COUNCIL DECISION (CFSP) 2020/1127
of 30 July 2020
amending Decision (CFSP) 2019/797 concerning restrictive measures against cyber-attacks threatening the Union or its Member States

THE COUNCIL OF THE EUROPEAN UNION,

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

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

Whereas:

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

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

(3) On 16 April 2018 the Council adopted conclusions in which it firmly condemned the malicious use of information and communications technologies, including in the cyber-attacks publicly known as 'WannaCry' and 'NotPetya', which caused significant damage and economic loss in the Union and beyond. On 4 October 2018 the Presidents of the European Council and of the European Commission and the High Representative of the Union for Foreign Affairs and Security Policy (the 'High Representative') expressed serious concerns in a joint statement about an attempted cyber-attack to undermine the integrity of the Organisation for the Prohibition of Chemical Weapons (OPCW) in the Netherlands, an aggressive act which demonstrated contempt for the solemn purpose of the OPCW. In a declaration made on behalf of the Union on 12 April 2019, the High Representative urged actors to stop undertaking malicious cyber-activities that aim to undermine the Union's integrity, security and economic 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 the Annex to Decision (CFSP) 2019/797. Those persons and entities or bodies are responsible for, provided support for or were involved in, or facilitated cyber-attacks or attempted cyber-attacks, including the attempted cyber-attack against the OPCW and the cyber-attacks publicly known as 'WannaCry' and 'NotPetya', as well as 'Operation Cloud Hopper'.

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

HAS ADOPTED THIS DECISION:

Article 1

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

Article 2

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

Done at Brussels, 30 July 2020.

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

'A. Natural persons

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

3. Alexey Valeryevich MININ

| 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.

4. Aleksei Sergeyevich MORENETS

| 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.
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.

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.

### B. Legal persons, entities and bodies

<table>
<thead>
<tr>
<th>Name</th>
<th>Identifying information</th>
<th>Reasons</th>
<th>Date of listing</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Tianjin Huaing Haitai Science and Technology Development Co. Ltd (Huaing Haitai)</td>
<td>a.k.a.: Haitai Technology Development Co. Ltd</td>
<td>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.</td>
<td>30.7.2020</td>
</tr>
</tbody>
</table>
"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.

Chosun Expo provided financial, technical or material support for and facilitated a series of cyber-attacks with a significant effect originating from outside the Union and constituting an external threat to the Union or its Member States and of cyber-attacks with a significant effect against third States, including the cyber-attacks publicly known as "WannaCry" and cyber-attacks against the Polish Financial Supervision Authority and Sony Pictures Entertainment, as well as cyber-theft from the Bangladesh Bank and attempted cyber-theft from the Vietnam Tien Phong Bank.

"WannaCry" disrupted information systems around the world by targeting information systems with ransomware and blocking access to data. It affected information systems of companies in the Union, including information systems relating to services necessary for the maintenance of essential services and economic activities within Member States.

The actor publicly known as “APT38” (“Advanced Persistent Threat 38”) or the "Lazarus Group" carried out "WannaCry".

Chosun Expo can be linked to APT38/the Lazarus Group, including through the accounts used for the cyber-attacks.

The Main Centre for Special Technologies (G TsST) of the Main Directorate of the General Staff of the Armed Forces of the Russian Federation (GU/GRIU), also known by its field post number 74455, is responsible for cyber-attacks with a significant effect originating from outside the Union and constituting an external threat to the Union or its Member States and for cyber-attacks with a significant effect against third States, including the cyber-attacks publicly known as “NotPetya” or “EternalPetya” in June 2017 and the cyber-attacks directed at an Ukrainian power grid in the winter of 2015 and 2016.
“NotPetya” or “EternalPetya” rendered data inaccessible in a number of companies in the Union, wider Europe and worldwide, by targeting computers with ransomware and blocking access to data, resulting amongst others in significant economic loss. The cyber-attack on a Ukrainian power grid resulted in parts of it being switched off during winter.

The actor publicly known as “Sandworm” (a.k.a. “Sandworm Team”, “BlackEnergy Group”, “Voodoo Bear”, “Quedagh”, “Olympic Destroyer” and “Telebots”), which is also behind the attack on the Ukrainian power grid, carried out “NotPetya” or “EternalPetya”.

The Main Centre for Special Technologies of the Main Directorate of the General Staff of the Armed Forces of the Russian Federation has an active role in the cyber-activities undertaken by Sandworm and can be linked to Sandworm.