



CENTRALE BANK VAN ARUBA

September 21, 2020

To the Managements of all financial institutions and DNFBPs

VMI/gcr/2.46/INT/9107

Subject: Sanctions State Decree Cyber-Attacks

Dear Management,

Pursuant to the Sanctions State Ordinance 2006 (AB 2007 no.24), rules may be laid down by State Decree containing general administrative orders for the implementation of a treaty or an international decision that Aruba is obliged to comply with, and which entail a restriction, prohibition or the imposition of an obligation for its residents. In connection herewith, a Sanctions State Decree Cyber-Attacks (AB 2020 no. 125) has been recently enacted.

Please find enclosed the following documents:

1. Official (Dutch) text of the aforementioned Sanctions State Decree and the Explanatory Notes (in Dutch) (enclosures 1 and 2), which are also available on the website of the CBA www.cbaruba.org under the heading "Financial Sanctions". An unofficial English translation of the State Decree and its Explanatory Notes is also available on the CBA's website (enclosures 3 and 4).
2. Decision 2019/797 (*Besluit 2019/797*) (enclosure 5) and Regulation 2019/796 (*Verordening 2019/796*) (enclosure 6) as referred to in the Sanctions State Decree Cyber-Attacks.
3. The list of natural and legal persons, entities, and bodies subject to the restrictive measures set out in Annex I to Regulation (EU) 2019/796, which was amended pursuant to the Council Implementing Regulation (EU) 2020/1125 of July 30, 2020, implementing Regulation (EU) 2019/796 concerning restrictive measures against cyber-attacks threatening the Union or its Member States (enclosure 7).

Your institution should ensure that it stays abreast of all updates related to mentioned regulations.

If you have any questions regarding this letter, please contact Ms. Vasilena Ivanova of the Integrity Supervision Department by e-mail v.ivanova@cbaruba.org.

Sincerely yours,

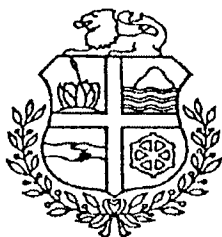


Centrale Bank van Aruba

Enclosures: 7

cc. Head of FIU-Aruba

2020 no. 125



**AFKONDIGINGSBLAD
VAN
ARUBA**

LANDSBESLUIT, houdende algemene maatregelen, van 26 augustus 2020 ter uitvoering van artikelen 2 en 2a van de Sanctieverordening 2006 (AB 2007 no. 24) (Sanctiebesluit cyberaanvallen)

Uitgegeven, 27 augustus 2020

De minister van Justitie,
Veiligheid en Integratie,

A.C.G. Bikker

IN NAAM VAN DE KONING!

DE GOUVERNEUR van Aruba,

In overweging genomen hebbende:

dat het in het belang van het buitenlandse beleid van het Koninkrijk alsmede in het belang van de internationale rechtsorde wenselijk is, gelet op de Verordening nr. 2019/796 van de Raad van de Europese Unie van 17 mei 2019 en het Besluit (GBVB) 2019/797 van 17 mei 2019 betreffende beperkende maatregelen tegen cyberaanvallen die de Europese Unie of haar lidstaten bedreigen, uit te voeren;

Gelet op:

artikelen 2 en 2a van de Sanctieverordening 2006 (AB 2007 no. 24);

Heeft besloten:

§ 1. Algemeen

Artikel 1

In dit landsbesluit wordt verstaan onder:

Bank	: de Centrale Bank van Aruba;
Besluit 2019/797	: het Besluit (GBVB) 2019/797 van 17 mei 2019 betreffende beperkende maatregelen tegen cyberaanvallen die de Unie of haar lidstaten bedreigen, met de bijbehorende bijlagen, met inbe-

	grip van de nadien in die bijlagen aangebrachte wijzigingen;
bevriezen	: een verbod op overmaking, omzetting, verplaatsing of terbeschikkingstelling;
dienst	: een werkzaamheid met betrekking tot een fonds of een ander vermogensbestanddeel;
dienstverlener	: een ieder die beroeps- of bedrijfsmatige een dienst verleent;
fondsen of andere vermogensbestanddelen	: goederen, hoe dan ook verkregen, als bedoeld in artikel 1 van Boek 3 van het Burgerlijk Wetboek van Aruba, alle bescheiden en gegevensdragers, in welke vorm of hoedanigheid dan ook, waaruit de gehele dan wel gedeelde eigendom of gerechtigdheid blijkt ten aanzien van een goed, en voortbrengselen onderscheidenlijk
Minister	: de minister, belast met financiële aangelegenheden;
Meldpunt	: het meldpunt ongebruikelijke transacties, bedoeld in artikel 20, eerste lid, van de Landsverordening voorkoming en bestrijding witwassen en terrorismefinanciering (AB 2011 no. 28);
Verordening nr. 2019/796	: de Verordening (EU) nr. 2019/796 van 17 mei 2019 betreffende beperkende maatregelen tegen cyberaanvallen die de Unie of haar lidstaten bedreigen, met de bijbehorende bijlagen, met inbegrip van de nadien in die bijlagen aangebrachte wijzigingen.

§ 2. De bevriezing van fondsen en andere vermogensbestanddelen

Artikel 2

1. Bevroren worden alle in Aruba aanwezige fondsen of andere vermo-

gensbestanddelen die direct of indirect toebehoren aan, eigendom zijn van, in het bezit zijn van of onder zeggenschap staan van een natuurlijke persoon, rechtspersoon, entiteiten of lichamen, opgenomen in de bijlage I behorende bij Verordening nr. 2019/796 en bijlage van Besluit 2019/797.

2. De bevroering, bedoeld in het eerste lid, is van overeenkomstige toepassing ten aanzien van vertegenwoordigers van de in dat lid genoemde natuurlijke personen, rechtspersoon, entiteiten of lichamen.
3. In afwijking van het eerste lid, kan aan een aangewezen persoon toegang tot diens bevroren fondsen of vermogensbestanddelen worden verleend voor tegoeden, financiële activa of economische middelen die:
 - a. noodzakelijk zijn voor het dekken van uitgaven voor de basisbehoeften van de natuurlijke personen, genoemd in de bijlage I behorende bij Verordening nr. 2019/796 en bijlage van Besluit 2019/797, en de gezinsleden die van deze natuurlijke personen afhankelijk zijn, zoals betalingen voor levensmiddelen, huur of hypotheeklasten, geneesmiddelen of medische behandelingen, belastingen, verzekeringspremies en nutsvoorzieningen;
 - b. uitsluitend bestemd zijn voor de betaling van redelijke honoraria of de vergoeding van gemaakte kosten in verband met de verlening van juridische diensten;
 - c. uitsluitend bestemd zijn voor de betaling van honoraria of kosten voor alleen het aanhouden of beheren van bevroren tegoeden of economische middelen, of
 - d. noodzakelijk zijn voor de betaling van buitengewone lasten, mits de Minister ten minste twee weken van tevoren in kennis is gesteld van de redenen waarom zij meent dat specifieke toestemming moet worden verleend.
4. De toegang tot bevroren fondsen of vermogensbestanddelen wordt slechts verleend met goedkeuring van de Minister.

Artikel 3

1. De Bank is belast met de bekendmaking op digitale wijze van de actuele tekst van de bijlage I behorende bij de Verordening nr. 2019/796 en bijlage van Besluit 2019/797.
2. Dienstverleners treffen zodanige voorzieningen waardoor zij te allen tijde op de hoogte zijn van de inhoud van de bijlage I behorende bij de Verordening nr. 2019/796 en bijlage van Besluit 2019/797.

Artikel 4

1. Het is eenieder verboden diensten te verlenen of handelingen te verrichten die ertoe leiden of redelijkerwijs ertoe kunnen leiden dat een natuurlijke persoon, rechtspersoon of andere entiteit opgenomen in de bijlage I behorende bij Verordening nr. 2019/796 en bijlage van Besluit 2019/797, op enigerlei wijze de beschikking krijgt over fondsen of andere vermogensbestanddelen.
2. Het is verboden bewust of opzettelijk deel te nemen aan activiteiten die tot doel of tot gevolg hebben dat de in het eerste lid bedoelde maatregelen direct of indirect worden omzeild.

Artikel 5

1. Een ieder die fondsen of andere vermogensbestanddelen onder zich heeft van een natuurlijke persoon, rechtspersoon of andere entiteit opgenomen in de bijlage I behorende bij de Verordening nr. 2019/796 en bijlage van Besluit 2019/797, treft zodanige maatregelen waardoor van deze fondsen en vermogensbestanddelen geen gebruik kan worden gemaakt, dan wel dat deze fondsen en andere vermogensbestanddelen niet overgemaakt, omgezet, verplaatst of ter beschikking gesteld kunnen worden.
2. Indien het een dienstverlener betreft die bij of krachtens een landsverordening onder toezicht van de Bank staat, doet deze onverwijld mededeling aan de Bank van de fondsen of andere vermogensbestanddelen die

zich onder hem bevinden. De vorige volzin is van overeenkomstige toepassing op aangewezen niet-financiële dienstverleners.

3. Dienstverleners stellen het Meldpunt onverwijld op de hoogte van alle voorgenomen of verrichte transacties door of namens personen, entiteiten en lichamen opgenomen in de bijlage I behorende bij de Verordening nr. 2019/796 en bijlage van Besluit 2019/797.

§ 3. Slotbepaling

Artikel 6

1. Dit landsbesluit treedt in werking met ingang van de dag na die van zijn plaatsing in het Afkondigingsblad van Aruba.
2. Het kan worden aangehaald als Sanctiebesluit cyberaanvallen.

Gegeven te Oranjestad, 26 augustus 2020

J.A. Boekhoudt

De minister van Algemene Zaken, Integriteit,
Overheidszorg, Innovatie en Energie,
E.C. Wever-Croes

De minister van Financiën, Economische Zaken
en Cultuur, a.i.
E.C. Wever-Croes

De minister van Justitie, Veiligheid
en Integratie,
A.C.G. Bikker

NOTA VAN TOELICHTING

Algemene toelichting

Op 17 mei 2019 heeft de Raad van de Europese Unie (hierna: EU) het cybersanctieregime vastgesteld dat bestaat uit het Besluit (GBVB) 2019/797¹ en de Verordening (EU) 2019/796.² Dit specifieke sanctieregime biedt de EU de mogelijkheid om wereldwijd maatregelen te nemen tegen personen en organisaties die verantwoordelijk zijn voor een cyberaanval of een poging daartoe, of op enig andere wijze betrokken zijn bij een cyberaanval (bijvoorbeeld middels financiële of technische steun). De maatregelen die kunnen worden opgelegd aan personen en organisaties bestaan uit de bevrozing van fondsen of andere vermogensbestanddelen en reisbeperkingen.

Op grond van dit wettelijk kader kan de EU dientengevolge sancties opleggen aan (a) personen of entiteiten die verantwoordelijk zijn voor cyberaanvallen of pogingen tot cyber-aanvallen, (b) die financiële, technische of materiële steun leveren voor zulke aanvallen of die er op een andere manier bij betrokken zijn en ook aan (c) de personen of entiteiten die daarmee zijn geassocieerd kunnen sancties worden opgelegd.

Cyberaanvallen bevatten één van de volgende activiteiten: zich toegang verschaffen tot informatiesystemen, verstoren van informatiesystemen, verstoren van gegevens, of onderscheppen van gegevens.

De personen en entiteiten die aan de beperkende maatregelen onderworpen zijn, zijn opgesomd in de bijlage I bij de Verordening (EU) 2019/796 respectievelijk de bijlage bij het Besluit (GBVB) 2019/797 en kunnen worden vastgesteld als afschrikking tegen en reactie op cyberaanvallen met aanzienlijke gevolgen die een externe bedreiging vormen voor de Europese Unie of haar lidstaten.

De personen en entiteiten die aan de beperkende maatregelen onderworpen zijn, worden voor het eerst genoemd in de bijlage behorende bij de Uitvoeringsverordening (EU) 2020/1125 respectievelijk het Besluit (GBVB) 2020/1127 van de Raad van 30 juli 2020 tot uitvoering van Verordening (EU) 2019/796 van de Raad betreffende

¹ Vide Besluit (GBVB) 2019/797 van de Raad van 17 mei 2019 betreffende beperkende maatregelen tegen cyberaanvallen die de Unie of haar lidstaten bedreigen (PbEU 2019, L1 129).

² Vide Verordening (EU) nr. 2019/796 van de Raad van 17 mei 2019 betreffende beperkende maatregelen tegen cyberaanvallen die de Unie of haar lidstaten bedreigen (PbEU 2019, L1 129).

beperkende maatregelen tegen cyberaanvallen die de Unie of haar lidstaten bedreigen.³ De Raad van de Europese Unie heeft besloten dat de in de voorgenoemde bijlage van Uitvoeringsverordening (EU) 2020/1125 respectievelijk het Besluit (GBVB) 2020/1127 vermelde personen en entiteiten, moeten worden toegevoegd aan de lijst van personen en entiteiten waarop de beperkende maatregelen van Verordening (EU) 2019/796 en Besluit (GBVB) 2019/797 van toepassing zijn.

De redenen voor de opnemng van de betrokken personen en entiteiten staan aangegeven in de desbetreffende vermeldingen in die bijlagen. De beperkende maatregelen betreffen 6 personen en 3 entiteiten die verantwoordelijk zijn voor of betrokken zijn bij verschillende cyberaanvallen. Het gaat onder meer om een poging tot een cyberaanval op de Organisatie voor het Verbod van Chemische Wapens (OPCW)⁴ in Nederland, en de aanvallen die bekend werden onder de namen 'WannaCry', 'NotPetya' en 'Operation Cloud Hopper'.

In het kader van het gemeenschappelijk buitenland- en veiligheidsbeleid van het Koninkrijk alsmede met het oog op de bescherming van de integriteit en reputatie van Aruba en haar financiële sector, heeft de regering besloten, met gebruikmaking van de artikelen 2 en 2a van de Sanctieverordening 2006 (AB 2007 no. 24), om het cybersanctieregime betreffende beperkende maatregelen tegen cyberaanvallen die de Europese Unie of haar lidstaten bedreigen met het oog op de bevrozing van fondsen of andere vermogensbestanddelen te implementeren. Het onderhavige landsbesluit voorziet in de bevrozing van fondsen of andere vermogensbestanddelen van natuurlijke personen, rechtspersonen en entiteiten, die betrokken zijn bij cyberaanvallen.

Aan de invoering van dit wijzigingsbesluit zijn geen financiële consequenties voor het Land verbonden. Tot slot zij vermeld dat de regering, omdat dit landsbesluit strekt tot de onverwijlde uitvoering van een aantal internationaal besluiten, heeft besloten het horen van de Raad van Advies achterwege te laten. De mogelijkheid daartoe wordt geboden door het tweede lid van artikel 2 van de Sanctieverordening 2006.

³ Vide Besluit (GBVB) 2020/1127 van de Raad van 30 juli 2020 tot wijziging van Besluit (GBVB) 2019/797 betreffende beperkende maatregelen tegen cyberaanvallen die de Unie of haar lidstaten bedreigen en Uitvoeringsverordening (EU) 2020/1125 van de Raad van 30 juli 2020 tot uitvoering van Verordening (EU) 2019/796 betreffende beperkende maatregelen tegen cyberaanvallen die de Unie of haar lidstaten bedreigen.

⁴ In het Engels: *Organisation for the Prohibition of Chemical Weapons*. De Organisatie voor het Verbod op Chemische Wapens (OPCW) is een autonome internationale, multilaterale organisatie die haar zetel heeft in Den Haag en werkt samen met de Verenigde Naties.

In de hierna volgende artikelsgewijze toelichting zal nader worden ingegaan op de artikelen van het onderhavige landsbesluit.

Artikelsgewijze toelichting

Artikel 1

Dit artikel bevat een aantal noodzakelijke begripsbepalingen. Het is niet uitgesloten dat aan de verschillende bijlagen behorende bij de vermelde Verordening (EU) 2019/796 en Besluit (GBVB) 2019/79, meer natuurlijke personen, rechtspersonen, entiteiten en lichamen worden toegevoegd. Om te voorkomen dat telkens een wijziging is vereist, wordt voorzien in een dynamische verwijzing voor in het bijzonder van de bijlagen behorende bij de Verordening (EU) 2019/796 en het Besluit (GBVB) 2019/797.

Artikel 2

Op grond van dit artikel dienen de fondsen en andere vermogensbestanddelen te worden bevroren van personen, ondernemingen of instellingen die op de verschillende bijlage van de EU-sancties staan vermeld. Dit geeft naar het oordeel van de regering voldoende juridische basis om in ieder geval aan de bevroeringsmaatregelen uitvoering te geven.

Artikel 3

Het eerste lid belast de Centrale Bank van Aruba (de Bank) met de bekendmaking van bijlage op een tijdige en digitale wijze via de website www.cbaruba.org. Zodoende kan op een efficiënte en doeltreffende wijze uitvoering worden gegeven met de beoogde bevroeringsmaatregelen. De EU-sancties zijn ook te vinden in het Publicatieblad van de Europese Unie en zijn eenvoudig te raadplegen via de website <http://eur-lex.europa.eu>.

Daarbij moet ook rekening worden gehouden met het feit dat de bijlage voortdurend aanpassingen kunnen ondergaan. Van deze wijzigingen dienen naast bijvoorbeeld de financiële dienstverleners ook de aangewezen niet-financiële dienstverleners (*Designated Non-Financial Businesses and Professions (DNFBP's)*) waaronder advocaten, accountants, belastingadviseurs, makelaars, notarissen, autohandelaren en juweliers steeds voortdurend op de hoogte te zijn.

Artikel 4

Dit artikel verplicht een ieder om geen diensten te verlenen en geen handelingen te verlenen die ertoe leiden of redelijkerwijs ertoe kunnen leiden dat een natuurlijke persoon, rechtspersoon of andere entiteit, vermeld op de bijlage van de EU-verordening respectievelijk EU-besluit, op enigerlei wijze de beschikking krijgt over de krachtens artikel 2 bevroren fondsen of andere vermogensbestanddelen. Daarbij gaat het niet alleen om diensten in de zin van artikel 1 van het onderhavige landsbesluit, maar tevens om elke feitelijke handeling die ertoe leidt dat een fonds of vermogensbestanddeel in de macht van een aangewezen persoon wordt gebracht. Voor de goede orde zij opgemerkt dat de overtreding van dit verbod strafbaar is gesteld op grond van artikel 17 van de Sanctieverordening 2006.

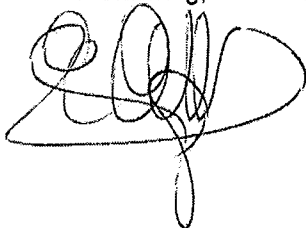
Artikel 5

Ingevolge dit artikel dienen de dienstverleners onverwijld maatregelen te treffen, voor zover zij fondsen of vermogensbestanddelen van een natuurlijke persoon, rechtspersoon of andere entiteit, vermeld in de bijlagen van de EU-sancties, onder zich hebben waardoor deze fondsen en vermogensbestanddelen niet in strijd met de bevrozing overgemaakt, omgezet, verplaatst of ter beschikking kunnen worden gesteld aan een natuurlijke persoon, rechtspersoon of andere entiteit, vermeld op die bijlage van de EU-sancties.

Artikel 6

Artikel 6 bevat tenslotte de inwerkingtredingsbepaling. Dit wijzigingsbesluit treedt in werking met ingang van de dag na de datum van uitgifte van het Afkondigingsblad van Aruba aangezien er internationale sancties worden geïmplementeerd.

De minister van Algemene Zaken, Integriteit,
Overheidszorg, Innovatie en Energie,



De minister van Financiën, Economische Zaken,
en Cultuur,



De minister van Justitie, Veiligheid
en Integratie,



Enclosure: 3

2020 No. 125

**OFFICIAL BULLETIN
OF
ARUBA**

STATE DECREE containing general administrative orders of August 26, 2020 for the implementation of Articles 2 and 2a of the Sanctions Ordinance 2006 ("AB" [*Official Bulletin*] 2007 No. 24) (Sanctions State Decree Cyber-Attacks)

Published on August 27, 2020

The Minister of Justice,
Security and Integration,

A.C.G. Bikker

IN THE NAME OF THE KING!

THE GOVERNOR of Aruba,

Having considered:

that, in the interests of the foreign policy of the Kingdom and in the interests of international legal order, it is desirable to implement Regulation No. 2019/796 of the Council of the European Union of May 17, 2019 and Decision (CFSP) 2019/797 of May 17, 2019 concerning restrictive measures against cyber-attacks threatening the European Union or its Member States;

Having regard to:

Articles 2 and 2a of the Sanctions Ordinance 2006 (AB 2007 No. 24);

Has decided:

§ 1. General

Article 1

For the purposes of this State Decree, the following definitions shall apply:

Bank	: the Central Bank of Aruba;
Decision 2019/797	: Decision (CFSP) 2019/797 of May 17, 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States, with its Annexes, including any subsequent amendments made to those Annexes;
to freeze	: a prohibition to transfer, convert, move or make available;
service	: an activity relating to a fund or other asset;

service provider	: any person providing a service on a professional or commercial basis;
funds or other assets	: property, however acquired, as referred to in Article 1 of Book 3 of the Civil Code of Aruba, all documents and data carriers, in any form or capacity whatsoever, evidencing full or shared ownership of or title to any property, and products, respectively;
Minister	: the Minister responsible for financial matters;
Financial Intelligence Unit	: the Financial Intelligence Unit, as referred to in Article 20, first paragraph, of the State Ordinance on the Prevention and Combating of Money Laundering and Terrorist Financing (AB 2011 No. 28);
Regulation No. 2019/796	: Regulation (EU) No. 2019/796 of May 17, 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States, with its Annexes, including any subsequent amendments made to those Annexes.

§ 2. The freezing of funds and other assets

Article 2

1. All funds or other assets in Aruba, directly or indirectly belonging to, owned, held or controlled by a natural person, a legal person, entities or bodies listed in Annex I to Regulation No. 2019/796 and the Annex to Decision 2019/797 shall be frozen.
2. The freezing, referred to in the first paragraph, shall apply *mutatis mutandis* to representatives of the natural persons, legal persons, entities or bodies mentioned in that paragraph.
3. Notwithstanding the first paragraph, a designated person may be granted access to his frozen funds or assets for funds, financial assets or economic resources that are:

- a. necessary to cover expenses for the basic needs of the natural persons listed in Annex I to Regulation No. 2019/796 and the Annex to Decision 2019/797 and dependent family members of such natural persons, including payments for foodstuffs, rent or mortgage, medicines or medical treatments, taxes, insurance premiums and public utility charges;
 - b. intended exclusively for the payment of reasonable professional fees or the reimbursement of incurred expenses in connection with the provision of legal services;
 - c. intended exclusively for the payment of fees or costs for the routine holding or management of frozen funds or economic resources, or
 - d. necessary for the payment of extraordinary expenses, provided that the Minister has been notified of the reasons why this person feels that specific permission should be granted at least two weeks in advance.
4. Access to frozen funds or assets shall only be granted with the approval of the Minister.

Article 3

1. The Bank shall be responsible for the digital publication of the current text of Annex I to Regulation No. 2019/796 and the Annex to Decision 2019/797.
2. Service providers shall make such arrangements as to ensure that they are at all times aware of the content of Annex I to Regulation No. 2019/796 and the Annex to Decision 2019/797.

Article 4

1. It shall be prohibited for everyone to provide services or to perform acts that result or can reasonably result in a natural person, legal person or other entity listed in Annex I to Regulation No. 2019/796 and the Annex to Decision 2019/797 gaining access in any way to funds or other assets.
2. It shall be prohibited to participate knowingly or intentionally in activities of which the object or effect is to circumvent directly or indirectly the measures referred to in the first paragraph.

Article 5

1. Anyone having custody of funds or other assets of a natural person, legal person or other entity listed in Annex I to Regulation No. 2019/796 and the Annex to Decision 2019/797 shall take such measures that these funds and assets cannot be used, or that these funds and other assets cannot be transferred, converted, moved or be made available.
2. If it concerns a service provider supervised by the Bank by or pursuant to a state ordinance, it shall immediately inform the Bank of the funds or other assets it has in its custody. The preceding sentence shall apply mutatis mutandis to designated non-financial service providers.
3. Service providers shall promptly inform the Financial Intelligence Unit of all transactions intended or performed by or on behalf of persons, entities and bodies listed in Annex I to Regulation No. 2019/796 and the Annex to Decision 2019/797.

§ 3. Final provision

Article 6

1. This State Decree shall enter into force as of the day following the day of its publication in the Official Bulletin of Aruba.
2. It may be cited as Sanctions State Decree Cyber-Attacks.

Given in Oranjestad, August 26, 2020
J.A. Boekhoudt

The Minister of General Affairs, Integrity,
Government Org., Innovation and Energy,
E.C. Wever-Croes

The acting Minister of Finance, Economic Affairs
and Culture,
E.C. Wever-Croes

The Minister of Justice, Security
and Integration,
A.C.G. Bikker

EXPLANATORY MEMORANDUM

General explanation

On 17 May 2019, the Council of the European Union (hereinafter: EU) adopted the cyber sanctions regime consisting of Decision (CFSP) 2019/797¹ and Regulation (EU) 2019/796.² This specific sanctions regime enables the EU to take measures worldwide against persons and organizations that are responsible for a cyber-attack or an attempted cyber-attack, or are involved in a cyber-attack in any other way (e.g. through financial or technical support). The measures that may be imposed on persons and organizations include the freezing of funds or other assets and travel restrictions.

Based on this legal framework, the EU may therefore impose sanctions on (a) persons or entities who are responsible for cyber-attacks or attempted cyber-attacks, (b) who provide financial, technical or material support for such attacks, or who are otherwise involved in such attacks, and (c) persons or entities associated with them may also be subject to sanctions. Cyber-attacks include any of the following activities: access to information systems, information system interference, data interference or data interception.

The persons and entities subject to the restrictive measures are listed in Annex I to Regulation (EU) 2019/796 and the Annex to Decision (CFSP) 2019/797, respectively, and such restrictive measures may be adopted to deter and counteract against cyber-attacks with a significant effect which constitute an external threat to the European Union or its Member States.

The persons and entities subject to the restrictive measures are mentioned for the first time in the Annex to Council Implementing Regulation (EU) 2020/1125 and Council Decision (CFSP) 2020/1127 of July 30, 2020 implementing Council Regulation (EU) 2019/796 concerning restrictive measures against cyber-attacks threatening the Union or its Member

¹ See Council Decision (CFSP) 2019/797 of May 17, 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States (OJEU 2019, L1 129).

² See Council Regulation (EU) No. 2019/796 of May 17, 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States (OJEU 2019, L1 129).

States.³ The Council of the European Union has decided that the persons and entities listed in aforementioned Annex to Implementing Regulation (EU) 2020/1125 and Decision (CFSP) 2020/1127, respectively, should be added to the list of persons and entities that are subject to the restrictive measures provided for in Regulation (EU) 2019/796 and Decision (CFSP) 2019/797.

The reasons for listing the persons and entities concerned appear in the relevant entries in those Annexes. The restrictive measures concern 6 persons and 3 entities responsible for or involved in several cyber-attacks. These include *inter alia* an attempted cyber-attack on the Organization for the Prohibition of Chemical Weapons (OPCW)⁴ in the Netherlands, and the attacks that became known as “WannaCry”, “NotPetya” and “Operation Cloud Hopper”.

Within the framework of the common foreign and security policy of the Kingdom and in order to protect the integrity and reputation of Aruba and its financial sector, the Government has decided, using Articles 2 and 2a of the Sanctions Ordinance 2006 (AB 2007 No. 24), to implement the cyber sanctions regime concerning restrictive measures against cyber-attacks threatening the European Union or its Member States aimed at the freezing of funds or other assets. This State Decree provides for the freezing of funds or other assets of natural persons, legal persons and entities involved in cyber-attacks.

The introduction of this amending decree does not entail any financial consequences for the Government. Finally, it should be noted that, since this State Decree is intended to implement a number of international decisions without delay, the Government has decided not to hear the Advisory Council. The possibility to do so is offered by the second paragraph of Article 2 of the Sanctions Ordinance 2006.

In the following explanatory notes on the individual Articles, the Articles of this State Decree will be discussed in more detail.

³ See Council Decision (CFSP) 2020/1127 of July 30, 2020 amending Decision (CFSP) 2019/797 concerning restrictive measures against cyber-attacks threatening the Union or its Member States and Council Implementing Regulation (EU) 2020/1125 of July 30, 2020 implementing Regulation (EU) 2019/796 concerning restrictive measures against cyber-attacks threatening the Union or its Member States.

⁴ The Organization for the Prohibition of Chemical Weapons (OPCW) is an autonomous international, multilateral organization that has its seat in The Hague and cooperates with the United Nations.

Explanatory notes on the individual Articles

Article 1

This Article contains a number of necessary definitions. It cannot be ruled out that more natural persons, legal persons, entities or bodies will be added to the various Annexes to aforementioned Regulation (EU) 2019/796 and Decision (CFSP) 2019/79. In order to avoid that an amendment is required each time, a dynamic reference is provided for, in particular, for the Annexes to Regulation (EU) 2019/796 and Decision (CFSP) 2019/797.

Article 2

Based on this Article, the funds and other assets of persons, enterprises or institutions listed in the various Annexes to the EU sanctions are frozen. The Government is of the opinion that this provides for a sufficient legal basis to implement the freezing measures, in any case.

Article 3

The first paragraph entrusts the Central Bank of Aruba (the Bank) with the timely and digital publication of the Annex via the website www.cbaruba.org. This will ensure that the intended freezing measures can be implemented efficiently and effectively. The EU sanctions can also be found in the Official Journal of the European Union and are easily accessible via the website <http://eur-lex.europa.eu>.

The fact that the Annex will be subject to constant adjustment must also be taken into account. In addition to financial service providers, the Designated Non-Financial Businesses and Professions (DNFBPs), including lawyers, accountants, tax consultants, brokers, civil-law notaries, car dealers and jewelers, should also be familiar with these adjustments at all times.

Article 4

This Article requires everyone not to provide services and to refrain from acts that result or can reasonably result in a natural person, legal person or other entity listed in the Annex to the EU Regulation and the EU Decision, respectively, disposing in any way of the funds or other assets frozen pursuant to Article 2. This applies not only to services within the meaning of Article 1 of this State Decree, but also to any act that has the effect of placing a fund or an asset under the control of a designated

person. For the record, it should be noted that the violation of this prohibition has been made punishable under Article 17 of the Sanctions Ordinance 2006.

Article 5

This Article requires service providers to take immediate action, insofar as they have funds or assets of a natural person, legal person or other entity listed in the Annexes to the EU sanctions in their custody, as a result of which those funds and assets cannot be transferred, converted, moved or made available to a natural person, legal person or other entity listed in the Annex to the EU sanctions in violation of the freezing order.

Article 6

Finally, Article 6 contains the provision on the entry into force. This amending decree enters into force as of the day following the date of issue of the Official Bulletin of Aruba, given that international sanctions are being implemented.

The Minister of General Affairs, Integrity,
Government Org., Innovation and Energy,
[was signed]

The Minister of Finance, Economic Affairs
and Culture,
[was signed]

The Minister of Justice, Security
and Integrity,
[was signed]

DECISIONS

COUNCIL DECISION (CFSP) 2019/797

of 17 May 2019

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 19 June 2017 the Council adopted conclusions on a framework for a joint diplomatic response to malicious cyber activities (the Cyber Diplomacy Toolbox), in which the Council expressed concerns about the increased ability and willingness of State and non-State actors to pursue their objectives by undertaking malicious cyber activities and affirmed the growing need to protect the integrity and security of the Union, its Member States and their citizens against cyber threats and malicious cyber activities.
- (2) The Council stressed that clearly signalling the likely consequences of a joint Union diplomatic response to such malicious cyber activities influences the behaviour of potential aggressors in cyberspace, thereby reinforcing the security of the Union and its Member States. It also affirmed that measures within the common foreign and security policy (CFSP), including, if necessary, restrictive measures, adopted under the relevant provisions of the Treaties, are suitable for a framework for a joint Union diplomatic response to malicious cyber activities, with the aim of encouraging cooperation, facilitating the mitigation of immediate and long-term threats, and influencing the behaviour of potential aggressors in the long term.
- (3) On 11 October 2017 implementing guidelines for the Cyber Diplomacy Toolbox were approved by the Political and Security Committee. The implementing guidelines refer to five categories of measures, including restrictive measures, within the Cyber Diplomacy Toolbox, and the process for invoking those measures.
- (4) The Council conclusions adopted on 16 April 2018 on malicious cyber activities firmly condemned the malicious use of information and communications technologies (ICTs) and stressed that the use of ICTs for malicious purposes is unacceptable as it undermines the stability, security and benefits provided by the internet and the use of ICTs. The Council recalled that the Cyber Diplomacy Toolbox contributes to conflict prevention, cooperation and stability in cyberspace by setting out measures within the CFSP, including restrictive measures, that can be used to prevent and respond to malicious cyber activities. It stated that the Union will continue strongly to uphold that existing international law is applicable to cyberspace and emphasised that respect for international law, in particular the United Nations Charter, is essential to maintaining peace and stability. The Council also underlined that States are not to use proxies to commit internationally wrongful acts using ICTs, and should seek to ensure that their territory is not used by non-State actors to commit such acts as expressed in the 2015 report of the United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security.
- (5) On 28 June 2018 the European Council adopted conclusions which stressed the need to strengthen capabilities against cybersecurity threats from outside the Union. The European Council asked the institutions and Member States to implement the measures referred to in the joint communication of the Commission and the High Representative of the Union for Foreign Affairs and Security Policy of 13 June 2018 entitled 'Increasing resilience and bolstering capabilities to address hybrid threats', including the practical use of the Cyber Diplomacy Toolbox.
- (6) On 18 October 2018 the European Council adopted conclusions which called for the work on the capacity to respond to and deter cyber-attacks through Union restrictive measures to be taken forward, further to the Council conclusions of 19 June 2017.

- (7) In this context, this Decision establishes a framework for targeted restrictive measures to deter and respond to cyber-attacks with a significant effect which constitute an external threat to the Union or its Member States. Where deemed necessary to achieve CFSP objectives in the relevant provisions of Article 21 of the Treaty on European Union, this Decision also allows for restrictive measures to be applied in response to cyber-attacks with a significant effect against third States or international organisations.
- (8) In order to have a deterrent and dissuasive effect, targeted restrictive measures should focus on cyber-attacks falling within the scope of this Decision that are wilfully carried out.
- (9) Targeted restrictive measures should be differentiated from the attribution of responsibility for cyber-attacks to a third State. The application of targeted restrictive measures does not amount to such attribution, which is a sovereign political decision taken on a case-by-case basis. Every Member State is free to make its own determination with respect to the attribution of cyber-attacks to a third State.
- (10) Further action by the Union is needed in order to implement certain measures,

HAS ADOPTED THIS DECISION:

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; 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.

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.

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.

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) necessary to satisfy the basic needs of the natural persons 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) 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.

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.

Article 10

This Decision shall apply until 18 May 2020 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.

Article 11

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

Done at Brussels, 17 May 2019.

For the Council
The President
E.O. TEODOROVICI

ANNEX

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

II

(Non-legislative acts)

REGULATIONS

COUNCIL REGULATION (EU) 2019/796

of 17 May 2019

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 the Functioning of the European Union, and in particular Article 215 thereof,

Having regard to Council Decision (CFSP) 2019/797 of 17 May 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States ⁽¹⁾,

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

Whereas:

- (1) On 18 October 2018 the European Council adopted conclusions which called for the work on the capacity to respond to and deter cyber-attacks through Union restrictive measures to be taken forward, further to the Council conclusions of 19 June 2017.
- (2) On 17 May 2019 the Council adopted Decision (CFSP) 2019/797. Decision (CFSP) 2019/797 establishes a framework for targeted restrictive measures to deter and respond to cyber-attacks with a significant effect which constitute an external threat to the Union or its Member States. Persons, entities and bodies subject to the restrictive measures are listed in the Annex to that Decision.
- (3) This Regulation respects the fundamental rights and observes the principles recognised by the Charter of Fundamental Rights of the European Union, in particular the right to an effective remedy and to a fair trial and the right to the protection of personal data. This Regulation should be applied in accordance with those rights.
- (4) The power to establish and amend the list in Annex I to this Regulation should be exercised by the Council in order to ensure consistency with the process for establishing, amending and reviewing the Annex to Decision (CFSP) 2019/797.
- (5) For the implementation of this Regulation, and in order to ensure maximum legal certainty within the Union, the names and other relevant data concerning natural and legal persons, entities and bodies whose funds and economic resources are to be frozen in accordance with this Regulation should be made public. Any processing of personal data should comply with Regulations (EU) 2016/679 ⁽²⁾ and (EU) 2018/1725 ⁽³⁾ of the European Parliament and of the Council.

⁽¹⁾ See page 13 of this Official Journal.

⁽²⁾ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016, p. 1).

⁽³⁾ Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39).

- (6) Member States and the Commission should inform each other of the measures taken pursuant to this Regulation and of other relevant information at their disposal in connection with this Regulation.
- (7) Member States should lay down rules on sanctions applicable to infringements of the provisions of this Regulation and make sure that they are implemented. Those sanctions should be effective, proportionate and dissuasive,

HAS ADOPTED THIS REGULATION:

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;
- (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;
 - (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;
- (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.

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) necessary to satisfy the basic needs of the natural persons 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.
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:
 - (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.

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.
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.

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.

Done at Brussels, 17 May 2019.

For the Council
The President
E.O. TEODOROVICI

ANNEX I

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

[...]

ANNEX II

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

BELGIUM

https://diplomatie.belgium.be/nl/Beleid/beleidstemas/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.financnianalytickyrad.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>

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/kvyhteisty/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

COUNCIL IMPLEMENTING REGULATION (EU) 2020/1125**of 30 July 2020****implementing Regulation (EU) 2019/796 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 the Functioning of the European Union,

Having regard to Council Regulation (EU) 2019/796 of 17 May 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States⁽¹⁾, and in particular Article 13(1) 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 Regulation (EU) 2019/796.
- (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 competitiveness, 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 Annex I to Regulation (EU) 2019/796. 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) Regulation (EU) 2019/796 should therefore be amended accordingly,

HAS ADOPTED THIS REGULATION:

Article 1

Annex I to Regulation (EU) 2019/796 is amended in accordance with the Annex to this Regulation.

⁽¹⁾ OJ L 129I, 17.5.2019, p. 1.

Article 2

This Regulation shall enter into force on the date 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.

Done at Brussels, 30 July 2020.

For the Council
The President
M. ROTI

The following persons and entities or bodies are added to the list of natural and legal persons, entities and bodies set out in Annex I to Regulation (EU) 2019/796:

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	<p>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.</p> <p>"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.</p> <p>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.</p>	30.7.2020
2.	ZHANG Shilong	Address: Hedong, Yuyang Road No 121, Tianjin, China Nationality: Chinese Gender: male	<p>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.</p> <p>"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.</p> <p>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".</p> <p>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.</p>	30.7.2020

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 Sergeyevich 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 Mikhailovich 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. "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.	30.7.2020

			<p>"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.</p> <p>The actor publicly known as "APT38" ("Advanced Persistent Threat 38") or the "Lazarus Group" carried out "WannaCry".</p> <p>Chosun Expo can be linked to APT38 / the Lazarus Group, including through the accounts used for the cyber-attacks.</p>	
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	<p>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.</p> <p>"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.</p> <p>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".</p> <p>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.</p>	30.7.2020'