



Council of the European Union
General Secretariat

Brussels, 02 August 2018

WK 8824/2018 REV 1

**DOCUMENT PARTIALLY ACCESSIBLE TO THE
PUBLIC (XX.XX.2021)**

LIMITE

**CYBER
COPEN
COPS
COSI
DATAPROTECT
IND
JAI
JAIEX
POLMIL
RELEX
TELECOM
DAPIX**

WORKING PAPER

This is a paper intended for a specific community of recipients. Handling and further distribution are under the sole responsibility of community members.

WORKING DOCUMENT

From:	Commission services
To:	Delegations
Subject:	Non-paper to support the discussion in the Horizontal Working Party on Cyber Issues

Delegations will find in Annex a non-paper by the Commission services which will be presented in the Horizontal Working Party on Cyber Issues on 17 July 2018.



Brussels, 2018-07-12

Limited

NON-PAPER TO SUPPORT THE DISCUSSION IN THE HWP CYBER ON 17 JULY

At the meeting of the Horizontal Working Part on Cyber Issues (HWP on Cyber) held on 28 October 2016, the Slovak Presidency presented a four-steps approach as a possible way forward to deal with the issue of encryption¹. One of the four steps invited the Commission to organise a reflection process for future work in the area. This approach was welcomed by the Coordinating Committee in the area of police and judicial cooperation in criminal matters (CATS) and during the Justice and Home Affairs Council of December 2016, Justice Ministers noted the importance of “*continuing the discussion to identify solutions that struck a balance between individual rights/citizens’ security and privacy and allowing law enforcement agencies to do their work*”².

With this in mind, the Commission launched an expert process in early 2017, engaging with relevant stakeholders in order to learn about the legal and technical issues relating to this area, identify relevant policy aspects and to assess options for possible solutions at the EU level. The Commission discussed the role of encryption in criminal investigations with a number of stakeholders, addressing both technical and legal aspects by engaging in discourse with experts from Europol, Eurojust, the European Judicial Cybercrime Network (EJCN), the European Union Agency for Network and Information Security (ENISA), the European Union Agency for Fundamental Rights (FRA) and law enforcement agencies of Member States, ministries, industry and various civil society organisations.

Law enforcement agencies confirmed that there is an increasing dependency on electronic evidence that is becoming harder to access due to wider use of encryption and an escalation in the number of applications providing encrypted services. It is envisaged that this trend may cause investigative measures to evolve significantly to better equip officers on the ground to functioning in such a cyber-environment. From a legal perspective, few Member States have addressed encryption in national legislation with little commonalities and convergence between the different legislative regimes. The Commission is mindful of the fact that as this area develops further, a clear balance between fundamental rights and security needs to be reached and maintained.

The 11th Security Union Progress Report (SUPR)³ set out a number of operational and practical measures to better defend citizens from terrorist threats and other serious and organised crime. Amongst these measures, a number of proposals related to supporting law enforcement and judicial authorities in tackling encryption in criminal investigations.

¹ Doc. 14711/16.

² Doc. 15391/16- Outcomes of the 3508th Council meeting of Justice and Home Affairs.

³ COM(2017) 608 final.

- The first priority in this series of shorter-term measures aims at assisting Europol to further develop their capabilities. As indicated in the 13th SUPR⁴, the Commission has transferred a one-time sum of EUR 5 million to Europol to allow for the setting up of decryption hardware for data-at-rest. This decision has been taken on the basis of an assessment that the Commission carried out with the support of EC3, and taking into account comments made by Member State experts in the area of encryption during the meeting held on September 2017, where the Commission sought Member States' views on possible measures to deal with encryption. This work is underway and is being taken forward in collaboration with the Commission's Joint Research Centre (JRC).
- Secondly, in order to support law enforcement and judicial authorities more adequately at the national level, the Commission is working to create a network of points of expertise, bringing together experts in the field from all Member States and setting up an information hub to facilitate collaboration and sharing of knowledge among these contact points.
- Thirdly, the Commission envisages the setting up of a toolbox of legal and technical instruments to be housed at EC3, providing experts working in the field with the possibility to tap into this resource. In order to ensure that the tools included in this toolbox are useful and relevant, the network of points of expertise should contribute to its development.
- EUR 500,000 are foreseen under the 2018 annual work programme for training in collaboration with the European Union Agency for Law enforcement Training (CEPOL) and European Cybercrime Training and Education Group (ECTEG), targeting law enforcement and judicial authorities in order to ensure that responsible officers are better prepared to deal with issues arising from encryption.
- The Commission believes that the importance of the role of service providers and other industry partners should be further highlighted. As its fifth measure the Commission will continue to support structured dialogues with industry and other businesses under the umbrella of the EU Internet Forum and also through the network of points of expertise. Such engagement will promote a better understanding of existing and evolving challenges in this area and possible avenues of mitigation.
- Finally, it is important to set up a continuous assessment of the technical and legal aspects surrounding the role of encryption in criminal investigations, especially given the constant developments in encryption techniques and its escalating use by criminals. The Commission will continue taking forward this work and also support the development of an observatory for this purpose in collaboration with EC3, the EJCN and Eurojust.

⁴ COM(2018) 46 final.

[Redacted]

[Redacted]

[Redacted]