The workshop „Building a Cyber Resilient Society in SEE” was held on 13th - 14th May 2015 in Ohrid, the Former Yugoslav Republic of Macedonia³. The event was jointly organized by RACVIAC - Centre for Security Cooperation and the Military Academy “General Mihailo Apostolski” with the support of the Federal Republic of Germany.

The aim of the workshop on “Building a Cyber Resilient Society in South-Eastern Europe” was to represent a platform for sharing of experiences at the regional level and to clarify the perception of and facilitate a common understanding of the concept of a “Cyber Resilient Society” in the region, beginning from the areas that are really vulnerable and have real potential for possible venues of action.

The event attempted to identify clear cyber security priorities and responsibilities and determine who, when, where and how is responsible for implementing effective cyber security activities in SEE countries.

³ Turkey recognizes the Republic of Macedonia with its constitutional name.
Besides the representatives of the RACVIAC member countries and the Military Academy “General Mihailo Apostolski”-Skopje, the workshop was supported by the OSCE representative and cyber security experts from respective academic institutions from the region who participated in the workshop too.

The morning session on 13th May 2015 was opened by Dr Metodi Hadji-Janev, Col, Vice Dean for education and Research, Head of the Social Science Department at the Military Academy “General Mihailo Apostolski”, who introduced the keynote speakers.

In their opening remarks the Deputy minister of Ministry of Foreign Affairs of the Former Yugoslav Republic of Macedonia*, Ms Dragana Kiprijanovska, RACVIAC Director Ambassador Branimir Mandić and the Dean of the Military Academy “General Mihailo Apostolski”-Skopje, Dr Orce Popovski, Col, welcomed all distinguished lecturers and experts from the countries of the South East European region who supported the event by taking part in it as well.

Deputy minister Ms Kiprijanovska said: “It is our common responsibility to strengthen the legislative framework concerning cyber security and establish institutional mechanisms to permit effective responses and coordinated action on national, regional and international levels. In order to protect cyber space, the coordination of national security strategies, cooperation between the public and the private sector and engagement of all actors must become a high priority.”

Ms Kiprijanovska also emphasized the importance of learning how to keep safe our virtual information and how to keep ourselves protected against cybercrime and cyber espionage.

In addition, she called for regional and international cooperation in this regard and highlighted the need for common tools and strategies to combat this very serious issue. At the end, Ms Kiprijanovska emphasized the importance of this meeting and congratulated the organizers for launching this important topic which will be a great challenge in the future.

Ambassador Mandić expressed gratitude to the Ministry of Defence and Ministry of Foreign Affairs for hosting the event. He also expressed his thanks to the Military Academy “General Mihailo Apostolski”-Skopje which was the co-organizer of the conference and the Federal Republic of Germany for supporting RACVIAC in organizing activities related to cyber security.

Referring to RACVIAC mission to foster dialogue and cooperation on security matters in South-Eastern Europe he stated that threats coming from cyber space can easily provoke political and economic instability and, consequently, prevent the proper functioning of the state.

Having in mind the goal of enhancing cooperation on security in South East Europe (SEE) within the regional and broader international framework and ways of contributing to the advancement of the countries in the region on their path towards the EU and Euro-Atlantic integrations, RACVIAC will continue to serve as a platform for policy makers, experts and analysts to identify and discuss solutions and exchange of best practices on issues related to cyber security.

Events such as this one are a good opportunity to promote a transparent dialogue about the various aspects of regional cyber security, based on a common strategic vision, the needs and potentials of the region.
The first day of the Workshop covered the following topics:

- “Contemporary trends and challenges in cyber security – legal, operational and technical aspects” – speaker: Mr Antun Matija Filipovic
- “Building a cyber-resilient society by forging a partnership in SEE: Important task for future SEE strategists” – speaker: Dr Metodi Hadji-Janev, Col
- “The role of the human factor in cyber threats resilience” – speaker Mr Predrag Pale;
- “The importance of national due diligence in efforts to enhance cyber/ICT security in the context of regional and international security – OSCE efforts related to enhancing confidence between states in the cyber arena” – speaker: Mr. Ben Hiller
- “Technical aspects of resilience in cyberspace with an emphasis on critical information infrastructure” – speaker: Dr Mitko Bogdanoski, LtC.

Mr Antun Matija Filipovic, representing the College of Applied Science in Safety, Zagreb gave a presentation on the most important trends and challenges when it comes to cyber security. He also used very good examples from the present to illustrate how cyber-attacks can be dangerous and how much damage they can provoke. Mr Filipovic said that today there are four types of cyber-attacks, such as: interruption, interception, modification and fabrication. The perfect targets for those attacks are hardware, software, different data and communications.

In respect of those different types of threats he suggested that today there are various types of methods which serve as protection from these attacks. Among those it is important to mention the two most important protective methods being used today: the proactive method and the reactive method. The first one is about taking actions before the attack was even executed, and the second one is about taking action when the attack has already been launched.

The second part of his presentation focused on the legal aspect of cyber-attacks. He stated that cybercrimes can be divided into five categories: intrusive offences, content related offences, copyright and trademark related offences, computer related offences and combination offences.

The last part of his presentation was aimed at explaining some operational and technical aspects of cybercrimes, which was followed by his conclusions and interesting discussion between the participants.

Dr Metodi Hadji-Janev, Col, Associated Professor of Law, Vice Dean for Education and Research at the Military Academy “General Mihailo Apostolski” and Associated Member of the University “Goce Delcev” Stip focused his presentation on explaining the need for building a cyber-resilient society which can only be created if we have good cooperation between the countries of the region. Mr Metodi also said that the process of globalization has brought about many advances and improvements in all spheres of life but also made our society more vulnerable. So, in order to fully enjoy those improvements and be safe, we need a good system of protection from potential threats.

He stated that there is an essential need to invest in cyber security. The first step in that process is to realize that the project is intended to raise the awareness among the countries and show them how important that is.

Col Hadji-Janev concluded his presentation by stating that “Global Cyber Security Trends urge SEE societies to seriously
consider cyber security threats. As we have seen, cybersecurity affects societies from different angles and in different ways. Therefore, building cyber resilient societies must be a strategic imperative for the SEE countries’ strategists. Cooperation and partnership in achieving the strategic end with cyber resilient societies in SEE is a must for all SEE countries. This cooperation should be built in several sectors across the governance sector. They need to consider sharing of best practices and experience and focus on raising awareness, education and building capacities among the SEE societies”.

Mr Predrag Pale, Faculty of Electrical Engineering and Computing, University of Zagreb. In his presentation Mr Pale talked about the human factor in different types of cyber threats and methods of protection. It is important to demonstrate how anyone using any type of new technology can be a perfect target for a cyber-attack. So, in order to do that, we need to raise the awareness among people, teach them how to protect themselves, create a culture based on that, impose certain discipline, get the information and the right infrastructure to be ready to protect ourselves at every moment.

Mr Ben Hiller, Cyber Security Officer, who is working within the Transnational Threats Department (TNTD) at the OSCE, reminded the participants during his presentation that all 57 OSCE States adopted the first set of Confidence Building Measures (CBMs) to reduce the risk of conflict stemming from the use of Information Communication Technologies (ICTs). Two UN Groups of Governmental Experts in 2010 and 2013 highlighted the unique role that CBMs can play to enhance transparency, co-operation and stability between States in cyberspace.

The CBMs are practical measures designed to reduce the causes of mistrust, fear, misunderstanding and miscalculations. The CBMs focus on three principal areas:
- CBMs which allow States to “read” another State’s posturing in cyberspace through activities such as the sharing of national views on cyber threats or military doctrines
- CBMs which offer an opportunity for timely communication between States including to defuse potential tensions by establishing channels for rising concerns
- CBMs which promote the exchange of information pertaining to national preparedness and due diligence to enhance national cyber/ICT security.

Active engagement by all OSCE participating States in the CBMs process is essential. This process needs to be supported by the relevant organizations on the regional, sub-regional and national level.

Dr Mitko Bogdanoski, LtC, Military Academy “General Mihailo Apostolski”, Associated Member of the University “Goce Delcev”-Stip. Mr Bogdanoski began his presentation by introducing the audience with the newest advancement in technology and explaining how dependent we are on them. The most important consequence of those advancements is the system and networks’ vulnerability due to destructive and disturbing attacks which are being launched by hackers all the time. He also explained that the perfect targets for hackers are the governments, the industry and the banks. He stated how today the most vulnerable are the financial and the energy sectors which can suffer enormous damage if they are being targeted by criminals.
Mr Bogdanoski also pointed out how the most alarming fact about cyber-attacks is that terrorists worldwide have started using modern technologies in order to fulfill their goals. The final part of his presentation was dedicated to providing solutions and countermeasures in order to fight the issue of cyber-crime and cyber terrorism.

The second day of the workshop covered the following topics:
- “State responsibility for cyber operations and capacity of current legal frameworks to effectively regulate malicious interstate cyber activities” – speaker: Mr Andraz Kastelic
- “Protecting civilians from activities related to cyber conflicts while respecting the International Human Rights Law principles” – speaker: Ms Ljubica Pendaroska
- “Ensuring business and economic continuity in time of insecure cyberspace through building resilience in the economic sector” – speaker: Mr Krenar Fortuzi
- “EU anti-botnet platform – advanced cyber defense center project” – speaker: Mr Darko Perhoc
- “Group work: small project development - Project methodology, objectives, and expectations” – presented by RACVIAC and the Military Academy “General Mihailo Apostolski” - Skopje.

Mr Andraz Kastelic, Sheffield University of Law. Mr Kastelic’ main focus was on explaining the basic cyber concepts in the legal context. He defined very well the difference between a cyber operation and a cyber-attack. He also tried to put cybercrimes in the context of international law and he provided a couple of examples in which cybercrime has been characterized as a serious breach of international law. In addition, he talked about the development of international law in regard to the cyber era. He concluded his presentation by saying that “cyberspace made the attribution of an unlawful cyber operation orchestration close to impossible. In particular, the modern spoofing techniques have rendered the standards of attribution and proof within the context of traditional international law of State responsibility unattainable. However, as much as it is deemed unlawful to orchestrate a cyber-operation, neglecting or ignoring such an act may rightfully be labelled as internationally wrongful. States are not only responsible for the orchestration of unlawful cyber operations but also for failing to prevent them.”

Ms Ljubica Pendaroska, Teaching Assistant at the Faculty of Law at the European University, MK (Corporate security and Crisis management Initiative – C3I). Mr Pendaroska’s presentation was based on International Human Rights Law principles in regard to the cyber era and cybercrime. Cyberspace presents new opportunities and new challenges for states and the international community as a whole, while creating policies in different areas of social life, including human rights and freedoms, national defense, security and communication. She mentioned that it is an undeniable fact that cyberspace is not a “law-free” zone where anyone can conduct hostile activities without rules or restraint. Today the international community has been working very hard in order to create appropriate laws and regulations to protect everyone against unlawful cyber operations. But still there remain many other difficult and important questions about the application of international law of human rights to activities in cyberspace – for example, about the implications of
Mr Darko Perhoč, Head of the Croatian National CERT, made a presentation on The Advanced Cyber Defence Centre (ACDC) and the goals of the project. ACDC delivers solutions and creates a pool of knowledge to help organizations across Europe fight botnets, and will provide tools and sensors to detect botnet related cyber threats and mitigate cyberattacks on networks, web sites, end user computers and mobile devices. Mr Perhoč explained in detail the ACDC architecture platform and practical use as well as ACDC and National CERT integration. More information regarding the ACDC can be obtained on http://www.botfree.eu/.

Taking into consideration that each country faces its own specific challenges and that they are more oriented towards national approaches rather than looking at the regional dimension, the spirit of working together, supporting and complementing each other should be more pronounced. In this spirit, RACVIAC - Centre for Security Cooperation and the Military Academy „General Mihailo-Apostolski“- Skopje as partners presented to the national representatives the research project and invited experts to participate in it. The overall idea of research is to provide critical thinking and an analytical approach while addressing specific topics indicated in the document which was presented and delivered to all participants.

Conclusions and Recommendations

This event provided the opportunity for dialogue between the participants about the current situation in their respective countries as well as various aspects of regional cyber security. They all agreed that National cybersecurity strategies and action plans are good tools and platforms in terms of responding to potential cyber threats and for development of cyber resilient societies.

Also, all participants emphasized that cooperation is of paramount importance for the development of the protective mechanisms as well as the creation of a stable regulatory framework, in order to establish a resilient and diversified society. This includes closer cooperation among the key players in cyber security, involving experts and policy makers including the private sector as crucial elements for establishing a Cyber Resilient Society in SEE.

It was agreed that the outcomes of the research project will be presented for the next event which will be organized in November 2015, and that the results will used as a reference for further activities.

Compiled by IRC Pillar
RACVIAC

http://acdc-project.eu/