CENTRE FOR SECURITY COOPERATION

"Cyber Security: Training on WMD Cyber Crimes Investigations"
23-27 April 2018
Rakitje, Croatia

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 the following countries: Albania (3), Bosnia and Herzegovina (2), Croatia (4), Montenegro (1), the former Yugoslav Republic of Macedonia* (2), Greece (1), Romania (1), Serbia (2), Turkey (1), Kosovo** (3), and RACVIAC Staff (1).

Execution

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

Opening the Course Ambassador Haydar Berk, Director of RACVIAC - Centre for Security Cooperation said 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. The idea is to create a long-term project with the aim to establish a self-sustainable regional team of instructors who will be able to deliver the trainings in the countries of the SEE region in the future", added Ambassador Berk.
Greeting the participants on behalf of the United States Defence Threat Reduction Agency Mr Russell Adam Dallas underlined that the cyber domain is very demanding since it changes all the time and touches everything in our lives, not only the investigations but the everyday aspect of our lives too.

Conclusion

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.

Classroom photo

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.

* Turkey recognizes the Republic of Macedonia with its constitutional name

** This Designation is without prejudice to positions on status and is in line with UNSCR 1244 and the ICJ Opinion on the Kosovo Declaration of Independence

The participants 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 the participants 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.

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.

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 a success organized due to excellent cooperation and relations between RACVIAC and the Defense Threat Reduction Agency (DTRA).

RACVIAC - Centre for Security Cooperation