►**B**

COUNCIL DECISION (CFSP) 2019/797

of 17 May 2019

concerning restrictive measures against cyber-attacks threatening the Union or its Member States

(OJ L 129I, 17.5.2019, p. 13)

Amended by:

		Official Journal		
		No	page	date
►**M1**	Council Decision (CFSP) 2020/651 of 14 May 2020	L 153	4	15.5.2020
►**M2**	Council Decision (CFSP) 2020/1127 of 30 July 2020	L 246	12	30.7.2020
►**M3**	Council Decision (CFSP) 2020/1537 of 22 October 2020	L 351 I	5	22.10.2020
►**M4**	Council Decision (CFSP) 2020/1748 of 20 November 2020	L 393	19	23.11.2020

Corrected by:

►**C1** Corrigendum, OJ L 230, 17.7.2020, p. 36 (2019/797)

▼B

COUNCIL DECISION (CFSP) 2019/797

of 17 May 2019

concerning restrictive measures against cyber-attacks threatening the Union or its Member States

Article 1

1. This Decision applies to cyber-attacks with a significant effect, including attempted cyber-attacks with a potentially significant effect, which constitute an external threat to the Union or its Member States.

2. Cyber-attacks constituting an external threat include those which:

(a) originate, or are carried out, from outside the Union;

(b) use infrastructure outside the Union;

(c) are carried out by any natural or legal person, entity or body established or operating outside the Union; or

(d) are carried out with the support, at the direction or under the control of any natural or legal person, entity or body operating outside the Union.

3. For this purpose, cyber-attacks are actions involving any of the following:

(a) access to information systems;

(b) information system interference;

(c) data interference; or

(d) data interception,

where such actions are not duly authorised by the owner or by another right holder of the system or data or part of it, or are not permitted under the law of the Union or of the Member State concerned.

4. Cyber-attacks constituting a threat to Member States include those affecting information systems relating to, inter alia:

(a) critical infrastructure, including submarine cables and objects launched into outer space, which is essential for the maintenance of vital functions of society, or the health, safety, security, and economic or social well-being of people;

(b) services necessary for the maintenance of essential social and/or economic activities, in particular in the sectors of: energy (electricity, oil and gas); transport (air, rail, water and road); banking;

▼B

financial market infrastructures; health (healthcare providers, hospitals and private clinics); drinking water supply and distribution; digital infrastructure; and any other sector which is essential to the Member State concerned;

(c) critical State functions, in particular in the areas of defence, governance and the functioning of institutions, including for public elections or the voting process, the functioning of economic and civil infrastructure, internal security, and external relations, including through diplomatic missions;

(d) the storage or processing of classified information; or

(e) government emergency response teams.

5. Cyber-attacks constituting a threat to the Union include those carried out against its institutions, bodies, offices and agencies, its delegations to third countries or to international organisations, its common security and defence policy (CSDP) operations and missions and its special representatives.

6. Where deemed necessary to achieve CFSP objectives in the relevant provisions of Article 21 of the Treaty on European Union, restrictive measures under this Decision may also be applied in response to cyber-attacks with a significant effect against third States or international organisations.

Article 2

For the purposes of this Decision, the following definitions apply:

(a) ‘information systems’ means a device or group of interconnected or related devices, one or more of which, pursuant to a programme, automatically processes digital data, as well as digital data stored, processed, retrieved or transmitted by that device or group of devices for the purposes of its or their operation, use, protection and maintenance.

(b) ‘information system interference’ means hindering or interrupting the functioning of an information system by inputting digital data, by transmitting, damaging, deleting, deteriorating, altering or suppressing such data, or by rendering such data inaccessible.

(c) ‘data interference’ means deleting, damaging, deteriorating, altering or suppressing digital data on an information system, or rendering such data inaccessible; it also includes theft of data, funds, economic resources or intellectual property.

(d) ‘data interception’ means intercepting, by technical means, non-public transmissions of digital data to, from or within an information system, including electromagnetic emissions from an information system carrying such digital data.

▼B

Article 3

The factors determining whether a cyber-attack has a significant effect as referred to in Article 1(1) include any of the following:

(a) the scope, scale, impact or severity of disruption caused, including to economic and societal activities, essential services, critical State functions, public order or public safety;

(b) the number of natural or legal persons, entities or bodies affected;

(c) the number of Member States concerned;

(d) the amount of economic loss caused, such as through large-scale theft of funds, economic resources or intellectual property;

(e) the economic benefit gained by the perpetrator, for himself or for others;

(f) the amount or nature of data stolen or the scale of data breaches; or

(g) the nature of commercially sensitive data accessed.

Article 4

1. Member States shall take the measures necessary to prevent the entry into, or transit through, their territories of:

(a) natural persons who are responsible for cyber-attacks or attempted cyber-attacks;

(b) natural persons who provide financial, technical or material support for or are otherwise involved in cyber-attacks or attempted cyber-attacks, including by planning, preparing, participating in, directing, assisting or encouraging such attacks, or facilitating them whether by action or omission;

(c) natural persons associated with the persons covered by points (a) and (b),

as listed in the Annex.

2. Paragraph 1 shall not oblige a Member State to refuse its own nationals entry into its territory.

3. Paragraph 1 shall be without prejudice to the cases where a Member State is bound by an obligation of international law, namely:

(a) as a host country of an international intergovernmental organisation;

(b) as a host country to an international conference convened by, or under the auspices of, the United Nations;

(c) under a multilateral agreement conferring privileges and immunities; or

(d) pursuant to the 1929 Treaty of Conciliation (Lateran Pact) concluded by the Holy See (Vatican City State) and Italy.

▼B

4. Paragraph 3 shall be considered to apply also in cases where a Member State is host country of the Organization for Security and Co-operation in Europe (OSCE).

5. The Council shall be duly informed in all cases where a Member State grants an exemption pursuant to paragraph 3 or 4.

6. Member States may grant exemptions from the measures imposed under paragraph 1 where travel is justified on the grounds of urgent humanitarian need, or on grounds of attending intergovernmental meetings or meetings promoted or hosted by the Union, or hosted by a Member State holding the Chairmanship in office of the OSCE, where a political dialogue is conducted that directly promotes the policy objectives of restrictive measures, including security and stability in cyberspace.

7. Member States may also grant exemptions from the measures imposed under paragraph 1 where entry or transit is necessary for the fulfilment of a judicial process.

8. A Member State wishing to grant exemptions referred to in paragraph 6 or 7 shall notify the Council in writing. The exemption shall be deemed to be granted unless one or more of the Council members raises an objection in writing within two working days of receiving notification of the proposed exemption. Should one or more of the Council members raise an objection, the Council, acting by a qualified majority, may decide to grant the proposed exemption.

9. Where, pursuant to paragraphs 3, 4, 6, 7 or 8, a Member State authorises the entry into, or transit through its territory of persons listed in the Annex, the authorisation shall be strictly limited to the purpose for which it is given and to the persons directly concerned thereby.

Article 5

1. All funds and economic resources belonging to, owned, held or controlled by:

(a) natural or legal persons, entities or bodies that are responsible for cyber-attacks or attempted cyber-attacks;

(b) natural or legal persons, entities or bodies that provide financial, technical or material support for or are otherwise involved in cyber-attacks or attempted cyber-attacks, including by planning, preparing, participating in, directing, assisting or encouraging such attacks, or facilitating them whether by action or omission;

(c) natural or legal persons, entities or bodies associated with the natural or legal persons, entities or bodies covered by points (a) and (b),

as listed in the Annex, shall be frozen.

▼B

2. No funds or economic resources shall be made available directly or indirectly to or for the benefit of the natural or legal persons, entities or bodies listed in the Annex.

3. By way of derogation from paragraphs 1 and 2, the competent authorities of the Member States may authorise the release of certain frozen funds or economic resources, or the making available of certain funds or economic resources, under such conditions as they deem appropriate, after having determined that the funds or economic resources concerned are:

(a) ►C1 necessary to satisfy the basic needs of the natural or legal persons, entities or bodies listed in the Annex ◄ and dependent family members of such natural persons, including payments for foodstuffs, rent or mortgage, medicines and medical treatment, taxes, insurance premiums, and public utility charges;

(b) intended exclusively for the payment of reasonable professional fees or the reimbursement of incurred expenses associated with the provision of legal services;

(c) intended exclusively for the payment of fees or service charges for the routine holding or maintenance of frozen funds or economic resources;

(d) necessary for extraordinary expenses, provided that the relevant competent authority has notified the competent authorities of the other Member States and the Commission of the grounds on which it considers that a specific authorisation should be granted, at least two weeks prior to the authorisation; or

(e) to be paid into or from an account of a diplomatic or consular mission or an international organisation enjoying immunities in accordance with international law, insofar as such payments are intended to be used for official purposes of the diplomatic or consular mission or international organisation.

The Member State concerned shall inform the other Member States and the Commission of any authorisation granted under this paragraph.

4. By way of derogation from paragraph 1, the competent authorities of the Member States may authorise the release of certain frozen funds or economic resources, provided that the following conditions are met:

(a) the funds or economic resources are the subject of an arbitral decision rendered prior to the date on which the natural or legal person, entity or body referred to in paragraph 1 was listed in the Annex, or of a judicial or administrative decision rendered in the Union, or a judicial decision enforceable in the Member State concerned, prior to or after that date;

▼B

(b) the funds or economic resources will be used exclusively to satisfy claims secured by such a decision or recognised as valid in such a decision, within the limits set by applicable laws and regulations governing the rights of persons having such claims;

(c) the decision is not for the benefit of a natural or legal person, entity or body listed in the Annex; and

(d) recognition of the decision is not contrary to public policy in the Member State concerned.

The Member State concerned shall inform the other Member States and the Commission of any authorisation granted under this paragraph.

5. Paragraph 1 shall not prevent a natural or legal person, entity or body listed in the Annex from making a payment due under a contract entered into prior to the date on which that natural or legal person, entity or body was listed therein, provided that the Member State concerned has determined that the payment is not, directly or indirectly, received by a natural or legal person, entity or body referred to in paragraph 1.

6. Paragraph 2 shall not apply to the addition to frozen accounts of:

(a) interest or other earnings on those accounts;

(b) payments due under contracts, agreements or obligations that were concluded or arose prior to the date on which those accounts became subject to the measures provided for in paragraphs 1 and 2; or

(c) payments due under judicial, administrative or arbitral decisions rendered in the Union or enforceable in the Member State concerned,

provided that any such interest, other earnings and payments remain subject to the measures provided for in paragraph 1.

Article 6

1. The Council, acting by unanimity upon a proposal from a Member State or from the High Representative of the Union for Foreign Affairs and Security Policy, shall establish and amend the list set out in the Annex.

2. The Council shall communicate the decisions referred to in paragraph 1, including the grounds for listing, to the natural or legal person, entity or body concerned, either directly, if the address is known, or through the publication of a notice, providing that natural or legal person, entity or body with an opportunity to present observations.

3. Where observations are submitted, or where substantial new evidence is presented, the Council shall review the decisions referred to in paragraph 1 and inform the natural or legal person, entity or body concerned accordingly.

▼B

Article 7

1. The Annex shall include the grounds for listing the natural and legal persons, entities and bodies referred to in Articles 4 and 5.

2. The Annex shall contain, where available, the information necessary to identify the natural or legal persons, entities or bodies concerned. With regard to natural persons, such information may include: names and aliases; date and place of birth; nationality; passport and identity card numbers; gender; address, if known; and function or profession. With regard to legal persons, entities or bodies, such information may include names, place and date of registration, registration number and place of business.

Article 8

No claims in connection with any contract or transaction the performance of which has been affected, directly or indirectly, in whole or in part, by the measures imposed under this Decision, including claims for indemnity or any other claim of this type, such as a claim for compensation or a claim under a guarantee, in particular a claim for extension or payment of a bond, guarantee or indemnity, in particular a financial guarantee or financial indemnity, of whatever form, shall be satisfied, if they are made by:

(a) designated natural or legal persons, entities or bodies listed in the Annex;

(b) any natural or legal person, entity or body acting through or on behalf of one of the natural or legal persons, entities or bodies referred to in point (a).

Article 9

In order to maximise the impact of the measures set out in this Decision, the Union shall encourage third States to adopt restrictive measures similar to those provided for in this Decision.

▼M1

Article 10

This Decision shall apply until 18 May 2021 and shall be kept under constant review. It shall be renewed, or amended as appropriate, if the Council deems that its objectives have not been met.

▼B

Article 11

This Decision shall enter into force on the day following that of its publication in the *Official Journal of the European Union*.

▼B

ANNEX

List of natural and legal persons, entities and bodies referred to in Articles 4 and 5

▼M2

A. Natural persons

▼M4

	Name	Identifying information	Reasons	Date of listing
1.	GAO Qiang	Date of birth: 4 October 1983 Place of birth: Shandong Province, China Address: Room 1102, Guanfu Mansion, 46 Xinkai Road, Hedong District, Tianjin, China Nationality: Chinese Gender: male	Gao Qiang is involved in 'Operation Cloud Hopper', a series of cyber-attacks with a significant effect originating from outside the Union and constituting an external threat to the Union or its Member States and of cyber-attacks with a significant effect against third States. 'Operation Cloud Hopper' has targeted information systems of multi-national companies in six continents, including companies located in the Union, and gained unauthorised access to commercially sensitive data, resulting in significant economic loss. The actor publicly known as 'APT10' ('Advanced Persistent Threat 10') (a.k.a. 'Red Apollo', 'CVNX', 'Stone Panda', 'MenuPass' and 'Potassium') carried out 'Operation Cloud Hopper'. Gao Qiang can be linked to APT10, including through his association with APT10 command and control infrastructure. Moreover, Huaying Haitai, an entity designated for providing support to and facilitating 'Operation Cloud Hopper', employed Gao Qiang. He has links with Zhang Shilong, who is also designated in connection with 'Operation Cloud Hopper'. Gao Qiang is therefore associated with both Huaying Haitai and Zhang Shilong.	30.7.2020
2.	ZHANG Shilong	Date of birth: 10 September 1981 Place of birth: China Address: Hedong, Yuyang Road No 121, Tianjin, China Nationality: Chinese Gender: male	Zhang Shilong is involved in 'Operation Cloud Hopper', a series of cyber-attacks with a significant effect originating from outside the Union and constituting an external threat to the Union or its Member States and of cyber-attacks with a significant effect against third States.	30.7.2020

▼M4

	Name	Identifying information	Reasons	Date of listing
			‘Operation Cloud Hopper’ has targeted information systems of multi-national companies in six continents, including companies located in the Union, and gained unauthorised access to commercially sensitive data, resulting in significant economic loss. The actor publicly known as ‘APT10’ (‘Advanced Persistent Threat 10’) (a.k.a. ‘Red Apollo’, ‘CVNX’, ‘Stone Panda’, ‘MenuPass’ and ‘Potassium’) carried out ‘Operation Cloud Hopper’. Zhang Shilong can be linked to APT10, including through the malware he developed and tested in connection with the cyber-attacks carried out by APT10. Moreover, Huaying Haitai, an entity designated for providing support to and facilitating ‘Operation Cloud Hopper’, employed Zhang Shilong. He has links with Gao Qiang, who is also designated in connection with ‘Operation Cloud Hopper’. Zhang Shilong is therefore associated with both Huaying Haitai and Gao Qiang.	

▼M2

3.	Alexey Valeryevich MININ	Алексей Валерьевич МИНИН Date of birth: 27 May 1972 Place of birth: Perm Oblast, Russian SFSR (now Russian Federation) Passport number: 120017582 Issued by: Ministry of Foreign Affairs of the Russian Federation Validity: from 17 April 2017 until 17 April 2022 Location: Moscow, Russian Federation Nationality: Russian Gender: male	Alexey Minin took part in an attempted cyber-attack with a potentially significant effect against the Organisation for the Prohibition of Chemical Weapons (OPCW) in the Netherlands. As a human intelligence support officer of the Main Directorate of the General Staff of the Armed Forces of the Russian Federation (GU/GRU), Alexey Minin was part of a team of four Russian military intelligence officers who attempted to gain unauthorised access to the Wi-Fi network of the OPCW in The Hague, the Netherlands, in April 2018. The attempted cyber-attack was aimed at hacking into the Wi-Fi network of the OPCW, which, if successful, would have compromised the security of the network and the OPCW’s ongoing investigatory work. The Netherlands Defence Intelligence and Security Service (DISS) (Militaire Inlichtingen- en Veiligheidsdienst – MIVD) disrupted the attempted cyber-attack, thereby preventing serious damage to the OPCW.	30.7.2020

▼M2

	Name	Identifying information	Reasons	Date of listing
4.	Aleksei Sergeyvich MORENETS	Алексей Сергеевич МОРЕНЕЦ Date of birth: 31 July 1977 Place of birth: Murmanskaya Oblast, Russian SFSR (now Russian Federation) Passport number: 100135556 Issued by: Ministry of Foreign Affairs of the Russian Federation Validity: from 17 April 2017 until 17 April 2022 Location: Moscow, Russian Federation Nationality: Russian Gender: male	Aleksei Morenets took part in an attempted cyber-attack with a potentially significant effect against the Organisation for the Prohibition of Chemical Weapons (OPCW) in the Netherlands. As a cyber-operator for the Main Directorate of the General Staff of the Armed Forces of the Russian Federation (GU/GRU), Aleksei Morenets was part of a team of four Russian military intelligence officers who attempted to gain unauthorised access to the Wi-Fi network of the OPCW in The Hague, the Netherlands, in April 2018. The attempted cyber-attack was aimed at hacking into the Wi-Fi network of the OPCW, which, if successful, would have compromised the security of the network and the OPCW's ongoing investigatory work. The Netherlands Defence Intelligence and Security Service (DISS) (Militaire Inlichtingen- en Veiligheidsdienst – MIVD) disrupted the attempted cyber-attack, thereby preventing serious damage to the OPCW.	30.7.2020
5.	Evgenii Mikhaylovich SEREBRIAKOV	Евгений Михайлович СЕРЕБРЯКОВ Date of birth: 26 July 1981 Place of birth: Kursk, Russian SFSR (now Russian Federation) Passport number: 100135555 Issued by: Ministry of Foreign Affairs of the Russian Federation Validity: from 17 April 2017 until 17 April 2022 Location: Moscow, Russian Federation Nationality: Russian Gender: male	Evgenii Serebriakov took part in an attempted cyber-attack with a potentially significant effect against the Organisation for the Prohibition of Chemical Weapons (OPCW) in the Netherlands. As a cyber-operator for the Main Directorate of the General Staff of the Armed Forces of the Russian Federation (GU/GRU), Evgenii Serebriakov was part of a team of four Russian military intelligence officers who attempted to gain unauthorised access to the Wi-Fi network of the OPCW in The Hague, the Netherlands, in April 2018. The attempted cyber-attack was aimed at hacking into the Wi-Fi network of the OPCW, which, if successful, would have compromised the security of the network and the OPCW's ongoing investigatory work. The Netherlands Defence Intelligence and Security Service (DISS) (Militaire Inlichtingen- en Veiligheidsdienst – MIVD) disrupted the attempted cyber-attack, thereby preventing serious damage to the OPCW.	30.7.2020

▼M2

	Name	Identifying information	Reasons	Date of listing
6.	Oleg Mikhaylovich SOTNIKOV	Олег Михайлович СОТНИКОВ Date of birth: 24 August 1972 Place of birth: Ulyanovsk, Russian SFSR (now Russian Federation) Passport number: 120018866 Issued by: Ministry of Foreign Affairs of the Russian Federation Validity: from 17 April 2017 until 17 April 2022 Location: Moscow, Russian Federation Nationality: Russian Gender: male	Oleg Sotnikov took part in an attempted cyber-attack with a potentially significant effect against the Organisation for the Prohibition of Chemical Weapons (OPCW), in the Netherlands. As a human intelligence support officer of the Main Directorate of the General Staff of the Armed Forces of the Russian Federation (GU/GRU), Oleg Sotnikov was part of a team of four Russian military intelligence officers who attempted to gain unauthorised access to the Wi-Fi network of the OPCW in The Hague, the Netherlands, in April 2018. The attempted cyber-attack was aimed at hacking into the Wi-Fi network of the OPCW, which, if successful, would have compromised the security of the network and the OPCW's ongoing investigatory work. The Netherlands Defence Intelligence and Security Service (DISS) (Militaire Inlichtingen- en Veiligheidsdienst – MIVD) disrupted the attempted cyber-attack, thereby preventing serious damage to the OPCW.	30.7.2020

▼M3

7.	Dmitry Sergeyevich BADIN	Дмитрий Сергеевич БАДИН Date of birth: 15 November 1990 Place of birth: Kursk, Russian SFSR (now Russian Federation) Nationality: Russian Gender: male	Dmitry Badin took part in a cyber-attack with a significant effect against the German federal parliament (Deutscher Bundestag). As a military intelligence officer of the 85th Main Centre for Special Services (GTsSS) of the Main Directorate of the General Staff of the Armed Forces of the Russian Federation (GU/GRU), Dmitry Badin was part of a team of Russian military intelligence officers which conducted a cyber-attack against the German federal parliament (Deutscher Bundestag) in April and May 2015. This cyber-attack targeted the parliament's information system and affected its operation for several days. A significant amount of data was stolen and the email accounts of several MPs as well as of Chancellor Angela Merkel were affected.	22.10.2020

▼M3

	Name	Identifying information	Reasons	Date of listing
8.	Igor Olegovich KOSTYUKOV	Игорь Олегович КОСТЮКОВ Date of birth: 21 February 1961 Nationality: Russian Gender: male	Igor Kostyukov is the current Head of the Main Directorate of the General Staff of the Armed Forces of the Russian Federation (GU/GRU), where he previously served as First Deputy Head. One of the units under his command is the 85th Main Centre for Special Services (GTsSS), also known as 'military unit 26165' (industry nicknames: 'APT28', 'Fancy Bear', 'Sofacy Group', 'Pawn Storm' and 'Stron-tium'). In this capacity, Igor Kostyukov is responsible for cyber-attacks carried out by the GTsSS, including those with a significant effect constituting an external threat to the Union or its Member States. In particular, military intelligence officers of the GTsSS took part in the cyber-attack against the German federal parliament (Deutscher Bundestag) which took place in April and May 2015 and the attempted cyber-attack aimed at hacking into the Wi-Fi network of the Organisation for the Prohibition of Chemical Weapons (OPCW) in the Netherlands in April 2018. The cyber-attack against the German federal parliament targeted the parliament's information system and affected its operation for several days. A significant amount of data was stolen and email accounts of several MPs as well as of Chancellor Angela Merkel were affected.	22.10.2020

▼M2

B. Legal persons, entities and bodies

	Name	Identifying information	Reasons	Date of listing
1.	Tianjin Huaying Haitai Science and Technology Development Co. Ltd (Huaying Haitai)	a.k.a.: Haitai Technology Development Co. Ltd Location: Tianjin, China	Huaying Haitai provided financial, technical or material support for and facilitated 'Operation Cloud Hopper', a series of cyber-attacks with a significant effect originating from outside the Union and constituting an external threat to the Union or its Member States and of cyber-attacks with a significant effect against third States.	30.7.2020

▼M2

	Name	Identifying information	Reasons	Date of listing
			‘Operation Cloud Hopper’ has targeted information systems of multi-national companies in six continents, including companies located in the Union, and gained unauthorised access to commercially sensitive data, resulting in significant economic loss. The actor publicly known as ‘APT10’ (‘Advanced Persistent Threat 10’) (a.k.a. ‘Red Apollo’, ‘CVNX’, ‘Stone Panda’, ‘MenuPass’ and ‘Potassium’) carried out ‘Operation Cloud Hopper’. Huaying Haitai can be linked to APT10. Moreover, Huaying Haitai employed Gao Qiang and Zhang Shilong, who are both designated in connection with ‘Operation Cloud Hopper’. Huaying Haitai is therefore associated with Gao Qiang and Zhang Shilong.	
2.	Chosun Expo	a.k.a.: Chosen Expo; Korea Export Joint Venture Location: DPRK	Chosun Expo provided financial, technical or material support for and facilitated a series of cyber-attacks with a significant effect originating from outside the Union and constituting an external threat to the Union or its Member States and of cyber-attacks with a significant effect against third States, including the cyber-attacks publicly known as ‘WannaCry’ and cyber-attacks against the Polish Financial Supervision Authority and Sony Pictures Entertainment, as well as cyber-theft from the Bangladesh Bank and attempted cyber-theft from the Vietnam Tien Phong Bank. ‘WannaCry’ disrupted information systems around the world by targeting information systems with ransomware and blocking access to data. It affected information systems of companies in the Union, including information systems relating to services necessary for the maintenance of essential services and economic activities within Member States. The actor publicly known as ‘APT38’ (‘Advanced Persistent Threat 38’) or the ‘Lazarus Group’ carried out ‘WannaCry’. Chosun Expo can be linked to APT38/the Lazarus Group, including through the accounts used for the cyber-attacks.	30.7.2020

▼M2

	Name	Identifying information	Reasons	Date of listing
3.	Main Centre for Special Technologies (GTsST) of the Main Directorate of the General Staff of the Armed Forces of the Russian Federation (GU/GRU)	Address: 22 Kirova Street, Moscow, Russian Federation	The Main Centre for Special Technologies (GTsST) of the Main Directorate of the General Staff of the Armed Forces of the Russian Federation (GU/GRU), also known by its field post number 74455, is responsible for cyber-attacks with a significant effect originating from outside the Union and constituting an external threat to the Union or its Member States and for cyber-attacks with a significant effect against third States, including the cyber-attacks publicly known as 'NotPetya' or 'EternalPetya' in June 2017 and the cyber-attacks directed at an Ukrainian power grid in the winter of 2015 and 2016. 'NotPetya' or 'EternalPetya' rendered data inaccessible in a number of companies in the Union, wider Europe and worldwide, by targeting computers with ransomware and blocking access to data, resulting amongst others in significant economic loss. The cyber-attack on a Ukrainian power grid resulted in parts of it being switched off during winter. The actor publicly known as 'Sandworm' (a.k.a. 'Sandworm Team', 'BlackEnergy Group', 'Voodoo Bear', 'Quedagh', 'Olympic Destroyer' and 'Telebots'), which is also behind the attack on the Ukrainian power grid, carried out 'NotPetya' or 'EternalPetya'. The Main Centre for Special Technologies of the Main Directorate of the General Staff of the Armed Forces of the Russian Federation has an active role in the cyber-activities undertaken by Sandworm and can be linked to Sandworm.	30.7.2020

▼M3

4.	85th Main Centre for Special Services (GTsSS) of the Main Directorate of the General Staff of the Armed Forces of the Russian Federation (GU/GRU)	Address: Komsomol'skiy Prospekt, 20, Moscow, 119146, Russian Federation	The 85th Main Centre for Special Services (GTsSS) of the Main Directorate of the General Staff of the Armed Forces of the Russian Federation (GU/GRU), also known as 'military unit 26165' (industry nicknames: 'APT28', 'Fancy Bear', 'Sofacy Group', 'Pawn Storm' and 'Strontium'), is responsible for cyber-attacks with a significant effect constituting an external threat to the Union or its Member States.	22.10.2020

▼M3

	Name	Identifying information	Reasons	Date of listing
			In particular, military intelligence officers of the GTsSS took part in the cyber-attack against the German federal parliament (Deutscher Bundestag) which took place in April and May 2015 and the attempted cyber-attack aimed at hacking into the Wi-Fi network of the Organisation for the Prohibition of Chemical Weapons (OPCW) in the Netherlands in April 2018. The cyber-attack against the German federal parliament targeted the parliament's information system and affected its operation for several days. A significant amount of data was stolen and email accounts of several MPs as well as of Chancellor Angela Merkel were affected.	