Rat der
Europäischen Union

Brüssel, den 7. Juli 2026
(OR. en)

8643/26

LIMITE

CORLX 388
CFSP/PESC 584
CYBER 192
JAI 505
FIN 592

GESETZGEBUNGSAKTE UND ANDERE RECHTSINSTRUMENTE

Betr.:	BESCHLUSS DES RATES zur Änderung des Beschlusses (GASP) 2019/797 über restriktive Maßnahmen gegen Cyberangriffe, die die Union oder ihre Mitgliedstaaten bedrohen

BESCHLUSS (GASP) 2026/… DES RATES

vom …

zur Änderung des Beschlusses (GASP) 2019/797 über restriktive Maßnahmen gegen Cyberangriffe, die die Union oder ihre Mitgliedstaaten bedrohen

DER RAT DER EUROPÄISCHEN UNION —

gestützt auf den Vertrag über die Europäische Union, insbesondere auf Artikel 29,

auf Vorschlag der Hohen Vertreterin der Union für Außen- und Sicherheitspolitik,

in Erwägung nachstehender Gründe:

(1) Der Rat hat am 17. Mai 2019 den Beschluss (GASP) 2019/797[1] angenommen.

(2) Als Teil dauerhafter, maßgeschneiderter und koordinierter Maßnahmen der Union gegen Akteure, von denen eine anhaltende Cyberbedrohung ausgeht, sollten acht natürliche Personen und vier Organisationen in die im Anhang des Beschlusses (GASP) 2019/797 enthaltene Liste der natürlichen und juristischen Personen, Organisationen und Einrichtungen, gegen die restriktive Maßnahmen verhängt wurden, aufgenommen werden. Diese Personen und Organisationen sind für Cyberangriffe mit erheblichen Auswirkungen, die eine äußere Bedrohung für die Union oder ihre Mitgliedstaaten darstellen, verantwortlich, unterstützen diese oder sind daran beteiligt.

(3) Der Beschluss (GASP) 2019/797 sollte daher entsprechend geändert werden —

HAT FOLGENDEN BESCHLUSS ERLASSEN:

[1] Beschluss (GASP) 2019/797 des Rates vom 17. Mai 2019 über restriktive Maßnahmen gegen Cyberangriffe, die die Union oder ihre Mitgliedstaaten bedrohen (ABl. L 129I vom 17.5.2019, S. 13, ELI: http://data.europa.eu/eli/dec/2019/797/oj).

Artikel 1

Der Anhang des Beschlusses (GASP) 2019/797 wird gemäß dem Anhang des vorliegenden Beschlusses geändert.

Artikel 2

Dieser Beschluss tritt am Tag seiner Veröffentlichung im *Amtsblatt der Europäischen Union* in Kraft.

Geschehen zu … am …

Im Namen des Rates
Der Präsident/Die Präsidentin

ANHANG

Der Anhang des Beschlusses (GASP) 2019/797 wird wie folgt geändert:

1. Unter der Überschrift „A. Natürliche Personen“ werden folgende Einträge angefügt:

	Name	Angaben zur Identität	Gründe	Datum der Aufnahme in die Liste
„20.	Vitaly Nikolayevich KOVALEV	Виталий Николаевич КОВАЛЕВ Aliasnamen: ‚Bentley‘, ‚Bergen‘, ‚Alex Konor‘, ‚Benny‘, ‚Ben‘, ‚Stern‘ Geburtsdatum: 23.6.1988 Anschrift: Serebristy Bulvar 34 (Serebristyy Bul’var); krp 1; flt 528; 197341; St Petersburg, Russian Federation Staatsangehörigkeit: russisch Geschlecht: männlich Verbundene Organisationen: TrickBot, Wizard Spider, Conti	Vitaly Kovalev ist eine führende Persönlichkeit im Zusammenhang mit den Schadsoftwares ‚Trickbot‘ und ‚Conti‘. Er ist auch bekannt unter den Online-Spitznamen ‚Bentley‘, ‚Bergen‘, ‚Alex Konor‘, ‚Benny‘, ‚Ben‘ und ‚Stern‘. Die Schadsoftwares ‚Conti‘ und ‚Trickbot‘ wurden ursprünglich von ‚Wizard Spider‘ geschaffen und entwickelt. ‚Wizard Spider‘ hat in verschiedenen Branchen, darunter wesentliche Dienstleistungsbereiche wie die Gesundheitsversorgung und das Bankwesen, Ransomware-Kampagnen durchgeführt, weltweit Computer infiziert und ihre Schadsoftware in eine hochmodulare Schadsoftware-Reihe entwickelt. Von ‚Wizard Spider‘ durchgeführte Kampagnen, bei denen Schadsoftware wie ‚Conti‘, und ‚TrickBot‘ eingesetzt wird, sind für erhebliche wirtschaftliche Schäden in der Europäischen Union verantwortlich. Vitaly Kovalev ist somit für Cyberangriffe mit erheblichen Auswirkungen, die eine äußere Bedrohung für die Union oder ihre Mitgliedstaaten darstellen, verantwortlich und daran beteiligt.	[+]

[+] ABl.: Bitte das Datum der Veröffentlichung dieses Beschlusses einfügen.

	Name	Angaben zur Identität	Gründe	Datum der Aufnahme in die Liste
21.	Alexander Alexandrovich VOLOSOVIK	Александр Александрович ВОЛОСОВИК Geburtsdatum: 30.1.1983 Geburtsort: UdSSR Staatsangehörigkeit: russisch Reisepass-Nr.: 762988138 Geschlecht: männlich Verbundene Organisationen: Yalishanda, LARVA-34, podzemniyl, Ohyeahhellno, Stas_vl, downlow	Alexander Volosovik ist Eigentümer von Media Land LLC. Seit 2016 erleichtert der Bulletproof-Hosting-Dienst Media Land LLC ein breites Spektrum von Angriffen mit Schadsoftware sowohl gegen die Union als auch weltweit, indem er Hostingdienste anbietet, mit denen Nutzeridentitäten verborgen werden und der Entfernung von Inhalten durch die Strafverfolgungsbehörden entgegengewirkt wird. Media Land LLC hat groß angelegte Ransomware-Operationen, Command-and-Control-Dienste sowie Phishing-Operationen ermöglicht, die auf kritische Infrastrukturen und wesentliche Dienstleistungsbereiche in den Mitgliedstaaten abzielen, was zu erheblichen finanziellen Verlusten geführt hat. Zu den von Media Land LLC unterstützten Operationen gehören unter anderem ‚LockBit', ‚EvilCorp' und ‚BlackBasta'. Somit ist Media Land LLC an Cyberangriffen mit erheblichen Auswirkungen beteiligt, die eine äußere Bedrohung für die Union oder ihre Mitgliedstaaten darstellen. Als Eigentümer von Media Land LLC ist Alexander Volosovik für diese Cyberangriffe verantwortlich und daran beteiligt. Er steht auch in Verbindung mit Media Land LLC.	+

+ ABl.: Bitte das Datum der Veröffentlichung dieses Beschlusses einfügen.

	Name	Angaben zur Identität	Gründe	Datum der Aufnahme in die Liste
22.	Denis Olegovich DEGTYARENKO	Денис Олегович ДЕГТЯРЕНКО Aliasname: ‚Dena‘ Geburtsdatum: 9.10.1989 Geburtsort: UdSSR Staatsangehörigkeit: russisch Geschlecht: männlich Anschrift: 130 Lenina Avenue, Novy Gorod microdistrict, Orsk, Orenburg Region, Russian Federation	Denis Degtyarenko alias Dena ist ein russischer Hacker für die Gruppe CARR (Cyber Army of Russia Reborn). CARR ist für Cyberangriffe auf Dienste, die für die Aufrechterhaltung wesentlicher wirtschaftlicher Tätigkeiten und kritischer staatlicher Funktionen in den Mitgliedstaaten erforderlich sind, sowie auf Infrastrukturen in der Ukraine und anderen Drittländern verantwortlich. CARR steht mit dem Hauptzentrum für Spezialtechnologien (GTsST) der Hauptdirektion des Generalstabs der Streitkräfte der Russischen Föderation (GRU) in Verbindung. Das GTsST führt weiterhin aktiv Cyberangriffe gegen die Union oder ihre Mitgliedstaaten durch. Zu den Zielen von CARR gehören staatliche Stellen, Finanzinstitute, Medien und kritische Infrastrukturen in den Mitgliedstaaten und den Vereinigten Staaten. CARR hat Distributed Denial-of-Service (DDoS)-Angriffe in der Ukraine und gegen Regierungen und Unternehmen in Ländern durchgeführt, die die Ukraine unterstützen. Somit ist Denis Degtyarenko, ein wichtiger Hacker für CARR, an Cyberangriffen mit erheblichen Auswirkungen beteiligt, einschließlich versuchter Cyberangriffe mit potenziell erheblichen Auswirkungen, die eine äußere Bedrohung für die Mitgliedstaaten sowie für Drittstaaten darstellen. Als Mitglied von CARR steht er auch in Verbindung mit GTsST.	+

+ ABl.: Bitte das Datum der Veröffentlichung dieses Beschlusses einfügen.

	Name	Angaben zur Identität	Gründe	Datum der Aufnahme in die Liste
23.	Yuliya Vladimirovna PANKRATOVA	Юлия Владимировна ПАНКРАТОВА Aliasname: ‚YUliYA‘ Geburtsdatum: 6.4.1984 Geburtsort: UdSSR Staatsangehörigkeit: russisch Geschlecht: weiblich Anschrift: 130 Lenina Avenue, Novy Gorod microdistrict, Orsk, Orenburg Region, Russian Federation	Yuliya Pankratova ist eine russische Hackerin, die für CARR (Cyber Army of Russia Reborn) tätig war und später die Gruppe Z-Pentest gegründet hat, für die sie weiterhin arbeitet. CARR ist für Cyberangriffe auf Dienste, die für die Aufrechterhaltung wesentlicher wirtschaftlicher Tätigkeiten und kritischer staatlicher Funktionen in den Mitgliedstaaten erforderlich sind, sowie auf Infrastrukturen in der Ukraine und anderen Drittländern verantwortlich. CARR steht mit dem Hauptzentrum für Spezialtechnologien (GTsST) der Hauptdirektion des Generalstabs der Streitkräfte der Russischen Föderation (GRU) in Verbindung. Das GTsST führt weiterhin aktiv Cyberangriffe gegen die Union oder ihre Mitgliedstaaten durch. Zu den Zielen von CARR gehören staatliche Stellen, Finanzinstitute, Medien und kritische Infrastrukturen in den Mitgliedstaaten und den Vereinigten Staaten. CARR hat Distributed Denial-of-Service (DDoS)-Angriffe in der Ukraine und gegen Regierungen und Unternehmen in Ländern durchgeführt, die die Ukraine unterstützen.	+

+ ABl.: Bitte das Datum der Veröffentlichung dieses Beschlusses einfügen.

	Name	Angaben zur Identität	Gründe	Datum der Aufnahme in die Liste
			Z-Pentest ist für Cyberangriffe mit erheblichen Auswirkungen unter anderem auf Dienste, die für die Aufrechterhaltung wesentlicher Tätigkeiten in den Mitgliedstaaten erforderlich sind, verantwortlich. Somit ist Yuliya Pankratova, eine wichtige Hackerin für CARR und für Z-Pentest, an Cyberangriffen mit erheblichen Auswirkungen beteiligt, einschließlich versuchter Cyberangriffe mit potenziell erheblichen Auswirkungen, die eine äußere Bedrohung für die Mitgliedstaaten sowie für Drittstaaten darstellen. Sie steht auch mit Z-Pentest in Verbindung.	

	Name	Angaben zur Identität	Gründe	Datum der Aufnahme in die Liste
24.	Maksim Evgenevich VORONIN	Максим Евгеньевич ВОРОНИН Aliasname: ‚Daugn0‘ Staatsangehörigkeit: mutmaßlich russisch Geschlecht: männlich	Maksim Voronin alias Daugn0 ist an der Entwicklung, dem Vertrieb und dem Verkauf der Schadsoftware LummaC2 (alias Lumma infostealer, Lumma Stealer) beteiligt, die zum Informationsdiebstahl verwendet wird. LummaC2 ist eine Malware-as-a-Service-Plattform (MaaS), die verwendet wird, um sensible Daten, Browser-Zugangsdaten, Krypto-Wallets oder Systeminformationen zu stehlen, zusätzliche Schadsoftware auf infizierten Geräten zu installieren, sowie für den Diebstahl von Kryptowährungen und für Spionagekampagnen. Cyberangriffe mit der LummaC2-Schadsoftware werden auch von finanziell motivierten Cyberbedrohungsakteuren wie Storm-113, Storm-1607, Storm-1674, Octo Tempest und anderen eingesetzt. Die LummaC2-Schadsoftware wird für Cyberangriffe auf kritische staatliche Funktionen und Dienste eingesetzt, die für die Aufrechterhaltung wesentlicher sozialer und wirtschaftlicher Tätigkeiten der Mitgliedstaaten erforderlich sind. 2024 und 2025 war LummaC2 eines der am häufigsten verwendeten Instrumente für Informationsdiebstahl weltweit. Somit ist Maksim Voronin als Entwickler, Vertreiber und Verkäufer von LummaC2 an Cyberangriffen mit erheblichen Auswirkungen, die eine äußere Bedrohung für die Mitgliedstaaten darstellen, beteiligt und erleichtert diese.	+

+ ABl.: Bitte das Datum der Veröffentlichung dieses Beschlusses einfügen.

	Name	Angaben zur Identität	Gründe	Datum der Aufnahme in die Liste
25.	Maksim Aleksandrovich GORDIENKO alias Maxim Alexandrovich GORDIENKO	Максим Александрович ГОРДИЕНКО Aliasname: ‚Lummaseller‘ Staatsangehörigkeit: mutmaßlich russisch Geschlecht: männlich	Maksim Gordienko alias Lummaseller ist an der Entwicklung und dem Vertrieb der Schadsoftware LummaC2 (alias Lumma infostealer, Lumma Stealer) beteiligt, die zum Informationsdiebstahl verwendet wird. LummaC2 ist eine Malware-as-a-Service-Plattform (MaaS), die verwendet wird, um sensible Daten, Browser-Zugangsdaten, Krypto-Wallets oder Systeminformationen zu stehlen, zusätzliche Schadsoftware auf infizierten Geräten zu installieren, sowie für den Diebstahl von Kryptowährungen und für Spionagekampagnen. Cyberangriffe mit der LummaC2-Schadsoftware werden auch von finanziell motivierten Cyberbedrohungsakteuren wie Storm-113, Storm-1607, Storm-1674, Octo Tempest und anderen eingesetzt. Die LummaC2-Schadsoftware wird für Cyberangriffe auf kritische staatliche Funktionen und Dienste eingesetzt, die für die Aufrechterhaltung wesentlicher sozialer und wirtschaftlicher Tätigkeiten der Mitgliedstaaten erforderlich sind. 2024 und 2025 war LummaC2 eines der am häufigsten verwendeten Instrumente für Informationsdiebstahl weltweit. Somit ist Maksim Gordienko als Entwickler, Vertreiber und Verkäufer von LummaC2 an Cyberangriffen mit erheblichen Auswirkungen, die eine äußere Bedrohung für die Mitgliedstaaten darstellen, beteiligt und erleichtert diese.	+

+ ABl.: Bitte das Datum der Veröffentlichung dieses Beschlusses einfügen.

	Name	Angaben zur Identität	Gründe	Datum der Aufnahme in die Liste
26.	Evgeniy Viktorovich BASHEV	Евгений Викторович БАШЕВ Geburtsdatum: 25.1.1980 Geburtsort: UdSSR Staatsangehörigkeit: russisch Geschlecht: männlich Verbundene Personen: Denis Igorevich Denisenko, Yuriy Fedorovich Denisov, Dmitriy Yuryevich Goloshubov, Nikolay Alexandrovich Korchagin Verbundene Organisationen: GRU-Einheit 29155, ‚Impuls' LLC	Evgeniy Bashev ist Mitglied der Einheit 29155 des russischen Militärgeheimdienstes GRU. Innerhalb der Einheit unterstützt und erleichtert er Cyberangriffe mit erheblichen Auswirkungen auf die Mitgliedstaaten, unter anderem durch die Kontrolle des Servers ‚Aegon', der für Hackerangriffe verwendet wird. Insbesondere leistet er über sein Unternehmen ‚Impuls' LLC technische und materielle Unterstützung für die Cyberangriffe der GRU Einheit 29155, und zwar durch die Bereitstellung von operativer Tarnung und von Infrastruktur, die Erleichterung von Zahlungen und die Verwaltung technischer Ressourcen, darunter Server, die für die Cyberangriffe verwendet werden. Zudem hat er die Zusammenarbeit zwischen GRU-Strukturen und externen Hackernetzen koordiniert. Die durch ihn ermöglichten Cyberangriffe zielten auf kritische staatliche Systeme, Funktionen und Dienste, die für die Aufrechterhaltung wesentlicher sozialer oder wirtschaftlicher Tätigkeiten in den Mitgliedstaaten erforderlich sind, insbesondere im Verkehrssektor. Im Rahmen der Kampagne ‚WhisperGate' hat die GRU-Einheit 29155 auch kritische Infrastrukturen der Ukraine ins Visier genommen.	+

+ ABl.: Bitte das Datum der Veröffentlichung dieses Beschlusses einfügen.

	Name	Angaben zur Identität	Gründe	Datum der Aufnahme in die Liste
			Somit leistet Evgeniy Bashev technische und materielle Unterstützung für Cyberangriffe mit erheblichen Auswirkungen, einschließlich versuchter Cyberangriffe mit potenziell erheblichen Auswirkungen, die eine äußere Bedrohung für Mitgliedstaaten darstellen, sowie für Cyberangriffe mit erheblichen Auswirkungen auf einen Drittstaat oder ist anderweitig an diesen beteiligt. Als Eigentümer und Generaldirektor steht er mit dem Unternehmen ‚Impuls' LLC in Verbindung. Als Mitglied der GRU-Einheit 29155 steht er auch mit dieser Organisation in Verbindung.	

	Name	Angaben zur Identität	Gründe	Datum der Aufnahme in die Liste
27.	Roman Alexandrovich PUNTUS	Роман Александрович ПУНТУС Geburtsort: Russische Föderation Staatsangehörigkeit: russisch Geschlecht: männlich Verbundene Personen: Denis Igorevich Denisenko, Yuriy Fedorovich Denisov, Dmitriy Yuryevich Goloshubov, Nikolay Alexandrovich Korchagin, Evgeniy Viktorovich Bashev Verbundene Organisationen: GRU-Einheit 29155	Roman Puntus ist Mitglied der Einheit 29155 des russischen Militärgeheimdienstes GRU. Innerhalb der Einheit spielt er eine führende Rolle bei der Organisation und Koordinierung von Cyberangriffen mit erheblichen Auswirkungen auf die Mitgliedstaaten. Er unterstützt auch die Entwicklung der internen Cyberfähigkeit der Einheit, unter anderem in dem er Personal, etwa Hacker und Programmierer, einstellt und beaufsichtigt. Durch die Gründung der Scheinfirma ‚Aegeon-Impulse' erleichterte er Cyberoperationen auf logistischer und finanzieller Ebene. Unter seiner Koordinierung führte die Einheit Cyberangriffe auf kritische staatliche Systeme, Funktionen und Dienste aus, die für die Aufrechterhaltung wesentlicher sozialer oder wirtschaftlicher Tätigkeiten in den Mitgliedstaaten erforderlich sind, insbesondere im Verkehrssektor. Im Rahmen der Kampagne ‚WhisperGate' hat die GRU-Einheit 29155 auch kritische Infrastrukturen der Ukraine ins Visier genommen.	[+]“

[+] ABl.: Bitte das Datum der Veröffentlichung dieses Beschlusses einfügen.

	Name	Angaben zur Identität	Gründe	Datum der Aufnahme in die Liste
			Somit ist Roman Puntus für Cyberangriffe mit erheblichen Auswirkungen, einschließlich versuchter Cyberangriffe mit potenziell erheblichen Auswirkungen, die eine äußere Bedrohung für die Mitgliedstaaten darstellen, sowie für Cyberangriffe mit erheblichen Auswirkungen auf einen Drittstaat verantwortlich oder anderweitig an diesen beteiligt. Als Mitglied der GRU-Einheit 29155 steht er auch mit dieser Organisation in Verbindung.	

2. Folgende Einträge werden unter der Überschrift „B. Juristische Personen, Organisationen und Einrichtungen“ angefügt:

	Name	Angaben zur Identität	Gründe	Datum der Aufnahme in die Liste
„8.	Media Land LLC	Anschrift: Tsvetnochnaya st., 16 Litera P, Room 27, Moskovskaya Zastava Municipal District St Petersburg, 196006, Russian Federation Art der Organisation: Limited Liability Company (Gesellschaft mit beschränkter Haftung) Ort der Registrierung: Sankt Petersburg Registrierungsdatum: 19.10.2015 Registrierungsnummer: 1152536009900 Ort des Hauptgeschäftssitzes: Sankt Petersburg, Russische Föderation Verbundene Organisation: ML.Cloud	Seit 2016 erleichtert der Bulletproof-Hosting-Dienst Media Land LLC ein breites Spektrum von Angriffen mit Schadsoftware gegen die Mitgliedstaaten und weltweit, indem er Hostingdienste anbietet, mit denen Nutzeridentitäten verborgen werden und der Entfernung von Inhalten durch die Strafverfolgungsbehörden entgegengewirkt wird, was zu erheblichen finanziellen Verlusten führt. Media Land LLC hat groß angelegte Ransomware Operationen, Command-and-Control-Dienste sowie Phishing-Operationen ermöglicht, die auf kritische Infrastrukturen und wesentliche Dienstleistungsbereiche in den Mitgliedstaaten abzielen. Zu den von Media Land LLC unterstützten Operationen gehören unter anderem ‚LockBit‘, ‚EvilCorp‘ und ‚BlackBasta‘. Somit ist Media Land LLC an Cyberangriffen mit erheblichen Auswirkungen beteiligt, die eine äußere Bedrohung für die Mitgliedstaaten darstellen.	[+]

[+] ABl.: Bitte das Datum der Veröffentlichung dieses Beschlusses einfügen.

	Name	Angaben zur Identität	Gründe	Datum der Aufnahme in die Liste
9.	ML.Cloud	Anschrift: Brivibas iela 52, Riga, LV-1011, Latvija; Russian Federation, Kazan, Peterburgskaya st. 52 Ort der Registrierung: Riga Verbundene Person: Alexander Volosovik Sonstige verbundene Organisationen: Media Land LLC	ML.Cloud ist die Schwestergesellschaft von Media Land LLC und stellt die technische Infrastruktur für Media Land LLC bereit. Seit 2016 erleichtert der Bulletproof-Hosting-Dienst Media Land LLC ein breites Spektrum von Angriffen mit Schadsoftware gegen die Mitgliedstaaten und weltweit, indem er Hostingdienste anbietet, mit denen Nutzeridentitäten verborgen werden und der Entfernung von Inhalten durch die Strafverfolgungsbehörden entgegengewirkt wird, was zu erheblichen finanziellen Verlusten führt. Media Land LLC hat groß angelegte Ransomware-Operationen, Command-and-Control-Dienste sowie Phishing-Operationen ermöglicht, die auf kritische Infrastrukturen und wesentliche Dienstleistungsbereiche in den Mitgliedstaaten abzielen. Zu den von Media Land LLC unterstützten Operationen gehören unter anderem ‚LockBit', ‚EvilCorp' und ‚BlackBasta'. Somit ist Media Land LLC an Cyberangriffen beteiligt, die eine äußere Bedrohung mit erheblichen Auswirkungen für Mitgliedstaaten der EU darstellen. Somit stellt ML.Cloud technische Unterstützung für Cyberangriffe mit erheblichen Auswirkungen bereit, die eine äußere Bedrohung für die Mitgliedstaaten darstellen.	+

+ ABl.: Bitte das Datum der Veröffentlichung dieses Beschlusses einfügen.

	Name	Angaben zur Identität	Gründe	Datum der Aufnahme in die Liste
10.	‚Impuls' LLC	Общество с ограниченной ответственностью ‚Импульс' Anschrift: 344015, Russian Federation, Rostov Region, Rostov-on-Don, ul. Eremenko, d. 56, k. 6, apt. 88 Art der Organisation: Limited Liability Company (Gesellschaft mit beschränkter Haftung) Ort der Registrierung: Interdistrict Inspectorate of the Federal Tax Service No. 26 for the Rostov Region, 344019, Rostov-on-Don, ul. Myasnikova, d. 52/32, Russian Federation Registrierungsdatum: 27.9.2010	‚Impuls' LLC ist ein russisches Unternehmen im Eigentum von Evgeniy Viktorovich Bashev, einem Mitglied der Einheit 29155 des russischen Militärgeheimdienstes GRU. Das Unternehmen leistet technische und materielle Unterstützung bei Cyberangriffen und versuchten Cyberangriffen, die von der GRU-Einheit 29155 durchgeführt werden. Insbesondere dient ‚Impuls' LLC als operativer Vermittler, der es ermöglicht, Hacking-Aktivitäten über ein Unternehmen durchzuführen, das offiziell nicht mit dem russischen Staat verbunden ist. Es hat für Cyberangriffe als operative Tarnung gedient, Infrastruktur geboten und Zahlungen erleichtert und stand in Verbindung mit technischen Ressourcen, einschließlich Servern, die zur Unterstützung von Hacking-Aktivitäten verwendet werden. Insbesondere hat ‚Impuls' LLC die Zusammenarbeit zwischen GRU-Strukturen und externen Hackernetzen ermöglicht. Die durch ‚Impuls' LLC erleichterten Cyberoperationen zielen auf kritische staatliche Funktionen und Dienste, die für die Aufrechterhaltung wesentlicher sozialer und wirtschaftlicher Tätigkeiten in den Mitgliedstaaten erforderlich sind, insbesondere im Verkehrssektor. Im Rahmen der Kampagne ‚WhisperGate' hat die GRU-Einheit 29155 auch kritische Infrastrukturen der Ukraine ins Visier genommen.	+

+ ABl.: Bitte das Datum der Veröffentlichung dieses Beschlusses einfügen.

	Name	Angaben zur Identität	Gründe	Datum der Aufnahme in die Liste
		Registrierungsnummer: INN (ИНН): 6168033776; OGRN (ОГРН): 1106194004850 Ort des Hauptgeschäftssitzes: Russische Föderation Verbundene Personen: Evgeniy Bashev Verbundene Organisationen: GRU-Einheit 29155	Somit leistet ‚Impuls' LLC technische und materielle Unterstützung für Cyberangriffe mit erheblichen Auswirkungen, die eine äußere Bedrohung für die Mitgliedstaaten darstellen, sowie für Cyberangriffe mit erheblichen Auswirkungen auf einen Drittstaat oder ist anderweitig an diesen beteiligt.	

	Name	Angaben zur Identität	Gründe	Datum der Aufnahme in die Liste
11.	Z-Pentest	Aliasnamen: ‚Z-Pentest Alliance', ‚Z-Alliance' Ort des Hauptgeschäftssitzes: Russische Föderation Verbundene Personen: Yuliya Pankratova Verbundene Organisationen: Cyber Army of Russia/CARR X-Account: ZPentest (Account gesperrt) Telegram-Account: Zpentestalliance	Z-Pentest ist eine prorussische Hacktivisten-Gruppe, die sich aus Mitgliedern von CARR (Cyber Army of Russia Reborn) und NoName057 zusammensetzt und weltweit kritische Infrastrukturen, vornehmlich Energiesysteme und die Wasserwirtschaft, ins Visier nimmt. Insbesondere griff die Gruppe im Dezember 2024 einen dänischen Wasserversorger an. Somit ist Z-Pentest für Cyberangriffe mit erheblichen Auswirkungen, die eine äußere Bedrohung für die Mitgliedstaaten darstellen, verantwortlich.	[+]“

[+] ABl.: Bitte das Datum der Veröffentlichung dieses Beschlusses einfügen.