Council of the European Union

Brussels, 8 February 2016
(OR. en)

5633/16

JAI 62
COPEN 30
DROIPEN 20
CYBER 5
COSI 15
GENVAL 17

NOTE

From:	Presidency
To:	Delegations
Subject:	Cybercrime - plans during the Netherlands Presidency

Background

1. Due to the digitalisation of society, the dependency on electronic evidence in criminal investigations on cybercrime but also on conventional types of crime has grown exponentially, including through the increased use of "always on" web applications, accessed through easy to use and portable devices. The borderless nature of cyberspace poses specific challenges for law enforcement and judicial authorities.

2. The EU has recognised the challenge cyber-related criminal investigations face and has acted accordingly, notably by enhancing international cooperation both between Member States and with third countries via Europol and Eurojust. The European Cyber Crime Centre (EC3) has evolved into a hub for international cybercrime investigations, and the implementation of the European Investigation Order in criminal matters will further improve cooperation between Member States also for obtaining digital information and evidence.

3. Nonetheless, more efforts would be needed to address some of the persisting challenges faced in cyber-related criminal investigations. For instance, mutual legal assistance (MLA) is not possible in situations where the location of data or the origin of a cyber attack is not known, no matter how efficient these procedures are. Conflicting regulations might hamper cooperation with private sector, in particular foreign Internet service providers (ISPs).

4. The activities of the Presidency will build on the discussions and results of the previous Luxembourg Presidency[1] and will draw on the European Internal Security Strategy and the European Agenda on Security which prioritises *"reviewing the obstacles to criminal investigations on cybercrime, notably on issues of competent jurisdiction and rules on access to evidence and information"*.

Informal meeting of Ministers of Justice and Home affairs, Amsterdam, 26 January 2016

5. At their informal meeting on 26 January 2016 the Ministers of Justice discussed the challenges faced in criminal investigations in situations of "loss of location", where MLA is not possible, as well as the issues concerning the cooperation with the private sector, in particular with foreign ISPs regarding preservation and obtaining of e-evidence. It was concluded that:
   - There is an urgency to improve law enforcement and judicial action that would allow for an effective rule of law in cyberspace.
   - Effective implementation of existing instruments on MLA and the European Investigation Order would optimise the current use of investigative powers and the cooperation with private sector.
   - Alternative approaches, such as establishing jurisdiction on criteria other than territoriality, should be considered in cases of "loss of location".
   - Enhancing cooperation among Member States, in particular between their judicial authorities, should be envisaged.

[1] 14369/15, 13689/15, 12612/15.

- Cooperation and strengthening working arrangements with third countries, especially the US, should be treated with special attention.
- Cooperation with private sector, especially ISPs, is essential for access to data and retrieval of evidence in cyber-related criminal investigations. In this respect clear procedures and regulations for cooperation with private sector are needed. Options to ensure the timely and effective access to data stored by foreign ISPs could be considered at technical level, e. g. applying a differentiated approach for certain types of data, for example subscriber data.
- Solutions would ideally be global but common views and approaches at EU level could be a useful first step.
- Fundamental rights and data protection rules, as well as procedural safeguards in criminal proceedings, should be respected and ensured.

Next steps

6. The suggestions made at the informal ministerial meeting of 26 January 2016 are a very useful input to the Presidency's priorities of how to ensure effective MLA processes, how to define a common approach to situations where existing regulations and international cooperation cannot provide a proper response, e.g. regarding the applicable jurisdiction rules where the location of the data or the origin of a cyber attack is not known, and how to establish a common framework for cooperation with the private sector, in particular with the foreign ISPs.

7. Further input and expertise on these subjects will be sought at the high-level expert meeting of 6-8 March in Amsterdam, which aims to bring together views from policy advisors, practitioners, academics and private parties (Chatham House Rule). Delegations are therefore invited to ensure their Member State is appropriately represented at this event.

8. The outcome of the conference will also be brought in conjunction with the implementation plan of the EU Internal Security Strategy, which is monitored by COSI. In this context, it is worth mentioning that within the EU policy cycle 2014-2017, the EMPACT project on cybercrime will execute Joint Action Days on 'money mules' and on the 'Darkweb'. These Joint Action Days will provide input for practical improvements on international cooperation of law enforcement organizations. Moreover, valuable suggestions about possible measures to improve cooperation can also be obtained from existing evaluations. For example, Europol and Eurojust have provided ideas on international cooperation at the Global Conference on Cyber Space 2015, and several Member States have been evaluated in the current round of GENVAL mutual evaluations on cybercrime. On these bases, the Presidency foresees a discussion in COSI to identify feasible improvements for operational international cooperation.

Network of cybercrime prosecutors and investigative judges

9. Next to the above discussions and activities, the Presidency wishes to draw attention to the idea of establishing a network of cybercrime prosecutors and investigative judges. This initiative would address the needs expressed by practitioners from Member States in meetings at Eurojust and in the context of the Illegal Trade on Online Marketplaces (ITOM) Project, and corresponds to the requests of several Justice Ministers expressed at the 26 January meeting to improve the cooperation between judicial practitioners in the field and exchange best practices enabling successful prosecutions in cybercrime cases.