EU2013.LT

Informal Justice and Home Affairs Ministers' meeting

18-19 July 2013, Vilnius (Lithuania)

Discussion paper

Cyber security issues

I. Introduction

The Joint COM/HR Cyber security Strategy of the European Union: An Open, Safe and Secure Cyberspace (doc. 6225/13) sets out five strategic priorities addressing the challenges identified therein:

1. Achieving general cyber resilience in all public and private organizations, mainly by harmonizing the preparedness of EU Member States to deal with security challenges in cyberspace;
2. Reducing cybercrime, by raising the operational capabilities and coordinating law enforcement activities at EU level;
3. Developing the EU's industrial and technological resources for cyber security, by promoting European cyber security products, developing security standards, fostering investments and innovation and pushing ahead R&D;
4. Developing cyber defence policy and capabilities related to the CSDP, inter alia by raising awareness, building concepts, establishing structures and reinforcing capabilities to face evolving cyber threats;
5. Establishing an EU international cyberspace policy, aiming mainly at preserving the benefits of cyberspace and promoting openness and freedom on the Internet while respecting the EU core values and applying existing international cyberspace laws as well as developing cyber security capacity building and information infrastructures in third countries.

The second strategic priority ('reducing cybercrime') is the one in which JHA Council involvement is of a direct relevance.

The introduction of a reporting obligation – under strictly defined circumstances- for specific types of cyber incidents is currently being discussed by Member States in the context of the negotiation of the proposed Directive on Network and Information Security ('NIS Directive'), which accompanied the Cyber Security Strategy.

The recently adopted Council Conclusions on the aforementioned strategy (doc. *11357/13*) set out the political commitments and possible undertakings of Member States, the Commission, agencies and other relevant stakeholders in this field. In particular, EC3 and

Eurojust have been invited to 'continue to strengthen their cooperation with all relevant stakeholders, including EU agencies, Interpol, the CERT community and the private sector in the fight against cybercrime, including by emphasizing synergies and complementarities in accordance with their respective mandates'.

II. The JHA contribution towards improved cyber security

JHA contribution towards improved cyber security can be explored within the following fields:

Addressing cyber security, notably by working towards reducing criminal activities online, in an integrated, multidisciplinary and horizontal way. Closer cooperation and coordination between defense actors, law enforcement authorities, the private sector and other relevant stakeholders is key to building mutual trust, exchanging expertise and responding better to cyber incidents and challenges, through initiatives such as the development of common standards, awareness-raising, training and education and ongoing review and testing (or development) of early warning and response mechanisms. Moreover the identification of both national and EU critical information infrastructure (CII) can further those efforts and bring an added value towards achieving an equal level of preparedness and capacity for reaction in all Member States in case of cyber threats and/or cyber incidents.

Multidisciplinary cyber exercises (including JHA actors) are another important element of a coherent strategy for cyber incident contingency planning and recovery both at national and at EU level. The findings of the last pan-European cyber incident exercise "Cyber Europe 2012"in which Member States took part highlighted the close cooperation and intensive information exchange at national level between public and private players and the challenge that the different public–private cooperation structures (parallel and sometimes overlapping) constituted for that cooperation.

The development of the ICT field needs to be reflected in the improvement of cyber capacity building in the law enforcement community, which must have adequate resources and capabilities if it is to function properly.

Synergies are necessary among the operators of CII, including national computer emergency response teams (CERTs), civilian and defence cyber actors as well as ICT and security research on cybersecurity and cybercrime related issues. These synergies should avoid redundant initiatives and should provide efficient mechanisms for exchange of information and cooperation, taking full use of the newly created EC3 and envisaging, if necessary, the conclusion of cooperation agreements or Memoranda of Cooperation. Furthermore, synergy activities might encompass financial aspects, which might lead not only to consideration of joint investment in the European cyber security industry similar to that in other sectors, but also to pooling and sharing of resources.

Law enforcement activities are relevant to the achievement of trustworthy ICT, inter alia, by means of close contact with and the active presence of the public, either through personal contacts, facilitating access for filing complaints, or through social networking.

Training of cyber security experts from relevant authorities, including the judicial ones, is another area where strong coordination needs to be further ensured, both within the EU Member States and in external capacity building programmes.

Discussion Points

Ministers are invited to discuss the following issues:

1. **How are JHA actors contributing both domestically and, where appropriate, in a multinational environment, to achieving synergies and strengthening cooperation between different cyber security stakeholders and how could this contribution be improved, in particular allowing better prevention and more targeted response to cyber incidents**?

2. **What measures are being taken or could be implemented to improve cyber capacity building and cooperation in the law enforcement community? How these can be further streamlined to ensure complementarity and optimal allocation of resources? What are the best practices from the law enforcement community on the achieving trustworthy ICT?**

The outcome of the discussion will help to identify the best way forward for the implementation of the EU Cyber security Strategy and to mainstream the role of JHA within the multi-stakeholder and multidisciplinary approach.

_____