Centre for Security Cooperation

Military Academy „General Mihailo Apostolski“ - Skopje

“Building a Cyber Resilient Society in SEE”

(IRC-O1-P-16)

27 April 2016
Rakitje, Croatia

The workshop „Building a Cyber Resilient Society in SEE” was held on 27 April 2016 in RACVIAC - Centre for Security Cooperation. 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.

This activity was a continuation of the Cyber Security Project whose aim is to provide a starting point in the development of the Advanced Training Course Programme.

The purpose of the workshop was to bring together cyber security experts from the SEE region in order to work on the development of the Advanced Training Course Programme. The designated topics for the Training Course are in line with the individual countries’ needs and best practices.

Besides the representatives of the RACVIAC Members and the Military Academy “General Mihailo Apostolski”- Skopje, the workshop was supported by the SBA Research Center for Information Security representative, Prof. Dr. Edgar Weippl (Republic of Austria).

In their opening remarks RACVIAC Director Ambassador Haydar Berk and the Dean of the Military Academy "General Mihailo Apostolski" - Skopje, Dr Orce Popovski, Col, welcomed all distinguished experts from the countries of the South East European region which supported the event by taking part in it.

The workshop participants worked in two groups and had an opportunity to discuss topics and objectives for the Advanced Training Course which are in line with their institutions' needs and best practices.

The workshop was concluded with a joint discussion and agreement on the following:

Topics and objectives for the Advanced Training Course

Topic: **Information Warfare: Defending against information warfare**
Objectives:
- Definition/ understanding Information Warfare
- Implications and protection measures (state/strategic level)
- Unconventional Information Warfare

Topic: **Resilient Wireless protocols for transmission of critical messages**
Objectives:
- Describing Wireless protocols
- Wireless protocols standards
- Protection of transmission of critical messages

Topic: **Security threats from non-state actors in cyber space**
Objectives:
- Defining non-state actors (cyber crime, hacktivism and terrorism)
- Targets, motivations
- Modus operandi
- Case studies (tbc)

Topic: **Security threats from state actors in cyber space**
Objectives:
- Defining state actors (state aggression, cyber espionage)
- Targets, motivations
- Modus operandi
- Case studies

Topic: **Critical Information Infrastructure Protection**
Objectives:
- Defining Critical Infrastructure
- SCADA and ICS systems
- Resilient mechanism for defense
- Protection procedures
- Case studies

Topic: **New Generation of Cryptographic Security**
Objectives:
- Improving security via cryptographic products
- Symmetric and asymmetric cryptography
- Basics of cryptoanalysis
- Best practices and misuses
- Next generation cryptographic devices

Topic: **Post-quantum security**
Objectives:
- Future challenges
- Quantum computing
- Quantum cryptography
- Traditional vs quantum

Topic: **Access control**
Objectives:
- Types and categories of Cccess control
- Authentication methods
- Password management
- Audit and log analysis of access control

Topic: **Cloud computing and security challenges**
Objectives:
- Defining cloud computing
- Advantages and disadvantages of cloud computing
- Achieving security in cloud computing

Topic: **Cyber warfare and cyber weapons**
Objectives:
- Defining cyber warfare and cyber weapons
- Legal aspects of using of cyber weapons
- International regulation on cyber weapons

Topic: **National/International Cyber Security regulations**
Objectives:
- Necessity of cyber security regulation
- Existing regulations, best practices, case studies
- Ways and levels of cooperation between nations/institutions

Topic: **New dimension of NATO cyber defense policy**
Objectives:
- Evolution of NATO cyber defense policies
- Decisions, NATO summits
- Smart defense policy

Topic: **Cyber security, cyber defense and cyber operations**
Objectives:
- Definition
- Different approaches
- National and international level
- National authorities with responsibilities in cyber security/defense

Topic: **Information obfuscation**
Objectives:
- Definition of obfuscation
- Methods used by attackers to obfuscate (traditional and current methods)
- Mechanism against attacks related to obfuscation

Topic: **Pen – testing**
Objectives:
- Introduction (what is pen-testing; crucial elements before, during and after; benefits)
- Pen-test methodologies
- Vulnerability discovering (reports, measures, etc.)
- Exercise with open source tool for pen-testing??

Topic: **Cyber special operations**
Objectives:
- Defensive and offensive operations
- Exploitations
- Hacking back, counter-cyber attack
- Cyber espionage

Topic: **Applying International Law of Armed conflict principles to cyber defense**
Objectives:
- Applicability of international law of Armed conflict related to cyber space
- Possible solutions for attribution issues
- NATO Article 5
- UN Charter
- Tallinn manual

Topic: **Introduction on Digital forensics**
Objectives:
- Preserving data and evidence
- Benefits of digital forensics
- Legal use (authorities responsible for forensics)
- Mobile Device Investigative Techniques
- Case studies

Topic: **Advances of using risk analysis in pursuing systems security**
Objectives:
- Why and when we need risk analysis
- Identifying weak points and potential targets for attacks
- Methods and objectives of risk analysis
- Risk analysis approaches

Topic: **Cyber risks & threats, state of the art & future trends**
Objectives:
- Perspective (dark web, IoT)
- Raising awareness of cyber threats and risks
- Converged networks, assessment/evaluation
- Possible future actors, assessment/evaluation

Topic: **Cyber incident handling**
Objectives:
- Defining cyber incident
- Defining procedures to respond
- Reporting cyber incident
- Responsibilities of CERT, CIRT, SOC
- Best practices

Topic: **Organizational aspects of Information Security**
Objectives:
- Information security management standards
- Responsible authorities
- Resilience mechanisms
- Data Disaster recovery and business continuity

Topic: **Online digital evidence**
Objectives:
- Introduction to online digital evidence
- Methods and instruments for searching and collecting online digital evidence
- Managing digital evidence
- Case studies

Topic: **Protection of privacy in cyberspace**
Objectives:
- Legal aspects
- Cyber insurance
- Responsibilities of service providers, national authorities…
- Techniques and technology for privacy protection

Topic: **Human factor in cyber space**
Objectives:
- Social engineering/insiders
- Awareness
- Staff Training

Topic: **Misusing Cyber Space for Inciting Violent Extremism**
Objectives:
- Definition of Cyber Space
- Identifying the platforms for misuse
- Suppresing the incitement of calling and recruiting for violent extremism
- Case study/examples

The selected topics will be included in the training agenda – Advanced Training Course which will be organized by RACVIAC - Centre for Security Cooperation.

Compiled by IRC Pillar
RACVIAC