Council of the European Union
General Secretariat
Directorate-General Communication and Information - COMM
Directorate Information and Outreach
Information Services Unit / Transparency
Head of Unit

Brussels, 9 September 2021

Mr Stefan Soesanto
Email: ask+request-9819-954ababf@asktheeu.org

Ref. 21/1378-rh-vl/ns

Request made on: 29.07.2021
Deadline extension: 19.08.2021

Dear Mr Soesanto,

Thank you for your request for access to documents of the Council of the European Union.[1]

Please find attached document **WK 5255/18**.

You will also find attached partially accessible versions of documents **WK 8824/18 REV 1** and **WK 6758/18 REV 2**.[2] However, I regret to inform you that full access cannot be given for the reasons set out below.

Document **WK 8824/18 REV 1** of 2 August 2018 is a working document from the Commission services to delegations containing a *Non-paper to support the discussion in the Horizontal Working Party on Cyber Issues*. It concerns a sensitive issue which is still under discussions within the Council.

In order to support the Council, in delivering on the resolution on encryption adopted by the Council in December 2020, the European Commission is working together with the Member States to identify technical, operational, and legal solutions to ensure lawful access to encrypted information, while maintaining the effectiveness of encryption in protecting privacy and security of communications.

1 The General Secretariat of the Council has examined your request on the basis of the applicable rules: Regulation (EC) No 1049/2001 of the European Parliament and of the Council regarding public access to European Parliament, Council and Commission documents (OJ L 145, 31.5.2001, p. 43) and the specific provisions concerning public access to Council documents set out in Annex II to the Council's Rules of Procedure (Council Decision No 2009/937/EU, OJ L 325, 11.12.2009, p. 35).

2 Article 4(6) of Regulation (EC) No 1049/2001.

This process involves an analysis of existing capabilities and approaches for lawful and targeted access to encrypted information in the context of investigations and prosecutions by the Member States. Thus, having consulted with the originating source of the document, the General Secretariat is of the opinion that the full disclosure of the document **WK 8824/18 REV 1** would cause difficulties for Member States to participate in this ongoing process.

Full disclosure of the document at this stage would therefore seriously undermine the decision-making process of the Council. As a consequence, the General Secretariat has to refuse full access to this document.[1]

Document **WK 6758/18 REV 2** of 7 June 2018 is a working document from the General Secretariat of the Council to delegations on *Draft Council Conclusions on EU Coordinated response to Large Scale Cybersecurity Incidents and Crises - Comments from Member States (CZ, DE, ES, FR, LV, LT, NL and SE)*. The document directly deals with the EU cybersecurity crisis management framework to Large scale cybersecurity incidents and crisis.

Full release of the information contained in the document would jeopardise the public security by revealing sensitive revisions reflecting national views, positions, ideas and comments of some Member States at a particular period of time and a particular revision of the document.

Therefore, having consulted with the originating sources of the document, the General Secretariat is of the opinion that full disclosure of the document would undermine the protection of the public interest as regards public security. As a consequence, the General Secretariat has to refuse access to this document.[3]

Having examined the context in which documents **WK 8824/18 REV 1** and **WK 6758/18 REV 2** were drafted, on balance the General Secretariat could not identify any evidence suggesting an overriding public interest in their full disclosure.

I regret to inform you that access to documents **WK 2429/18, WK 2641/18, WK 7839/18, WK 14758/18** and **WK 15391/18** cannot be given for the reasons set out below.

Document **WK 2429/18** of 27 February 2018 is a working document from the General Secretariat of the Council to delegations containing *INTCEN presentation on NotPetya* given at the Horizontal Working Party on Cyber Issues meeting by the EU Intelligence and Situation Centre (INTCEN) - Hybrid Fusion Cell.

Document **WK 2641/18** of 2 March 2018 is a working document from the European External Action Service to the Horizontal Working Party on Cyber issues on *EU response to NotPetya malicious cyber activity.*

---

[1] Article 4(3), first subparagraph, of Regulation (EC) No 1049/2001.
3 Article 4(1)(a), first indent, of Regulation (EC) No 1049/2001.

Document **WK 7839/18** of 27 June 2018 is a working document from the European External Action Service to delegations containing a *Non-paper on 'Attribution in the context of the Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ("cyber diplomacy toolbox").*

We have carefully considered and examined whether public access can be granted in the framework of Regulation 1049/2001 to the documents. We have come to the conclusion that public access cannot be given to these documents pursuant to Article 4(1)(a), first indent, of the Regulation 1049/2001 (protection of public security), Article 4(1)(a)(3) (protection of international relations and pursuant to Article 4(3), second subparagraph, since disclosure would also seriously undermine the decision making process of the Council.

Document **WK 2429/18** contains information based on classified contributions from EU Member States intelligence and security services which indicates that the documents may contain information and material a disclosure of which could harm the essential interests of the European Union or of one or more of its Member States. Disclosure would risk endangering the sources and methods through which the information was collected in the Member States. If even partially released, it would lead to a serious breach of trust between the INTCEN and the contributing Member States, which could result in Member States refusing to contribute to INTCEN assessments. That would deprive the EU institutions of crucial information in this field which they need in order to execute their policy. The discloser of this document would represent a risk to INTCEN decision making process and international relations. It is vital to protect this information and analysis, and any data that might indicate, even indirectly, how intelligence and security services compile such information.

Document **WK 2641/18** provides options for an EU response in the context of the framework for a joint EU diplomatic response to malicious cyber activities (“cyber diplomacy toolbox”) for discussion among Member States on a specific case. The document provides an insight in the options available, and includes an assessment of their possible impact. Disclosure of such details would have harmful consequences. The disclosure of the options paper would expose the margin of manoeuvre available when using the cyber diplomacy toolbox. If the options paper is released to the public domain, adverse actors to the EU would be able to get familiar with the internal logic behind the EU decision-making not only in this matter, but also in other areas where EU wishes to use Common Foreign and Security Policy measures to respond to malicious behaviour. In consequence, those adverse actors would adapt their activities in a way to minimise the effectiveness and the impact of the envisaged EU action.

Document **WK 7839/18** provides a way how the EU could foresee to attribute malicious cyber activities. As such, disclosure of these consideration could provide valuable information to adverse actors about how the EU forms decisions on joint diplomatic responses and attribution of malicious cyber activities. In consequence, those adverse actors could adapt their activity in order to hinder a decision on attribution, which would in consequence lose its desired effect.

Document **WK 14758/18** and **WK 15391/18** are two working documents drawn up by the Presidency containing a compilation of comments on the Cyber Diplomacy Toolbox as regards

respectively a) options for a restrictive measures framework to respond to or deter cyber activities that threaten the security or foreign policy interests of the Union or its Member States, and b) the implementation of the Framework for a joint EU diplomatic response to malicious cyber activities.[4] Having due regard to the outcome of our consultation with the services responsible for this policy matter, the release of the information therein contained cannot be disclosed as it would cause prejudice to public security and to the ongoing EU's strategic and diplomatic efforts in preventing, detecting and organising effective responses to counter cyber-threats.

We have also looked into the possibility of releasing parts of documents **WK 2429/18, WK 2641/18, WK 7839/18, WK 14758/18** and **WK 15391/18**.[5] However, as the exceptions to the right of access applies to their entire content, the General Secretariat is unable to give partial access at this stage.

Having examined the context in which these documents were drafted, on balance the General Secretariat could not identify any evidence suggesting an overriding public interest in their disclosure.

Pursuant to Article 7(2) of Regulation (EC) No 1049/2001, you may ask the Council to review this decision within 15 working days of receiving this reply. Should you see the need for such a review, you are invited to indicate the reasons thereof.[6]

Yours sincerely,

Fernando FLORINDO

Enclosures: 3.

4 See background information in https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02019D0797-20201124&qid=1620137455138 and document 10474/17 (Council Conclusions on 19 June 2017, downloadable from the public register of Council documents).

5 Article 4(6) of Regulation (EC) No 1049/2001.

6 Council documents on confirmatory applications are made available to the public. Pursuant to data protection rules at EU level (Regulation (EU) No 2018/1725, if you make a confirmatory application your name will only appear in related documents if you have given your explicit consent.