Conseil de
l'Union européenne

Bruxelles, le 13 mai 2024
(OR. en)

8502/24

LIMITE

CORLX 356
CFSP/PESC 512
RELEX 467
CYBER 110
JAI 572
FIN 341

ACTES LÉGISLATIFS ET AUTRES INSTRUMENTS

Objet:	RÈGLEMENT D'EXÉCUTION DU CONSEIL mettant en œuvre le règlement (UE) 2019/796 concernant des mesures restrictives contre les cyberattaques qui menacent l'Union ou ses États membres

RÈGLEMENT D'EXÉCUTION (UE) 2024/... DU CONSEIL

du …

mettant en œuvre le règlement (UE) 2019/796 concernant des mesures restrictives contre les cyberattaques qui menacent l'Union ou ses États membres

LE CONSEIL DE L'UNION EUROPÉENNE,

vu le traité sur le fonctionnement de l'Union européenne,

vu le règlement (UE) 2019/796 du 17 mai 2019 du Conseil concernant des mesures restrictives contre les cyberattaques qui menacent l'Union ou ses États membres[1], et notamment son article 13, paragraphe 1,

vu la proposition du haut représentant de l'Union pour les affaires étrangères et la politique de sécurité,

[1] JO L 129I du 17.05.2019, p. 1.

considérant ce qui suit:

(1) Le 17 mai 2019, le Conseil a adopté le règlement (UE) 2019/796.

(2) Compte tenu de la poursuite et de l'augmentation des actes de cybermalveillance, y compris des comportements dirigés contre des États tiers, il convient de mettre à jour les motifs de l'inscription de six personnes et de deux entités sur la liste des personnes physiques et morales, des entités et des organismes faisant l'objet de mesures restrictives qui figure à l'annexe I du règlement (UE) 2019/796.

(3) Il y a donc lieu de modifier l'annexe I du règlement (UE) 2019/796 en conséquence,

A ADOPTÉ LE PRÉSENT RÈGLEMENT:

Article premier

L'annexe I du règlement (UE) 2019/796 est modifiée conformément à l'annexe du présent règlement.

Article 2

Le présent règlement entre en vigueur le jour suivant celui de sa publication au *Journal officiel de l'Union européenne*.

Le présent règlement est obligatoire dans tous ses éléments et directement applicable dans tout État membre.

Fait à …, le

Par le Conseil
Le président/La présidente

ANNEXE

L'annexe I du règlement (UE) 2019/796 ("Liste des personnes physiques et morales, des entités et des organismes visés à l'article 3") est modifiée comme suit:

1) Dans la liste intitulée "A. Personnes physiques", les mentions de 3 à 8 sont remplacées par le texte suivant:

	Nom	Informations d'identification	Exposé des motifs	Date d'inscription
"3.	Alexey Valeryevich MININ	Алексей Валерьевич МИНИН Date de naissance: 27.5.1972 Lieu de naissance: oblast de Perm, République socialiste fédérative soviétique de Russie (aujourd'hui Fédération de Russie) Numéro de passeport: 120017582 Délivré par le ministère des affaires étrangères de la Fédération de Russie Validité: du 17.4.2017 au 17.4.2022 Lieu: Moscou, Fédération de Russie Nationalité: russe Sexe: masculin	Alexey Minin a participé à une tentative de cyberattaque ayant des effets potentiels importants dirigée contre l'Organisation pour l'interdiction des armes chimiques (OIAC) aux Pays-Bas et à des cyberattaques ayant des effets importants dirigées contre des États tiers. En tant qu'agent de soutien en matière de renseignement humain au sein de la direction générale du renseignement de l'état-major des forces armées de la Fédération de Russie (GU/GRU), Alexey Minin a fait partie d'une équipe de quatre membres du renseignement militaire russe qui ont tenté d'obtenir un accès non autorisé au réseau Wi-Fi de l'OIAC à La Haye (Pays-Bas) en avril 2018. Si elle avait été couronnée de succès, la tentative de cyberattaque, qui visait le piratage du réseau Wi-Fi de l'OIAC, aurait compromis la sécurité du réseau et les travaux d'enquête en cours de l'OIAC. Le Service du renseignement et de la sécurité militaires des Pays-Bas (Militaire Inlichtingen- en Veiligheidsdienst) a perturbé la tentative de cyberattaque, évitant ainsi de graves dommages à l'OIAC. Une chambre d'accusation du district ouest de l'État de Pennsylvanie (États-Unis d'Amérique) a inculpé Alexey Minin, en tant qu'agent de la direction générale du renseignement russe (GRU), pour piratage informatique, fraude électronique, usurpation d'identité aggravée et blanchiment d'argent.	30.7.2020

	Nom	Informations d'identification	Exposé des motifs	Date d'inscription
4.	Aleksei Sergeyvich MORENETS	Алексей Сергеевич МОРЕНЕЦ Date de naissance: 31.7.1977 Lieu de naissance: oblast de Murmanskaya, République socialiste fédérative soviétique de Russie (aujourd'hui Fédération de Russie) Numéro de passeport: 100135556 Délivré par le ministère des affaires étrangères de la Fédération de Russie Validité: du 17.4.2017 au 17.4.2022 Lieu: Moscou, Fédération de Russie Nationalité: russe Sexe: masculin	Aleksei Morenets a participé à une tentative de cyberattaque ayant des effets potentiels importants dirigée contre l'Organisation pour l'interdiction des armes chimiques (OIAC) aux Pays-Bas et à des cyberattaques ayant des effets importants dirigées contre des pays tiers. En tant que cyber-opérateur au sein de la direction générale du renseignement de l'état-major des forces armées de la Fédération de Russie (GU/GRU), Aleksei Morenets a fait partie d'une équipe de quatre membres du renseignement militaire russe qui ont tenté d'obtenir un accès non autorisé au réseau Wi-Fi de l'OIAC à La Haye (Pays-Bas) en avril 2018. Si elle avait été couronnée de succès, la tentative de cyberattaque, qui visait le piratage du réseau Wi-Fi de l'OIAC, aurait compromis la sécurité du réseau et les travaux d'enquête en cours de l'OIAC. Le Service du renseignement et de la sécurité militaires des Pays-Bas (Militaire Inlichtingen- en Veiligheidsdienst) a perturbé la tentative de cyberattaque, évitant ainsi de graves dommages à l'OIAC. Une chambre d'accusation du district ouest de l'État de Pennsylvanie (États-Unis d'Amérique) a inculpé Aleksei Morenets, affecté à l'unité militaire 26165, pour piratage informatique, fraude électronique, usurpation d'identité aggravée et blanchiment d'argent.	30.7.2020

	Nom	Informations d'identification	Exposé des motifs	Date d'inscription
5.	Evgenii Mikhaylovich SEREBRIAKOV	Евгений Михайлович СЕРЕБРЯКОВ Date de naissance: 26.7.1981 Lieu de naissance: Koursk, République socialiste fédérative soviétique de Russie (aujourd'hui Fédération de Russie) Numéro de passeport: 100135555 Délivré par le ministère des affaires étrangères de la Fédération de Russie Validité: du 17.4.2017 au 17.4.2022 Lieu: Moscou, Fédération de Russie Nationalité: russe Sexe: masculin	Evgenii Serebriakov a participé à une tentative de cyberattaque ayant des effets potentiels importants dirigée contre l'Organisation pour l'interdiction des armes chimiques (OIAC) aux Pays-Bas et à des cyber-attaques ayant des effets importants dirigées contre des pays tiers. En tant que cyber-opérateur au sein de la direction générale du renseignement de l'état-major des forces armées de la Fédération de Russie (GU/GRU), Evgenii Serebriakov a fait partie d'une équipe de quatre membres du renseignement militaire russe qui ont tenté d'obtenir un accès non autorisé au réseau Wi-Fi de l'OIAC à La Haye (Pays-Bas) en avril 2018. Si elle avait été couronnée de succès, la tentative de cyberattaque, qui visait le piratage du réseau Wi-Fi de l'OIAC, aurait compromis la sécurité du réseau et les travaux d'enquête en cours de l'OIAC. Le Service du renseignement et de la sécurité militaires des Pays-Bas (Militaire Inlichtingen- en Veiligheidsdienst) a perturbé la tentative de cyberattaque, évitant ainsi de graves dommages à l'OIAC. Depuis le printemps 2022, Evgenii Serebriakov dirige "Sandworm" (autrement connu sous le nom de "Sandworm Team", "BlackEnergy Group", "Voodoo Bear", "Quedagh", "Olympic Destroyer" ou "Telebots"), acteur et groupe de pirates informatiques lié à l'unité 74455 de la direction générale du renseignement russe. Sandworm a mené des cyberattaques contre l'Ukraine, y compris des agences gouvernementales ukrainiennes, à la suite de la guerre d'agression menée par la Russie contre l'Ukraine.	30.7.2020

	Nom	Informations d'identification	Exposé des motifs	Date d'inscription
6.	Oleg Mikhaylovich SOTNIKOV	Олег Михайлович СОТНИКОВ Date de naissance: 24.8.1972 Lieu de naissance: Ulyanovsk, République socialiste fédérative soviétique de Russie (aujourd'hui Fédération de Russie) Numéro de passeport: 120018866 Délivré par le ministère des affaires étrangères de la Fédération de Russie Validité: du 17.4.2017 au 17.4.2022 Lieu: Moscou, Fédération de Russie Nationalité: russe Sexe: masculin	Oleg Sotnikov a participé à une tentative de cyberattaque ayant des effets potentiels importants dirigée contre l'Organisation pour l'interdiction des armes chimiques (OIAC) aux Pays-Bas et à des cyber-attaques ayant des effets importants dirigées contre des pays tiers. En tant qu'agent de soutien en matière de renseignement humain au sein de la direction générale du renseignement de l'état-major des forces armées de la Fédération de Russie (GU/GRU), Oleg Sotnikov a fait partie d'une équipe de quatre membres du renseignement militaire russe qui ont tenté d'obtenir un accès non autorisé au réseau Wi-Fi de l'OIAC à La Haye (Pays-Bas) en avril 2018. Si elle avait été couronnée de succès, la tentative de cyberattaque, qui visait le piratage du réseau Wi-Fi de l'OIAC, aurait compromis la sécurité du réseau et les travaux d'enquête en cours de l'OIAC. Le Service du renseignement et de la sécurité militaires des Pays-Bas (Militaire Inlichtingen- en Veiligheidsdienst) a perturbé la tentative de cyberattaque, évitant ainsi de graves dommages à l'OIAC. Une chambre d'accusation du district ouest de l'État de Pennsylvanie a inculpé Oleg Sotnikov, en tant qu'agent de la direction générale du renseignement russe (GRU), pour piratage informatique, fraude électronique, usurpation d'identité aggravée et blanchiment d'argent.	30.7.2020

	Nom	Informations d'identification	Exposé des motifs	Date d'inscription
7.	Dmitry Sergeyevich BADIN	Дмитрий Сергеевич БАДИН Date de naissance: 15.11.1990 Lieu de naissance: Koursk, République socialiste fédérative soviétique de Russie (aujourd'hui Fédération de Russie) Nationalité: russe Sexe: masculin	Dmitry Badin a participé à une cyberattaque ayant des effets importants dirigée contre le parlement fédéral allemand (Deutscher Bundestag) et à des cyberattaques ayant des effets importants dirigées contre des pays tiers. En tant que membre du renseignement militaire du 85e Centre principal des services spéciaux (GTsSS) de la direction générale du renseignement de l'état-major des forces armées de la Fédération de Russie (GU/GRU), Dmitry Badin a fait partie d'une équipe de membres du renseignement militaire russe qui a mené une cyberattaque contre le parlement fédéral allemand en avril et mai 2015. Cette cyberattaque a ciblé le système d'information du parlement et en a perturbé le fonctionnement pendant plusieurs jours. Une importante quantité de données a été volée et les comptes de courrier électronique de plusieurs parlementaires, ainsi que de l'ancienne chancelière Angela Merkel, ont été affectés. Une chambre d'accusation du district ouest de l'État de Pennsylvanie (États-Unis d'Amérique) a inculpé Dmitry Badin, affecté à l'unité militaire 26165, pour piratage informatique, fraude électronique, usurpation d'identité aggravée et blanchiment d'argent.	22.10.2020

	Nom	Informations d'identification	Exposé des motifs	Date d'inscription
8.	Igor Olegovich KOSTYUKOV	Игорь Олегович КОСТЮКОВ Date de naissance: 21.2.1961 Nationalité: russe Sexe: masculin	Igor Kostyukov est actuellement le chef de la direction générale du renseignement de l'état-major des forces armées de la Fédération de Russie (GU/GRU), dont il a précédemment été le premier chef adjoint. L'une des unités sous son commandement est le 85e Centre principal des services spéciaux (GTsSS) (autrement connu sous les noms "unité militaire 26165", "APT28", "Fancy Bear", "Sofacy Group", "Pawn Storm" et "Strontium"). À ce titre, Igor Kostyukov est responsable des cyberattaques menées par le GTsSS, y compris de celles ayant des effets importants qui constituent une menace extérieure pour l'Union ou ses États membres. En particulier, des membres du renseignement militaire du GTsSS ont participé à la cyberattaque contre le parlement fédéral allemand (*Deutscher Bundestag*) en avril et mai 2015 et à la tentative de cyberattaque, qui visait le piratage du réseau WiFi de l'Organisation pour l'interdiction des armes chimiques (OIAC) aux Pays-Bas en avril 2018. La cyberattaque contre le parlement fédéral allemand a ciblé le système d'information du parlement et en a perturbé le fonctionnement pendant plusieurs jours. Une importante quantité de données a été volée et les comptes de courrier électronique de plusieurs parlementaires, ainsi que de l'ancienne chancelière Angela Merkel, ont été affectés.	22.10.2020".

2) Dans la liste intitulée "B. Personnes morales, entités et organismes", les mentions 3 et 4 sont remplacées par le texte suivant:

	Nom	Informations d'identification	Exposé des motifs	Date d'inscription
"3	Centre principal des technologies spéciales (GTsST) de la direction générale du renseignement de l'état-major des forces armées de la Fédération de Russie (GU/GRU)	Adresse: 22 Kirova Street, Moscou, Fédération de Russie	Le Centre principal des technologies spéciales (GTsST) de la direction générale du renseignement de l'état-major des forces armées de la Fédération de Russie (GU/GRU), également connu par son numéro de poste de campagne 74455, est impliqué dans des cyberattaques ayant des effets importants, provenant de l'extérieur de l'Union et constituant une menace extérieure pour l'Union ou ses États membres, et dans des cyberattaques ayant des effets importants dirigés contre des pays tiers, y compris les cyberattaques de juin 2017 connues sous les noms de "NotPetya" ou "EternalPetya" et les cyberattaques lancées contre un réseau électrique ukrainien pendant l'hiver 2015-2016. "NotPetya" ou "EternalPetya" a rendu des données inaccessibles dans un certain nombre d'entreprises au sein de l'Union, de l'Europe au sens large et du monde entier, en ciblant les ordinateurs au moyen d'un rançongiciel et en bloquant l'accès aux données, ce qui a entraîné, entre autres, d'importantes pertes économiques. La cyberattaque lancée contre un réseau électrique ukrainien a provoqué l'arrêt d'une partie de celui-ci pendant l'hiver.	30.7.2020

	Nom	Informations d'identification	Exposé des motifs	Date d'inscription
			L'acteur connu publiquement sous le nom de "Sandworm" (autrement connu sous le nom de "Sandworm Team", "BlackEnergy Group", "Voodoo Bear", "Quedagh", "Olympic Destroyer" ou "Telebots"), qui est également à l'origine de l'attaque lancée contre le réseau électrique ukrainien, a mené "NotPetya" ou "EternalPetya". Sandworm a mené des cyberattaques contre l'Ukraine, y compris des agences gouvernementales ukrainiennes et des infrastructures critiques ukrainiennes, à la suite de la guerre d'agression menée par la Russie contre l'Ukraine. Ces cyberattaques comprennent des campagnes d'hameçonnage ciblé et d'attaques par logiciels malveillants et rançongiciels. Le Centre principal des technologies spéciales de la direction générale du renseignement de l'état-major des forces armées de la Fédération de Russie joue un rôle actif dans les cyberactivités menées par Sandworm et peut être relié à celui-ci.	

	Nom	Informations d'identification	Exposé des motifs	Date d'inscription
4.	85e Centre principal des services spéciaux (GTsSS) de la direction générale du renseignement de l'état-major des forces armées de la Fédération de Russie (GU/GRU)	Adresse: Komsomol'skiy Prospekt, 20, Moscou, 119146, Fédération de Russie	Le 85e Centre principal des services spéciaux (GTsSS) de la direction générale du renseignement de l'état-major des forces armées de la Fédération de Russie (GU/GRU) (autrement connu sous les noms: "unité militaire 26165", "APT28", "Fancy Bear", "Sofacy Group", "Pawn Storm" et "Strontium") est impliqué dans des cyberattaques ayant des effets importants, qui constituent une menace extérieure pour l'Union ou ses États membres et à des cyberattaques ayant des effets importants dirigées contre des pays tiers. En particulier, des membres du renseignement militaire du GTsSS ont participé à la cyberattaque contre le parlement fédéral allemand (Deutscher Bundestag) en avril et mai 2015 et à la tentative de cyberattaque, qui visait le piratage du réseau WiFi de l'Organisation pour l'interdiction des armes chimiques (OIAC) aux Pays-Bas en avril 2018. La cyberattaque contre le parlement fédéral allemand a ciblé le système d'information du parlement et en a perturbé le fonctionnement pendant plusieurs jours. Une importante quantité de données a été volée et les comptes de courrier électronique de plusieurs parlementaires, ainsi que de l'ancienne chancelière Angela Merkel, ont été affectés. À la suite de la guerre d'agression menée par la Russie contre l'Ukraine, des cyberattaques du GTsSS (hameçonnage ciblé et attaques par logiciels malveillants) ont été menées contre l'Ukraine.	22.10.2020".