Amtsblatt
der Europäischen Union

DE
Reihe L

2025/171

27.1.2025

BESCHLUSS (GASP) 2025/171 DES RATES

vom 27. Januar 2025

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 des Hohen Vertreters 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) Gezielte restriktive Maßnahmen gegen Cyberangriffe mit erheblichen Auswirkungen, die eine externe Bedrohung für die Union oder ihre Mitgliedstaaten darstellen, gehören zu den Maßnahmen des Rahmens für eine gemeinsame diplomatische Reaktion der Union auf böswillige Cyberaktivitäten, nämlich die „Cyber Diplomacy Toolbox“, und sind ein wichtiges Instrument, um solche Aktivitäten zu verhindern, von solchen Aktivitäten abzuschrecken, davon abzuhalten und darauf zu reagieren.

(3) Böswillige Cyberaktivitäten, die gegen kritische Infrastruktur oder wesentliche Dienstleistungen gerichtet sind und zu denen unter anderem der Einsatz von Ransomware und Wiper-Schadsoftware gehört, die gezielte Ausrichtung gegen Lieferketten und Cyberspionage, einschließlich des Diebstahls geistigen Eigentums, nehmen an Zahl, Häufigkeit und Komplexität zu. Durch ihre beeinträchtigenden und zerstörerischen Auswirkungen stellen diese Aktivitäten eine systemische Bedrohung für die Sicherheit, die Wirtschaft und die Demokratie der Union und für die Gesellschaft insgesamt dar.

(4) Im Jahr 2020 wurden Cyberangriffe mit erheblichen Auswirkungen auf Estland durchgeführt. Es wurden Cyberangriffe auf die Computersysteme mehrerer Institutionen durchgeführt, mit dem Ziel, die Daten zu verwenden, um die Sicherheit Estlands zu bedrohen. Diese Cyberangriffe betrafen die Speicherung von Verschlusssachen.

(5) Als Teil dauerhafter, maßgeschneiderter und koordinierter Maßnahmen der Union gegen Akteure, von denen eine anhaltende Cyberbedrohung ausgeht, sollten drei natürliche Personen 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 sind für Cyberangriffe mit erheblichen Auswirkungen, die eine externe Bedrohung für die Union oder ihre Mitgliedstaaten darstellen, verantwortlich oder daran beteiligt.

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

HAT FOLGENDEN BESCHLUSS ERLASSEN:

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 Brüssel am 27. Januar 2025.

Im Namen des Rates

Die Präsidentin

K. KALLAS

[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 129 I vom 17.5.2019, S. 13, ELI: http://data.europa.eu/eli/dec/2019/797/oj).

ANHANG

Im Anhang des Beschlusses (GASP) 2019/797 werden unter der Überschrift „A. Natürliche Personen“ folgende Einträge angefügt:

	Name	Angaben zur Identität	Gründe	Datum der Aufnahme in die Liste
„15.	Nikolay Alexandrovich KORCHAGIN	Николай Александрович Корчагин Geburtsdatum: 16.9.1997 Staatsangehörigkeit: russisch Geschlecht: männlich Verbundene Organisation: Hauptdirektion des Generalstabs der Streitkräfte der Russischen Föderation	Nikolay Korchagin ist an Cyberangriffen mit erheblichen Auswirkungen beteiligt und dafür verantwortlich, indem er nachrichtendienstliche Aktivitäten gegen Estland durchführt und sich illegal Zugang zu einem Computersystem verschafft hat. Nikolay Korchagin ist Offizier der Militäreinheit 29155 der Hauptdirektion des Generalstabs der Streitkräfte der Russischen Föderation (GRU). In dieser Funktion ist er an Cyberangriffen auf Computersysteme beteiligt und dafür verantwortlich mit dem Ziel, Daten von den Datensystemen mehrerer Institutionen abzugreifen, die unabhängig voneinander oder in Kombination miteinander einen Überblick über die Cybersicherheitspolitik Estlands, die Cyberfähigkeiten des Staates, sensible personenbezogene Daten und andere sensible Daten gewähren, mit dem Ziel, die Daten zu verwenden, um die Sicherheit Estlands zu bedrohen. Die Angriffe betreffen daher die Speicherung von Verschlusssachen. Die Angriffe betrafen Verbündete und Partner Estlands. Somit ist Nikolay Korchagin an Cyberangriffen mit erheblichen Auswirkungen, die eine äußere Bedrohung für einen Mitgliedstaat darstellen, beteiligt und dafür verantwortlich.	27.1.2025
16.	Vitaly SHEVCHENKO	Виталий Шевченко Geburtsdatum: 1.9.1997 Staatsangehörigkeit: russisch Geschlecht: männlich Verbundene Organisation: Hauptdirektion des Generalstabs der Streitkräfte der Russischen Föderation	Vitaly Shevchenko ist an Cyberangriffen mit erheblichen Auswirkungen beteiligt und dafür verantwortlich, indem er nachrichtendienstliche Aktivitäten gegen Estland durchführt und sich illegal Zugang zu einem Computersystem verschafft hat. Vitaly Shevchenko ist Offizier der Militäreinheit 29155 der Hauptdirektion des Generalstabs der Streitkräfte der Russischen Föderation (GRU). In dieser Funktion ist er an Cyberangriffen auf Computersysteme beteiligt und dafür verantwortlich mit dem Ziel, Daten von den Datensystemen mehrerer Institutionen abzugreifen, die unabhängig voneinander oder in Kombination miteinander einen Überblick über die Cybersicherheitspolitik Estlands, die Cyberfähigkeiten des Staates, sensible personenbezogene Daten und andere sensible Daten gewähren, mit dem Ziel, die Daten zu verwenden, um die Sicherheit Estlands zu bedrohen. Die Angriffe betreffen daher die Speicherung von Verschlusssachen. Die Angriffe betrafen Verbündete und Partner Estlands. Somit ist Vitaly Shevchenko an Cyberangriffen mit erheblichen Auswirkungen, die eine äußere Bedrohung für einen Mitgliedstaat darstellen, beteiligt und dafür verantwortlich.	27.1.2025

ELI: http://data.europa.eu/eli/dec/2025/171/oj

	Name	Angaben zur Identität	Gründe	Datum der Aufnahme in die Liste
17.	Yuriy Fedorovich DENISOV	Юрий Федорович Денисов Geburtsdatum: 17.6.1980 Staatsangehörigkeit: russisch Geschlecht: männlich Verbundene Organisation: Hauptdirektion des Generalstabs der Streitkräfte der Russischen Föderation	Yuriy Denisov ist an Cyberangriffen mit erheblichen Auswirkungen beteiligt und dafür verantwortlich, indem er nachrichtendienstliche Aktivitäten gegen Estland durchführt und sich illegal Zugang zu einem Computersystem verschafft hat. Yuriy Denisov ist Offizier der Militäreinheit 29155 der Hauptdirektion des Generalstabs der Streitkräfte der Russischen Föderation (GRU). In dieser Funktion ist er an Cyberangriffen auf Computersysteme beteiligt und dafür verantwortlich mit dem Ziel, Daten von den Datensystemen mehrerer Institutionen abzugreifen, die unabhängig voneinander oder in Kombination miteinander einen Überblick über die Cybersicherheitspolitik Estlands, die Cyberfähigkeiten des Staates, sensible personenbezogene Daten und andere sensible Daten gewähren, mit dem Ziel, die Daten zu verwenden, um die Sicherheit Estlands zu bedrohen. Die Angriffe betreffen daher die Speicherung von Verschlusssachen. Die Angriffe betrafen Verbündete und Partner Estlands. Somit ist Yuriy Denisov an Cyberangriffen mit erheblichen Auswirkungen, die eine äußere Bedrohung für einen Mitgliedstaat darstellen, beteiligt und dafür verantwortlich.	27.1.2025“