Council of the European Union

PRESS
EN

COUNCIL CONCLUSIONS
Luxembourg, 9 June 2016

Council conclusions on improving criminal justice in cyberspace

The Justice and Home Affairs Council adopted the following conclusions:

"**THE COUNCIL OF THE EUROPEAN UNION**

DETERMINED to deny criminals a safe haven in cyberspace,

NOTING the increasing impact of cybercrime, cyber-enabled crime or any other criminal activity which has left a digital footprint in cyberspace,

STRESSING the increasing importance of e-evidence in criminal proceedings in all types of crime, and in particular for terrorism,

STRESSING the importance of protecting cyberspace from abuse and criminal activities for the benefit of our economies and societies, and therefore the need for law enforcement and judicial authorities to have effective tools to investigate and prosecute criminal acts related to cyberspace,

RECALLING that the fight against cybercrime is a priority under the European Agenda on Security of 28 April 2015, which includes a commitment from the Commission to review obstacles to cybercrime investigations, notably on rules on access to evidence and information,

RECALLING the discussion of the Ministers of Justice on the challenges ahead for effective criminal justice in the digital age at the Justice and Home Affairs Council in December 2015[1],

RECALLING the support by the Ministers of Justice to develop concrete elements for a common EU approach on jurisdiction in cyberspace, expressed at the informal Justice and Home Affairs meeting of 26 January 2016,

RECALLING the joint statement of Ministers of Justice and Home Affairs and representatives of the EU institutions on the terrorist attacks in Brussels on 22 March 2016 stressing the need, as a matter of priority, to find ways to secure and obtain e-evidence more quickly and effectively by intensifying cooperation with third countries and with service providers that are active on European territory, in order to enhance compliance with EU and Member States' legislation, and direct contacts with law enforcement authorities and to identify concrete measures to address this complex matter during the Justice and Home Affairs Council in June[2],

RECALLING the Communication from 20 April 2016 to the European Parliament, the European Council and the Council delivering on the European Agenda on Security to fight against terrorism and pave the way towards an effective and genuine Security Union as part of which the Commission committed to propose solutions, to address the problems of obtaining digital evidence in relation to criminal investigations,

---

1 doc. 14369/15

2 doc. 7371/16

NOTING the Report[3] of the Conference on jurisdiction in cyberspace held on the 7th and 8th of March 2016 in Amsterdam, which reflects discussions on possible solutions for improving investigations in cyberspace, especially regarding the procedures for mutual legal assistance, cooperation with the private sector, and investigations in cyberspace where the location of data or the origin of cyber-attacks are not (yet) known,

NOTING the adoption by COSI of a set of recommendations to improve operational cooperation in criminal investigations in cyberspace[4],

NOTING the ongoing 7th round of mutual evaluations devoted to the practical implementation and operation of the European policies on prevention and combating cybercrime as an important contribution to the efforts to step up the fight against cybercrime,

NOTING the results of the review on the EU-U.S. MLA Agreement[5],

NOTING the Council conclusions establishing the European Judicial Cybercrime Network[6],

RECALLING the Council of Europe Convention on Cybercrime of 23 November 2001 and its Additional Protocol which is promoted by the Union as a global framework of reference to fight cybercrime,

RECALLING Directive 2014/41/EU on the European Investigation Order in criminal matters, which aims to make cross-border investigations across the EU faster and more efficient i.e. on the basis of mutual recognition, as well as Directive 2013/40/EU on attacks against information system calling on Member States, inter alia, to ensure that they have an operational national point of contact in the existing 24/7 cooperation networks,

RECOGNISING that although these instruments provide broader possibilities for law enforcement in cyberspace, practical and legal obstacles continue to exist, also due to the rapid development of technologies, e.g. in cases where the origin of cyber- attacks or location of e- evidence is not (yet) known or volatile, or in cases where conflicting regulations hamper the cooperation with service providers,

NOTING that cyber-enabled and cybercrime violate fundamental rights and freedoms, and the need to ensure full protection of these rights and freedoms,

RECOGNISING that the use of investigative measures should be guided by the protection of fundamental rights and freedoms and the principles of necessity and proportionality,

NOTING the adoption of the EU's data protection reform instruments, in particular the Data Protection Directive for the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data,

NOTING the 2012 and 2013 reports of the Trans-border Group of the Cybercrime Convention Committee, stating that several countries are already engaged in trans-border access to data beyond the scope of the Budapest Convention on an unclear legal basis,

RECOGNISING that the Member States have a legitimate interest to determine in criminal investigations, as a minimum, the location of e-evidence or the origin of a cyber-attack,

DETERMINED to act in order to uphold the rule of law in cyberspace,

---

3 doc. 7323/16

4 doc. Xxxx/16

5 doc. Xxxx/16

6 doc. Xxxx/16

THE COUNCIL OF THE EU,

ACKNOWLEDGES that the following guidelines should apply for future work to improve the enforcement of the rule of law in cyberspace and obtaining e-evidence in criminal proceedings:

- Practical solutions to enhance the effective conduct of criminal proceedings in cyberspace should respect fully data protection and fundamental rights frameworks;
- Enhancing cooperation with service providers or any other comparable solution that allows for quick disclosure of data should be considered; less rigorous legal processes could be envisaged for obtaining specific categories of data, in particular subscriber data and could benefit all stakeholders;
- Mutual Legal Assistance (MLA) procedures related to electronic data should be accelerated and streamlined; the volume of MLA requests between competent authorities could be reduced by enhancing cooperation with service providers, or any other comparable solution;
- Mutual recognition procedures should be efficiently used to ensure effective securing and obtaining of e-evidence;
- Other measures should be considered, based on a review of connecting factors for enforcing jurisdiction[7] in cyberspace, including in cases where the location of data is not (yet) known or volatile.

CONSIDERS it necessary to cooperate with relevant third countries and private parties allowing for combined effects of various measures for effective law enforcement in cyberspace.

CONSIDERS that the development of a common EU approach on improving criminal justice in cyberspace should be treated as a matter of priority. This should be done in a way which is consistent with the work under way on the Council of Europe Budapest Convention framework.

CONCLUDES, THEREFORE, THAT:

I. COOPERATION WITH SERVICE PROVIDERS IS TO BE ENHANCED.

To that end,

1. The COMMISSION is requested, to develop a common framework for cooperation with service providers for the purpose of obtaining specific categories of data, in particular subscriber data, when allowed by third countries legislation, or any other comparable solution that allows for a quick lawful disclosure of such data[8]. The Commission is requested to do so in association with Member States and relevant third countries and in cooperation with the private sector.
2. Such solutions should set out commonly agreed requirements including requirements of necessity and proportionality for the requests that are addressed to service providers enabling lawful access to data held by them. It should seek to prevent inconsistent interpretations, conflicts between existing regulations and to address the issue of non-disclosure of data requests. Proposed solutions are not to impede arrangements at national level.

3. To this end, the COMMISSION in association with Member States is requested to explore with service providers the possibility of using aligned forms and tools as those referred to in Section II in order to facilitate authentication, to ensure swift procedures and to increase transparency and accountability of the process of securing and obtaining e-evidence.

---

[7] The terms "enforcing jurisdiction" and "enforcement jurisdiction", for the purposes of these conclusions, refer to the competence of the relevant authorities to undertake an investigative measure. Pursuant to these conclusions, a common EU approach with a view to improving investigations in cyberspace is to be explored for specific situations where existing frameworks are not sufficient.

[8] Where a request for data involves a transfer of personal data by a Member State authority, the relevant data protection law has to be complied with.

THE COMMISSION is requested to present an assessment report on progress on this issue by December 2016 and present deliverables by June 2017.

II. MUTUAL LEGAL ASSISTANCE (MLA) PROCEEDINGS (AND WHERE APPLICABLE, MUTUAL RECOGNITION) NEED TO BE STREAMLINED

To that end,

4. The COMMISSION is requested to find ways, in association with MEMBER STATES and where necessary third countries, as a matter of priority, to secure and obtain e-evidence more quickly and effectively by streamlining the use of mutual legal assistance proceedings and where applicable, mutual recognition.
5. To that end, the COMMISSION is requested, in association with MEMBER STATES, EUROJUST and third countries, to consider and make recommendations on how to adapt, where appropriate, existing standardised forms and procedures to request the securing and obtaining of e-evidence.
6. To increase the efficient use of such standardised forms and procedures in order to obtain e-evidence, the COMMISSION is requested to develop, in association with MEMBER STATES, EUROJUST, CEPOL and where necessary third countries, while using where appropriate, existing electronic tools, and while respecting competences and channels of communication under existing legal frameworks:
   - a secure online portal for electronic requests and responses concerning e-evidence and the corresponding procedures, including optional use of automated translation of such requests, as well as for their tracking and tracing;
   - guidelines and dedicated training modules, in cooperation with the European Judicial Training Network, the European Judicial Cybercrime Network and the authorities of third countries where necessary, on the efficient use of the current frameworks that are used for securing and obtaining e-evidence, including guidelines to clarify when, under the existing rules, using MLA or mutual recognition instruments are not required.

The COMMISSION is requested to deliver a mid-term report on the progress of these activities by December 2016 and present deliverables at the latest by June 2017. The COMMISSION is requested to present the online portal by December 2017.

7. The COMMISSION, in association with MEMBER STATES and where necessary third countries, is requested to consider additional steps in order to secure and obtain e-evidence more effectively, through the use of amongst others the EU-U.S. MLA framework.
8. The COMMISSION is requested, with a view to making full use of Directive 2014/41/EU on the European Investigation Order in Criminal Matters ("the EIO Directive") for the purposes of securing and obtaining e-evidence in the EU, to continue monitoring and supporting Member States in the transposition process of this directive by 22 May 2017.
9. The MEMBER STATES are requested:
   - to ratify and implement fully the Convention on Cybercrime of 23 November 2001;
   - to swiftly transpose EIO Directive, at the latest by 22 May 2017;
   - to ensure sufficient capacity for handling MLA requests related to investigations in cyberspace and to provide relevant training to the staff on how to handle such requests;
   - to optimise the use of the existing 24/7 points of contact and to increase the use of joint investigation teams, in order to facilitate the sharing of information and/or accelerate the MLA proceedings.

III. RULES ON ENFORCEMENT JURISDICTION IN CYBERSPACE SHOULD BE REVIEWED.

To that end,

10. THE COMMISSION is requested, in the light of the political guidance provided by Ministers of Justice at the Council of June 2016 and in association with MEMBER STATES, EUROJUST and EUROPOL, to explore possibilities for a common EU approach on enforcement jurisdiction in cyberspace in situations where existing frameworks are not sufficient, e.g. situations where a number of information systems are used simultaneously in multiple jurisdictions to commit one single crime, situations where relevant e-evidence moves between jurisdictions in short fractions of time, or where sophisticated methods are used to conceal the location of e-evidence or the criminal activity, leading to "loss of location".[9]
11. While taking into account the specifics of each situation, the approach should determine:

    - which connecting factors can provide grounds for enforcement jurisdiction in cyberspace;
    - whether, and if so which investigative measures can be used regardless of physical borders.

12. Consideration is to be given to:

    - the nature and seriousness of the offences that might otherwise remain unpunished;
    - possible grounds for enforcement jurisdiction, i.e. on the basis of connecting factors such as for example the location of the headquarters of a service provider, the economic activity of a service provider in the investigating state i.e. when the service provider offers products or services on the territory of the investigating state ("business link"), the habitual residence and/or nationality of the accused or suspected person, and/or the location of the person affected;
    - the use and effectiveness of domestic production orders based on such possible connecting factors for enforcement jurisdiction in cyberspace;
    - a cooperation solution for direct trans-border access to data without technical assistance;
    - proper safeguards, such as the protection of fundamental rights and freedoms, personal data, and proportionality and subsidiarity as guiding principles for the use of investigative measures to guarantee their lawfulness;
    - possible analogies with other cross-border legal regimes e.g. the Treaty on Open Skies and the Convention on the Law of the Sea, EU rules on Data Protection and EU Competition Law;
    - the effect of such an approach on the existing legal framework.

THE COMMISSION is requested to report on process of the development of this approach by December 2016 and present the outcomes of this assessment by June 2017. The assessment should include specific elements for a common EU approach and proposals for its realisation, including the possibility to pursue a legislative initiative in this respect."

---

[9] These are mere examples. The Commission is requested to examine solutions that would address such or similarly serious situations which would justify such an approach.