Council of the
European Union

Brussels, 4 June 2021
(OR. en)

9394/21

INF 168
API 92

NOTE

From:	General Secretariat of the Council
To:	Working Party on Information
Subject:	Public access to documents - Confirmatory application No 25/c/01/21

Delegations will find attached:

- the request for access to documents sent to the General Secretariat of the Council on 24 February 2021 and registered on the same day (Annex 1);
- the reply from the General Secretariat of the Council dated 28 May 2021 (Annex 2);
- the confirmatory application dated 1 June 2021 (Annex 3).

ANNEX 1

[E-mail message sent to access@consilium.europa.eu on 24 February 2021 - 00:45]

Dear Council of the European Union,

Under the right of access to documents in the EU treaties, as developed in Regulation 1049/2001, I am requesting access to the following documents:

- WK 14056 2019 INIT - Cyber Diplo TTX 2019 Survey results and lessons learned

- WK 12995 2019 INIT - CYBER DIPLO TTX 19: Cyber Diplomacy Toolbox – Visualisation

- WK 12992 2019 INIT - CYBER DIPLO TTX 19: Europol contribution

- WK 12988 2019 INIT - CYBER DIPLO TTX 19

- WK 12987 2019 INIT - CYBER DIPLO TTX 19: Commission contribution on the Blueprint

- WK 12985 2019 INIT - CYBER DIPLO TTX 19: Framework for a joint EU diplomatic response to malicious cyber activities "cyber diplomacy toolbox"

- WK 12984 2019 INIT - CYBER DIPLO TTX 19: Intelligence Support

- WK 9643 2019 INIT - Outreach engagement to support the EU Cyber Diplomacy efforts

- WK 6958 2019 INIT - Narrative paper on a vision for an open, free, stable and secure cyberspace by EEAS

- WK 3547 2019 INIT - Innovation in fighting cybercrime

- WK 3085 2019 INIT - Cyber Rapid Response Teams and Mutual Assistance in Cyber Security

- WK 1298 2019 INIT - Recent cyber threats and trends - APT 10 - Background of a cyber threat

- WK 215 2019 INIT Cyber Diplomacy Toolbox – 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

Yours faithfully,

DELETED

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, 28 May 2021

DELETED
Email: **DELETED**

Ref. 21/0471-vl/nb-ADD

Request made on: 24.02.2021
Deadline extension: 17.03.2021

1st reply letter: 12.04.2021

Dear **DELETED**,

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

As a complement to our initial reply on 12 April 2021, and with our apologies for this late answer caused by the delay in receiving feedback from the departments of the European External Action Service (EEAS) who had produced the documents concerned, please find here below the conclusions reached by the General Secretariat of the Council as regards the remaining documents that you had requested (**WK 1298/2019**, **WK 9643/2019**, **WK 12984/2019**, **WK 12985/2019**, **WK 12987/2019**, **WK 12988/2019**, **WK 12995/2019 and 14056/2019**).

You may have full access to documents **WK 12985/2019** and **WK 12987/2019**.

[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).

Moreover, please find attached a partially accessible version of documents **WK 9643/2019 and WK 12988/19**.[2]

- As regards document **WK 9643/2019**, you may have access to the whole text, with the exception of one entry in the table at page 3;
- As regards document **WK 12988/2019**, the disclosed parts are pages 1 to 3, 8, 11, 13, 16 and 17
- The undisclosed parts of these two documents contain sensitive information that, having due regard to the outcome of our consultations with the EEAS, if released to the wide public would undermine the protection of public interest as regards public security and international relations.[3]

Finally, we regret to inform you that access to documents **WK 1298/2019, WK 12984/2019, WK 12995/2019** and **14056/2019** cannot be given for the reasons set out below.

Document **WK 1298/2019** focuses on recent cyber threats and trends and contains background info on a cyber-threat delivered by the EEAS services at a meeting of the Horizontal Working Party (HWP) on Cyber issues on 28 January 2019.

Documents **WK 12984/2019** and **WK 12995/2019** contain two presentations, respectively on Intelligence support and on the organisational interconnections among the key actors in the context of a Cyber-related exercise delivered, given at a meeting of the abovementioned Working Party on 7 November 2019.

Document **WK 14056/2019** contains the results of an internal survey and lessons learned from the abovementioned exercise, forwarded by the EEAS to the HWP meeting on 5 December 2019.

These documents contain information of a sensitive and delicate diplomatic nature. In the light of our consultations, the General Secretariat is of the opinion that their release to the wide public cannot be authorized, since it would reveal valuable strategic details to adverse actors about how the EU designs and exercises its engagement in this field, including through joint diplomatic responses to malicious cyber activities and the pitfalls and available margins of manoeuvring.

Moreover, information gathering by national intelligence and security services in this regard, and the analysis of this information by the responsible authorities at national level and at EU level, are vital to protecting the public from a serious threat

Hence, disclosure would allow hostile entities/actors to become familiar with the internal logic and the strategic approach of the EU to these sensitive matters and carry out activities undermining the EU's ability to and efficiency in designing future responses to cyber threats, causing prejudice to public security, to the effectiveness of the EU and its Member States in this framework and to the relations with the EU's international partners.

---

2 Article 4(6) of Regulation (EC) No 1049/2001.
3 Article 4(1), first and third indent, of Regulation (EC) No 1049/2001.

Consequently, public access to documents **WK 1298/2019, WK 12984/2019, WK 12995/2019** and **14056/2019** cannot be granted.(1)

We have also looked into the possibility of releasing parts of these four documents.[4] However, as the exception to the right of access applies to their entire content, the General Secretariat is unable to give partial access.

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.[5]

Yours sincerely,

Fernando FLORINDO

Enclosures: 4

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

5 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.

[E-mail message sent to access@consilium.europa.eu on 1 June 2021 - 14:33]

Dear Council of the European Union,

Please pass this on to the person who reviews confirmatory applications.

I am filing the following confirmatory application with regards to my access to documents request '2019 HWP on Cyber Working Papers'.

On Friday, May 28, 2021, at 8:31AM, the General Secretariat of the Council mistakenly uploaded 9 files onto the AsktheEU.org platform as a belated follow-up answer to my request. The upload included four files to which the Council refused access to (WK 1298/2019, WK 12984/2019, WK 12995/2019 and 14056/2019), as well one file the Council's explanatory letter did not mention at all (WK 215/2019 INIT).

For more than 72 hours, the files were publicly accessible and were indeed widely downloaded by a array of cybersecurity and policy researchers, as well as journalists from across the world interested in the released documents. The Council notably fixed its mishap at around 12:41 on Monday, May 31, 2021, when it requested the deletion of its May 28 reply and replaced it with a reply that encompassed the correct document batch.

Given these unfortunate circumstances, and to avoid that cybersecurity/policy researchers living in the EU are ethically prevented from discussing and utilizing these still classified EU documents in their research endeavors - while others outside the EU will face no such ethical conundrums - it might be prudent for the Council and the EEAS to revisit their decision on not granting public access to documents WK 1298/2019, WK 12984/2019, WK 12995/2019, 14056/2019, and WK 215/2019.

A full history of my request and partial correspondence (notably the absence of the now deleted reply by the Council on May 28) is available on the Internet at this address: **DELETED**

Yours faithfully,

DELETED