Office of Financial Sanctions Implementation
HM Treasury

CONSOLIDATED LIST OF FINANCIAL SANCTIONS TARGETS IN THE UK

Last Updated:07/05/2024

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:** CHERNOV **1:** MIKHAIL **2:** VADIMOVICH **3:** n/a **4:** n/a **5:** n/a.
DOB: 26/01/1986. **a.k.a:** (1) BULLET (2) M2686 **Nationality:** Russia **Other Information:** (UK Sanctions List Ref):CYB0030. (UK Statement of Reasons):Mikhail Vadimovich CHERNOV is or has been involved in relevant cyber activity, including being responsible for, engaging in providing support for, or promoting the commission, planning or preparation of relevant cyber activity; and providing technical assistance that could contribute to relevant cyber activity, namely ransomware attacks which undermined, or were intended to undermine, the integrity, prosperity and security of the United Kingdom and other countries, and were intended to cause economic loss to, or prejudice the commercial interests of, those companies affected by the activity. Specifically, Mikhail Vadimovich CHERNOV was part of the internal utilities group which were responsible for projects including autotests, cryptopanel and avclean. (Gender):Male **Listed on:** 07/09/2023 **UK Sanctions List Date Designated:** 07/09/2023 **Last Updated:** 07/09/2023 **Group ID:** 16072.
3. **Name 6:** ERMAKOV **1:** ALEKSANDR **2:** GENNADIEVICH **3:** n/a **4:** n/a **5:** n/a.
Name (non-Latin script): Александр Геннадьевич Ермаков
DOB: 16/05/1990. **POB:** Russia **a.k.a:** (1) BLADE_RUNNER (2) ERMAKOV, Aleksandr, Gennadyevich (non-Latin script: Александр Геннадьевич Ермаков) (3) GISTAVEDORE (4) GUSTAVEDORE (5) JIMJONES **Nationality:** Russia **Address:** Moscow, Russia.**Other Information:** (UK Sanctions List Ref):CYB0043. (UK Statement of Reasons):Aleksandr ERMAKOV is or has been involved in relevant cyber activity, including being responsible for, engaging in, providing support for, malicious cyber activity that resulted in unauthorised access and exfiltration of sensitive data. The action compromised Medibank Private Limited, one of Australia's largest private health insurance providers, and the resulting leak of millions of personal and medical records undermined the integrity, prosperity and security of Australia. (Gender):Male **Listed on:** 23/01/2024 **UK Sanctions List Date Designated:** 23/01/2024 **Last Updated:** 23/01/2024 **Group ID:** 16345.
4. **Name 6:** GALOCHKIN **1:** MAKSIM **2:** SERGEYEVICH **3:** n/a **4:** n/a **5:** n/a.
DOB: 19/05/1982. **a.k.a:** (1) BENTLEY (2) GALOCHKIN, Maxsim (3) MAX17 (4) VOLHVB **Nationality:** Russia **Other Information:** (UK Sanctions List Ref):CYB0031. (UK Statement of Reasons):Maksim Sergeyevich GALOCHKIN is or has been involved in relevant cyber activity, including being responsible for, engaging in providing support for, or promoting the commission, planning or preparation of relevant cyber activity; and providing technical assistance that could contribute to relevant cyber activity, namely ransomware attacks which undermined, or were intended to undermine, the integrity, prosperity and security of the United Kingdom and other countries, and were intended to cause economic loss to, or prejudice the commercial interests of, those companies affected by the activity. Specifically, Maksim Sergeyevich GALOCHKIN led a group of testers, with responsibilities for development, supervision and implementation of tests. He was also responsible for the issuing of crypts. (Gender):Male **Listed on:** 07/09/2023 **UK Sanctions List Date Designated:** 07/09/2023 **Last Updated:** 07/09/2023 **Group ID:** 16073.

5. **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.

6. **Name 6:** ISKRITSKIY **1:** MIKHAIL **2:** n/a **3:** n/a **4:** n/a **5:** n/a.
DOB: 05/11/1981. **a.k.a:** (1) ISKRITSKI, Mikhail (2) ISKRITSKIY, Mihail (3) ISKRITSKY, Mikhail (4) TROPA **Nationality:** Russia **Other Information:** (UK Sanctions List Ref):CYB0026. (UK Statement of Reasons):Mikhail ISKTRITSKIY is or has been involved in relevant cyber activity, including being responsible for, engaging in, providing support for, or promoting the commission, planning or preparation of relevant cyber activity; and providing technical assistance that could contribute to relevant cyber activity, namely ransomware attacks which were intended to undermine the integrity, prosperity and security of the United Kingdom and other countries, and were intended to cause economic loss to, or prejudice the commercial interests of, those companies affected by the activity. **Listed on:** 09/02/2023 **UK Sanctions List Date Designated:** 09/02/2023 **Last Updated:** 10/02/2023 **Group ID:** 15741.

7. **Name 6:** KARYAGIN **1:** VALENTIN **2:** OLEGOVICH **3:** n/a **4:** n/a **5:** n/a.
DOB: 19/04/1992. **a.k.a:** GLOBUS **Nationality:** Russia **Other Information:** (UK Sanctions List Ref):CYB0023. (UK Statement of Reasons):Valentin Olegovich KARYAGIN is or has been involved in relevant cyber activity, including being responsible for, engaging in, providing support for, or promoting the commission, planning or preparation of relevant cyber activity; and providing technical assistance that could contribute to relevant cyber activity, namely ransomware attacks which were intended to undermine the integrity, prosperity and security of the United Kingdom and other countries, and were intended to cause economic loss to, or prejudice the commercial interests of, those companies affected by the activity. **Listed on:** 09/02/2023 **UK Sanctions List Date Designated:** 09/02/2023 **Last Updated:** 09/02/2023 **Group ID:** 15738.

8. **Name 6:** KHALIULLIN **1:** MAKSIM **2:** MARSELEVICH **3:** n/a **4:** n/a **5:** n/a.
DOB: 28/02/1993. **a.k.a:** (1) KAGAS (2) KHALIULLIN, Maxsim **Nationality:** Russia **Other Information:** (UK Sanctions List Ref):CYB0032. (UK Statement of Reasons):Maksim Marselevich KHALIULLIN is or has been involved in relevant cyber activity, including being responsible for, engaging in providing support for, or promoting the commission, planning or preparation of relevant cyber activity; and providing technical assistance that could contribute to relevant cyber activity, namely ransomware attacks which undermined, or were intended to undermine, the integrity, prosperity and security of the United Kingdom and other countries, and were intended to cause economic loss to, or prejudice the commercial interests of, those companies affected by the activity. Specifically, Maksim Marselevich KHALIULLIN was an HR manager for the Group. He was associated with the purchase of Trickbot infrastructure including procuring Virtual Private Servers (VPS). (Gender):Male **Listed on:** 07/09/2023 **UK Sanctions List Date Designated:** 07/09/2023 **Last Updated:** 07/09/2023 **Group ID:** 16074.

9. **Name 6:** KHOROSHEV **1:** DMITRY **2:** YUREYVICH **3:** n/a **4:** n/a **5:** n/a.
Name (non-Latin script): Дмитрий Юрьевич Хорошев
DOB: 17/04/1993. **a.k.a:** (1) KHOROSHEV, Dmitriy, Yureyvich (2) LOCKBITSUPP **Nationality:** Russia **Address:** Russia.**Other Information:** (UK Sanctions List Ref):CYB0047. (UK Statement of Reasons):Dmitry Yureyvich KHOROSHEV is or has been involved in relevant cyber activity in that he has been responsible for, engaged in, provided support for or promoted the commission, planning or preparation of relevant cyber activity, or provided technical assistance that could contribute to relevant cyber activity. In particular, KHOROSHEV has been the primary user of the online moniker and public facing identity LockBitSupp. We assess that KHOROSHEV is a senior leader of the LockBit ransomware group and was centrally involved in the administration, its infrastructure and operations. KHOROSHEV, has been a significant direct financial beneficiary of LockBit ransomware activity. LockBit are responsible for ransomware attacks against thousands of victims around the world, including in the UK, which have been estimated to result in billions of dollars of losses globally, impacting businesses and the livelihoods of ordinary citizens. LockBit has conducted or enabled malicious ransomware campaigns against a range of targets, involving actual or attempted unauthorised access to and interference with information systems and data, activities which undermined or were intended to undermine the integrity, prosperity or security of the United Kingdom or a country other than the United Kingdom, or directly or indirectly caused or were intended to cause economic loss to or prejudice to the commercial interests of those affected by the activity. (Gender):Male **Listed on:** 07/05/2024 **UK Sanctions List Date Designated:** 07/05/2024 **Last Updated:** 07/05/2024 **Group ID:** 16494.

10. **Name 6:** KORINETS **1:** ANDREY **2:** STANISLAVOVICH **3:** n/a **4:** n/a **5:** n/a.
Name (non-Latin script): Андрей Станиславович КОРИНЕЦ
DOB: 18/05/1987. **POB:** Russia **a.k.a:** DOGUZHIEV, Alexey **Nationality:** Russia **Passport Number:** 8707233962 **Address:** Komi Republic, Syktyvkar, Russia.**Other Information:** (UK Sanctions List Ref):CYB0042. (UK Statement of Reasons):Andrey Stanislavovich KORINETS, a member of the Callisto Group (AKA Seaborgium, Star Blizzard, Cold River), is or has been involved in relevant cyber activity, including providing technical assistance that could contribute to relevant cyber activity. This included the preparation of spear-phishing campaigns and associated activity that resulted in unauthorised access and exfiltration of sensitive data. This action undermined, or was intended to undermine, the integrity, prosperity and security of UK organisations and more broadly, the UK government, and directly or indirectly caused, or was intended to cause, economic loss to, or prejudice to the commercial interests of, those affected by the activity. The Callisto Group, a cyber programme operated by officers of the Russian FSB, was responsible for intrusions into the Institute for Statecraft (IfS), a UK-based think tank responsible for a programme to research, publicise, and counter the threat to European democracies from disinformation and other forms of hybrid warfare. Official documents belonging to IfS were released in the hack and subsequent leak, resulting from the preparation of spear-phishing campaigns and associated activity. (Gender):Male **Listed on:** 07/12/2023 **UK Sanctions List Date Designated:** 07/12/2023 **Last Updated:** 07/12/2023 **Group ID:** 16278.

11. **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.

12. **Name 6:** KOVALEV **1:** VITALIY **2:** NIKOLAYEVICH **3:** n/a **4:** n/a **5:** n/a.
DOB: 23/06/1988. **a.k.a:** (1) BEN (2) BENTLEY (3) KOVALEV, Vitaly **Nationality:** Russia **Other Information:** (UK Sanctions List Ref):CYB0027. The 'Bentley' alias is for historical use of the moniker. (UK Statement of Reasons):Vitaliy Nikolayevich KOVALEV is or has been involved in relevant cyber activity, including being responsible for, engaging in, providing support for, or promoting the commission, planning or preparation of relevant cyber activity; and providing technical assistance that could contribute to relevant cyber activity, namely ransomware attacks which were intended to undermine the integrity, prosperity and security of the United Kingdom and other countries, and were intended to cause economic loss to, or prejudice the commercial interests of, those companies affected by the activity. **Listed on:** 09/02/2023 **UK Sanctions List Date Designated:** 09/02/2023 **Last Updated:** 06/04/2023 **Group ID:** 15742.

13. **Name 6:** KUROV **1:** ARTEM **2:** IGOREVICH **3:** n/a **4:** n/a **5:** n/a.
DOB: 30/03/1993. **a.k.a:** NANED **Nationality:** Russia **Other Information:** (UK Sanctions List Ref):CYB0033. (UK Statement of Reasons):Artem Igorevich KUROV is or has been involved in relevant cyber activity, including being responsible for, engaging in providing support for, or promoting the commission, planning or preparation of relevant cyber activity; and providing technical assistance that could contribute to relevant cyber activity, namely ransomware attacks which undermined, or were intended to undermine, the integrity, prosperity and security of the United Kingdom and other countries, and were intended to cause economic loss to, or prejudice the commercial interests of, those companies affected by the activity. Specifically, Artem Igorevich KUROV worked as a coder with development duties in the Trickbot group. (Gender):Male **Listed on:** 07/09/2023 **UK Sanctions List Date Designated:** 07/09/2023 **Last Updated:** 07/09/2023 **Group ID:** 16075.

14. **Name 6:** LOGUNTSOV **1:** SERGEY **2:** n/a **3:** n/a **4:** n/a **5:** n/a.
DOB: 15/07/1983. **a.k.a:** (1) BEGEMOT (2) BEGEMOT_SUN (3) ZULAS **Nationality:** Russia **Other Information:** (UK Sanctions List Ref):CYB0038. (UK Statement of Reasons):Sergey LOGUNTSOV is or has been involved in relevant cyber activity, including being responsible for, engaging in providing support for, or promoting the commission, planning or preparation of relevant cyber activity; and providing technical assistance that could contribute to relevant cyber activity, namely ransomware attacks which undermined, or were intended to undermine, the integrity, prosperity and security of the United Kingdom and other countries, and were intended to cause economic loss to, or prejudice the commercial interests of, those companies affected by the activity. Specifically, Sergey LOGUNTSOV was a developer for the Group. (Gender):Male **Listed on:** 07/09/2023 **UK Sanctions List Date Designated:** 07/09/2023 **Last Updated:** 07/09/2023 **Group ID:** 16080.

15. **Name 6:** MIKHAILOV **1:** MAKSIM **2:** SERGEEVICH **3:** n/a **4:** n/a **5:** n/a.
DOB: 29/07/1976. **a.k.a:** (1) BAGET (2) MAXMS76 (3) MIKHAILOV, Maxim **Nationality:** Russia **Other Information:** (UK Sanctions List Ref):CYB0024. (UK Statement of Reasons):Maksim Sergeevich MIKHAILOV is or has been involved in relevant cyber activity, including being responsible for, engaging in, providing support for, or promoting the commission, planning or preparation of relevant cyber activity; and providing technical assistance that could contribute to relevant cyber activity, namely ransomware attacks which were intended to undermine the integrity, prosperity and security of the United Kingdom and other countries, and were intended to cause economic loss to, or prejudice the commercial interests of, those companies affected by the activity. **Listed on:** 09/02/2023 **UK Sanctions List Date Designated:** 09/02/2023 **Last Updated:** 09/02/2023 **Group ID:** 15739.

16. **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.

17. **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.

18. **Name 6:** MOZHAEV **1:** ALEXANDER **2:** VYACHESLAVOVICH **3:** n/a **4:** n/a **5:** n/a.
DOB: 02/10/1978. **a.k.a:** (1) GREEN (2) MOZHAEV, Alexandr, Vyacheslavovich (3) ROCCO **Nationality:** Russia **Other Information:** (UK Sanctions List Ref):CYB0034. (UK Statement of Reasons):Alexander Vyacheslavovich MOZHAEV is or has been involved in relevant cyber activity, including being responsible for, engaging in providing support for, or promoting the commission, planning or preparation of relevant cyber activity; and providing technical assistance that could contribute to relevant cyber activity, namely ransomware attacks which undermined, or were intended to undermine, the integrity, prosperity and security of the United Kingdom and other countries, and were intended to cause economic loss to, or prejudice the commercial interests of, those companies affected by the activity. Specifically, Alexander Vyacheslavovich MOZHAEV was part of the admin team responsible for general administration duties. (Gender):Male **Listed on:** 07/09/2023 **UK Sanctions List Date Designated:** 07/09/2023 **Last Updated:** 07/09/2023 **Group ID:** 16076.

19. **Name 6:** NI **1:** GAOBIN **2:** n/a **3:** n/a **4:** n/a **5:** n/a.
Name (non-Latin script): 倪高彬
DOB: 27/10/1985. **POB:** Jingzhou Municipality, China **Nationality:** China **National Identification Number:** 421003198510272917 **Address:** Hubei Province, China.**Other Information:** (UK Sanctions List Ref):CYB0046. (UK Statement of Reasons):NI Gaobin, a member of Advanced Persistent Threat Group 31 (APT31), is, or has been, involved in relevant cyber activity, including being responsible for, engaging in, or providing support for the commission, planning, or preparation of relevant cyber activity. This included the preparation for, and/or the provision of support to, sophisticated cyber activity, including spear-phishing campaigns and information systems interference which resulted in the unauthorised access to, and exfiltration of, sensitive data. Such campaigns included cyber activities targeting officials, government entities and parliamentarians conducted by APT31 against such individuals in the UK and internationally. As such, NI Gaobin, is a member, and an involved person in the activity of the APT31 group operating on behalf of the Chinese Ministry of State Security (MSS) as part of the PRC's state-sponsored apparatus and himself has engaged in relevant cyber activity, in support of malicious cyber activity that targeted officials, government entities and parliamentarians. This action undermined, or was intended to undermine, the integrity, prosperity and security of UK and international organisations and individuals engaged in political and democratic processes. (Gender):Male **Listed on:** 25/03/2024 **UK Sanctions List Date Designated:** 25/03/2024 **Last Updated:** 25/03/2024 **Group ID:** 16462.

20. **Name 6:** PERETYATKO **1:** RUSLAN **2:** ALEKSANDROVICH **3:** n/a **4:** n/a **5:** n/a.
Name (non-Latin script): Руслан Александрович ПЕРЕТЯТЬКО
DOB: 03/08/1985. **POB:** Russia **Nationality:** Russia **Passport Number:** 8705080546 **Address:** Komi Republic, Russia.**Other Information:** (UK Sanctions List Ref):CYB0041. (UK Statement of Reasons):Ruslan Aleksandrovich PERETYATKO, a Russian FSB Intelligence Officer and a member of the Callisto Group (AKA Seaborgium, Star Blizzard, Cold River), is or has been involved in relevant cyber activity, including being responsible for, engaging in, providing support for, or promoting the commission, planning or preparation of relevant cyber activity. This included the preparation of spear-phishing campaigns and associated activity that resulted in unauthorised access and exfiltration of sensitive data. This action undermined, or was intended to undermine, the integrity, prosperity and security of UK organisations and more broadly, the UK government, and directly or indirectly caused, or was intended to cause, economic loss to, or prejudice to the commercial interests of, those affected by the activity. The Callisto Group, a cyber programme operated by officers of the Russian FSB , was responsible for intrusions into the Institute for Statecraft (IfS), a UK-based think tank responsible for a programme to research, publicise, and counter the threat to European democracies from disinformation and other forms of hybrid warfare. Official documents belonging to IfS were released in the hack and subsequent leak, resulting from the preparation of spear-phishing campaigns and associated activity. (Gender):Male **Listed on:** 07/12/2023 **UK Sanctions List Date Designated:** 07/12/2023 **Last Updated:** 07/12/2023 **Group ID:** 16277.

21. **Name 6:** PLESHEVSKIY **1:** DMITRY **2:** n/a **3:** n/a **4:** n/a **5:** n/a.
DOB: 30/07/1992. **a.k.a:** (1) ISELDOR (2) PLESHEVSKIY DIMA (3) PLESHEVSKIY, Dimitri (4) PLESHEVSKIY, Dimitry **Nationality:** Russia **Other Information:** (UK Sanctions List Ref):CYB0025. (UK Statement of Reasons):Dmitry PLESHEVSKIY is or has been involved in relevant cyber activity, including being responsible for, engaging in, providing support for, or promoting the commission, planning or preparation of relevant cyber activity; and providing technical assistance that could contribute to relevant cyber activity, namely ransomware attacks which were intended to undermine the integrity, prosperity and security of the United Kingdom and other countries, and were intended to cause economic loss to, or prejudice the commercial interests of, those companies affected by the activity. **Listed on:** 09/02/2023 **UK Sanctions List Date Designated:** 09/02/2023 **Last Updated:** 10/02/2023 **Group ID:** 15740.

22. **Name 6:** PUTILIN **1:** DMITRY **2:** SERGEEVICH **3:** n/a **4:** n/a **5:** n/a.
DOB: 24/03/1993. **a.k.a:** (1) GRAD (2) STAFF **Nationality:** Russia **Other Information:** (UK Sanctions List Ref):CYB0035. (UK Statement of Reasons):Dmitry Sergeevich PUTILIN is or has been involved in relevant cyber activity, including being responsible for, engaging in providing support for, or promoting the commission, planning or preparation of relevant cyber activity; and providing technical assistance that could contribute to relevant cyber activity, namely ransomware attacks which undermined, or were intended to undermine, the integrity, prosperity and security of the United Kingdom and other countries, and were intended to cause economic loss to, or prejudice the commercial interests of, those companies affected by the activity. Specifically, Dmitry Sergeevich PUTILIN was associated with the purchase of Trickbot infrastructure. (Gender):Male **Listed on:** 07/09/2023 **UK Sanctions List Date Designated:** 07/09/2023 **Last Updated:** 07/09/2023 **Group ID:** 16077.

23. **Name 6:** RUDENSKIY **1:** MAKSIM **2:** n/a **3:** n/a **4:** n/a **5:** n/a.

DOB: 01/11/1977. **a.k.a:** (1) BINMAN (2) BUZA (3) SILVER **Nationality:** Russia **Other Information:** (UK Sanctions List Ref):CYB0036. (UK Statement of Reasons):Maksim RUDENSKIY is or has been involved in relevant cyber activity, including being responsible for, engaging in providing support for, or promoting the commission, planning or preparation of relevant cyber activity; and providing technical assistance that could contribute to relevant cyber activity, namely ransomware attacks which undermined, or were intended to undermine, the integrity, prosperity and security of the United Kingdom and other countries, and were intended to cause economic loss to, or prejudice the commercial interests of, those companies affected by the activity. Specifically, Maksim RUDENSKIY was a key member of the Trickbot group. He was the team lead for coders. (Gender):Male **Listed on:** 07/09/2023 **UK Sanctions List Date Designated:** 07/09/2023 **Last Updated:** 07/09/2023 **Group ID:** 16078.

24. **Name 6:** SEDLETSKI **1:** VALERY **2:** VENIAMINOVICH **3:** n/a **4:** n/a **5:** n/a.
DOB: 29/07/1974. **a.k.a:** (1) SEDLETSKIY, Valeri (2) STRIX (3) VALERIUS **Nationality:** Russia **Other Information:** (UK Sanctions List Ref):CYB0029. (UK Statement of Reasons):Valery Veniaminovich SEDLETSKI is or has been involved in relevant cyber activity, including being responsible for, engaging in, providing support for, or promoting the commission, planning or preparation of relevant cyber activity; and providing technical assistance that could contribute to relevant cyber activity, namely ransomware attacks which were intended to undermine the integrity, prosperity and security of the United Kingdom and other countries, and were intended to cause economic loss to, or prejudice the commercial interests of, those companies affected by the activity. **Listed on:** 09/02/2023 **UK Sanctions List Date Designated:** 09/02/2023 **Last Updated:** 09/02/2023 **Group ID:** 15744.

25. **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.

26. **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.

27. **Name 6:** TSAREV **1:** MIKHAIL **2:** n/a **3:** n/a **4:** n/a **5:** n/a.
DOB: 20/04/1989. **a.k.a:** (1) FRANCES (2) KHANO (3) MANGO **Nationality:** Russia **Other Information:** (UK Sanctions List Ref):CYB0037. (UK Statement of Reasons):Mikhail TSAREV is or has been involved in relevant cyber activity, including being responsible for, engaging in providing support for, or promoting the commission, planning or preparation of relevant cyber activity; and providing technical assistance that could contribute to relevant cyber activity, namely ransomware attacks which undermined, or were intended to undermine, the integrity, prosperity and security of the United Kingdom and other countries, and were intended to cause economic loss to, or prejudice the commercial interests of, those companies affected by the activity. Specifically, Mikhail TSAREV was a mid-level manager who assisted with the Group's finances and overseeing of HR functions. (Gender):Male **Listed on:** 07/09/2023 **UK Sanctions List Date Designated:** 07/09/2023 **Last Updated:** 07/09/2023 **Group ID:** 16079.

28. **Name 6:** VAKHROMEYEV **1:** IVAN **2:** VASILYEVICH **3:** n/a **4:** n/a **5:** n/a.
DOB: 29/12/1988. **a.k.a:** (1) IVANALERT (2) MUSHROOM (3) VAKHROMEEV, Ivan, Vasilievich **Nationality:** Russia **Other Information:** (UK Sanctions List Ref):CYB0028. (UK Statement of Reasons):Ivan Vasilyevich VAKHROMEYEV is or has been involved in relevant cyber activity, including being responsible for, engaging in, providing support for, or promoting the commission, planning or preparation of relevant cyber activity; and providing technical assistance that could contribute to relevant cyber activity, namely ransomware attacks which were intended to undermine the integrity, prosperity and security of the United Kingdom and other countries, and were intended to cause economic loss to, or prejudice the commercial interests of, those companies affected by the activity. **Listed on:** 09/02/2023 **UK Sanctions List Date Designated:** 09/02/2023 **Last Updated:** 09/02/2023 **Group ID:** 15743.

29. **Name 6:** VALIAKHMETOV **1:** VADYM **2:** FIRDAVYSOVYCH **3:** n/a **4:** n/a **5:** n/a.
DOB: 07/05/1981. **a.k.a:** (1) MENTOS (2) VALIAKHMETOV, Vadim, Firdavysovych (3) VASM (4) WELDON **Nationality:** Russia **Other Information:** (UK Sanctions List Ref):CYB0039. (UK Statement of Reasons):Vadym Firdavysovych VALIAKHMETOV is or has been involved in relevant cyber activity, including being responsible for, engaging in providing support for, or promoting the commission, planning or preparation of relevant cyber activity; and providing technical assistance that could contribute to relevant cyber activity, namely ransomware attacks which undermined, or were intended to undermine, the integrity, prosperity and security of the United Kingdom and other countries, and were intended to cause economic loss to, or prejudice the commercial interests of, those companies affected by the activity. Specifically, Vadym Firdavysovych VALIAKHMETOV worked as a coder and his duties included backdoor and loader projects. (Gender):Male **Listed on:** 07/09/2023 **UK Sanctions List Date Designated:** 07/09/2023 **Last Updated:** 07/09/2023 **Group ID:** 16081.

30. **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.

31. **Name 6:** ZHAO **1:** GUANGZONG **2:** n/a **3:** n/a **4:** n/a **5:** n/a.
Name (non-Latin script): 赵光宗
DOB: 12/11/1985. **POB:** Jingzhou Municipality, China **Nationality:** China **National Identification Number:** 421003198511121539 **Address:** Hubei Province, China.**Other Information:** (UK Sanctions List Ref):CYB0045. (UK Statement of Reasons):ZHAO Guangzong, a member of Advanced Persistent Threat Group 31 (APT31), is, or has been, involved in relevant cyber activity, including being responsible for, engaging in, or providing support for the commission, planning, or preparation of relevant cyber activity. This included the preparation for, and/or the provision of support to, sophisticated cyber activity, including spear-phishing campaigns and information systems interference which resulted in the unauthorised access to, and exfiltration of, sensitive data. Such campaigns included cyber activities targeting officials, government entities and parliamentarians conducted by APT31 against such individuals in the UK and internationally. As such, ZHAO Guangzong, is a member, and an involved person in the activity of the APT31 group operating on behalf of the Chinese Ministry of State Security (MSS) as part of the PRC's state-sponsored apparatus and himself has engaged in relevant cyber activity, in support of malicious cyber activity that targeted officials, government entities and parliamentarians. This action undermined, or was intended to undermine, the integrity, prosperity and security of UK and international organisations and individuals engaged in political and democratic processes. (Gender):Male **Listed on:** 25/03/2024 **UK Sanctions List Date Designated:** 25/03/2024 **Last Updated:** 25/03/2024 **Group ID:** 16461.

32. **Name 6:** ZHUYKOV **1:** ANDREY **2:** YURYEVICH **3:** n/a **4:** n/a **5:** n/a.
DOB: 18/02/1982. **a.k.a:** (1) ADAM (2) DEFENDER (3) DIF **Nationality:** Russia **Other Information:** (UK Sanctions List Ref):CYB0040. (UK Statement of Reasons):Andrey Yuryevich ZHUYKOV is or has been involved in relevant cyber activity, including being responsible for, engaging in providing support for, or promoting the commission, planning or preparation of relevant cyber activity; and providing technical assistance that could contribute to relevant cyber activity, namely ransomware attacks which undermined, or were intended to undermine, the integrity, prosperity and security of the United Kingdom and other countries, and were intended to cause economic loss to, or prejudice the commercial interests of, those companies affected by the activity. Specifically, Andrey Yuryevich ZHUYKOV was a central actor in the Group and a senior administrator. (Gender):Male **Listed on:** 07/09/2023 **UK Sanctions List Date Designated:** 07/09/2023 **Last Updated:** 07/09/2023 **Group ID:** 16082.

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.

6. **Organisation Name:** WUHAN XIAORUIZHI SCIENCE AND TECHNOLOGY COMPANY LIMITED
Name (non-Latin script): 武汉晓睿智科技有限责任公司
Address: 2nd Floor, No. 16, Huashiyuan North Road, East Lake New Technology Development Zone, Hubei Province, Wuhan, China.**Other Information:** (UK Sanctions List Ref):CYB0044. (UK Statement of Reasons):WUHAN XIAORUIZHI SCIENCE AND TECHNOLOGY COMPANY LIMITED is associated with Advanced Persistent Threat Group 31 (APT31) and is, or has been, involved in relevant cyber activity, including being responsible for, engaging in, or providing support for the commission, planning, or preparation of relevant cyber activity on behalf of the Chinese State. This included the preparation for, and/or the provision of support to, sophisticated cyber activity, including spear-phishing campaigns and information systems interference which resulted in the unauthorised access to, and exfiltration of, sensitive data. Such campaigns included cyber activities targeting officials, government entities and parliamentarians conducted by APT31 against such individuals in the UK and internationally. As such, WUHAN XIAORUIZHI SCIENCE AND TECHNOLOGY COMPANY LIMITED, is an associated person in the activity of the APT31 group operating on behalf of the Chinese Ministry of State Security (MSS) as part of the PRC's state-sponsored apparatus and itself has engaged in relevant cyber activity, in support of malicious cyber activity that targeted officials, government entities and parliamentarians. This action undermined, or was intended to undermine, the integrity, prosperity and security of UK and international organisations and individuals engaged in political and democratic processes. (Type of entity):Company **Listed on:** 25/03/2024 **UK Sanctions List Date Designated:** 25/03/2024 **Last Updated:** 25/03/2024 **Group ID:** 16460.