CYBER RAPID RESPONSE TEAMS AND MUTUAL ASSISTANCE IN CYBER SECURITY

Egle Vasiliauskaite
Policy Analyst, Ministry of National Defence of the Republic of Lithuania
Permanent Structured Cooperation in Security and Defence Policy (PESCO)

• Foreseen in Lisbon Treaty;
• Goal: Enhance cooperation in the field of security and defence;
• December, 2017: Council of the EU approved 17 projects, which will be implemented within the PESCO framework;
• Lithuania is a lead-nation for PESCO project “Cyber Rapid Response Teams and Mutual Assistance in Cyber Security”.
Overview: SQ

- In 2017 Lithuania experienced 55 thousand cyber attacks;
- In 2017 in the EU 4 thousand cyber attacks were recorded every day;
- Increasing threats against the objects of critical infrastructure;
- If the EU fails to counter security challenges in effective manner, the European economy may incur 640 billion euro damage;
- One global cyber-attack may cause damage equal to that of the hurricane Katrina, costing 120 billion U.S. dollars;

Problem – Solution

Limited EU MS resources are wasted while duplicating capabilities in the fight against cyber threats

Cyber Rapid Response Teams using a common cyber toolkit
Cyber Rapid Response Teams (CRRTs)

- Team should be composed of project participating MS delegated cyber security experts

Functions of CRRTs
- Incident management:
  - Support to Member States
  - Support to EU CSDP Missions and Operations
  - Support to EU institutions
  - Support to partner countries
- Vulnerability assessments
- Preventative actions
Implementation of the project

• Assurance of political support?

• Legal basis, enabling the CRRTs to operate?

• Common set of principles and procedures?

• Common capability to be used by the CRRTs?
Assurance of Political Support

JOIN

FINLAND
NETHERLANDS
SPAIN
FRANCE
ROMANIA

CROATIA
LITHUANIA
ESTONIA
POLAND

OBSERVE

SLOVENIA
GREECE
GERMANY
Assurance of Political Support

Signing of Declaration of Intent

Signed Cyber Rapid Response Teams and Mutual Assistance in Cyber Security Declaration of Intent

Foreign Affairs Council
June 25, 2018
Luxembourg
Legal Basis

Supporting Member States

Supporting CSDP Missions

Supporting Partner Countries

Supporting EU institutions

CERT-EU
Legal Basis

Evaluation report of legal basis for the CRRTs: how can teams legally operate and how the project fits into current legal framework

A round-table discussion of Legal POCs, August 29, Vilnius
Principles & Procedures

• Request for the CRRTs
• The decision-making process
• Activation of the CRRTs
• Composition of the CRRTs
• Mandate in the hosting MS
Principles & Procedures

Terms of Reference

1st common cyber exercise
Cyber Shield/ Amber Mist 2018
October 11-12, Vilnius

Lessons learnt
Memorandum of Understanding
Common capability: creating cyber toolbox

- Consultations with National Cyber Security Centre
- Best practices: NATO’s CRRT
- Testing of forensics tool
- Workshops with Lithuanian academia and private sector

Baltic MilTech Summit 2018
November 15-16, Vilnius
PESCO CRRTs technical POCs meeting
Project timeline

- **Kick-off meeting**
  - February 19, Vilnius

- **Signing Declaration of Intent**
  - June 25, Foreign Affairs Council meeting, Luxembourg

- **Evaluation report of legal basis for the CRRT**
  - August 29, Vilnius

- **1st common exercises**
  - October 11-12, Vilnius

- **2nd common exercises**
  - November 15-16, Vilnius

- **Baltic Miltech Summit 2018**

- **Signing of MOU**
  - 2019, Q4
Project’s benefit

• Shared cyber expertise
• Developed a common capability
• Enhanced EU resilience against cyber threats
• Less spent for cyber security
• Involvement of industry
• Mutual assistance in cyber incident management: The missing puzzle piece to complement the existing cyber security mechanisms
Thank you!