Council of the European Union
General Secretariat

Brussels, 24 October 2018

WK 12742/2018 INIT

LIMITE

JAI
COPEN
CYBER
COSI
ENFOPOL

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 on the Role of Encryption in Criminal Investigations

Delegations find attached the non-paper from the Commission on the subject mentionned above.

Non-Paper to support the ongoing discussion with JHA Counsellors on the Role of Encryption in Criminal Investigations

1. Introduction

The abuse of encryption by criminals and terrorist suspects increasingly impedes law enforcement and judicial authorities from accessing electronic evidence in criminal investigations and potentially prevents authorities from initiating or completing investigations successfully. The increased availability and default use of encryption has played a major role in this trend, e.g. in applications offered by service providers, combined with the enhanced technological expertise of criminals and the growing range of criminal threats that materialise in digital environments.

During the Justice and Home Affairs Council of December 2016, -on the challenges to criminal justice arising from the use of encryption technologies- Justice Ministers noted the importance of taking the discussion forward to identify solutions striking a balance between individual rights/citizens' security and privacy and allowing law enforcement agencies to do their work[1].

The Commission, recognizing the important need for a balanced approach which takes into consideration policy related, political and technical factors, launched an expert process in early 2017, and engaged with relevant stakeholders in order to learn about the legal and technical issues surrounding this area, identify relevant policy aspects and assess options for possible solutions at the EU level.

A further call was made by the Head of State/Governments during the European Council of June 2017[2], tasking the Commission to work on addressing the challenges posed by systems that allow terrorists to communicate in ways that competent authorities cannot access, including those safeguarded by end-to-end encryption, whilst at the same time ensuring that the benefits such systems impart in relation to protection of privacy, data and communication are maintained.

The Commission discussed 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. The culmination of these discussions was presented in the 11th Security Union Progress Report[3] (SUPR) as a set of six operational and practical measures aimed at supporting law enforcement and judicial authorities in tackling the abuse of encryption in criminal investigations.

---

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

2 European Council Conclusions: EUCO 8/17.

3 COM(2017) 608 final.

The first priority in this set of measures aims at assisting Europol to further develop its capabilities in this context. As indicated in the 13th SUPR[4], the Commission has transferred a one-time sum of EUR 5 million to Europol to allow for the setting up of decryption capabilities for data-at-rest. 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, a network of points of expertise from Member States has been set up, the first meeting of which shall be convened shortly by Europol.

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.

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 with a view to ensuring that responsible officers are better prepared to deal with issues arising from the criminal abuse of encryption.

The Commission believes that industry partners have a key collaborative role to play in this discourse. For its fifth measure the Commission committed to facilitating structured dialogues with industry, civil society organisation and academia under the umbrella of the EU Internet Forum. This engagement is underway and a first round of discussions has been successfully concluded. The Commission plans to host a second round of dialogues focusing on attaining a more in-depth understanding of specific thematic issues that have been brought to light during the initial discussions.

Finally, the Commission is supporting Europol and Eurojust in their work on a joint forward-looking observatory function that is monitoring the legal and technical evolution of the topic. The publication of a first report is expected during the last quarter of 2018.

[4] COM(2018) 46 final.

2. Problem Definition

According to Europol's annual Internet Organised Crime Threat Assessment (IOCTA), Member States report an alarming rise in the use of encryption by criminals to protect stored data, hide their location and obfuscate financial transactions as well as an increased use of encryption for communication purposes. The 2018 IOCTA also highlights the active abuse of encryption by criminals for ransomware attacks. The results of discussions initiated by the Slovak Presidency during the second half of 2016 confirms that the majority of Member States encounter encryption-related difficulties in the context of criminal investigations.

At present, a variety of legal setups remain at play across Member States, with a number of national law enforcement agencies having the legal possibility to carry out lawful interception in accordance with national legislation whilst for other Member States, the process of lawful interception remains within the domain of security services. Furthermore, in those Member States in whose legislation it is possible to carry out lawful interception, various levels of preparedness come into play, some already having technical capabilities in place, whereas others currently do not have the opportunity of carry out such interception due to financial and other restrictions.

Europol and the Commission have facilitated dialogues between Member States' operational security experts and Justice and Home Affairs (JHA) Counsellors on the possibility of focusing on solutions that would not prohibit, limit or weaken encryption. Member States' experts were made aware of the technical capabilities of a potential measure to address end-to-end encryption. On the basis of the information provided, representatives of Member States at the Horizontal Working Party on Cyber Issues of 21 July 2018 expressed support in principle for the implementation of such a solution and asked that a further discussion is taken at the appropriate level in Council.

3. Possible way forward

If a consensus among Member States is reached on the way forward, the Commission would consider how in practice to support Member States and the European Cybercrime Centre at Europol (EC3) in order to go forward with the development of such capabilities. This way forward would ensure that Member States whose law enforcement agencies have the legal possibility to utilise special investigative techniques, are not limited in doing so by a lack of technical expertise or limiting budgetary considerations.

To this end, the Commission services are looking into the creation of a comprehensive, integrated approach through the setting out of a balanced package of measures that include amongst others, the technical capability in the form of a Pilot Project, and the setting up of a governance structure to frame the use and to specify the necessary safeguards and parameters of the solution. The outcomes of this approach would be presented in a report to Council and Parliament.

3.1 Technical information

The envisaged solution would allow for the development of the necessary capabilities at Europol to support Member State lawful interception regimes. Such regimes would provide lawful access to relevant data in the context of criminal investigations before the data becomes encrypted. This would be supported by appropriate safeguards as well as measures to ensure oversight and transparency while following the basic principles of legality, proportionality and necessity, making certain techniques a measure of last resort, whilst respecting the fundamental rights of both current and potential subjects.

Depending on Member State requirements, the solution would offer capacities to support several Member State investigations in parallel.

Purchasing the solution "as-a-service" would provide support to Member State lawful interception regimes if and when needed in the context of criminal investigations. With this in mind, Europol has already held exploratory technical discussions with Member States' Operational Security experts. The actual scope and capabilities of the solution would be defined in cooperation with Member State experts as part of the tendering process for the purchasing of the solution.

The funding provided to Europol would allow for such a solution to be rigorously tested in pilot format prior to considering the permanent inclusion of this functionality to support Member State lawful interception regimes within Europol's budget. A final decision in this regard would be taken following thorough consideration of data protection and fundamental human rights concerns, and be based on a thorough evaluation of the solution's feasibility, risk implications, value of output and user experience.

3.2 Governance

In accordance with EU and national legislation and the guiding principles of proportionality, legality and necessity, the setting up and use of such capabilities should be governed by strict oversight regimes to ensure transparency and accountability and to uphold fundamental rights while achieving an effective and genuine Security Union.

Throughout discussions facilitated by the Commission in relation to encryption in the context of criminal investigations, a number of Member States voiced concerns with respect to the governance guiding the setting up and use of such a tool. The governance can be clearly divided in three phases regulating the preparatory, implementation and follow-up aspects of this tool.

Preparatory Phase

A restricted procedure[5] would be used for the purchasing of such a solution. In response to interest by Member States to be involved in the procedure, Europol would take into strong consideration the advice of operational security experts in order to ensure that the solution meets the specific needs of Member States and provides all the capabilities required to make it fit for purpose. In order to achieve this, Europol would aim at obtaining high quality involvement of Member States through a number of expert meetings as needed, to achieve the mentioned goal. Moreover, and in order to ensure that all Member States have been provided opportunity to contribute in the drafting of the tender, operational experts would be asked to assess the draft tender, and propose feasible changes.

Implementation Phase

A clear framework to guide the use of the tool under discussion should be elaborated in complementarity with the obligations set out under Europol's Regulation on the management of data. The management of the data would follow the same principles, use the same safeguards and fall under the same rules as any other operational data handled by Europol to ensure its confidentiality, integrity and availability.

Formal requests by Member States' law enforcement agencies to make use of such tool are to be lodged through the appropriate communication channels using Europol's Secure Information Exchange Network Application (SIENA) and would be treated in accordance with national legislative processes and safeguards governing each Member States' use of special investigative techniques. In particular, the use of a court order or similar documentation as per national legal regime should be made mandatory, with subjection of such documentation to consideration and scrutiny by Europol, to ensure their legality, proportionality, necessity and that such a request was being put forward for the use of investigative purposes relating to serious and organised crime and terrorism affecting more than one Member State. The use of such measures, similarly to any other form of lawful interception should be covered by measures of redress and means of ensuring that the rights of the individual on whom the solution is used would be safeguarded. To this end, the Commission services and Europol would also review the proposed governance architecture with FRA in order to ensure that it respects fundamental human rights.

The implementation of a rigorous technical check to ensure that the solution was functioning as expected would also be included in the governance architecture once the properties of the solution under discussion were defined. This would provide further assurance to users that the rights of the individual under investigation were being protected, and that data was produced and preserved in a way that it could be made admissible in Court.

---

5 Paragraph 1(b) of Article 164 of the Regulation (EU, Euratom) 2018/1046 of the European Parliament and of the Council of 18 July 2018 on the financial rules applicable to the general budget of the Union

Follow-up Phase

Upon termination of the application of the concrete measure, national procedures within the Member States' criminal codes would have to be applied to ensure the continued protection of the affected individual's fundamental right to privacy and secrecy of correspondence. To this end, it would remain within the Member State's responsibility to disclose information relating to the data obtained through the technical solution as per the national legal regime of that Member State.

4. Funding

Should Member States express stronger support for this approach, the Commission services would explore possible avenues to provide the required funding to Europol to run this project. The funding would cover the development of technical capabilities required to build up capacity commensurate with Member States' needs for the duration of the Pilot Project under discussion. The Commission would then decide on whether it wished to pursue this Pilot Project.

5. Evaluation

The evaluation of the solution and governance process elaborated within this document would commence 12 months after first operational use of the solution. Europol shall be responsible for gathering and holding statistics in relation to:

- The number of applications for use per Member State
- The types of crime involved

Member States benefiting from the solution would be expected to supplement the statistical data being gathered by providing information on:

- The number of applications resulting in successful convictions in a Court of Law
- The number of cases successfully challenged in Court by the affected user

Furthermore an expert focus group would be run by Europol, bringing together users of the tool and operational experts in the area of encryption from Member States to discuss user experience, on the basis of which together with the statistical data gathered, a report would be drawn up by Europol and presented to Commission services.

6. Next Steps

The practical measures listed within the 11th Security Union Progress report and the possible solution under discussion to support Member State lawful interception regimes are aimed at achieving progress in this area in the short and medium term. The use of encryption-by-default continues to be included in a number of applications, particularly those used for the purpose of communication, and the sophistication of encryption technology is on the rise.

The Commission will continue working to answer the call made by Heads of State and Governments during the European Council of June 2017[6] through a comprehensive and integrated approach to efforts countering challenges posed by encryption in the context of criminal investigations, whilst upholding the commitments made to not limit, weaken or ban encryption in general. The engagement with key parts of industry, human rights and civil society organisations, the European Data Protection Supervisor, and other trusted partners remains of great importance in this context. The Commission will continue to invest in in-depth dialogue with stakeholders, and look into the evolution of standardisation in this area as part of a longer-term response emanating from the collective of initiatives presented in this paper. The output of the observatory function delegated to Europol and Eurojust, will also be an important contribution.

Should the Commission decide to proceed with the Pilot Project, it would provide a report to Council and Parliament 18 months after the first operational use of the solution in question. The report would be accompanied by a set of recommendations to further the setting up of long-term solutions that do not run counter to fundamental human rights and the integrity of the digital single market.

---

[6] Heads of State/Government called for "*addressing the challenges posed by systems that allow terrorists to communicate in ways that competent authorities cannot access, including end-to-end encryption, while safeguarding the benefits these systems bring for the protection of privacy, data and communication.* (EUCO 8/17- Conclusions of the European Council meeting of 22-23 June 2017).