C4ISR SUPPORT TO THE COMPREHENSIVE APPROACH

Current and emerging security challenges, technological advances and evolving concepts of operations changed considerably the requirements to defence organisations and supporting C4ISR systems. Of particular interest are developments under the rubric of 'Comprehensive Approach' or 'whole of issue' approach to security challenges. The comprehensive approach rests on several pillars:

- increasing levels of coordination among security sector organizations, other governmental and non-governmental organizations;
- integrating efforts within the security sector and respective funding streams for development and operation of crisis management capabilities, including C4ISR capabilities; and
- interagency and international cooperation in the whole life cycle of the C4ISR systems and capabilities.

This volume of *Information & Security* reflects respective developments in defence and civil security sectors, as well as the interaction between civilian and military actors and provides an up-to-date view on:

- Development of concepts, doctrines, organizational arrangements and tools for implementation of the comprehensive approach in crisis management and addressing the emerging security challenges;
- Strategic assessment of capabilities, in particular comprehensive C4ISR capabilities;
- Governance of IT in support of C4ISR capability development, including models for multinational cooperation between allies and partners in C4ISR capabilities development.

The first section in this volume presents NATO, European Union, and national views on the comprehensive approach and the respective policies for multinational cooperation, civil-military interoperability and emerging security challenges, crisis management and disaster relief, and the respective aspects of NATO-EU cooperation.

Here the reader will be introduced to the views of two NATO deputy assistant secretaries, a deputy defence minister, and the General Manager the NATO C3 Agency.

The second section is dedicated to advanced technologies in support of the comprehensive approach. It starts with a paper outlining the advantages of having NC3A as a platform to support C4ISR capabilities development. The five remaining papers present respectively the experiment on network enabled capabilities, conducted jointly by NATO and a partner country – Sweden, the NC3A activities in countering improvised explosive devices, a multinational approach to the delivery of cyber defence capabilities, an example of a SOA-based intelligence information system, and the challenges in providing language assistance to multinational partners in coalition operations with focus on medical support.

Section 3 presents IT support requirements and solutions to civil security, and all three articles treat the interaction between civilian and military actors in crisis management and disaster relief operations. The first article by Canadian analysts provides an overview of decision support tools used in the preparation for and execution of domestic security operations. The second one underlines the importance of multinational cooperation in distributed training, CAX and experimentation and presents the concept for creating a NATO Centre of Excellence in Crisis Management and Disaster Relief to be hosted by Bulgaria. The third article presents an environment for managing computer assisted exercises for civil security.

The final section is dedicated to policies and technologies for comprehensive approach to maritime security. It starts with an article analysing a national investment policy in maritime security. The second article looks at the challenges of multinational acquisition of capabilities, with focus on potential Black Sea regional cooperation. The final article in this volume provides a detailed overview of organisational concepts and technological solutions in support of maritime situational awareness in the Mediterranean.

The Editorial Board of *Information & Security* believes that this volume will provide novel ideas and solid examples on the linkage between security thinking and advanced technologies. At the same time, we see it as the first in a series of publications examining IT and other technological requirements for effective implementation of new concepts such as smart defence and security sector transformation.

Information & Security