Council of the
European Union

Brussels, 23 September 2020
(OR. en)

11070/20

INF 163
API 111

NOTE

From:	General Secretariat of the Council
To:	Working Party on Information
Subject:	Public access to documents - Confirmatory application No 21/c/01/20

Delegations will find attached the:

- request for access to documents sent to the General Secretariat of the Council on 8 August 2020 and registered on 10 August 2020 (Annex 1);
- reply from the General Secretariat of the Council dated 21 September 2020 (Annex 2);
- confirmatory application dated 22 September 2020 and registered on 23 September 2020 (Annex 3).

[E-mail message sent to access@consilium.europa.eu on 8 August 2020 - 03:27]

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 documents which contain the following information:

(1) ST 5807 2019 INIT - 06-02-2019
(2) ST 13580 2018 INIT - 30-10-2018
(3) ST 12770 2017 INIT - 02-10-2017
(4) ST 8146 2017 REV 1 - 08-05-2017

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, 21 September 2020

Mr **DELETED**
Email: **DELETED**

Ref. 20/1431-rh/vk

Request made on: 08.08.2020
Registered on: 10.08.2020
Deadline extension: 31.08.2020

Dear Mr **DELETED**,

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

Please find attached document **8146/17 REV1**.

I regret to inform you that access to document **12770/17** cannot be given for the reasons set out below.

Document **12770/17** is a classified document, bearing the classification "RESTREINT UE". This means that the unauthorised disclosure of its contents could be disadvantageous to the interests of the European Union or of one or more of its Member States.[2]

[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] Council Decision of 23 September 2013 on the security rules for protecting EU classified information (2013/488/EU), OJ L 274, 15.10.2013, p. 1.

It is a note from the EEAS to the Political and Security Committee (PSC) containing *Military Advice on the operational impact of recent Cyber attacks on Operation AIFOS and on possible options to mitigate the situation.* This exercise related document contains horizontal information on the organisation of operation AIFOS.

After consulting the European External Action Service (EEAS)[3], the General Secretariat of the Council has come into the following conclusion.

Release of the information contained in this document would reveal to third parties the sensitive details of Operation AIFOS. This would affect the efficiency of the European Union's action and question the feasibility of similar operations in the future.

Disclosure of the document would therefore undermine the protection of the public interest as regards defence and military matters. As a consequence, the General Secretariat has to refuse access to this document. [4]

Moreover, I regret to inform you that access to documents **5807/19** and **13580/18** cannot be given for the reasons set out below.

Document **5807/19** of 6 February 2019 is a note from the EEAS on 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*. It provides options for cyber sanctions when the framework for cyber sanctions was under discussion, and relates both to the specific case of cyber sanctions but also to sanctions in general.

Sanctions are part of the EU's Common Foreign and Security Policy, and as such the document contains information of a sensitive and delicate diplomatic nature which should not be made public. 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 imposing sanctions. 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 impose sanctions. In consequence, those adverse actors would adapt their activities in a way to minimise the effectiveness and the impact of the envisaged sanction regimes.

3 Article 4(4) of Regulation (EC) No 1049/2001.
4 Article 4(1)(a), second indent, of Regulation (EC) No 1049/2001.

Document **13580/18** of 30 October 2018 - C*ommon messages in the context of the framework for a joint EU diplomatic response to malicious cyber activities* is a classified document, bearing the classification "RESTREINT UE". This means that the unauthorised disclosure of its contents could be disadvantageous to the interests of the European Union or of one or more of its Member States.[5]

It provides an insight in the way how the EU responds to malicious cyber activities. As such, disclosure of these messages could provide valuable information to adverse actors about how the EU forms joint diplomatic responses to malicious cyber activities. In consequence, those adverse actors could adapt their activity in order to hinder the joint EU diplomatic response, which would in consequence loose its desired effect.

Therefore, having consulted the originating source of both documents, the General Secretariat of the Council is of the opinion that public access cannot be given to these documents pursuant to Article 4(1)(a), third indent, of the Regulation 1049/2001 (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. As a consequence, the General Secretariat has to refuse access to these documents.

We have also looked into the possibility of releasing parts of the above-mentioned documents.[6] However, as the information contained in the documents forms an inseparable whole, 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.[7]

Yours sincerely,

Fernando FLORINDO

Enclosure: 1

---

5 Council Decision of 23 September 2013 on the security rules for protecting EU classified information (2013/488/EU), OJ L 274, 15.10.2013, p. 1.

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

7 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.

ANNEX 3

[e-mail message sent to access@consilium.europa.eu on 22 September 2020 - 15:04]

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 'Document requests: Cyber-related'.

Access to Document 5807/19 of 6 February 2019 was refused due to:
(1) its sensitive and delicate nature,
(2) harmful consequences,
(3) exposing the margins of manoeuvre available when imposing sanctions,
(4) allowing adversaries to gain familiarity with the internal logic of EU-decision making, and
(5) enable actors to minimize the effectiveness and impact of the envisaged sanction regimes.

On point 1: Given that the document was not classified, the "sensitive and delicate nature" of said document seems to be a rather insufficient reason to refuse access.

On point 2: The notion of "harmful consequences" does not specify as to what kind of harmful consequences disclosure might cause, nor whom disclosure might inflict harm upon. As a general statement, "harmful consequences" might be applicable, but is a rather shaky argument for document access refusal.

On point 3: Given that the current EU cyber sanction regime (7299/19) encompasses only two sanction elements, i.e. travel restrictions (Article 4) and financial sanctions (Article 5), the "margins of maneuverability when imposing sanctions" has been set for the time being. Whether those margins might possibility change in the future should not be grounds from barring access to 1.5 year old document.

On point 4: It is in the interest of both academic research, EU transparency, and EU citizen education alike to understand and follow EU decision-making processes on EU cyber sanctions. Whether this also allows adversarial actors to gain familiarity with said EU process should not be ground for non-disclosure. Similarly, the 'internal-logic' as laid down in 1.5 year old document might have changed and is thus not anymore reflecting current positions and logics.

On point 5: The argument that disclosure might "minimize the effectiveness and impact of the envisaged sanction regimes" seems to be rather theoretical. If the effectiveness and impact of future sanction regimes can be minimized due to the mere knowledge of what is written in 5807/19 then those measures seem to be easily circumventable in practice. If this is true, then their effectiveness and impact will by design be rather limited or non-existent.

A full history of my request and all correspondence is available on the Internet at this address:
DELETED

Yours faithfully,

DELETED