►**B**

COUNCIL REGULATION (EU) 2019/796

of 17 May 2019

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

(OJ L 129I, 17.5.2019, p. 1)

Amended by:

		Official Journal		
		No	page	date
►**M1**	Council Implementing Regulation (EU) 2020/1125 of 30 July 2020	L 246	4	30.7.2020
►**M2**	Council Implementing Regulation (EU) 2020/1536 of 22 October 2020	L 351 I	1	22.10.2020
►**M3**	Council Implementing Regulation (EU) 2020/1744 of 20 November 2020	L 393	1	23.11.2020

Corrected by:

►**C1** Corrigendum, OJ L 230, 17.7.2020, p. 37 (2019/796)

▼B

COUNCIL REGULATION (EU) 2019/796

of 17 May 2019

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

Article 1

1. This Regulation 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; 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;

▼B

(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 common foreign and security policy (CFSP) objectives in the relevant provisions of Article 21 of the Treaty on European Union, restrictive measures under this Regulation may also be applied in response to cyber-attacks with a significant effect against third States or international organisations.

7. For the purposes of this Regulation, 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.

8. For the purposes of this Regulation, the following additional definitions apply:

(a) ‘claim’ means any claim, whether asserted by legal proceedings or not, made before or after the date of entry into force of this Regulation, under or in connection with a contract or transaction, and includes in particular:

(i) a claim for performance of any obligation arising under or in connection with a contract or transaction;

(ii) a claim for extension or payment of a bond, financial guarantee or indemnity of whatever form;

(iii) a claim for compensation in respect of a contract or transaction;

(iv) a counterclaim;

▼B

(v) a claim for the recognition or enforcement, including by the procedure of *exequatur*, of a judgment, an arbitration award or an equivalent decision, wherever made or given;

(b) ‘contract or transaction’ means any transaction of whatever form and whatever the applicable law, whether comprising one or more contracts or similar obligations made between the same or different parties; for this purpose, ‘contract’ includes a bond, guarantee or indemnity, particularly a financial guarantee or financial indemnity, and credit, whether legally independent or not, as well as any related provision arising under, or in connection with, the transaction;

(c) ‘competent authorities’ refers to the competent authorities of the Member States as identified on the websites listed in Annex II;

(d) ‘economic resources’ means assets of every kind, whether tangible or intangible, movable or immovable, which are not funds, but may be used to obtain funds, goods or services;

(e) ‘freezing of economic resources’ means preventing the use of economic resources to obtain funds, goods or services in any way, including, but not limited to, by selling, hiring or mortgaging them;

(f) ‘freezing of funds’ means preventing any move, transfer, alteration, use of, access to, or dealing with funds in any way that would result in any change in their volume, amount, location, ownership, possession, character or destination or any other change that would enable the funds to be used, including portfolio management;

(g) ‘funds’ means financial assets and benefit of every kind, including, but not limited to:

(i) cash, cheques, claims on money, drafts, money orders and other payment instruments;

(ii) deposits with financial institutions or other entities, balances on accounts, debts and debt obligations;

(iii) publicly-and privately-traded securities and debt instruments, including stocks and shares, certificates representing securities, bonds, notes, warrants, debentures and derivatives contracts;

(iv) interest, dividends or other income on or value accruing from or generated by assets;

(v) credit, right of set-off, guarantees, performance bonds or other financial commitments;

(vi) letters of credit, bills of lading and bills of sale; and

(vii) documents showing evidence of an interest in funds or financial resources;

▼B

(h) ‘territory of the Union’ means the territories of the Member States to which the Treaty is applicable, under the conditions laid down in the Treaty, including their airspace.

Article 2

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 3

1. All funds and economic resources belonging to, owned, held or controlled by any natural or legal person, entity or body listed in Annex I shall be frozen.

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

3. Annex I shall include, as identified by the Council in accordance with Article 5(1) of Decision (CFSP) 2019/797:

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

(b) natural persons 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) of this paragraph.

▼B

Article 4

1. By way of derogation from Article 3, 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 Annex I ◄ 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.

2. The Member State concerned shall inform the other Member States and the Commission of any authorisation granted under paragraph 1 within two weeks of the authorisation.

Article 5

1. By way of derogation from Article 3(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 Article 3 was listed in Annex I, 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) 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 Annex I; and

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

▼B

2. The Member State concerned shall inform the other Member States and the Commission of any authorisation granted under paragraph 1 within two weeks of the authorisation.

Article 6

1. By way of derogation from Article 3(1) and provided that a payment by a natural or legal person, entity or body listed in Annex I is due under a contract or agreement that was concluded by, or an obligation that arose for, the natural or legal person, entity or body concerned before the date on which that natural or legal person, entity or body was included in Annex I, the competent authorities of the Member States may authorise, under such conditions as they deem appropriate, the release of certain frozen funds or economic resources, provided that the competent authority concerned has determined that:

(a) the funds or economic resources will be used for a payment by a natural or legal person, entity or body listed in Annex I; and

(b) the payment is not in breach of Article 3(2).

2. The Member State concerned shall inform the other Member States and the Commission of any authorisation granted under paragraph 1 within two weeks of the authorisation.

Article 7

1. Article 3(2) shall not prevent the crediting of frozen accounts by financial or credit institutions that receive funds transferred by third parties onto the account of a listed natural or legal person, entity or body, provided that any additions to such accounts will also be frozen. The financial or credit institution shall inform the relevant competent authority about any such transaction without delay.

2. Article 3(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 before the date on which the natural or legal person, entity or body referred to in Article 3(1) was included in Annex I; or

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

provided that any such interest, other earnings and payments remain subject to the measures provided for in Article 3(1).

Article 8

1. Without prejudice to the applicable rules concerning reporting, confidentiality and professional secrecy, natural and legal persons, entities and bodies shall:

▼B

(a) supply immediately any information which would facilitate compliance with this Regulation, such as information on accounts and amounts frozen in accordance with Article 3(1), to the competent authority of the Member State where they are resident or located, and transmit such information, directly or through the Member State, to the Commission; and

(b) cooperate with the competent authority in any verification of the information referred to in point (a).

2. Any additional information received directly by the Commission shall be made available to the Member States.

3. Any information provided or received in accordance with this Article shall be used only for the purposes for which it was provided or received.

Article 9

It shall be prohibited to participate, knowingly and intentionally, in activities the object or effect of which is to circumvent the measures referred to in Article 3.

Article 10

1. The freezing of funds and economic resources or the refusal to make funds or economic resources available, carried out in good faith on the basis that such action is in accordance with this Regulation, shall not give rise to liability of any kind on the part of the natural or legal person or entity or body implementing it, or its directors or employees, unless it is proved that the funds and economic resources were frozen or withheld as a result of negligence.

2. Actions by natural or legal persons, entities or bodies shall not give rise to any liability of any kind on their part if they did not know, and had no reasonable cause to suspect, that their actions would infringe the measures set out in this Regulation.

Article 11

1. 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 Regulation, 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 Annex I;

(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).

2. In any proceedings for the enforcement of a claim, the onus of proving that satisfying the claim is not prohibited by paragraph 1 shall be on the natural or legal person, entity or body seeking the enforcement of that claim.

3. This Article is without prejudice to the right of the natural or legal persons, entities and bodies referred to in paragraph 1 to judicial review of the legality of the non-performance of contractual obligations in accordance with this Regulation.

▼B

Article 12

1. The Commission and Member States shall inform each other of the measures taken under this Regulation and share any other relevant information at their disposal in connection with this Regulation, in particular information in respect of:

(a) funds frozen under Article 3 and authorisations granted under Articles 4, 5 and 6;

(b) violation and enforcement problems and judgments handed down by national courts.

2. The Member States shall immediately inform each other and the Commission of any other relevant information at their disposal which might affect the effective implementation of this Regulation.

Article 13

1. Where the Council decides to subject a natural or legal person, entity or body to the measures referred to in Article 3, it shall amend Annex I accordingly.

2. The Council shall communicate the decision 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 decision referred to in paragraph 1 and inform the natural or legal person, entity or body concerned accordingly.

4. The list in Annex I shall be reviewed at regular intervals and at least every 12 months.

5. The Commission shall be empowered to amend Annex II on the basis of information supplied by Member States.

Article 14

1. Annex I shall include the grounds for the listing of natural or legal persons, entities or bodies concerned.

2. Annex I 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 15

1. Member States shall lay down the rules on penalties applicable to infringements of the provisions of this Regulation and shall take all measures necessary to ensure that they are implemented. The penalties provided for shall be effective, proportionate and dissuasive.

▼B

2. Member States shall notify the Commission of the rules referred to in paragraph 1 without delay after the entry into force of this Regulation and shall notify it of any subsequent amendment.

Article 16

1. The Commission shall process personal data in order to carry out its tasks under this Regulation. These tasks include:

(a) adding the contents of Annex I to the electronic, consolidated list of persons, groups and entities subject to Union financial sanctions and to the interactive sanctions map, both publicly available;

(b) processing information on the impact of the measures of this Regulation such as the value of frozen funds and information on authorisations granted by the competent authorities.

2. For the purposes of this Regulation, the Commission service listed in Annex II is designated as 'controller' for the Commission within the meaning of Article 3(8) of Regulation (EU) 2018/1725, in order to ensure that the natural persons concerned can exercise their rights under that Regulation.

Article 17

1. Member States shall designate the competent authorities referred to in this Regulation and identify them on the websites listed in Annex II. Member States shall notify the Commission of any changes in the addresses of their websites listed in Annex II.

2. Member States shall notify the Commission of their competent authorities, including the contact details of those competent authorities, without delay after the entry into force of this Regulation, and shall notify it of any subsequent amendment.

3. Where this Regulation sets out a requirement to notify, inform or otherwise communicate with the Commission, the address and other contact details to be used for such communication shall be those indicated in Annex II.

Article 18

This Regulation shall apply:

(a) within the territory of the Union, including its airspace;

(b) on board any aircraft or vessel under the jurisdiction of a Member State;

(c) to any natural person inside or outside the territory of the Union who is a national of a Member State;

(d) to any legal person, entity or body, inside or outside the territory of the Union, which is incorporated or constituted under the law of a Member State;

(e) to any legal person, entity or body in respect of any business done in whole or in part within the Union.

▼B

Article 19

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

This Regulation shall be binding in its entirety and directly applicable in all Member States.

▼B

ANNEX I

List of natural and legal persons, entities and bodies referred to in Article 3

▼M1

A. Natural persons

	Name	Identifying information	Reasons	Date of listing
▼M3 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 multinational 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. 'Operation Cloud Hopper' has targeted information systems of multinational companies in six continents, including companies located in the Union, and gained unauthorised access to commercially sensitive data, resulting in significant economic loss.	30.7.2020

▼M3

	Name	Identifying information	Reasons	Date of listing
			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.	

▼M1

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
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

▼M1

	Name	Identifying information	Reasons	Date of listing
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
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

▼M1

	Name	Identifying information	Reasons	Date of listing
▼M2				
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
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 'Strontium'). 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

▼M1

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. 'Operation Cloud Hopper' has targeted information systems of multinational 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.	30.7.2020
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.	30.7.2020

▼M1

	Name	Identifying information	Reasons	Date of listing
			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.	
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.	30.7.2020
			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.	

▼M1

	Name	Identifying information	Reasons	Date of listing
▼M2				
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. 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

▼B

ANNEX II

Websites for information on the competent authorities and address for notifications to the Commission

BELGIUM

https://diplomatie.belgium.be/nl/Beleid/beleidsthemas/vrede_en_veiligheid/sancties

https://diplomatie.belgium.be/fr/politique/themes_politiques/paix_et_securite/sanctions

https://diplomatie.belgium.be/en/policy/policy_areas/peace_and_security/sanctions

BULGARIA

https://www.mfa.bg/en/101

CZECHIA

www.financnianalytickyurad.cz/mezinarodni-sankce.html

DENMARK

http://um.dk/da/Udenrigspolitik/folkeretten/sanktioner/

GERMANY

http://www.bmwi.de/DE/Themen/Aussenwirtschaft/aussenwirtschaftsrecht,did=404888.html

ESTONIA

http://www.vm.ee/est/kat_622/

IRELAND

http://www.dfa.ie/home/index.aspx?id=28519

GREECE

http://www.mfa.gr/en/foreign-policy/global-issues/international-sanctions.html

SPAIN

http://www.exteriores.gob.es/Portal/en/PoliticaExteriorCooperacion/GlobalizacionOportunidadesRiesgos/Paginas/SancionesInternacionales.aspx

FRANCE

http://www.diplomatie.gouv.fr/fr/autorites-sanctions/

CROATIA

http://www.mvep.hr/sankcije

ITALY

https://www.esteri.it/mae/it/politica_estera/politica_europea/misure_deroghe

CYPRUS

http://www.mfa.gov.cy/mfa/mfa2016.nsf/mfa35_en/mfa35_en?OpenDocument

LATVIA

http://www.mfa.gov.lv/en/security/4539

LITHUANIA

http://www.urm.lt/sanctions

▼B

LUXEMBOURG

https://maee.gouvernement.lu/fr/directions-du-ministere/affaires-europeennes/mesures-restrictives.html

HUNGARY

http://www.kormany.hu/download/9/2a/f0000/EU%20szankci%C3%B3s%20t%C3%A1j%C3%A9koztat%C3%B3_20170214_final.pdf

MALTA

https://foreignaffairs.gov.mt/en/Government/SMB/Pages/Sanctions-Monitoring-Board.aspx

NETHERLANDS

https://www.rijksoverheid.nl/onderwerpen/internationale-sancties

AUSTRIA

http://www.bmeia.gv.at/view.php3?f_id=12750&LNG=en&version=

POLAND

https://www.gov.pl/web/dyplomacja

PORTUGAL

http://www.portugal.gov.pt/pt/ministerios/mne/quero-saber-mais/sobre-o-ministerio/medidas-restritivas/medidas-restritivas.aspx

ROMANIA

http://www.mae.ro/node/1548

SLOVENIA

http://www.mzz.gov.si/si/omejevalni_ukrepi

SLOVAKIA

https://www.mzv.sk/europske_zalezitosti/europske_politiky-sankcie_eu

FINLAND

http://formin.finland.fi/kvyhteistyo/pakotteet

SWEDEN

http://www.ud.se/sanktioner

UNITED KINGDOM

https://www.gov.uk/sanctions-embargoes-and-restrictions

Address for notifications to the European Commission:

European Commission
Service for Foreign Policy Instruments (FPI)
EEAS 07/99
B-1049 Brussels, Belgium
E-mail: relex-sanctions@ec.europa.eu