Advanced Training Course
“Building a Cyber Resilient Society in SEE”
(SPS.EAP.ATC.G5194)

17 - 21 October 2016
RACVIAC - Centre for Security Cooperation
Zagreb, Republic of Croatia

Activity Background
The Advanced Training Course “Building a Cyber Resilient Society in SEE” was conducted in the Republic of Croatia in RACVIAC - Centre for Security Cooperation (hereinafter: RACVIAC), on 17-21 October 2016.

The Course was supported by the NATO Science for Peace and Security Programme (reference: SPS.EAP.ATC.G5194) and partially by the Federal Republic of Germany, with the aim to provide military and civilian personnel with high-level knowledge, skills and experience required for describing and evaluating the risks and threats of cyber space, improving cyber defence measures and providing advice to decision makers.
Furthermore, the purpose of this event was to bring together the representatives of the relevant institutions from the SEE region in order to facilitate the exchange of experience, and to promote and increase cooperation by using dialogue and exchange of information, transfer of knowledge, views and ideas, as well as to disseminate international standards. Moreover, the aim was to expose the Course participants to the experiences of experts from international organizations and countries of the region.

**Activity Venue and Participation**

The activity took place in RACVIAC, Rakitje (Zagreb), Republic of Croatia, on 17-21 October 2016.

The participants and lecturers included the representatives from the Republic of Albania, Republic of Austria, Bosnia and Herzegovina, Republic of Bulgaria, Republic of Croatia, the former Yugoslav Republic of Macedonia*, Federal Republic of Germany, Romania, Republic of Serbia, Republic of Slovenia, Republic of Turkey, EU Institutions, the NATO Cooperative Cyber Defence Centre of Excellence, UNODC and RACVIAC staff.

**The Course Opening**

During the Opening session, Ambassador Haydar Berk and defence attaché of the Federal Republic of Germany, Lieutenant Colonel Januz Kaschta, welcomed distinguished speakers and all participants.

Ambassador Berk noted that the close regional and wider cooperation among the SEE countries, through dialogue and various forms of coordination, is a strong response to today’s challenges to international security and defence policy, leading to building of confidence and security among the countries.

During the Course participants heard a series of lectures and discussions related to various aspects of Cyber Security. For the purpose of this report we will offer some lecturers’ abstracts.

---

* Turkey recognizes the Republic of Macedonia with its constitutional name

Today, Cyber Space is treated as a virtual dimension of the society, consisting of the Internet and a number of connected communication and information systems of the public, academic and economic sectors, as well as citizens. The contemporary cyberspace is composed not only of this interconnected infrastructure, but also of the ever growing amounts of available information, and people communicating increasingly using a growing number of different services - some completely new and some traditional, but in a new, virtual form. In this presentation the problem of overwhelming terms based on the prefix “cyber-“ was shown. Such terms are being used more and more nowadays and are often being confused with the already established terminology used within the realm of traditional information security. The frequent interchangeable use of cyber terms such as “cyber security” and “cyber defence” aims for the establishment of a widely accepted cyber taxonomy that would include not only the name of a term, but also the meaning and interrelations with other terms. Policy development in the form of national cyber security strategies, as well as the frameworks developed to help different legal entities to operate in Cyber Space with a more consistent approach were compared with the traditional field of information security. The lack of a consistent educational approach in cyber security programmes was stressed and a related solution from the Croatian Strategy was shown in connection with the area of education and awareness. Selected examples from the Croatian security policy development, both from the National information security programme adopted in 2005 and from the National Cyber Security Strategy adopted in 2015, were shown as illustrations in the lecture, as well as the correlation between the Croatian National Cyber Security Strategy from 2015 and EU’s NIS Directive from 2016. Some other similar EU and NATO requirements of member states were shown, such as the new conclusion drawn at the NATO Warsaw Summit in July 2016 regarding the cyber domain that is now treated as a new military domain which has been added to the traditional domains of land, air and navy. All examples illustrate both the necessity of having more similarities in different national/international cyber security approaches used in nations and international organizations and the need to cooperate more efficiently on the national/international level.
The first presentation given by **dr. sc. Sabina Baraković** was related to the topic “Cloud Computing and Security Challenges”.

The emerging and developing technology of cloud computing may be defined as an availability of scalable and easily accessible virtualised resources allowing the various paradigms. Cloud computing thus helps to reduce the cost of ownership and management of virtualized resources, lowering the market entry threshold to new players and enabling the provisioning of new services. Nevertheless, it is not being massively adopted mainly due to tremendous security challenges. Therefore, Ms Baraković’s presentation aimed to provide a short overview of cloud computing basics from the beginner’s point of view, including the architecture as well as the service (Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS) and deployment models (private, community, public and hybrid). Also, the presentation addressed the cloud computing security challenges and benefits, given that as any other thing in life, it can be observed as a negative and challenging issue, but also as a positive and beneficial thing. Usually, the term cloud computing security is related to potential problems that arise in this field and is perceived as a concern. However, given that cloud computing security may also be considered as a potential and positive engine, in addition to the security issues, categorization (policy and organizational, technical and data), which is followed by identification of the most prominent ones today, the presentation was supplemented with the list of benefits that cloud computing security may offer. The current security situation in major cloud players was addressed as well.

The second presentation by **dr. sc. Sabina Baraković** covered the topic “Cyber Risks and Threats: State of the Art and Future Trends”.

Cyber security commonly refers to safeguards and actions that can be used to protect the cyber domain, both in the civilian and military fields, from those threats that are associated with or that may harm its interdependent networks and information infrastructure. Cyber security strives to preserve the availability and integrity of the networks and infrastructure and the confidentiality of the information contained therein. In the last few decades, actors posing risks and threats in cyber

---

**¹ dr. sc. Sabina Baraković is employed as a Senior Adviser at the Ministry of Security of Bosnia and Herzegovina, in the Sector for Informatics and Telecommunication Systems, and works as Assistant Professor at the University of Sarajevo and the American University in Bosnia and Herzegovina.**
space have shifted from tactical actors that affect operations or finances to terrorist groups and nation-states whose strategic intent is to cause long-term harm to human well-being or national security.

There is no doubt that cyber security of today, which is characterized by the intelligence-led approach, resurgence of phishing, visibility of things, attacks on payment cards, state-sponsored attacks, more Snowden leaks, security industry, as well as issues related to connected cars, machine learning, and wearables, is a top boardroom priority, but it needs to include a rethinking of the nature of security, and a shift from an approach that stresses protecting vulnerable assets to one based on the strengthening of assets. The cyber security world of the future will still be talking about malware, firewalls, network security, and social engineering. But it will also be talking about personal memories, new distinctions between what is public and private, the power of prediction, faith in public institutions, the provision of public good, psychological stability, the division of labor between humans and machines, coercive power (both visible and invisible), what it means for a human-machine system to have “intention,” and more. That is a very different and much broader agenda for cyber security than the one we may find today. At the intersection of human beings and digital machines we will find the repository of people’s greatest hopes and fears. That is why cyber security deserves the highest level of attention, research, imagination, and action.

The topic “Introduction to Digital Forensics” was presented by Ms. Savina Gruičić, mag. ing. inf. et comm. techn., from INsig2 do.o.o., Zagreb, Republic of Croatia.

The presentation began with an introduction to computer crime and digital evidence including its types and artifacts and digital forensics. The main branches of digital forensics were laid out. The benefits and challenges of digital forensics were listed and authorities responsible for digital forensics were addressed. The main 4 principles of computer-based electronic evidence were also listed and elaborated in detail, followed by 4 core aspects of operation within a forensic laboratory.

The methodology in digital forensics investigation with an explanation of each step in the process was given with a focus on procedures needed to preserve data and evidence. The term „chain of custody” was explained as well. Introduction to mobile forensics and correlating artifacts was presented with some of the existing challenges. Mobile device investigative techniques and standard operating procedures were briefly discussed too. The presentation ended with case studies regarding digital forensics.

Ms. Gruičić also presented the topic “Online Digital Evidence”.

This presentation included a short introduction to cybercrime and online digital evidence, followed by a definition of the term „digital evidence“ and challenges it imposes on forensic investigators.
The concept of online digital evidence was elaborated and its classification was laid out. The types of data that can be obtained online were listed. Each type of evidence was further discussed with examples when the mentioned artifacts are created. The focus was on artifacts created by usage of online social networks and their numerous features.

The meaning and importance of OSINT (Open Source Intelligence) and potential online digital evidence was elaborated as well. The means and methods of hiding identity on the Internet were briefly discussed. The structure and functioning of Cloud computing and differences between models were shortly explained, followed by advantages and disadvantages of such a concept. The importance and procedures of cloud forensics were also mentioned. The methods and instruments for searching and collecting online digital evidence were addressed, followed by principles of managing digital evidence. Some of the tools used for collection and analysis of online digital evidence were mentioned as well. There were a few examples and short case studies when online digital evidence was used in investigations or in a court.

Mr. Krešimir Hausknecht, M.Sci., from INsig2 d.o.o., Zagreb, Republic of Croatia gave a presentation titled “Information Obfuscation”.

Viewed generically, obfuscation is the practice of making something difficult to understand. When put into an information and data perspective, it’s a practice of making it hard to understand. A typical example is when the programming code is often obfuscated to protect intellectual property and prevent an attacker from reversely engineering a proprietary software program. This presentation was focused on Anti-forensics which in sense is how information obfuscation is affecting digital forensic investigation. Mr. Hausknecht described some of the many AF tools and methods, under the broad classifications of data hiding, artefact wiping, trail obfuscation, and attacks on the forensics tools themselves.

With any modern day investigation relying more and more on digital forensics, investigators are required to deal with anti-forensics methods on a daily basis. This session explored the challenges investigators and forensics practitioners are facing when conducting investigations. The methods used were separated into traditional and modern techniques, how they are being used, how they are affecting digital forensic investigation and what the possible mitigating techniques are. The main focus was on the new modern techniques that will not stop the investigation but rather prolong or make the process extremely time consuming.
Dr. Pedro Casas, Scientist at ICT Security at the AIT (Austrian Institute of Technology GmbH) presented the topic “Steps Towards Autonomous Cyber Security: a Case Study on Self Network Defense Using Machine Learning”.

Network traffic monitoring and cyber security have become very active research areas in the networking community in the recent years. Network security monitoring systems strongly rely on the guidance and knowledge provided by a human network operator, limiting their ability for self-management. Indeed, current monitoring techniques permit to detect and to identify the well-known attacks and traffic patterns which they are programmed to alert on, and/or to flag those anomalous traffic patterns that deviate from known normal-operation profiles.

In his presentation Mr. Casas discussed the limitations of current knowledge-based monitoring strategy for cyber security in the increasingly complex and ever-evolving Internet, particularly through a case study on Network Security. In a diametrically opposite but complementary perspective, he focused on the development of machine-learning-based approaches for cyber security and 0-day attacks detection, capable of functioning with a limited guidance or previous knowledge. Mr. Casas also introduced a novel traffic monitoring and analysis system based on robust unsupervised and semi-supervised machine-learning techniques. As a final point, he presented the feasibility and performance of such a limited-knowledge-based monitoring system through evaluations on both real and simulated traffic traces.

The topic “Personal Data Protection in Cyberspace: “Online” & “Offline” was presented by Mrs. Ljubica Pendaroska, President of Cyber Security, Corporate Security and Crisis Management Initiative - C3I, the former Yugoslav Republic of Macedonia*.

Having in mind the high importance of privacy and personal data in “cyberspace” in time of fast and enormous technological and communication developments, the speaker drew the participants closer to the essence of the concept of human rights. From such a perspective, the presentation was focused on the necessity and value of trust of personal data subjects regarding the processing of their data, both in “online” and “offline” operations. Furthermore, the author highlighted the most significant aspects of the protection of personal data that we all should be aware of while communicating the data. The speaker set out the intention to contribute to increased awareness and

* Turkey recognizes the Republic of Macedonia with its constitutional name
knowledge among the participants regarding their rights when processing their data in cyberspace, through most significant changes and innovations within the European Union and abroad. In this regard, the presentation mainly concentrated on the latest developments in Europe, elaborating the most influential novelties, how the reform of personal data protection legislation will affect the citizens’ rights, businesses and global communication worldwide.

“The Financial System as an Open Field for Cyber Crime” was the topic presented by Assis. Prof. Ivica Simonovski.

The development of information and communication technologies together with the Internet enabled and opened many opportunities for everyone. The connection of the information and communication technology devices via the Internet allows people and organizations worldwide to communicate, exchange information, to offer and make use of services, and to exercise their rights. On the other side, the use of the Internet and other ICTs makes consumers and societies vulnerable to threats such as cybercrime. The fact that any economic or serious crime may involve computer systems makes cybercrime a very broad and cross-cutting concept. It is increasingly targeted at generating economic proceeds involving different types of fraud and economic and organized crime. For these reasons, benefits and services offered by the financial sector are the main targets. Precisely the introduction and distribution of new products into the banking system is an open field in which the perpetrators of crimes found a solution to commit criminal activities and abuse. The most common risks posed in a financial institution which offers e-banking services to users of e-banking services are Internet fraud, harmful software, misuse of payment cards and DDoS attacks on information infrastructure. These actions represent the predicate offenses in which the offender may acquire illegal profit. In order to conceal the source of illegal properties (usually in the form of cash), the perpetrator puts the cash into the financial system and pursues a process of money laundering.

The increase in cyberattacks, especially in the financial information infrastructure as a vital segment of each nation, whereby damage is done directly to the customer, and then to the bank’s reputation, threatening the circulation of financial transactions and causing a handicap to the economy, has become a challenge for all countries so that they are giving priority to the national defense and security doctrines/strategies.

The Internet has given a new geographic dimension of crime by “removing” national borders of states. Therefore, the location of the crime scene and the identification of perpetrators or executors of cybercrime has become a real challenge. In response to increasing criminal money flows to the internet, there is a need for cooperation between the private and public sectors both at a national and international level in terms of prevention and repression.
Conclusions:

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. Twenty-five participants in total gave responses to the Course questionnaire and most of them assessed the activity in a positive manner. Twenty-three of them suggested that it would be useful to repeat the activity with same or similar content next year too.

Several participants suggested that it would be desirable to organize a practical training which would include topics such as digital forensics, penetration testing, and defense against hacker attacks, by using the tools at their disposal.

In terms of administrative and logistical implementation of the activity the majority of participants assessed this part of the Course as excellent, both as regards organization and execution.

Compiled by:
LiC Josip Mlakic, Activity Manager and PfP Co-Director for the Advanced Training Course “Building a Cyber Resilient Society in SEE”.

This activity is supported by: The NATO Science for Peace and Security Programme