Conference on
“Unprecedented Wave of Security Vulnerability: Cyber Security Threats in SEE”
13-15 December 2010, Zagreb, Croatia

Activity Background

With the aim of raising awareness and enhancing regional co-operation in the field of cyber security threats and vulnerabilities and discussing the defensive capabilities of SEE countries, RACVIAC – Centre for Security Cooperation conducted the Conference entitled “Unprecedented Wave of Security Vulnerability: Cyber Security Threats in SEE”.

The dangers of cyber threats continue to evolve at a pervasive rate. The risks are further compounded as increasingly connected societies transcend geographical and physical borders, and stakeholders are able to communicate in real time. By utilizing the same networks and links that bind us at the global level, the perpetrators of cyber attacks are able to strike from virtually anywhere in the world.

Governments cannot fight these cyber threats single-handedly through domestic measures. Nor should they be left to struggle with this danger on their own any longer, as the expertise and the know-how for combating these cyber threats are dispersed across the globe.

There is an absolute need to converge and share the information and resources that can improve our cyber security. Without expert collaboration and knowledge sharing, individual countries lessen their ability to adequately respond to cyber threats. This may cause potential exposure of their neighbors to greater risks online, as perpetrators continuously learn to exploit national, regional and global information and communication technology weaknesses. Thus, RACVIAC is trying to serve as a forum for raising both the awareness of and the protection from cyber security threats in the SEE region.

The Conference objectives were:

- to encourage cooperative and effective efforts in combating diverse cyber threats and cyber terrorism;
- to build trust and confidence that will allow for continued information-sharing in SEE;
- to exchange best practices and experiences in fostering a culture of cyber security in SEE;
- to present law enforcement units’ efforts in investigations on national and international levels.
Activity Venue, Duration and Participation

The Conference took place in Zagreb (Croatia) between 13 – 15 December 2010 in RACVIAC’s facilities. It comprised four sessions which were designed to include both presentations and discussions, with sufficient time to properly address the participants’ questions and to exchange the views.

The participants and lecturers were representatives from nine countries and eleven organizations, namely: Austria (1), Albania (3), Bosnia and Herzegovina (2), Croatia (4), Italy (1), Serbia (4), the former Yugoslav Republic of Macedonia (5), Montenegro (3), Turkey (1), United States (1), UNICRI (2), OSCE (1), RCC (1), Cybercrime Research Institute Germany (1), Host Exploit, United Kingdom (1), NCIS, Cooperative Cyber Defence Centre of Excellence, Estonia (1), International Cyber Investigation Training Academy, Bulgaria (1), Information Systems Security Bureau Croatia (1), and RACVIAC (6).

Conference Opening

Opening Session, HE Amb. Nikola Todorcevski, Director of RACVIAC

Opening the Conference, Director of RACVIAC Ambassador Nikola Todorcevski emphasized the importance of taking new topics such as cybercrime, cyber war, information warfare, etc. seriously both at the regional and the global level. Having thanked the Speakers and Delegates for their attendance, he underlined that it was vital for RACVIAC, being a centre for security cooperation and having in mind that cyber security must be based on international cooperation, to further develop conferences of this type.

Keynote Speech

After welcome addresses, the Conference participants had the honor to hear the keynote speech delivered by Mr. Nemanja Malisevic, representative of the Organization for Security and Co-operation in Europe (OSCE), Action against Terrorism Unit (ATU). Mr. Malisevic first outlined the evolving nature of threats emanating from cyberspace. Then, emphasizing the need to enhance cyber security, he offered several concrete policy options to be considered by decision makers when developing and implementing a comprehensive approach to cyber security issues.

In the course of his excellent presentation, he offered a comprehensive, yet succinct picture of the current threats and he provided the participants with some interesting figures and facts to be considered:

1 Turkey recognizes the Republic of Macedonia with its constitutional name
• Income derived from cybercrime amounts to about €2 billion;
• There are 1 billion wireless email users in the world;
• There are 80 million mobile internet users / 60 million active mobile internet users in the world;
• By 2013 the number of mobile devices will have surpassed 1 billion;
• By 2015 most users will not be using PC but mobile assets.

Session I: Towards an Integrated Approach for Cyber Security and the Protection of Critical Information Infrastructures

Mr. Raoul Chiesa and Mr. Ioan Landry, United Nations Interregional Crime and Justice Research Institute (UNICRI), examined some of the most pertinent cyber attack vectors and potential responses to them. They showcased the work done within the framework of UNICRI and underpinned the importance of promoting a culture of cyber security in today’s world. In this respect they explained some fundamental concepts and terminology.

Mr. Stefano Mele, ICT Law, Intelligence & Security (Italy), delivered the second presentation in this session. He outlined the future of cyber investigations, focusing on information warfare and its legal aspects.

The topic of ‘Cyber Attacks on Global Information Networks – Countering Cyber Terrorism’ was presented by Mr. Mato Brautovic, University of Dubrovnik, Department of Mass Communications. In his presentation, Mr. Brautovic focused on cyber warfare and cyber terrorism, giving some examples of ‘how things really work’.

Session II: Legal Frameworks, Law enforcement Issues and International Cooperation

First to deliver his address in the second session was Dr. Marco Gercke, Director of Cologne Cybercrime Research Institute, Germany. In his valuable contribution to the conference, he examined the legal frameworks which could be used to combat threats emanating from cyberspace. He also drew attention to some best practices as well as to the thematic areas where more work should be done. Furthermore, he cautioned against overusing the term cyber “war”, as the word carried significant legal ramifications, suggesting that in the majority of cases the term cyber “conflict” would be more appropriate. Besides covering a wide range of topics, Mr. Gercke successfully
interlinked the existent laws with the actual e-crimes.

Mr. Virgil Ivan-Cucu, Senior Expert, Head of Justice and Home Affairs Unit, Regional Cooperation Council (RCC), highlighted the need for extensive law-enforcement and judicial co-operation in the region and beyond, drawing on past experiences in this issue. He emphasized that such co-operation was crucial for a successful investigation of cyber crimes.

Ms. Albena Spasova, President of the Management Board of the International Cyber Investigation Training Academy (Bulgaria), presented the lessons learned and experiences gained in combating international cybercrime and cyber terrorism. In particular, she demonstrated how some of the most frequently used types of attack worked (e.g. botnet-driven DDoS attacks) and presented some options of countering them.

**Session III: Future Perspectives on Cyber Threats**

Mr. Kenneth Geers, Scientist / U.S. NCIS Representative (Europe & Africa Field Office) and Cooperative Cyber Defence Centre of Excellence, Tallinn (Estonia) provided the participants with the lessons learned from responses to CBRN threats. He also explained how and to what degree concepts such as “deterrence” could be applied to contemporary threats emanating from cyberspace.

This presentation instigated a very lively discussion about 2007 cyber attacks on Estonia.

Mr. Jart Armin, Host Exploit (United Kingdom), dealt with the key issues with regard to the recent Stuxnet attacks. Furthermore, he examined technical measures that could be put in place in order to make the tracing of cyber attacks possible. He illustrated the current possibilities and limitations, arguing that much closer co-operation among the public and the private sectors was needed to effectively and sustainably combat, prevent and mitigate cyber attacks.

Mr. Vladimir Urosevic, Chief of Electronic Crime Sector (MoI, Serbia), called for more extensive co-operation among the countries in the region in combating threats emanating from cyberspace, stating that countries could share much more information on a much more frequent basis. In addition, he emphasized that regional and international organizations, when organizing such events in the region, should first address the needs of the countries in question by giving them a chance to specify their particular areas of need and by tailoring the response accordingly.

Mr. Goran Culjak, Information Systems Security Bureau, illustrated the work of the Croatian CERT, highlighting that broader
international co-operation and co-operation between the private and the public sector was essential.

**Session IV: Best Practices and Experiences in Combating Diverse Cyber Threats; Presentations of National Representatives**

The session dedicated to regional presentations gave the countries’ representatives a possibility to present their own experiences in combating diverse cyber threats.

In this session, the conference participants were addressed by:
- Col Josef Schröfl, Senior Military Advisor on Comprehensive Approach and Terrorism at the Military Strategy Division, Austrian MoD;
- Ms. Jelena Kecman, Investigator Cyber crime department, MoI BA;
- Mr. Ivan Mijatovic, Chief Inspector and Mr. Sinisa Banak, Inspector, MoI HR;
- Mr. Marjan Stoilkovski, Head of the Cybercrime Unit, MoI MK;
- Mr. Novica Gecaj, Senior Inspector, Police Directorate, ME;
- PhD Vladimir Urosevic, Chief of Electronic Crime Sector, MoI RS.

In the course of this session, the participants were introduced to measures bolstering cyber security, as part of the country’s overall measures to prepare against asymmetric threats. It was also emphasized that states should never disregard tools and technologies that had been effectively used prior to the IT revolution, as they provided an easily maintained additional line of defense, effective even against contemporary cyber threats.

The final session of the Conference was brought to an end by the general conclusion that the countries should spare no effort in providing specialized ICT personnel training.

This worthwhile conference proved to be a great opportunity for officials in the region to share experience and know-how and to build crucial partnerships in fighting cybercrime. The discussions generated by the distinguished lecturers, from the first to the last one, were deeply interesting and focused on vital issues. All participants assessed the conference as very successful and useful. The conference was recognized as an important initiative that should be continued in years to come as RACVIAC’s permanent activity. Organizing conferences such as this provides unparalleled opportunity for global experts to come together and exchange valuable insight and experience on relevant topics.

The participants acknowledged that the information provided and issues discussed were of great benefit to them and their countries and they expressed their willingness to be part of any future RACVIAC’s activity on this subject.

*Compiled by: Major Dobrislav Bilos, Subject Matter Expert, the Conference Coordinator, RACVIAC – CENTRE FOR SECURITY COOPERATION.*