Врз основа на член 7 став 1 од Законот за рестриктивни мерки („Службен весник на Република Македонија" број 190/17), Владата на Република Северна Македонија, на седницата, одржана на 16 февруари 2021 година, донесе

О Д Л У К А

за воведување на рестриктивни мерки согласно Одлуката (ЗНБП) 2020/1127 на Советот од 30 јули 2020 година за изменување на Одлуката (ЗНБП) 2019/797 за рестриктивни мерки против сајбер напади што претставуваат закана за Унијата или нејзините земји членки

Член 1

Со оваа одлука се воведуваат рестриктивни мерки согласно Одлуката (ЗНБП) 2020/1127 на Советот од 30 јули 2020 година за изменување на Одлуката (ЗНБП) 2019/797 за рестриктивни мерки против сајбер напади што претставуваат закана за Унијата или нејзините земји членки.

Член 2

Оваа одлука се однесува на следните видови рестриктивни мерки:

- ембарго на стоки и услуги;
- финансиски мерки;
- забрана за влез во Република Северна Македонија;
- други рестриктивни мерки согласно меѓународното право

Член 3

Се определуваат Министерството за внатрешни работи, Министерството за економија, Министерството за надворешни работи, Министерството за транспорт и врски и Министерството за финансии - Управата за финансиско разузнавање за надлежни органи за спроведување на рестриктивните мерки.

Член 4

Одлуката (ЗНБП) 2020/1127 на Советот од 30 јули 2020 година за изменување на Одлуката (ЗНБП) 2019/797 за рестриктивни мерки против сајбер напади што претставуваат закана за Унијата или нејзините земји членки во оригинал на англиски и во превод на македонски јазик е дадена во прилог и е составен дел на оваа одлука.

Член 5

Рестриктивните мерки против сајбер напади што претставуваат закана за Унијата или нејзините земји членки се воведуваат на неопределено време.

Член 6

Оваа одлука влегува во сила наредниот ден од денот на објавувањето во „Службен весник на Република Северна Македонија".

Бр. 40-1550/1
16 февруари 2021 година
Скопје

ПРВ ЗАМЕНИК НА ПРЕТСЕДАТЕЛОТ НА ВЛАДАТА НА РЕПУБЛИКА СЕВЕРНА МАКЕДОНИЈА

Artan Grubi

COUNCIL DECISION (CFSP) 2020/1127

of 30 July 2020

amending Decision (CFSP) 2019/797 concerning restrictive measures against cyber-attacks threatening the Union or its Member States

THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on European Union, and in particular Article 29 thereof,

Having regard to the proposal from the High Representative of the Union for Foreign Affairs and Security Policy,

Whereas:

(1) On 17 May 2019 the Council adopted Decision (CFSP) 2019/797 [1].

(2) Targeted restrictive measures against cyber-attacks with a significant effect which constitute an external threat to the Union or its Member States are among the measures included in the Union's framework for a joint diplomatic response to malicious cyber-activities (the cyber diplomacy toolbox) and are a vital instrument to deter and respond to such activities. Restrictive measures can also be applied in response to cyber-attacks with a significant effect against third States or international organisations, where deemed necessary to achieve common foreign and security policy objectives set out in the relevant provisions of Article 21 of the Treaty on European Union.

(3) On 16 April 2018 the Council adopted conclusions in which it firmly condemned the malicious use of information and communications technologies, including in the cyber-attacks publicly known as 'WannaCry' and 'NotPetya', which caused significant damage and economic loss in the Union and beyond. On 4 October 2018 the Presidents of the European Council and of the European Commission and the High Representative of the Union for Foreign Affairs and Security Policy (the 'High Representative') expressed serious concerns in a joint statement about an attempted cyber-attack to undermine the integrity of the Organisation for the Prohibition of Chemical Weapons (OPCW) in the Netherlands, an aggressive act which demonstrated contempt for the solemn purpose of the OPCW. In a declaration made on behalf of the Union on 12 April 2019, the High Representative urged actors to stop undertaking malicious cyber-activities that aim to undermine the Union's integrity, security and economic competiveness, including acts of cyber-enabled theft of intellectual property. Such cyber-enabled thefts include those carried out by the actor publicly known as 'APT10' ('Advanced Persistent Threat 10').

(4) In this context, and to prevent, discourage, deter and respond to continuing and increasing malicious behaviour in cyberspace, six natural persons and three entities or bodies should be included in the list of natural and legal persons, entities and bodies subject to restrictive measures set out in the Annex to Decision (CFSP) 2019/797. Those persons and entities or bodies are responsible for, provided support for or were involved in, or facilitated cyber-attacks or attempted cyber-attacks, including the attempted cyber-attack against the OPCW and the cyber-attacks publicly known as 'WannaCry' and 'NotPetya', as well as 'Operation Cloud Hopper'.

(5) Decision (CFSP) 2019/797 should therefore be amended accordingly,

HAS ADOPTED THIS DECISION:

Article 1

The Annex to Decision (CFSP) 2019/797 is amended in accordance with the Annex to this Decision.

[1] Council Decision (CFSP) 2019/797 of 17 May 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States (OJ L 129 I, 17.5.2019, p. 13).

Article 2

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

Done at Brussels, 30 July 2020.

For the Council
The President
M. ROTH

ANNEX

The following persons and entities or bodies are added to the list of natural and legal persons, entities and bodies set out in the Annex to Decision (CFSP) 2019/797:

'A. Natural persons

	Name	Identifying information	Reasons	Date of listing
1.	GAO Qiang	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" 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	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. 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".	30.7.2020

			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.	
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

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

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

			"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.	
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
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.	30.7.2020'

			"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.	

ОДЛУКА (ЗНБП) 2020/1127 НА СОВЕТОТ

од 30 јули 2020 година

за изменување на Одлуката (ЗНБП) 2019/797 за рестриктивни мерки против сајбер напади што претставуваат закана за Унијата или нејзините земји членки

СОВЕТОТ НА ЕВРОПСКАТА УНИЈА,

имајќи го предвид Договорот за Европската Унија, а особено член 29 од истиот,

имајќи го предвид предлогот на Високиот претставник на Унијата за надворешни работи и безбедносна политика,

со оглед на тоа што:

(1) На 17 мај 2019 година, Советот ја донесе Одлуката (ЗНБП) 2019/797 ([1]).

(2) Насочените рестриктивни мерки против сајбер напади со значително влијание што претставуваат надворешна закана за Унијата или нејзините земји членки се дел од мерките вклучени во рамката на Унијата за заеднички дипломатски одговор на злонамерни сајбер активности (алатки за сајбер дипломатика) и се клучен инструмент за сузбивање и одговор на ваквите активности. Исто така, може да се применат рестриктивни мерки како одговор на сајбер напади со значително влијание против трети земји или меѓународни организации, каде што ова се смета за потребно за да се постигнат целите на заедничката надворешна и безбедносна политика предвидени во соодветните одредби од член 21 од Договорот за Европската Унија.

(3) На 16 април 2018 година, Советот донесе заклучоци со кои најостро се осудува злонамерната употреба на информатички и комуникациски технологии, вклучително и сајбер напади познати во јавноста како „WannaCry“ и „NotPetya“, кои предизвикаа значителна штета и економска загуба во Унијата и надвор од Унијата. На 4 октомври 2018 година, претседателите на Европскиот совет и на Европската комисија и високиот претставник на Унијата за надворешни работи и безбедносна политика („високиот претставник“) во заедничката изјава изразија сериозна загриженост во врска со обидот за сајбер напад со цел да се наруши интегритетот на Организацијата за забрана на хемиско оружје (ОЗХО) во Холандија, агресивен чин на непочитување на важната цел спроведена од ОЗХО. Во изјавата во име на Унијата од 12 април 2019 година, високиот претставник ги повика учесниците да престанат со злонамерни активности во сајбер просторот насочени кон поткопување на интегритетот, безбедноста и економската конкурентност на Унијата, вклучително и кражба на интелектуална сопственост овозможена од сајбер технологиите.

---

[1] Одлука (ЗНБП) 2019/797 на Советот од 17 мај 2019 година за рестриктивни мерки против сајбер напади што претставуваат закана за Унијата или нејзините земји членки (Сл. весник бр. L 129 I, 17.5.2019 година, стр. 13).

Таквите кражби овозможени од сајбер технологиите вклучуваат кражби извршени од сторител познат во јавноста како „APT10“ („Напредна постојана закана 10“).

(4) Во овој контекст и со цел да се спречи, обесхрабри, сузбие и одговори на континуираното и растечкото злонамерно однесување во сајбер просторот, шест физички лица и три субјекти или тела треба да бидат вклучени во списокот на физички и правни лица, субјекти и тела кои подлежат на рестриктивни мерки утврдени во Анексот кон Одлуката (ЗНБП) 2019/797. Овие лица и субјекти или тела се одговорни за сајбер напади или обиди за сајбер напади, или поддржале, учествувале или олеснувале извршување на такви сајбер напади или обиди за сајбер напади, вклучително и обиди за сајбер напади против ОЗХО и сајбер напади познати во јавноста како што се „WannaCry“ и „ NotPetya“, како и операцијата „Cloud Hopper“.

(5) Затоа, Одлуката (ЗНБП) 2019/797 треба соодветно да се измени,

ЈА ДОНЕСЕ ОВАА ОДЛУКА:

Член 1

Анексот кон Одлуката (ЗНБП) 2019/797 се изменува како што е утврдено во Анексот кон оваа одлука.

Член 2

Оваа одлука влегува во сила на денот на нејзиното објавување во *Службениот весник на Европската Унија.*

Брисел, 30 јули 2020 година.

За Советот

Претседател

М. РОТ

АНЕКС

Следните лица и субјекти или тела се додаваат во списокот на физички и правни лица, субјекти и тела утврдени во Анексот кон Одлуката (ЗНБП) 2019/797:

„А. Физички лица

	Име	Информации за идентификација	Причини	Датум на внесување во список
1.	ГАО Кјанг (GAO Qiang)	Место на раѓање: Провинција Шандонг, Кина Адреса: Room 1102, Guanfu Mansion, 46 Xinkai Road, Hedong District, Тијанџин, Кина Државјанство: кинеско Пол: машки	Гао Кјанг е вклучен во операцијата „Cloud Hopper“, серија на сајбер напади со значително влијание што потекнува надвор од Унијата и претставува надворешна закана за Унијата или нејзините земји членки и сајбер напади со значително влијание врз трети земји. Операцијата „Cloud Hopper“ била насочена кон информациските системи на мултинационални компании од шест континенти, вклучително и компании со седиште во Унијата и овозможила да се добие неовластен пристап до комерцијални чувствителни податоци, што доведува до значителни економски загуби. Операцијата „Cloud Hopper“ е дело на сторител познат во јавноста како „APT10“ („Напредна постојана закана 10“) (исто така познат како „Red Apollo“, „CVNX“, „Stone Panda“, „MenuPass“ и „Potassium”).	30.7.2020 година

			Гао Кјанг може да се поврзе со APT10, вклучително и преку неговото поврзување со контролно-управувачката инфраструктура на „APT10“. Покрај тоа, Гао Кјанг работел за Хуаинг Хаитаи, субјект наведен во списокот за обезбедување поддршка и олеснување на операцијата „Cloud Hopper“. Тој е поврзан со Цанг Шилонг, кој е наведен во списокот и во врска со операцијата „Cloud Hopper“. Затоа, Гао Кјанг е поврзан и со Хуаинг Хаитаи и со Цанг Шилонг.	
2.	ЦАНГ Шилонг (ZHANG Shilong)	Адреса: Hedong, Yuyang Road No 121, Тијанцин, Кина Државјанство: кинеско Пол: машки	Цанг Шилонг (Zhang Shilong) е вклучен во операцијата „Cloud Hopper“, серија на сајбер напади со значително влијание што потекнува надвор од Унијата и претставува надворешна закана за Унијата или нејзините земји членки и сајбер напади со значително влијание врз трети земји. Операцијата „Cloud Hopper“ била насочена кон информациските системи на мултинационални компании од шест континенти, вклучително и компании со седиште во Унијата и овозможила да се добие неовластен пристап до комерцијални чувствителни податоци, што доведува до значителни економски загуби. Операцијата „Cloud Hopper“ е дело на сторител	30.7.2020 година

			познат во јавноста како „APT10“ („Напредна постојана закана 10“) (исто така познат како „Red Apollo“, „CVNX“, „Stone Panda“, „MenuPass“ и „Potassium”). Џанг Шилонг може да биде поврзан со субјектот APT10, вклучително и преку штетниот софтвер развиен и тестиран во врска со сајбер напади извршени од субјектот APT10. Покрај тоа, Хуаинг Хаитаи работел за Џанг Шилонг, субјект наведен во списокот за обезбедување на поддршка и олеснување на операцијата „Cloud Hopper“. Тој е поврзан со Гао Кјанг, кој е наведен во списокот и во врска со операцијата „Cloud Hopper“. Затоа, Џанг Шилонг е поврзан и со Хуаинг Хаитаи и со Гао Кјанг.	
3.	Алексеј Валериевич МИНИН (Alexey Valeryevich MININ)	Алексей Валерьевич МИНИН Датум на раѓање: 27 мај 1972 година Место на раѓање: Пермска област, Руска СФСР (сега Руска Федерација) Број на пасош: 120017582 Издаден од: Министерство за надворешни работи на Руската Федерација: Важност: од 17 април 2017	Алексеј Минин учествувал во обид за сајбер напад со потенцијално значително влијание врз Организацијата за забрана на хемиско оружје (ОЗХО) во Холандија. Како службеник за поддршка на човечкото разузнавање во Главната управа на Генералштабот на вооружените сили на Руската Федерација (ГУ/ГРУ), Алексеј Минин бил дел од тим составен од четворица руски воени разузнавачи кои се обиделе да добијат неовластен пристап до	30.7.2020 година

		година до 17 април 2022 година Место: Москва, Руска Федерација Државјанство: руско Пол: машки	безжичната мрежа на ОЗХО во Хаг, Холандија, во април 2018 година. Обидот за сајбер напад бил насочен кон хакирање на безжичната мрежа на ОЗХО, што, доколку било успешн, би ги загрозило безбедноста на мрежата и тековните истраги на ОЗХО. Холандската воена служба за безбедност и разузнавање (ВСБР) (Militaire Inlichtingen- en Veiligheidsdienst – MIVD) го прекина обидот за сајбер нападот, со што се спречи сериозна штета на ОЗХО.	
4.	Алексеј Сергеевич МОРЕНЕЦ (Aleksei Sergeyvich MORENETS)	Алексей Сергеевич МОРЕНЕЦ Датум на раѓање: 31 јули 1977 година Место на раѓање: Мурманска област, Руска СФСР (сега Руска Федерација) Број на пасош: 100135556 Издаден од: Министерство за надворешни работи на Руската Федерација Важност: од 17 април 2017 година до 17 април 2022 година Место: Москва, Руска Федерација Државјанство: руско Пол: машки	Алексеј Моренец учествувал во обид за сајбер напад со потенцијално значително влијание врз Организацијата за забрана на хемиско оружје (ОЗХО) во Холандија. Како сајбер оператор во Главната управа на Генералштабот на вооружените сили на Руската Федерација (ГУ/ГРУ), Алексеј Моренец бил дел од тим составен од четворица руски воени разузнавачи кои се обиделе да добијат неовластен пристап до безжичната мрежа на ОЗХО во Хаг, Холандија, во април 2018 година. Обидот за сајбер напад бил насочен кон хакирање на безжичната мрежа на ОЗХО, што, доколку било успешн, би ги загрозило безбедноста на мрежата и тековните истраги на ОЗХО. Холандската воена служба за безбедност и	30.7.2020 година

			разузнавање (ВСБР) (Militaire Inlichtingen- en Veiligheidsdienst – MIVD) го прекина обидот за сајбер нападот, со што се спречи сериозна штета на ОЗХО.	
5.	Евгениј Михаилович СЕРЕБРЈАКОВ (Evgenii Mikhaylovich SEREBRIAKOV)	Евгений Михайлович СЕРЕБРЯКОВ Датум на раѓање: 26 јули 1981 година Место на раѓање: Курск (Kursk), Руска СФСР (сега Руска Федерација) Број на пасош: 100135555 Издаден од: Министерство за надворешни работи на Руската Федерација Важност: од 17 април 2017 година до 17 април 2022 година Место: Москва, Руска Федерација Државјанство: руско Пол: машки	Евгениј Серебрјаков учествувал во обид за сајбер напад со потенцијално значително влијание врз Организацијата за забрана на хемиско оружје (ОЗХО) во Холандија. Како сајбер оператор во Главната управа на Генералштабот на вооружените сили на Руската Федерација (ГУ/ГРУ), Евгениј Серебрјаков бил дел од тим составен од четворица руски воени разузнавачи кои се обиделе да добијат неовластен пристап до безжичната мрежа на ОЗХО во Хаг, Холандија, во април 2018 година. Обидот за сајбер напад бил насочен кон хакирање на безжичната мрежа на ОЗХО, што, доколку било успешн, би ги загрозило безбедноста на мрежата и тековните истраги на ОЗХО. Холандската воена служба за безбедност и разузнавање (ВСБР) (Militaire Inlichtingen- en Veiligheidsdienst – MIVD) го прекина обидот за сајбер нападот, со што се спречи сериозна штета на ОЗХО.	30.7.2020 година
6.	Олег Михаилович СОТНИКОВ (Oleg	Олег Михайлович СОТНИКОВ Датум на раѓање: 24 август 1972 година	Олег Сотников учествувал во обид за сајбер напад со потенцијално значително влијание врз	30.7.2020 година

	Mikhaylovich SOTNIKOV)	Место на раѓање: Улјановск (Ulyanovsk), Руска СФСР (сега Руска Федерација) Број на пасош: 120018866 Издаден од: Министерство за надворешни работи на Руската Федерација Важност: од 17 април 2017 година до 17 април 2022 година Место: Москва, Руска Федерација Државјанство: руско Пол: машки	Организацијата за забрана на хемиско оружје (ОЗХО) во Холандија. Како службеник за поддршка на човечкото разузнавање во Главната управа на Генералштабот на вооружените сили на Руската Федерација (ГУ/ГРУ), Олег Сотников бил дел од тим составен од четворица руски воени разузнавачи кои се обиделе да добијат неовластен пристап до безжичната мрежа на ОЗХО во Хаг, Холандија, во април 2018 година. Обидот за сајбер напад бил насочен кон хакирање на безжичната мрежа на ОЗХО, што, доколку било успешн, би ги загрозило безбедноста на мрежата и тековните истраги на ОЗХО. Холандската воена служба за безбедност и разузнавање (ВСБР) (Militaire Inlichtingen- en Veiligheidsdienst – MIVD) го прекина обидот за сајбер нападот, со што се спречи сериозна штета на ОЗХО.	

Б. Правни лица, субјекти и тела

	Име	**Информации за идентификација**	**Причини**	**Датум на внесување во список**
1.	Tianjin Huaying Haitai Science and Technology Development Co. Ltd (Huaying Haitai)	познат како: Haitai Technology Development Co. Ltd	Хуаинг Хаитаи обезбедил финансиска, техничка или материјална поддршка и ја олеснил операцијата „Cloud Hopper“, серија на сајбер напади со значително влијание што потекнува надвор од	30.7.2020 година

		Место: Тијанџин, Кина	Унијата и претставува надворешна закана за Унијата или нејзините земји членки и сајбер напади со значително влијание врз трети земји. Операцијата „Cloud Hopper“ била насочена кон информациските системи на мултинационални компании од шест континенти, вклучително и компании со седиште во Унијата и овозможила да се добие неовластен пристап до комерцијални чувствителни податоци, што доведува до значителни економски загуби. Операцијата „Cloud Hopper“ е дело на сторител познат во јавноста како „APT10“ („Напредна постојана закана 10“) (исто така познат како „Red Apollo“, „CVNX“, „Stone Panda“, „MenuPass“ и „Potassium”). Хуаинг Хаитаи може да биде поврзан со APT10. Покрај тоа, во Хуинг Хаитаи ги вработил Гао Кјанг и Џанг Шилонг, кои се поврзани со операцијата „Cloud Hopper“. Затоа, Хуаинг Хаитаи е поврзан со Гао Кјанг и Џанг Шилонг.	
2.	Чосун Експо (Chosun Expo)	познат како: Chosen Expo; Korea Export Joint Venture Место: НДРК	Chosun Expo обезбедил финансиска, техничка или материјална поддршка и олеснувал серија на сајбер напади со значително влијание што потекнува надвор од Унијата и претставува надворешна закана за Унијата или нејзините земји членки и сајбер напади со значително влијание врз трети земји, вклучително и сајбер напади познати во јавноста како „WannaCry“, сајбер напади против „Polish Financial Supervision Authority and Sony Pictures Entertainment“, како и сајбер кражба во Bangladesh Bank и обид за сајбер кражба во Vietnam Tien Phong	30.7.2020 година

			Bank. „WannaCry“ предизвикала нарушувања на информациските системи ширум светот напаѓајќи ги со рансомвер и блокирајќи пристап до податоци. Тоа влијаело на информациските системи на компаниите во Унијата, вклучувајќи ги и информациските системи поврзани со услугите потребни за одржување на клучните услуги и економските активности во рамки на земјите членки. „WannaCry“ е дело на сторител познат во јавноста како „APT38“ („Напредна постојана закана 38“) или „Lazarus Group“. Chosun Expo може да се поврзе со APT38/Lazarus Group, вклучително и преку профилите што се користат во сајбер нападите.	
3.	Главен центар за специјални технологии (GTsST) на Главната управа на Генералштабот на вооружените сили на Руската Федерација (ГУ/ГРУ)	Адреса: Кирова 22, Москва, Руска Федерација	Генералниот центар за специјални технологии (GTsST) на Генералната управа на Генералштабот на вооружените сили на Руската Федерација (ГУ/ГРУ), исто така познат по својот број на воена пошта 74455, е одговорен за сајбер напади со значително влијание кои потекнуваат од надвор од Унијата и претставуваат надворешна закана за Унијата или нејзините земји членки и за сајбер напади со значително влијание врз трети земји, вклучувајќи ги и сајбер нападите јавно познати како „NotPetya“ или „EternalPetya“ во јуни 2017 година и сајбер напади насочени кон украинската електрична мрежа во зимата 2015 и 2016 година. „NotPetya“ или „EternalPetya“ го прекинаа пристапот до податоците во голем број компании во Унијата, ширум Европа и	30.7.2020 година“

			светот напаѓајќи компјутери со софтвер за уцена и блокирајќи пристап до податоци, што доведе до значителна економска загуба, меѓу другото. Сајбер нападот врз украинската електричната мрежа доведе до нејзино делумно исклучување во текот на зимата. „NotPetya“ или „EternalPetya“ е дело на сторител познат во јавноста како „Sandworm“ (познат и како Sandworm Team”, “BlackEnergy Group”, “Voodoo Bear”, “Quedagh”, “Olympic Destroyer” и “Telebots”) кој стои и зад нападот врз украинската електрична мрежа. Главниот центар за специјални технологии на Генералната управа на Генералштабот на вооружените сили на Руската Федерација има активна улога во сајбер активностите спроведени од „Sandworm “ и може да биде поврзан со субјектот „Sandworm“.	