial marketplace to steer technology in ways that are most productive and supportive of peace, stability, and prosperity.

To reflect the respective conceptual, doctrinal, technological, and organizational developments and to facilitate adequate responses by governments and industry, the Editorial Board of *Information & Security: An International Journal* (I&S), jointly with CITMO.net, decided to prepare a special I&S issue on IT, emerging commercial capabilities, and terrorism. As a result, this volume reflects ideas, concepts and approaches discussed during the international conference on "*Commercial Information Technologies for Military Operations*" (CITMO-2005) that took place in Plovdiv, Bulgaria, in the period 15-17 June 2005. The conference explored approaches and presented recommendations for:

- Implementation of available and appropriate technologies;

- R&D that could support development of IT and which could overcome obvious gaps;
- A strategy to coevolve the policy and IT in near-term toward achieving common goals.

This volume has two main parts. The first part starts with a look at how terrorists use Internet and what are the opportunities to counter this use without jeopardizing democratic principles and economic development. It then presents lessons learned in the use of commercial technologies in preparing our societies to respond to terrorist acts and other disasters. The final article in the first part explores emerging technologies for iris-based recognition and possible applications to enhance the security of variety of public and private facilities.

The second part covers comprehensively the roles of the military in countering terrorism. Three articles look respectively at the response of NATO to the events of September 11, 2001, missions and tasks of special operations forces in countering terrorist activity on own territory, and the responses to maritime terrorism (which, as the authors argue, shares many features with piracy at sea). All three articles commend on needs and requirements of military and other governmental organizations that could be met with commercial-off-the-shelf technologies.

This special issue provides also a comprehensive, up-to-date list with on-line resources on counterterrorism, important policy documents, related journals, institutions, technologies and scientific support, resource repositories, as well as some milestone publications.

The reader will not find answers to all related questions in this issue. We believe, though, that this I&S volume will provide ideas and novel concepts, analysis of approaches and experience.

Information & Security