Council of the European Union
General Secretariat



**Brussels, 06 March 2019**

**WK 3085/2019 INIT**

**LIMITE**

**CYBER**

WORKING PAPER

*This is a paper intended for a specific community of recipients. Handling and further distribution are under the sole responsibility of community members.*

**WORKING DOCUMENT**

| | |
|---|---|
| From: | Lithuanian delegation |
| To: | Delegations |
| Subject: | Cyber Rapid Response Teams and Mutual Assistance in Cyber Security |

Delegations will find in Annex a presentation on the project "Cyber Rapid Response Teams and Mutual Assistance in Cyber Security" which will be given in the Horizontal Working Party on Cyber issues on 8 March 2019.

KRAŠTO APSAUGOS MINISTERIJA



# CYBER RAPID RESPONSE TEAMS AND MUTUAL ASSISTANCE IN CYBER SECURITY

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**;
- One global cyber-attack may cause damage equal to that of the hurricane Katrina, costing **120 billion U.S. dollars**;

Sources: NCSC, „2017 yearly Nacional Cyber Security Centre Report"; ENISA Threat Landscape Report; European Commision Talinn Digital Summit factsheet 2017; Lloyds of London Report 2017.

# 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 institutions
  - Support to EU CSDP Missions and Operations
  - 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**
- **Technical tools** to be used by the CRRTs

# Assurance of Political Support

## JOIN

- FINLAND
- CROATIA
- NETHERLANDS
- LITHUANIA
- SPAIN
- ESTONIA
- ROMANIA
- POLAND

## OBSERVE

- SLOVENIA
- GREECE
- GERMANY
- BELGIUM
- FRANCE

# Assurance of Political Support

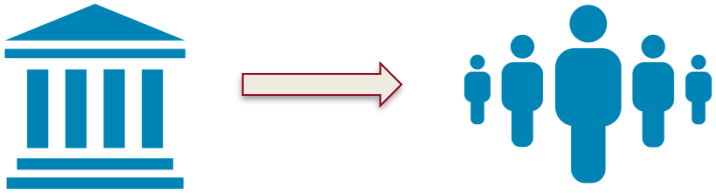
## Signing the Declaration of Intent

Foreign Affairs Council Meeting
June 25, 2018, Luxembourg

Baltic Defence Ministers Committee Meeting
November 24, 2018, Vilnius


# Legal Basis

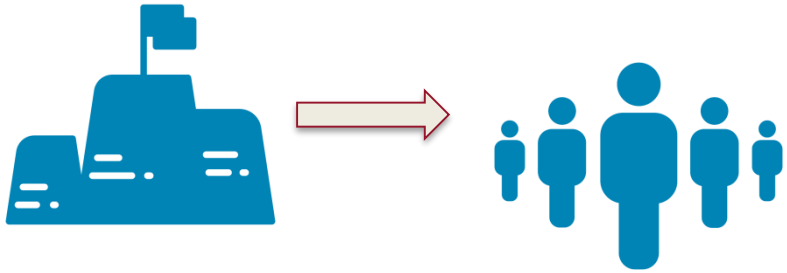




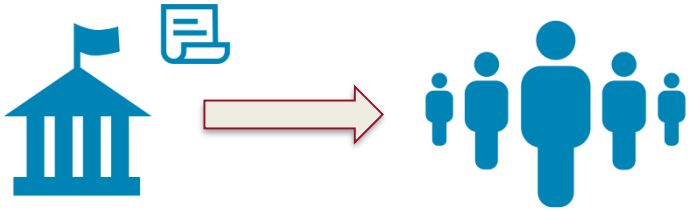
Supporting Member States

CERT-EU

Supporting EU institutions



Supporting CSDP Missions



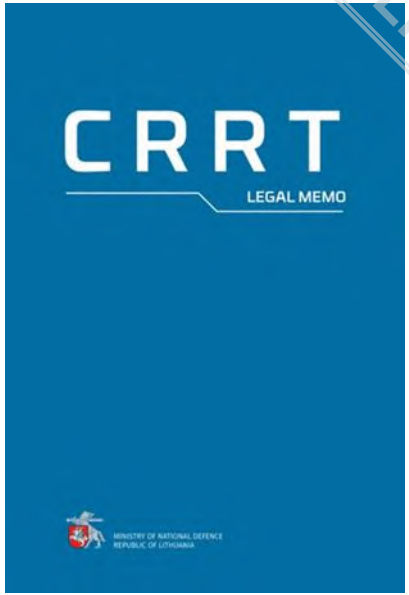
Supporting Partner Countries

# Legal Basis


**A round-table discussion of Legal POCs, August 29, Vilnius**

- Results of Member States' answers to legal questionnaires
- Proposition of 4 legal models enabling the CRRTs' operations
- Analysis of existing EU mechanisms in the field of Cyber Security

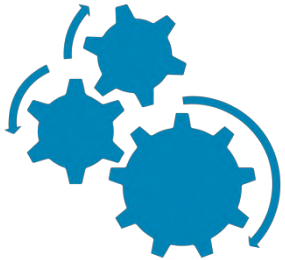
# Legal Basis




**Legal MEMO**
**for the CRRTs' Operations**
**January 15, 2019, 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

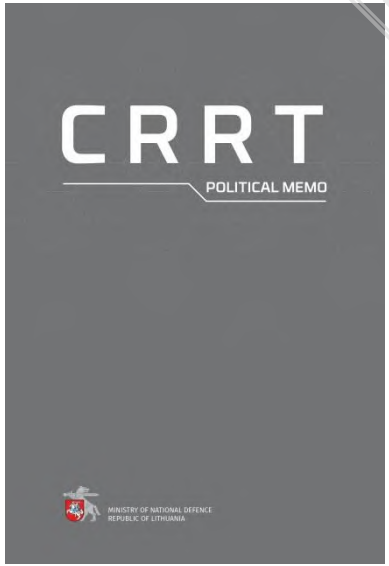


Key Roles & Procedures for the CRRT's Operations drafted and tested during the 1st common cyber table top exercise

**Cyber Shield/ Amber Mist 2018**
**October 11-12, Vilnius**

# Principles & Procedures






**Political MEMO**
**for the CRRTs' Operations**
**January 16, 2019, Vilnius**

# Technical tools: common cyber toolkit

Consultations with National Cyber Security Centre

Best practices: NATO's CRRT

Testing of forensics tool

Workshops with Lithuanian academia and private sector

# Technical tools: common cyber toolkit

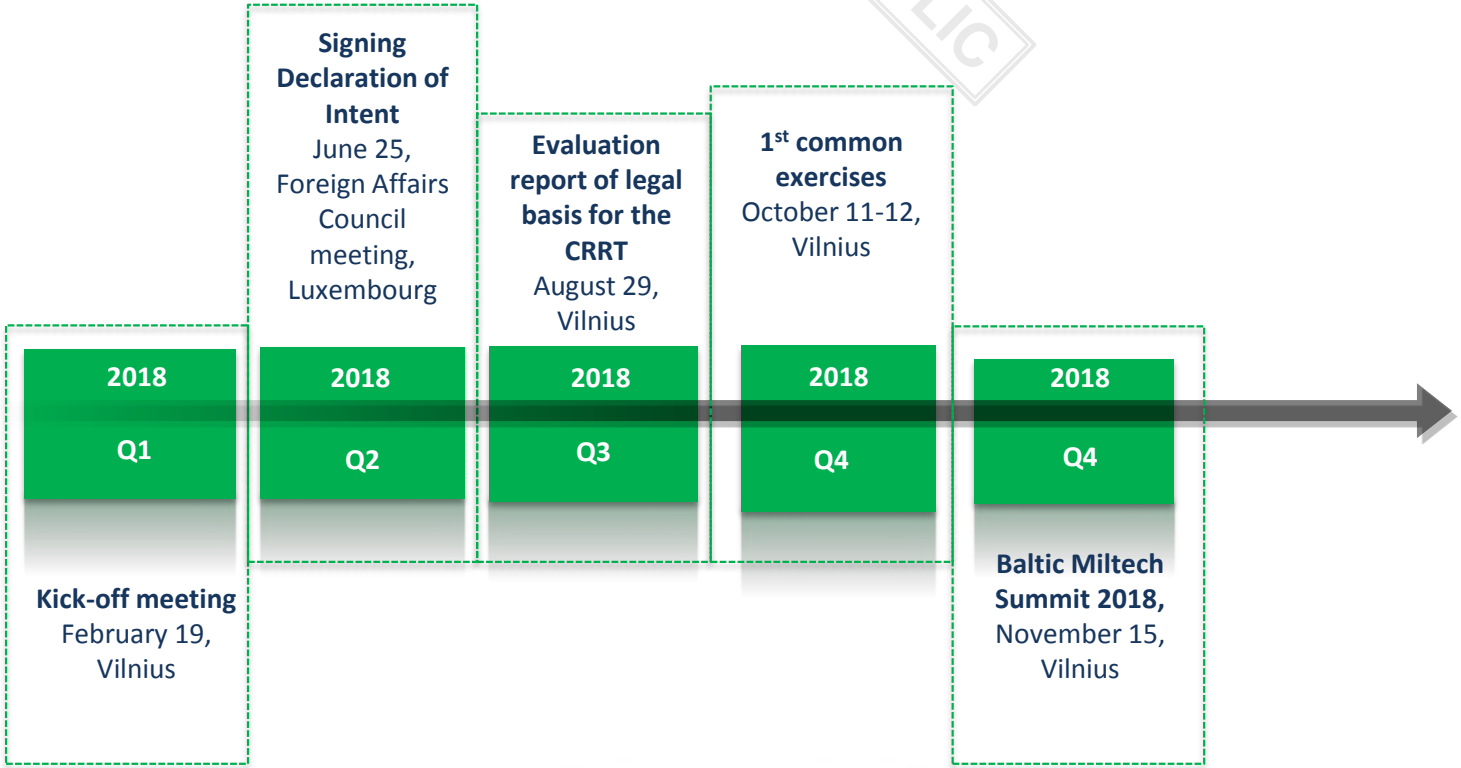


Baltic Miltech summit2018

- **Participants:**
  - International experts,
  - European Defence Agency,
  - NATO,
  - Lithuanian academia,
  - Business representatives from 6 countries,
  - National Points of Contact from project's CRRTs and Mutual Assistance in Cyber Security participating Member States
- **Proposal made** by the Lithuanian National Cyber Security Centre for cyber toolkit creation

**Baltic Miltech Summit, November 15, 2018, Vilnius**

# Project timeline for 2018



# Annual stakeholders meeting

**January 17-18, 2019, Amsterdam**

**Present:**

- Points of Contact of the project's Member States
- European Defence Agency
- CERT-EU
- NATO

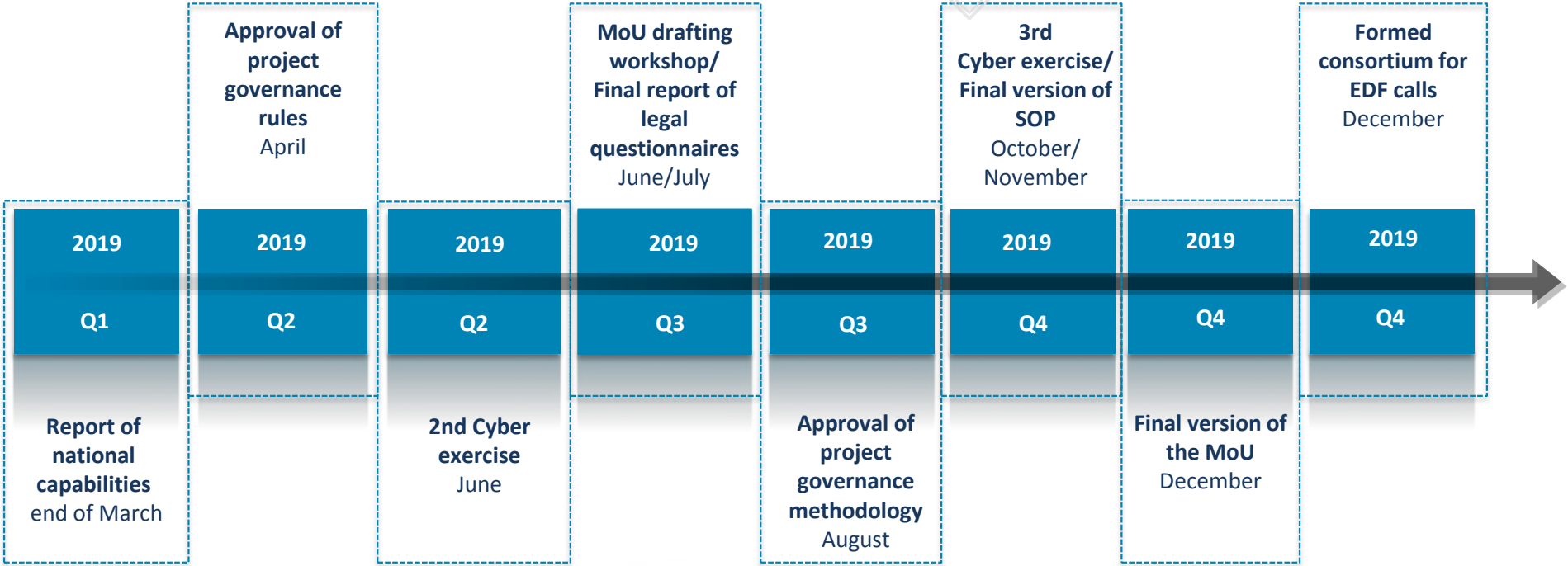
**Presented:**

- Results of the 2018
- Current challenges
- Milestones for 2019

# Operational capability

**1st CRRTs' rotation –**
**led by the Netherlands**
**(2019)**

# Project timeline for 2019



# Project's benefit

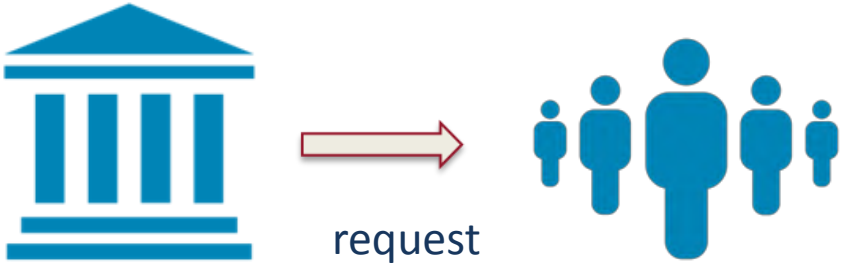
- Shared cyber expertise
- Developed a common capability
- Enhanced EU resilience against cyber threats
- Less spent for cyber security
- Involvement of industry
- Mutual assistance in cyber incident management: The missing puzzle piece to complement the existing cyber security mechanisms

# Frequently asked questions

- Legal basis for the CRRTs operations explained
- The CRRTs in relation to the CSIRTs Network
- The CRRTs' in relation to Blueprint for coordinated response to large-scale cybersecurity incidents and crises

# Legal basis for the CRRTs' operations explained

## Supporting Member States*




State's request = legal basis

- A Member State is **entitled** to ask for assistance by any legal entity – this is how State sovereignty is exercised.
- Thus, **State invitation** – a sufficient legal basis for the CRRT to operate in its jurisdiction.
- Key: identification of a national institution in the cyber security field, which has the **authority** to act on behalf of the State when requesting the CRRT.
- **Principle**: Upon arrival, the CRRT operate only within the mandate of the national institution (most likely national CERT), which requested support of the CRRT.

*Legal analysis made also includes the CRRTs' support for the EU institutions, CSDP missions & operations as well as partner countries (described in legal MEMO).

# The CRRTs in relation to the CSIRTs Network

- **CSIRTs Network:**

Provides a forum where MS' National CSIRTs can cooperate, exchange information, build trust.

- **NIS Directive (Article 12):**

The CSIRTs network shall: "At the request of a representative of a Member State's CSIRT, discussing and, where possible, identifying a **coordinated response** to an incident that has been identified within the jurisdiction of that same Member State."

- A **coordinated response** involves facilitation of the crisis, collection of information, gathering the evidence.
- This does **not** involve operational support for incident response.
- The network does **not** delegate teams to go to Member States.

Therefore, although both CSIRTs Network and the CRRTs operate in the field of cyber incident management , the specificity of their work significantly differs. The CRRTs would offer an **operational capability**, which would be at Member States' disposal.

# The CRRTs in relation to Blueprint

## Bilateral Support

Blueprint applies to incidents, which:

- Cause disruption **too extensive** for a MS **to handle on its own**;
- Affect **two or more MS/ EU institutions** with such a wide-ranging and significant impact that they **require** policy coordination & response at **the Union's level**;

Such incidents are considered as cybersecurity „**crisis**".

In many cases, including those when a MS would require assistance from the CRRTs, cybersecurity incidents would fall **under the threshold** of a cybersecurity „crisis". Thus, the CRRTs' support would be invaluable aid to the MS through **a bilateral support** as a response to cyber incidents/ attacks, which are dangerous but have not yet reached the threshold of a cybersecurity „crisis".

## The Union Response

- The CRRTs could also be used as assistance in case of national/ international cybersecurity **crises**, when Blueprint is invoked.
- The implementation of Blueprint is carried out by the Council, using the Integrated Political Crisis Response (IPCR) rules, while the Commission and the HR identify **all relevant Union instruments and military capabilities at the disposal** that could best contribute to the response of the crisis.
- The CRRTs **could be identified as a capability** in the cyber field, which could contribute to the solution of the crisis, **used by the Union**.

# Thank you

If you have any questions related to the project, please do not hesitate to contact us:

Eglė Vasiliauskaitė (egle.vasiliauskaite@kam.lt)
Tadas Šakūnas (tadas.sakunas@kam.lt)