Council of the European Union

NOTE

From:	Presidency
To:	Council
No. prev. doc.:	6890/17
Subject:	Criminal justice in cyberspace
	- Improving collaboration and coordination

The fight against crime has become more than ever dependant on access to electronic data - data which do not belong to law enforcement or judicial authorities, nor can be regulated by JHA policy makers alone. However, the availability of and access to these data has been reduced due to technical and/or legal reasons[1]: cloud-based storage, limited retention of data[2], use of encryption[3], use of Carrier Grade NAT[4] solutions or virtual currencies[5]. **Collaboration and coordination with partners and stakeholders is therefore essential to establish workable solutions.**

---

[1] Doc. 6890/17
[2] Following the Data Retention Directive invalidation by the Digital Rights ECJ judgement and in view of the latest Tele2 ECJ judgement.
[3] Doc. 14711/16
[4] In order to address the gradual exhaustion of IPv4 addresses, many network operators and service providers have adopted a temporary solution called Carrier-Grade Network Address Translation (CGN) that impedes the identification of individual users (doc. 5127/17).
[5] Enabled by blockchain technologies. See also doc. 7021/17 (to be issued)

In June 2016, the Council (JHA) asked the Commission, in close cooperation with the Member States, to develop possibilities to improve the **access to and exchange of electronic evidence**, through improved cooperation with service providers, more efficient mutual legal assistance, including by setting up a technical exchange platform for e-evidence and the elaboration of solutions to determine and enforce jurisdiction in cyberspace ("connecting factors"). The Commission is carrying out these work strands in an expert process on e-evidence. Following the discussions in the December 2016 Council (JHA) on the **role of encryption in criminal investigations**, the Commission set up another expert process to establish a problem definition and assess policy options on this subject. The Commission will update Ministers on this on-going work.

As working on these matters needs to take account of **various sectors and legitimate interests** (e.g. of LEA/judiciary, data protection/human rights, internal market/trade, electronic communications), there is a clear **need of improved coordination and collaboration at national and EU level** between the different policy fields. It is essential to ensure that security and privacy considerations are fed in early into relevant technical and general policy developments, to find solutions for law enforcement and judicial cooperation needs, without overlooking consequences for the companies concerned and their different business models.

As an illustration, contacts with the telecommunication providers will be required to examine a solution for the retention of electronic communications data. Driving jointly the *IPv6 transition*[6] with stakeholders in the digital single market could provide for a better functioning of the Internet and prevent loss of data for the identification of criminals online. Regular *cyber and/or ICT dialogues with third countries* would facilitate international cooperation, in particular with those third countries where most of the service providers are located. Imbedding safety features already in the research and development of the *Internet of things* would increase consumers' trust in the connected devices as well as help reducing related security risks.

Against this background, the Presidency invites Ministers to:

- **share good practices of cross-sector national collaboration and coordination; and**
- **present any suggestions on how to improve coordination at EU level to ensure the necessary synergies among parallel but related processes in different policy fields.**

---

[6]   Transition to the new version of the Internet Protocol, which offers unlimited number of IP addresses (i.e. one per device/user) is slower than expected due to the lack of commercial incentive, which has resulted in many network operators and service providers to run both versions in parallel.