Ohrid, 04.11.2019

Opening speech

I wish to extend to all of you a very warm welcome to Ohrid and to ***this NATO Science for Peace and Security Advance Training Course titled "Toward effective cyber defense in accordance with the rules of law".*** *The diverse and talented professionals and scholars who are here today demonstrates that we should not under estimate the power of the Information and communication technologies. Thank you to each and every one of you for being here today.*

The importance of the topic for this training cannot be sufficiently underscored. Cyber attacks can cause electrical blackouts, failure of military equipment and breaches of national security secrets. They can result in the theft of valuable, sensitive data like medical records. They can disrupt phone and computer networks or paralyze systems, making data unavailable. It is not an exaggeration to say that cyber threats may affect the functioning of life as we know it.

Accordingly, state and non-state actors must be involved in raising the awareness and help emphasize the advantages and disadvantages of cybersecurity and cyber defense.

As you all well know, cyberspace is a widespread, interconnected digital technology domain and it is experienced in communications (emails, cell phones, texting, many social cyber platforms), transportation (traffic control signals, car engine systems, airplane navigation), state administration (birth/death records, Social Security, licensing, tax records, e-government), finance (bank accounts, loans, electronic paychecks, e-commerce services in general), medicine (medical equipment, medical records e-medicine), and education (virtual classrooms, online report cards, research). Information and communication technologies (ICT) play an important role in every society. During the last decade, the digital revolution in the SEE countries' has given more people access to communication, education, news, social networking and various virtual community than ever before.

Cybersecurity and defenses should be important to everyone. ***Everyone may be a stakeholder, not only policy makers - as everyone is affected - so no one should be neglected. That is why this ATC will be focused on raising awareness about the general necessity of building cyber defense capacities, from the operational, technical and legal aspects.***

The training course has been organized in 4 blocks:

The first block will introduce the necessary cyber operations for effective cyber defense. The main objective during this block is to provide trainees with introductory information about the

strategic-political, technical and operational aspects of cyber defense operations. It will address the effects of exploiting cyberspace for geopolitical advancement and challenges to security through technology involved in cyber operations; including defensive and offensive tools and techniques and ending with challenges to technical attribution. The first block will establish a solid background and foundation for understanding, discussion and critical thinking among the trainees and prepare them for the legal blocks (II and III).

The II block will cover the peacetime legal aspects governing cyber defense. This block will take place in the third day and the fourth day. It will address questions such as states' rights and obligations in cyberspace, sovereignty, jurisdiction, human rights, the distinction between cyber-crime activities and state-sponsored commerce action in cyberspace, the prohibition of intervention and self-defense. During this block the trainees will understand which cyber activities can trigger an SEE states response and at what level (with which resources and structures) in cyber defense operations in accordance with the rules of law (i.e., when SEE states: can hack back; when can a country conduct surveillance activities; how can it respond to cyber espionage that occurs in the private sector and / or government facilities; when and under which conditions can SEE states engage in self-defense).

The III block will cover cyber defense activities during an armed conflict. During this block trainees will understand how SEE countries should classify cyber conflict, identify protected persons during cyber defense operations in an armed conflict; understand why SEE countries should respect principles of International law of armed conflict (humanitarian law); identify and learn what steps the authorities in SEE countries' should consider during the legal analyses in the cyber targeting process.

The IV block will be dedicated to the analysis and recommendations for improvement of cyber defense policies in accordance with the rules of law in each respective SEE country.

This gathering shows a great potential for current and future collaboration, fusion of theory and practice shaped by the strong will of the sponsor, the speakers and the participants that are here today. Once again, I would like to extend my personal appreciation to the speakers who have crossed half of the earth to be here today, for those who rearranged and adjusted their busy schedules just to be here and share their knowledge and expertise on this important training. Also, many thanks for the unselfish effort given by various speakers and from members of this ATC Toward effective cyber defense in accordance with the rules of law.

Enjoy the training and I wish you fruitful work and positive impressions.

Co-director

Dr. Kristina Misheva

NATO OTAN

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