CENTRE FOR SECURITY COOPERATION

INCREASING NATIONAL CYBER RESILIENCY: POLITICAL AND LEGAL INSTRUMENTS

Date and Venue
07 – 09 May 2013; RACVIAC - Centre for Security Cooperation, Stari hrast 53, Rakitje, 10437 Bestovje, Croatia

Background
It is very difficult to make a clear-cut division between cyber defence and cyber security. While cyber defence refers to the field of national security and cyber security refers to the field of national information infrastructure, the fact is that these two fields overlap in many areas and in many ways. Thus, it is much harder for national cyber defence system to successfully fulfil its mission if it is not backed by a wider system of cyber security. Things get even more complicated by the fact that not all elements of national cyber security system are contained within national cyberspace.

In this situation, a fundamental component of any national, strategy-led cyber defence system is the adoption and implementation of legislation against the activities aimed at undermining the integrity of critical national infrastructure or threatening national security in other ways. This system should be supported by a wider cyber security system based on legislation and strategies against the misuse of information and communication technology for criminal and other malicious purposes. The two systems have to achieve unity of efforts and be mutually supportive to the point at which, at least from the outside, they look as a single system. This requires not only harmonized legislation and strategic documents, but also constant cooperation and coordination among different agencies.

As cyber threats can come from anywhere in the world and travel around the globe almost instantly, the challenges posed by these threats are immanently international. That is why it is not only important to develop national legislation, but also to harmonize it on the international level. Harmonization facilitates regional and international cooperation in dealing with cyber threats, which would, ideally, deprive cyber threats of safe havens.

Legislation on cyber defence and cyber security has to reconcile two opposing requirements. On the one hand, it has to prohibit certain kinds of conduct in the cyber world and impose sanctions for unlawful behaviour, which, inevitably, means establishing some sort of monitoring and control mechanisms. On the other hand, it must not jeopardize freedom as a necessary prerequisite for development. Developing such well-balanced legislation is a serious challenge, especially for the countries without a wealth of experience. This is what makes cooperation and knowledge sharing with other countries and organizations, more advanced in the field, a step in the right direction.

Purpose & Objectives
The purpose of the Workshop is to enable participants from and outside of the SEE region to exchange experience and thus facilitate international and inter-institutional cooperation. The Workshop should also expose participants from the SEE region to the relevant experience of experts coming from international organizations and countries outside the region.

The objectives are:
• To help participants to better understand the national and international implications of cyber threats, as well as legal and political aspects of cyber security and defence;
• To facilitate international cooperation aimed at harmonization of cyber security-related legal frameworks;
• To enable Workshop participants to exchange knowledge, experience and know-how, as well as to facilitate networking among them.

Participants
There should be up to 50 participants. Three participants should be invited from each of the RACVIAC Member countries. Representatives of other MAG countries and relevant international organizations (UNICRI, OSCE, EDA, ENISA, CCDCOE, ITU, etc.) are also to be invited. The participants should include civilian or military officials dealing with cyber security / defence issues in parliaments, law enforcement agencies, MoDs, national CERTs and/or National Security Authorities.

Methodology
The Workshop will last for two working days and will be conducted as a combination of presentations and speeches, followed by Q&A sessions. The official working language of the workshop is English.

Point of Contact
MAJOR Sasa KONJEVIC
Planning and Liaison Officer / SEE
E-mail: skonjevic@racviac.org, ☎ +385 1 3330 862, ☎ +385 1 333 0839

This workshop is supported by: The NATO Science for Peace and Security Programme