DECLARATION OF INTENT

ON COOPERATION

IN THE FIELD OF CYBER RAPID RESPONSE TEAMS

AND MUTUAL ASSISTANCE IN CYBER SECURITY

The Minister of Defence of the Republic of Croatia, the Minister of Defence of the Republic of Estonia, the Minister of National Defence of the Republic of Lithuania, the Minister of Defence of the Kingdom of the Netherlands, the Minister of National Defence of Romania, the Minister of Defence of the Kingdom of Spain

Recalling three strategic EU priorities deriving from the EU Global Strategy, in particular, protection of the Union and its citizens;

Stressing the need to take full advantage of new defence initiatives to accelerate the development of cyber capabilities in Europe;

Recognising the need to maximise synergies between cyber defence and cyber security, including response to cyber incidents, and step up cooperation in the cyber field;

Recognising the need to strengthen national cyber security capabilities;

Referring to the Directive 2016/1148 of the European Parliament and of the Council concerning measures for a high common level of security of network and information systems across the Union ('NIS Directive') cooperation mechanisms;

Welcoming the Joint Communication on cyber resilience, deterrence and defence adopted on 13 September 2017;

Recalling Article 42(6) of the Treaty on European Union (TEU), Council Decision 2017/2315 of 11 December 2017 establishing permanent structured cooperation (PESCO) and Council Recommendation of 6 March 2018 concerning a roadmap for the implementation of PESCO;

Seeking to act together to prevent, deter and respond to cyber incidents;

Emphasising opportunities in developing cyber projects through PESCO, have expressed the intention:

- to develop and deepen voluntary cooperation in the cyber field through mutual assistance in response to major cyber incidents, including information sharing, joint training, mutual operational support, research and development and creation of joint capabilities;
- to create Cyber Rapid Response Teams, hereinafter referred to as the CRRTs, as a priority to provide mutual assistance between participating Member States (MS), and as appropriate to help other EU MS, EU institutions, including CSDP missions and operations, and eventually Partners to ensure higher level of cyber resilience and to respond to cyber incidents;
- CRRTs will complement national, EU, regional and multinational efforts in the cyber field, without duplicating existing efforts, structures and formats;
- to survey existing national and EU legal frameworks in order to investigate possibilities for an effective deployment of CRRTs and, if necessary, explore the need of their adaptation.

The Signatories intend to conclude detailed multilateral arrangements regarding the establishment and operation of the CRRTs project, including their mandate, tasks and responsibilities. The main elements of the CRRTs project should be the following:

Formation and cooperation: CRRTs should be formed by pooling participating MS experts on a rotational basis (including training and 6 months stand-by periods). CRRTs will be mobilised for a planned or urgent tasks agreed by all participating MS. CRRTs will only act upon the invitation from a MS, EU institution or Partner country;

Each CRRT should have a team leader and be composed of the participating MS cyber security experts (from Computer Security Incident Response Teams (CSIRTs)). Designated experts will combine work in their original CSIRT and CRRT. CRRTs should closely cooperate with EU institutions, including CSIRT Network, European Union Agency for Network and Information Security (ENISA) and CERT-EU in order to ensure complementarity with existing cyber security initiatives. The work of the CRRTs will be only within the scope, agreed by the MS.

Civil-Military nature
CRRTs would be a civil-military capability that should help foster civil-military culture in cyber domain and broaden cyber defence concept in the EU. The civ-mil nature of CRRTs could also facilitate further cooperation between military and civilian CSIRTs. It is up to each MS to decide, which national CERT (civil or military) will participate in the project.

Equipment
In order to reach better operational capabilities of CRRTs, the Participants could explore and set the baseline of common Cyber Toolkits designed to detect, recognise and mitigate cyber threats. To start operational activities CRRTs could use available on the market or nationally developed tools. However, to expand cyber security activities there is a need to develop a second generation unified deployable toolkit. European Defence Fund co-funding and funding from other EU sources could be considered in this regard. It would facilitate industrial cooperation between participating MS and foster European cybersecurity industry.

Next steps
The Signatories intend to further shape and define the initiative, seeking to reach initial operational capabilities of CRRTs in 2019. The signatories intend to sign the Memorandum of Understanding by the end of 2018. The Signatories participate on an equal basis in the process of creation of CRRTs. The Ministry of National Defence of the Republic of Lithuania intends to be a lead nation of a project.

Petar Mihatov

On behalf of the Minister of Defence of the Republic of Croatia the Assistant Minister

Date: 2018-06-25

Jüri Luik

The Minister of Defence of the Republic of Estonia

Date: 2018-06-25

Raimundas Karoblis

The Minister of National Defence of the Republic of Lithuania

Date: 2018-06-25

Ank Bijleveld

The ~~Minister of Defence~~ of the Kingdom of the Netherlands

Date: 2018-06-25

Mircea Duşa

On behalf of the Minister of National Defence of Romania
State Secretary

Date: 2018-06-25

Margarita Robles

The Minister of Defence of the Kingdom of Spain

Date: 2018-06-25