WISI Opinion no. 5/2018

Author: Karol Cheda

WARSAW INSTITUTE
FOR STRATEGIC INITIATIVES

EUROPEAN CYBER RAPID RESPONSE TEAMS

Since the Treaty of Lisbon came into force, the European Union (EU) has significantly expanded the areas of integration. The economic dimension is not being considered anymore the only factor for integration. Although it still remains important, in 2009 UE decided to put more emphasis on the issue of common foreign policy and common security policy. Nevertheless, we had to wait for almost eight years for the establishment of permanent structured cooperation – PESCO, which gathers all EU member states, excluding Denmark, Malta and Great Britain. The aim of the very first stage of forming PESCO is to ensure the implementation of 17 common security projects.

One of the projects entails the establishment of Cyber Rapid Response Teams (CRSTs) and calls for mutual support in the area of cybersecurity. For this purpose, on June 26th 2018, six member states: Croatia, Estonia, Lithuania (initiator of the project), Netherlands, Romania and Spain, signed a joined declaration. The document refers to European Parliament's and of the European Council's Directive concerning the legal measures to boost the overall level of cybersecurity in the EU (i.e. the security of network and information systems – NIS Directive). The declaration is based on the identification of needs as well as the development of cooperation by:

- Mutual assistance in responsive activities to major cyber incidents, including information sharing, joint trainings, support for mutual operations, B+R and the development of mutual capabilities within permanent European structures;
- Creation of CRRTs necessary of its functioning and for the support of national CERTs;
- Development of the second generation of Cyber Toolkit, i.e. special tools dedicated for detection, identification and combating cyber threats. In accordance to the initial plan, the project will be financed either fully or partly by the European Defence Fund;
- Promotion of civil-military cooperation and support for the European ICT industry.

The document does not reveal any details on the establishment of structures. However, this might be a result of the specific character of the inaugural declaration. It shall be rather treated as an initial pillar. Such interpretation surely brings more optimism to it. The fact that the need for identification of cyber capabilities at the European level has appeared in the document seems to be its biggest advantage. Bringing awareness about such issues can be treated as the first step for the creation of effective European cybersecurity system. Although, we will have to wait for its final establishment, the declaration is setting time frames in this manner – till 2018 a memorandum of understanding shall be signed, and the state of initial operating capability shall be archived by 2019. Continued development and the adaptation to new challenges is crucial for effective cyber defence. There is still time to judge how effective CRRTs really are, however what may cast some doubt is the fact that CRRTs are not being established within the European cybersecurity system. Although the proposal is claimed to not duplicate any of the structures, the establishment of CRRTs might result in dispersion of competences in this area. That is why the distinction of competences seems to be crucial. European Network and Information Security Agency (ENISA), together will CERT-EU serve as supporting bodies, whereas combined with the European network of CSIRTs (Computer Security Incident Response Team), will have the potential to become the front structure for cyber defence.

POLISH POINT OF VIEW:

Poland together with Finland and France, is mentioned as a state which will join the project. This will be the 9th permanent structural initiative in which Poland would participate. After the time of low activeness, Poland seems to be more engaged in European security projects.

From the Polish point of view, engagement in projects concerning the establishment of European response teams as well as the establishment of inter-European cooperation platform, seems to be crucial. It will increase the quality of cyber defence and it will lead to the exchange of experiences, which is very important at the time of reorganization caused by the NIS Directive. Increased cooperation will have a positive impact on the multiplication of countering and responsive actions. The European character of the initiative provides the ability to conduct combined operations under the aegis of the European Union.

The following initiative is also important in terms of geopolitics. Poland in order to remain the regional leader, also in terms of military capabilities, needs to be engaged in various international projects. The initiative can be used for strengthening of Poland’s bilateral relations – many of the states engaged in the initiative are situated in a direct zone of Polish interests, for instance the initiation of the project – Lithuania. The initiative also puts emphasis on the engagement of cybernetic industry and thus creates a good opportunity for promotion of Polish business abroad.

Based on:

- Declaration of Intent on Cooperation in the field of Cyber Rapid Response Teams and Mutual Assistance in Cybersecurity;
- https://eeas.europa.eu/headquarters/headquarters-Homepage_en, European Union External Action;
- http://mon.gov.pl/, Ministry of National Defence.