Office of Financial Sanctions Implementation
HM Treasury

CONSOLIDATED LIST OF FINANCIAL SANCTIONS TARGETS IN THE UK

Last Updated:05/07/2022

Status: Asset Freeze Targets

REGIME: Cyber

INDIVIDUALS

1. **Name 6:** BADIN **1:** DMITRY **2:** SERGEYEVICH **3:** n/a **4:** n/a **5:** n/a.
DOB: 15/11/1990. **POB:** Kursk **Nationality:** Russia **Position:** Military Intelligence Officer **Other Information:** (UK Sanctions List Ref):CYB0010 (UK Statement of Reasons):Dmitry Sergevey Badin took part in a cyber attack against the German Federal Parliament (Deutscher Bundestag) with significant effect. As a military intelligence officer of the 85th Main Centre for Special Technologies (GTsSS) of the Russian General Staff of the Armed Forces of the Russian Federation (GRU), Dmitry Badin was part of a team of Russian Military intelligence officers which conducted a cyber attack against the German federal parliament (Deutscher Bundestag) in April and May 2015. This cyber attack targeted the parliament's information system and affected its operation for several days. A significant amount of data was stolen and the email accounts of several MPs, as well as Chancellor Angela Merkel, were affected. (Gender):Male **Listed on:** 23/10/2020 **UK Sanctions List Date Designated:** 31/12/2020 **Last Updated:** 31/12/2020 **Group ID:** 13983.
2. **Name 6:** GAO **1:** QIANG **2:** n/a **3:** n/a **4:** n/a **5:** n/a.
DOB: 04/10/1983. **POB:** Shandong Province, China **a.k.a:** FISHERXP **Nationality:** China **Address:** Room 1102, Guanfu Mansion, 46 Xinkai Road, Hedong District, Tianjin, China.**Other Information:** (UK Sanctions List Ref):CYB0001 (UK Statement of Reasons):Gao Qiang was involved in relevant cyber activity through his employment with Huaying Haitai and setting up command and control infrastructure used to conduct relevant cyber activity. He was therefore responsible for, engaged in, provided support for, or promoted the commission, planning or preparation of relevant cyber activity. (Gender):Male **Listed on:** 31/07/2020 **UK Sanctions List Date Designated:** 31/12/2020 **Last Updated:** 31/12/2020 **Group ID:** 13903.
3. **Name 6:** KOSTYUKOV **1:** IGOR **2:** OLEGOVICH **3:** n/a **4:** n/a **5:** n/a.
Name (non-Latin script): Игорь Олегович КОСТЮКОВ
DOB: (1) 21/02/1961. (2) 21/01/1961. **POB:** Amur Oblast **Nationality:** Russia **Position:** Head of the Main Directorate of the General Staff of the Armed Forces of the Russian Federation (GRU/GU). Head of the Russian General Staff's Main Intelligence Department (GRU) of the Russian Federation **Other Information:** (UK Sanctions List Ref):CHW0009 and CYB0011 Listed under the Chemical Weapons and Cyber sanctions regimes. (UK Statement of Reasons):Igor Olegovich Kostyukov, given his senior leadership role as First Deputy Head of the GRU (a.k.a. GU) at that time, is responsible for the possession, transport and use in Salisbury during the weekend of 4 March 2018 of the toxic nerve agent "Novichok" by officers from the GRU. Igor Kostyukov is the Head of the Russian General Staff's Main Intelligence Department (GRU), and was previously First Deputy Head. In this capacity, Igor Kostyukov is responsible for cyber attacks carried out by the 85th Main Centre of Special Services (GTsSS), also referred to as Field Post Number 26165, APT28, Fancy Bear, Sofacy Group, Pawn Storm, Strontium. These attacks include the cyber attack against the German federal parliament (Deutscher Bundestag) in April and May 2015. The cyber attack against the German federal parliament (Deutscher Bundestag) targeted the parliament's information system and affected its operation for several days. A significant amount of data was stolen and e-mail accounts of several MPs as well as Chancellor Angela Merkel were affected. (Gender):Male **Listed on:** 23/10/2020 **UK Sanctions List Date Designated:** 31/12/2020 **Last Updated:** 31/12/2020 **Group ID:** 13748.
4. **Name 6:** MININ **1:** ALEXEI **2:** VELERYEVICH **3:** n/a **4:** n/a **5:** n/a.
DOB: 27/05/1972. **POB:** Perm Oblast, Russia **a.k.a:** MININ, Alexey, Valeryevich **Nationality:** Russia **Passport Number:** 120017582 **Address:** Moscow, Russia.**Position:** HUMINT Support (GRU) **Other Information:** (UK Sanctions List Ref):CYB0005 (UK Statement of Reasons):Alexey Valeryevich Minin was part of a team of intelligence officers of the Russian General Staff Main Intelligence Directorate (GRU) unit known as field post number 26165 that attempted to gain unauthorised access to the information systems of the Organisation for the Prohibition of Chemical Weapons (OPCW) in April 2018. The Netherlands authorities disrupted the cyber attack before it was successful. This attempted relevant cyber activity was intended to undermine the independence or effective

functioning of an international organisation. (Gender):Male **Listed on:** 31/07/2020 **UK Sanctions List Date Designated:** 31/12/2020 **Last Updated:** 31/12/2020 **Group ID:** 13905.

5. **Name 6:** MORENENTS **1:** ALEKSEI **2:** SERGEYVICH **3:** n/a **4:** n/a **5:** n/a.
DOB: 31/07/1977. **POB:** Moermanskaya Oblast, Russia **Nationality:** Russia **Passport Number:** 100135556 **Address:** Moscow, Russia.**Position:** Cyber Operator (GRU) **Other Information:** (UK Sanctions List Ref):CYB0006 (UK Statement of Reasons):Aleksei Sergeyvich Morenets was part of a team of intelligence officers of the Russian General Staff Main Intelligence Directorate (GRU) unit known as field post number 26165 that attempted to gain unauthorised access to the information systems of the Organisation for the Prohibition of Chemical Weapons (OPCW) in April 2018. The Netherlands authorities disrupted the cyber attack before it was successful. This attempted relevant cyber activity was intended to undermine the independence or effective functioning of an international organisation. (Gender):Male **Listed on:** 31/07/2020 **UK Sanctions List Date Designated:** 31/12/2020 **Last Updated:** 31/12/2020 **Group ID:** 13906.

6. **Name 6:** SEREBRIAKOV **1:** EVGENII **2:** MIKHAYLOVICH **3:** n/a **4:** n/a **5:** n/a.
DOB: 26/07/1981. **POB:** Koersk, Russia **Nationality:** Russia **Passport Number:** 100135555 **Address:** Moscow, Russia.**Position:** Cyber Operator (GRU) **Other Information:** (UK Sanctions List Ref):CYB0007 (UK Statement of Reasons):Evgenli Mikhaylovich Serebriakov was part of a team of intelligence officers of the Russian General Staff Main Intelligence Directorate (GRU) unit known as field post number 26165 that attempted to gain unauthorised access to the information systems of the Organisation for the Prohibition of Chemical Weapons (OPCW) in April 2018. The Netherlands authorities disrupted the cyber attack before it was successful. This attempted relevant cyber activity was intended to undermine the independence or effective functioning of an international organisation (Gender):Male **Listed on:** 31/07/2020 **UK Sanctions List Date Designated:** 31/12/2020 **Last Updated:** 31/12/2020 **Group ID:** 13907.

7. **Name 6:** SOTONIKOV **1:** OLEG **2:** MIKHAYLOVICH **3:** n/a **4:** n/a **5:** n/a.
DOB: 24/08/1972. **POB:** Oeljanovsk, Russia **Nationality:** Russia **Passport Number:** 120018866 **Address:** Moscow, Russia.**Position:** HUMINT Support (GRU) **Other Information:** (UK Sanctions List Ref):CYB0008 (UK Statement of Reasons):Oleg Mijailovich Sotnikov was part of a team of intelligence officers of the Russian General Staff Main Intelligence Directorate (GRU) unit known as field post number 26165 that attempted to gain unauthorised access to the information systems of the Organisation for the Prohibition of Chemical Weapons (OPCW) in April 2018. The Netherlands authorities disrupted the cyber attack before it was successful. This attempted relevant cyber activity was intended to undermine the independence or effective functioning of an international organisation (Gender):Male **Listed on:** 31/07/2020 **UK Sanctions List Date Designated:** 31/12/2020 **Last Updated:** 31/12/2020 **Group ID:** 13908.

8. **Name 6:** ZHANG **1:** SHILONG **2:** n/a **3:** n/a **4:** n/a **5:** n/a.
DOB: 10/09/1981. **a.k.a:** BAOBEILONG **Nationality:** China **Other Information:** (UK Sanctions List Ref):CYB0002 (UK Statement of Reasons):Zhang Shilong was involved in relevant cyber activity through his employment with Huaying Haitai, and therefore being responsible for, engaging in, providing support for, or promoting the commission, planning or preparation of relevant cyber activity. (Gender):Male **Listed on:** 31/07/2020 **UK Sanctions List Date Designated:** 31/12/2020 **Last Updated:** 31/12/2020 **Group ID:** 13904.

ENTITIES

1. **Organisation Name:** CENTRAL SCIENTIFIC RESEARCH INSTITUTE OF CHEMISTRY AND MECHANICS
a.k.a: (1) GNTs RF FGUP TsNIIKhM (2) NIII6 (3) Scientific Research Institute No 6 (4) State Research Centre of the Russian Federation Federal State Unitary Enterprise Central Scientific Research Institute for Chemistry and Mechanics (5) TsNIIKhM **Address:** 16a Nagatinskaya Street, Moscow, Russia.**Other Information:** (UK Sanctions List Ref):CYB0022 (UK Statement of Reasons):The Central Scientific Research Institute of Chemistry and Mechanics (TsNIIKhM) was responsible for a cyber attack on a petro-chemical company in August 2017. The cyber attack gained remote access to the Safety Instrumented Systems connected to the Industrial Control System of a petrochemical refinery. This shut down the plant for over a week. There is evidence to suggest that the shutdown was inadvertent while TsNIIKhM were attempting to cause a highly dangerous physical consequence through disabling the safety systems, which could have included an explosion. These actions caused economic loss and prejudice to commercial interests and/or was intended to undermine the security and prosperity of a country other than the United Kingdom. (Type of entity):Government-owned technical research institution **Listed on:** 24/03/2022 **UK Sanctions List Date Designated:** 24/03/2022 **Last Updated:** 24/03/2022 **Group ID:** 15044.

2. **Organisation Name:** CHOSUN EXPO (APT 38)
a.k.a: (1) Chosen Expo (2) Korean Export Joint Venture **Address:** North Korea.**Other Information:** (UK Sanctions List Ref):CYB0004 (UK Statement of Reasons):The Lazarus Group was responsible for relevant cyber activity that resulted in data interference which directly or indirectly caused, or is intended to cause, economic loss to, or prejudice to the commercial interests of, those affected by the activity through stealing money from Bangladesh Bank, attempting to steal money from Vietnam Tien Phong Bank and targeting the Polish Financial Conduct Authority information systems. Through the WannaCry attack they undermined the integrity of the United Kingdom through interfering with an information system so that it prevented the provision of essential healthcare services to the population. (Type of entity):Company (Subsidiaries):Reconnaissance General Bureau **Listed on:** 31/07/2020 **UK Sanctions List Date Designated:** 31/12/2020 **Last Updated:** 31/12/2020 **Group ID:** 13910.

3. **Organisation Name:** GRU 85TH MAIN SPECIAL SERVICE CENTRE (GTSSS) (APT 28)
a.k.a: (1) APT28 (Advanced Persistent Threat) (2) Fancy Bears (3) Iron Twilight (4) Pawn Storm (5) Sednit (6) Sofacy Group (7) Stronitium (8) Threat Group-4127/Iron Twilight (9) Tsar Team **Address:** Komsomol'skiy Prospekt, 20 Moscow, Russia, 119146.**Other Information:** (UK Sanctions List Ref):CYB0012 (UK Statement of Reasons):The 85th Main Centre for Special Technologies (GTsSS) of the Russian General Staff of the Armed Forces of the Russian Federation (GRU) - also known by its field post

number ‘26165’ and industry nicknames: APT28, Fancy Bear, Sofacy Group, Pawn Storm, Strontium - was involved in illegally accessing the information systems of the German Federal Parliament (Deutscher Bundestag) without permission in April and May 2015. The military intelligence officers of the 85th controlled, directed and took part in this activity, accessing the email accounts of MPs and stealing their data. Their activity interfered with the parliament’s information systems affecting its operation for several days, undermining the exercise of parliamentary functions in Germany. (Type of entity):Department within Government (Parent company):Russian Ministry of Defence **Listed on:** 23/10/2020 **UK Sanctions List Date Designated:** 31/12/2020 **Last Updated:** 31/12/2020 **Group ID:** 13984.

4. **Organisation Name:** MAIN CENTRE FOR SPECIAL TECHNOLOGIES (GTSST) OF THE MAIN DIRECTORATE OF THE GENERAL STAFF OF THE ARMED FORCES OF THE RUSSIAN FEDERATION (GU/GRU) ('SANDWORM') **a.k.a:** (1) BlackEnergy Group (2) Field Post Number 74455 (3) Olympic Destroyer (4) Quedagh (5) Sandworm Team (6) Telebots (7) Voodoo Bear **Address:** 22 Kirova Street, Moscow, Russia.**Other Information:** (UK Sanctions List Ref):CYB0009 (UK Statement of Reasons):The Main Centre for Special Technologies (GTsST) of the Russian General Staff Main Intelligence Directorate (GRU), also known by its field post number ‘74455’ and “Sandworm” by industry, was responsible for cyber attacks which disrupted critical national infrastructure in Ukraine, cutting off the electricity grid. The perpetrators were directly responsible for relevant cyber activity by carrying out information system interference intended to undermine integrity, prosperity and security of the Ukraine. These cyber attacks originated in Russia and were unauthorised (Type of entity):Department within Government/Military Unit (Parent company):Russian Ministry of Defence **Listed on:** 31/07/2020 **UK Sanctions List Date Designated:** 31/12/2020 **Last Updated:** 31/12/2020 **Group ID:** 13911.
5. **Organisation Name:** TIANJIN HUAYING HAITAI SCIENCE AND TECHNOLOGY DEVELOPMENT CO. LTD **a.k.a:** (1) APT10 (2) CVNX (3) Haitai Technology Development Co. Ltd (4) MenuPass (5) Potassium (6) Red Apollo (7) Stone Panda **Other Information:** (UK Sanctions List Ref):CYB0003 (UK Statement of Reasons):Huaying Haitai, known in cyber security circles as APT10 (Advanced Persistent Threat 10), Red Apollo, CVNX, Stone Panda, MenuPass and Potassium, was involved in relevant cyber activity Operation Cloud Hopper, one of the most significant and widespread cyber instructions to date. They conducted data interference through the theft of intellectual property and sensitive commercial data over many years. Huaying Haitai targeted companies across six continents and sectors banking and finance, government, aviation, space, and satellite technology, manufacturing technology, medical, oil and gas, mining, communications technology, computer processing technology, and defence technology. This activity undermined the prosperity of the United Kingdom and countries other than the United Kingdom (Website):huayinghaitai.com (Type of entity):Company **Listed on:** 31/07/2020 **UK Sanctions List Date Designated:** 31/12/2020 **Last Updated:** 31/12/2020 **Group ID:** 13909.