RACVIAC
SE EUROPE

CENTRE FOR SECURITY COOPERATION

International and Regional Cooperation with focus on
Euro-Atlantic Integration Pillar

**"Cyber Security:
Training on WMD Cyber Crimes Investigations"
27-31 May 2019**
Rakitje, Croatia

*in cooperation with the Defense Threat Reduction Agency (DTRA) from the USA, and
with the support of the Federal Republic of Germany*

Group photo

Introduction

Based on the conclusions of a series of events organized within the C-WMD Network where cyber issues were identified as a common modern threat to our security, RACVIAC - Centre for Security Cooperation in cooperation with the International Counterproliferation Program, Defense Threat Reduction Agency (DTRA) from the USA (http://www.dtra.mil/), organized the Cyber Security Course related to WMD Cyber Crimes Investigations.

The aim of the WMD Cyber Crimes Investigations Course was to instruct nontechnical investigators in the fundamental skills needed to exploit digital technology to combat the

proliferation of weapons of mass destruction (WMD) and misuse of dual-use materials and technologies. Furthermore, the goal was to improve the ties between the representatives of the relevant institutions from the SEE region, and to exchange information, transfer knowledge, views and ideas.

Moreover, the aim was to expose the Course participants to the experiences of experts from various U.S. government agencies who have the legal authority and the technical knowledge concerning cyber threats.

The Course participants were the representatives of the relevant ministries and agencies from: Albania (3), Bosnia and Herzegovina (2), Croatia (4), North Macedonia (2), Serbia (3), Turkey (1), Kosovo* (3), Moldova (1), and RACVIAC Staff (4).

Execution

The Course lasted 5 days and consisted of theoretical and practical computer exercises.

Classroom

Opening the Course MG (ret.) Jeronim Bazo, Director of RACVIAC - Centre for Security Cooperation, said: *„We all know that Cyber space is commonly recognized as the battlefield of the future, and that it perhaps already is just that. Therefore, it is of utmost importance to develop the capabilities in our region, to be well prepared to protect our*

countries' critical infrastructure, to detect and to take the necessary measures against illegal, criminal cyber activity, against terrorism or other forms of destabilizing attacks."

Course Opening

Ms Victoria Taylor, Deputy Chief of Mission of the United States Embassy in Zagreb, welcomed the participants by saying: *"Today's security challenges are global. Whether it's terrorism, trafficking in drugs, people and weapons, or cyber security, these security issues are cross border and require a global approach. Regional courses such as this one are crucial to effectively address the security challenges",* she added, continuing: *"Security and stability in South East Europe are critical to European security and are a United States' priority. The United States continues to believe that anchoring South East Europe in Euro-Atlantic institutions is the best path for regional stability and development,"* Ms Taylor underlined.

Greeting the participants on behalf of the United States Defence Threat Reduction Agency Lt Col Matthew Summey indicated how pleased he was to see the return of this Course to RACVIAC which facilitates critical regional interaction and coordination in tackling threats that "do not respect borders." He said: *"Threats such as cybercrime and criminal financial transactions do not stop at a border or*

checkpoint, or port of entry. For crimes like this regional, inter-governmental cooperation, is paramount."

During the Course the participants learned about the current cyber environment and the technologies presently employed by cyber experts to further criminal investigations. In doing so, the participants were introduced to and gained limited competency in cutting-edge, open-source software and tools that help investigators analyze the data from devices, digital media, or social networks. The participants were also introduced to the technology of the future, including the use of the Darknet, botnets/malware, and cryptocurrencies.

During the Course the participants had an opportunity to analyse the methods and tools for preventing, deterring, detecting, and countering the threat of WMD proliferation by securely utilizing digital technology in support of WMD-related investigations.

They also learned how to use open-source tools and technologies that can be used to support ongoing investigations across a range of criminal activities. Throughout the practical part of the Course they learned how to gather intelligence using the web-based open sources tools, to collect and analyse seized digital evidence, and how cyber investigative techniques can be integrated with the "traditional" investigative techniques through case studies and exercises.

In addition to this the participants learned about digital forensics in order for Investigators to locate potential evidence.

Conclusion

The Course proved to be worthwhile, as it provided an opportunity to the participants to exchange knowledge, discuss topics and generate ideas about cyber security with lecturers and individually.

At the end of the Course the participants provided responses to the Course Questionnaire and all of them assessed the activity in a positive manner. They suggested that it would be useful to repeat the activity next year too.

All participants considered the Course overall, and practical exercises specifically, valuable for their future work.

All throughout the Questionnaire the participants also assessed the lecturers as very well prepared and ready to share their experience and knowledge with the participants.

The Course was very well organized due to excellent cooperation and relations between RACVIAC and the Defense Threat Reduction Agency (DTRA).

RACVIAC - Centre for Security Cooperation
at
www.racviac.org