PC.DEL/459/11
20 May 2011

ENGLISH only

Presentation for the OSCE Conference on the Comprehensive Approach to Cyber Security: Exploring the future OSCE Role (Vienna, May 9-10, 2011) Working session II

CYBER THREATS - EMERGING THREATS TO THE NATIONAL, REGIONAL AND INTERNATIONAL SECURITY ARCHITECTURE THE ROLE OF THE OSCE

Mr. Gabriel Statescu,
Director of the Knowledge Management Center,
Romanian Intelligence Service, Romania

The cyberspace has generated an unprecedented phenomenon of spreading ideas that influence large communities, changing global strategies, aiming at drawing new frontiers.

Terrorist groups can perpetrate large-scale and huge impact attacks motivated by the desire to obtain the maximum of publicity for their cause. The cyberspace brings increasing connectivity which allows the radical groups to act globally in order to recruit and train new members, propagate extremist ideologies, manage their illegal financing networks, manipulate public opinion or coordinate terrorist attacks.

A successful cyber attack against the financial operators of a state could have serious effects on the national currency and the national economy.

Intelligence assessments show that more and more states develop and improve technical capabilities aimed at targeting and penetrating the critical infrastructure of other states, thus being able to affect security and national defense.

On the other hand, criminal groups continue to develop the level of complexity and sophistication of technical capabilities but also of targets they started to envisage. Today, trans-border organized crime acts through a real cyber-criminal economy, where the victims are represented by an increasing spectrum of entities, using electronic transactions, from individual to financial-banking institutions.

In the above-mentioned cases, the cyberspace of a state is a proper environment for disseminating and intensifying threats (asymmetric and trans-border, and from now on, conventional) to the national security.

Regarding cyber threats, the cyber space of a state is the target for cyber attacks and often the aggression against the national informatics systems is in itself a purpose.

In this case, the cyber attacks primarily target the ICT systems (information and communication technology) that are Critical Infrastructures per se but also the ICT systems, essential for the good functioning of other Critical Infrastructures of a state (the air, railway, road infrastructure, energy, gas, oil and water supply systems, the medical services, the banking system etc.)

Due to its features, the cyber space is already considered a new challenge area alongside with the land, maritime, air and space areas.

States can not afford to discover post-factum a successful attack or cyber intrusion or to accept disastrous losses and be confined to reduce the impact of the consequences.

States should establish an institutional framework that could offer better understanding of cyber threats, design solutions for preventing such attacks and develop detailed action plans to counteract such aggressions.

It is of outstanding importance that all the actions be taken with due respect of fundamental rights and freedoms, including the right to free flow of information and the freedom of expression.

It is also clear that the knowledge and expertise of the private and academic sector are of critical importance.

In this context, as CyberInt national authority, our Service established a national capacity for active defense against cyber attacks, with the mission to provide the necessary intelligence for preventing or ending the aggression and eventually reducing the consequences of such threats.

The trans-border and asymmetric cyber threats character multiplies in an interdependent and globalized environment, reveals the importance of increasing inter-State co-operation, by involving regional and international organizations.

The OSCE could contribute to achieving the objective of developing a set of principles regulating the cyber space, including through the exchange of best practices among participating States. A compilation of good practices and lessons learned in the OSCE participating States, compilation done in the framework of the OSCE, would be highly welcome.

It is important to use the tremendous OSCE expertise in the field of confidence building measures and apply it to the cyber security field.

We also support the possibility to have OSCE workshops on practical co-operation issues regarding responses to hypothetical cyber attacks. Organizing capacity building events would be another very important tool.

From this perspective, we consider that the OSCE can play an important role in the global information technology era and it could become an expertise pole in this field.

Thank you very much.