

Dieser Text dient lediglich zu Informationszwecken und hat keine Rechtswirkung. Verbindliche Fassungen der betreffenden Rechtsakte einschließlich ihrer Präambeln sind nur die im Amtsblatt der Europäischen Union veröffentlichten und auf EUR-Lex verfügbaren Texte.

VERORDNUNG (EU) 2019/796 DES RATES
vom 17. Mai 2019 [\(1\)](#)
über restriktive Maßnahmen gegen Cyberangriffe, die die Union oder ihre Mitgliedstaaten bedrohen
zuletzt geändert durch die
DURCHFÜHRUNGSVERORDNUNG (EU) 2025/886 DES RATES
vom 12. Mai 2025 [\(**\)](#)

DER RAT DER EUROPÄISCHEN UNION —

gestützt auf den Vertrag über die Arbeitsweise der Europäischen Union, insbesondere auf Artikel 215,

gestützt auf den Beschluss (GASP) 2019/797 des Rates vom 17. Mai 2019 über restriktive Maßnahmen gegen Cyberangriffe, die die Union oder ihre Mitgliedstaaten bedrohen [\(1\)](#)

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

in Erwägung nachstehender Gründe:

- (1) Am 18. Oktober 2018 hat der Europäische Rat Schlussfolgerungen angenommen, in denen er dazu aufforderte, die Arbeit an der Fähigkeit, mit restriktiven Maßnahmen der Union auf Cyberangriffe zu reagieren und diese zu verhindern, anknüpfend an die Schlussfolgerungen des Rates vom 19. Juni 2017 voranzubringen.
- (2) Am 17. Mai 2019 hat der Rat den Beschluss (GASP) 2019/797 angenommen. Mit dem Beschluss (GASP) 2019/797 wird ein Rahmen für gezielte restriktive Maßnahmen zur Verhinderung von Cyberangriffen und zur Reaktion auf Cyberangriffe mit erheblichen Auswirkungen, die eine externe Bedrohung für die Union oder ihre Mitgliedstaaten darstellen, geschaffen. Die Personen, Organisationen und Einrichtungen, die restriktiven Maßnahmen unterliegen, sind im Anhang jenes Beschlusses aufgeführt.
- (3) Diese Verordnung steht im Einklang mit den Grundrechten und Grundsätzen, die vor allem mit der Charta der Grundrechte der Europäischen Union anerkannt wurden, insbesondere mit dem Recht auf einen wirksamen Rechtsbehelf und ein unparteiisches Gericht und dem Recht auf Schutz personenbezogener Daten. Diese Verordnung sollte unter Wahrung dieser Rechte angewandt werden.
- (4) Zur Wahrung der Übereinstimmung mit dem Verfahren zur Änderung und Überprüfung des Anhangs des Beschlusses (GASP) 2019/797 sollte die Befugnis zur Änderung der Liste in Anhang I dieser Verordnung vom Rat ausgeübt werden.
- (5) Zur Durchführung dieser Verordnung und zur Gewährleistung eines Höchstmaßes an Rechtssicherheit innerhalb der Union sollten die Namen und übrigen sachdienlichen Angaben zu den natürlichen und juristischen Personen, Organisationen und Einrichtungen, deren Gelder und wirtschaftliche Ressourcen nach dieser Verordnung eingefroren werden sollen, veröffentlicht werden. Die Verarbeitung personenbezogener Daten sollte unter Einhaltung der Verordnungen (EU) 2016/679 [\(2\)](#) und der Verordnung (EU) 2018/1725 [\(3\)](#) des Europäischen Parlaments und des Rates erfolgen.
- (6) Die Kommission und die Mitgliedstaaten sollten einander über die gemäß dieser Verordnung getroffenen Maßnahmen unterrichten und andere ihnen vorliegende sachdienliche Informationen im Zusammenhang mit dieser Verordnung austauschen.
- (7) Die Mitgliedstaaten sollten Regeln für Sanktionen bei Verstößen gegen die Bestimmungen dieser Verordnung festlegen und die Durchsetzung dieser Sanktionen sicherstellen. Die Sanktionen sollten wirksam, verhältnismäßig und abschreckend sein –

HAT FOLGENDE VERORDNUNG ERLASSEN:

Artikel 1

- (1) Diese Verordnung gilt für Cyberangriffe mit erheblichen Auswirkungen, einschließlich versuchter Cyberangriffe mit potenziell erheblichen Auswirkungen, die eine äußere Bedrohung für die Union oder ihre Mitgliedstaaten darstellen.

- (2) Zu Cyberangriffen, die eine äußere Bedrohung darstellen, zählen Cyberangriffe, die
- a) ihren Ausgang außerhalb der Union haben oder von dort durchgeführt werden,
 - b) außerhalb der Union befindliche Infrastrukturen nutzen,
 - c) von natürlichen oder juristischen Personen, Organisationen oder Einrichtungen, die außerhalb der Union ansässig oder tätig sind, durchgeführt werden oder
 - d) mit Unterstützung, auf Anweisung oder unter der Kontrolle von natürlichen oder juristischen Personen, Organisationen oder Einrichtungen, die außerhalb der Union tätig sind, durchgeführt werden.
- (3) Zu diesem Zweck sind Cyberangriffe Handlungen, die
- a) den Zugang zu Informationssystemen,
 - b) den Eingriff in Informationssysteme,
 - c) den Eingriff in Daten oder
 - d) das Abfangen von Daten
- umfassen, wenn diese Handlungen vom Eigentümer oder einem anderen Rechtsinhaber des Systems oder der Daten oder eines Teils des Systems oder der Daten nicht ordnungsgemäß gestattet wurden oder nach dem Recht der Union oder des betreffenden Mitgliedstaats nicht zulässig sind.
- (4) Zu Cyberangriffen, die eine Bedrohung für die Mitgliedstaaten darstellen, zählen Cyberangriffe auf Informationssysteme, u. a. in den folgenden Bereichen:
- a) kritische Infrastrukturen, einschließlich Seekabel und in den Weltraum gestarteter Gegenstände, die von wesentlicher Bedeutung für die Aufrechterhaltung wichtiger gesellschaftlicher Funktionen oder der Gesundheit, der Sicherheit und des wirtschaftlichen oder sozialen Wohlergehens der Bevölkerung sind;
 - b) Dienstleistungen, die für die Aufrechterhaltung wesentlicher sozialer und/oder wirtschaftlicher Tätigkeiten erforderlich sind, insbesondere in den Sektoren: Energie (Elektrizität, Öl und Gas), Verkehr (Luft, Schiene, Wasser und Straße), Bankenwesen, Finanzmarktinfrastrukturen, Gesundheitswesen (Gesundheitsdienstleister, Krankenhäuser und Privatkliniken), Trinkwasserlieferung und -versorgung oder digitale Infrastruktur und in anderen Sektoren, die für den betreffenden Mitgliedstaat von wesentlicher Bedeutung sind;
 - c) kritische staatliche Funktionen, insbesondere in den Bereichen Verteidigung, Staatsführung und Funktionieren der Institutionen, u. a. im Zusammenhang mit Wahlen oder dem Wahlvorgang, Funktionieren der wirtschaftlichen und der zivilen Infrastruktur, innere Sicherheit sowie Außenbeziehungen, einschließlich mittels diplomatischer Missionen;
 - d) Speicherung oder Verarbeitung von Verschlusssachen oder
 - e) Katastrophenstäbe der Regierungen.
- (5) Zu Cyberangriffen, die eine Bedrohung für die Union darstellen, zählen Cyberangriffe, die gegen ihre Organe, Einrichtungen und sonstigen Stellen, ihre Delegationen in Drittstaaten oder bei internationalen Organisationen, ihre Operationen und Missionen im Bereich der Gemeinsame Sicherheits- und Verteidigungspolitik (GSVP) und ihre Sonderbeauftragten geführt werden.
- (6) Sofern dies für notwendig erachtet wird, um die in den einschlägigen Bestimmungen des Artikels 21 des Vertrags über die Europäische Union festgelegten Ziele der Gemeinsamen Außen- und Sicherheitspolitik (GASP) zu erreichen, können restriktive Maßnahmen gemäß dieser Verordnung auch zur Reaktion auf gegen Drittstaaten oder internationale Organisationen gerichtete Cyberangriffe mit erheblichen Auswirkungen angewandt werden.
- (7) Für die Zwecke dieser Verordnung bezeichnet der Ausdruck
- a) „Informationssysteme“ eine Vorrichtung oder eine Gruppe miteinander verbundener oder zusammenhängender Vorrichtungen, die einzeln oder zu mehreren auf der Grundlage eines Programms die automatische Verarbeitung von digitalen Daten durchführen, sowie die von ihr oder ihnen zum Zwecke des Betriebs, der Nutzung, des Schutzes und der Pflege gespeicherten, verarbeiteten, abgerufenen oder übertragenen digitalen Daten;
 - b) „Eingriff in Informationssysteme“ eine Behinderung oder Störung des Betriebs eines Informationssystems durch Eingeben von digitalen Daten, durch Übermitteln, Beschädigen, Löschen, Beeinträchtigen, Verändern oder Unterdrücken von digitalen Daten oder durch Unzugänglichmachen von digitalen Daten;
 - c) „Eingriff in Daten“ das Löschen, Beschädigen, Beeinträchtigen, Verändern, Unterdrücken oder Unzugänglichmachen von digitalen Daten eines Informationssystems; hierunter fällt auch der Diebstahl von Daten, Geldern, wirtschaftlichen Ressourcen oder geistigem Eigentum;

- d) „Abfangen von Daten“ das mit technischen Hilfsmitteln bewirkte Abfangen nichtöffentlicher digitaler Datenübermittlungen an ein Informationssystem, aus einem Informationssystem oder innerhalb eines Informationssystems, einschließlich elektromagnetischer Abstrahlungen aus einem Informationssystem, das Träger solcher digitaler Daten ist.
- (8) Zusätzlich zu den vorstehenden Begriffsbestimmungen bezeichnet für die Zwecke dieser Verordnung der Ausdruck
- a) „Anspruch“ jede vor oder nach Inkrafttreten dieser Verordnung erhobene Forderung, die mit der Durchführung eines Vertrags oder einer Transaktion im Zusammenhang steht, unabhängig davon, ob sie gerichtlich geltend gemacht wird oder wurde, und umfasst insbesondere
- i) Ansprüche auf Erfüllung einer Verpflichtung aus oder in Verbindung mit einem Vertrag oder einer Transaktion,
 - ii) Ansprüche auf Verlängerung oder Zahlung einer finanziellen Garantie oder Gegengarantie in jeder Form,
 - iii) Ansprüche auf Schadensersatz in Verbindung mit einem Vertrag oder einer Transaktion,
 - iv) Gegenansprüche,
 - v) Ansprüche auf Anerkennung oder Vollstreckung – auch im Wege der Zwangsvollstreckung – von Gerichtsurteilen, Schiedssprüchen oder gleichwertigen Entscheidungen, ungeachtet des Ortes, an dem sie ergangen sind;
- b) „Vertrag oder Transaktion“ jede Transaktion, ungeachtet der Form und des anwendbaren Rechts, bei dem dieselben oder verschiedene Parteien einen oder mehrere Verträge abschließen oder vergleichbare Verpflichtungen eingehen; als „Vertrag“ gelten auch alle Garantien, insbesondere finanzielle Garantien und Gegengarantien, sowie Kredite, rechtlich unabhängig oder nicht, ebenso alle Nebenvereinbarungen, die auf einem solchen Geschäft beruhen oder mit diesem im Zusammenhang stehen;
- c) „zuständige Behörden“ die auf den in Anhang II aufgeführten Internetseiten angegebenen zuständigen Behörden der Mitgliedstaaten;
- d) „wirtschaftliche Ressourcen“ Vermögenswerte jeder Art, unabhängig davon, ob sie materiell oder immateriell, beweglich oder unbeweglich sind, bei denen es sich nicht um Gelder handelt, die aber für den Erwerb von Geldern, Waren oder Dienstleistungen verwendet werden können;
- e) „Einfrieren von wirtschaftlichen Ressourcen“ die Verhinderung jeder Art von Verwendung wirtschaftlicher Ressourcen für den Erwerb von Geldern, Waren oder Dienstleistungen, die auch den Verkauf, das Vermieten oder das Verpfänden dieser Ressourcen einschließt, sich aber nicht darauf beschränkt;
- f) „Einfrieren von Geldern“ die Verhinderung jeglicher Form der Bewegung, des Transfers, der Veränderung und der Verwendung von Geldern sowie des Zugangs zu ihnen oder ihres Einsatzes, wodurch das Volumen, die Höhe, die Belegenheit, das Eigentum, der Besitz, die Eigenschaften oder die Zweckbestimmung der Gelder verändert oder jegliche sonstigen Veränderungen bewirkt werden, die eine Nutzung der Gelder einschließlich der Vermögensverwaltung ermöglichen;
- g) „Gelder“ finanzielle Vermögenswerte und Vorteile jeder Art, die Folgendes einschließen, aber nicht darauf beschränkt sind:
- i) Bargeld, Schecks, Geldforderungen, Wechsel, Zahlungsanweisungen und andere Zahlungsmittel,
 - ii) Einlagen bei Finanzinstituten oder anderen Einrichtungen, Guthaben auf Konten, Zahlungsansprüche und verbriefte Forderungen,
 - iii) öffentlich und privat gehandelte Wertpapiere und Schuldtitel einschließlich Aktien und Anteilen, Wertpapierzertifikate, Obligationen, Schuldscheine, Optionsscheine, Pfandbriefe und Derivate,
 - iv) Zinserträge, Dividenden oder andere Einkünfte oder Wertzuwächse aus Vermögenswerten,
 - v) Kredite, Rechte auf Verrechnung, Bürgschaften, Vertragserfüllungsgarantien und andere finanzielle Ansprüche,
 - vi) Akkreditive, Konnossemente und Übereignungsurkunden sowie
 - vii) Dokumente zur Verbriefung von Anteilen an Fondsvermögen oder anderen Finanzressourcen;
- h) „Gebiet der Union“ die Hoheitsgebiete der Mitgliedstaaten, in denen der Vertrag Anwendung findet, nach Maßgabe der im Vertrag festgelegten Bedingungen, einschließlich ihres Luftraums.

Artikel 2

Zu den Faktoren, anhand deren festgestellt wird, ob ein Cyberangriff erhebliche Auswirkungen im Sinne von Artikel 1 Absatz 1 hat, gehören die folgenden:

- a) Umfang, Ausmaß, Wirkung oder Schwere der verursachten Störung, einschließlich für wirtschaftliche und gesellschaftliche Tätigkeiten, wesentliche Dienste, kritische staatliche Funktionen, die öffentliche Ordnung oder die öffentliche Sicherheit;
- b) die Zahl der betroffenen natürlichen oder juristischen Personen, Organisationen oder Einrichtungen;
- c) die Zahl der betroffenen Mitgliedstaaten;
- d) die Höhe des wirtschaftlichen Schadens, der z. B. durch einen groß angelegten Diebstahl von Geldern, wirtschaftlichen Ressourcen oder geistigem Eigentum verursacht wurde;
- e) der vom Täter für sich selbst oder für andere erlangte wirtschaftliche Nutzen;
- f) die Menge oder Art der gestohlenen Daten oder das Ausmaß der Datenschutzverstöße oder
- g) die Art der wirtschaftlich sensiblen Daten, auf die zugegriffen wurde.

Artikel 3

- (1) Sämtliche Gelder und wirtschaftlichen Ressourcen, die Eigentum oder Besitz der in Anhang I aufgeführten natürlichen oder juristischen Personen, Organisationen oder Einrichtungen sind oder von diesen gehalten oder kontrolliert werden, werden eingefroren.
- (2) Den in Anhang I aufgeführten natürlichen oder juristischen Personen, Organisationen oder Einrichtungen dürfen weder unmittelbar noch mittelbar Gelder oder wirtschaftliche Ressourcen zur Verfügung gestellt werden oder zugutekommen.
- (3) Anhang I enthält auf der Grundlage von Feststellungen durch den Rat gemäß Artikel 5 Absatz 1 des Beschlusses (GASP) 2019/797 eine Liste
 - a) der natürlichen oder juristischen Personen, Organisationen oder Einrichtungen, die für Cyberangriffe oder versuchte Cyberangriffe verantwortlich sind,
 - b) der natürlichen oder juristischen Personen, Organisationen oder Einrichtungen, die finanzielle, technische oder materielle Unterstützung für Cyberangriffe oder versuchte Cyberangriffe leisten oder auf andere Weise, einschließlich durch Planung, Vorbereitung, Mitwirkung, Steuerung, Unterstützung oder Ermutigung, daran beteiligt sind oder sie durch Handlung oder Unterlassung erleichtern,
 - c) der natürlichen oder juristischen Personen, Organisationen oder Einrichtungen, die mit den unter den Buchstaben a und b genannten natürlichen oder juristischen Personen, Organisationen und Einrichtungen in Verbindung stehen.

Artikel 4

- (1) Abweichend von Artikel 3 können die zuständigen Behörden der Mitgliedstaaten die Freigabe bestimmter eingefrorener Gelder oder wirtschaftlicher Ressourcen oder die Zurverfügungstellung bestimmter Gelder oder wirtschaftlicher Ressourcen unter ihnen geeignet erscheinenden Bedingungen genehmigen, nachdem festgestellt wurde, dass die betreffenden Gelder oder wirtschaftlichen Ressourcen
 - a) zur Befriedigung der Grundbedürfnisse der in Anhang I genannten natürlichen Personen oder juristischen Personen, Organisationen oder Einrichtungen sowie von unterhaltsberechtigten Familienangehörigen jener natürlichen Personen, unter anderem für die Bezahlung von Nahrungsmitteln, Mieten oder Hypotheken, Medikamenten und medizinischer Behandlung, Steuern, Versicherungsprämien und Gebühren öffentlicher Versorgungseinrichtungen, erforderlich sind;
 - b) ausschließlich der Bezahlung angemessener Honorare oder der Rückerstattung von Ausgaben im Zusammenhang mit der Bereitstellung rechtlicher Dienste dienen;
 - c) ausschließlich der Bezahlung von Gebühren oder Kosten für die routinemäßige Verwahrung oder Verwaltung eingefrorener Gelder oder wirtschaftlicher Ressourcen dienen;
 - d) für die Deckung außerordentlicher Ausgaben erforderlich sind, vorausgesetzt, dass die relevante zuständige Behörde den zuständigen Behörden der anderen Mitgliedstaaten und der Kommission mindestens zwei Wochen vor Erteilung der Genehmigung mitgeteilt hat, aus welchen Gründen sie der Auffassung ist, dass eine spezifische Genehmigung erteilt werden sollte; oder
 - e) auf Konten oder von Konten einer diplomatischen Vertretung oder einer Konsularstelle oder einer internationalen Organisation überwiesen werden sollen, die Immunität nach dem Völkerrecht genießt, sofern diese Zahlungen für amtliche Zwecke dieser diplomatischen Vertretung oder Konsularstelle oder internationalen Organisation bestimmt sind.
- (2) Der betreffende Mitgliedstaat unterrichtet die anderen Mitgliedstaaten und die Kommission innerhalb von zwei Wochen über jede nach Absatz 1 erteilte Genehmigung.

Artikel 4a

- (1) Artikel 3 Absätze 1 und 2 findet keine Anwendung auf die Bereitstellung von Geldern oder wirtschaftlichen Ressourcen, die notwendig sind, um die rasche Bereitstellung humanitärer Hilfe zu gewährleisten oder andere Tätigkeiten zur Deckung grundlegender menschlicher Bedürfnisse zu unterstützen, wenn die Hilfe bzw. die anderen Tätigkeiten durchgeführt werden von
- a) den Vereinten Nationen (VN), einschließlich ihrer Programme, Gelder und sonstigen Einrichtungen und Stellen, sowie ihren Sonderorganisationen und verwandten Organisationen,
 - b) internationalen Organisationen,
 - c) humanitäre Hilfe leistenden Organisationen mit Beobachterstatus in der Generalversammlung der VN und Mitgliedern dieser Organisationen,
 - d) bilateral oder multilateral finanzierten nichtstaatlichen Organisationen, die sich an den Plänen der VN für humanitäre Maßnahmen, den Plänen der VN für Flüchtlingshilfemaßnahmen oder anderen Appellen der VN oder an vom Amt der VN für die Koordinierung humanitärer Angelegenheiten koordinierten humanitären ‚Clustern‘ beteiligen,
 - e) Organisationen und Agenturen, denen die Union das Zertifikat für humanitäre Partnerschaft erteilt hat oder die von einem Mitgliedstaat als Partner für humanitäre Hilfe nach nationalen Verfahren zertifiziert oder anerkannt sind,
 - f) spezialisierten Agenturen der Mitgliedstaaten oder
 - g) den Beschäftigten, Zuschussempfängern, Tochtergesellschaften oder Durchführungspartnern der unter den Buchstaben a bis f genannten Einrichtungen, während und soweit sie in dieser Eigenschaft tätig sind.
- (2) Unbeschadet des Absatzes 1 können die zuständigen Behörden der Mitgliedstaaten abweichend von Artikel 3 Absätze 1 und 2 unter ihnen geeignet erscheinenden Bedingungen die Freigabe bestimmter eingefrorener Gelder oder wirtschaftlicher Ressourcen oder die Bereitstellung bestimmter Gelder oder wirtschaftlicher Ressourcen genehmigen, nachdem sie festgestellt haben, dass die Zurverfügungstellung dieser Gelder oder wirtschaftlichen Ressourcen erforderlich ist, um die rasche Bereitstellung humanitärer Hilfe zu gewährleisten oder andere Tätigkeiten zur Deckung grundlegender menschlicher Bedürfnisse zu unterstützen.
- (3) Ergeht innerhalb von fünf Arbeitstagen nach Eingang eines Genehmigungsantrags nach Absatz 2 keine ablehnende Entscheidung, kein Auskunftersuchen oder keine Mitteilung über eine Fristverlängerung der einschlägigen zuständigen Behörde, so gilt die Genehmigung als erteilt.
- (4) Der betreffende Mitgliedstaat unterrichtet die anderen Mitgliedstaaten und die Kommission über jede nach den Absätzen 2 und 3 erteilte Genehmigung innerhalb von vier Wochen nach einer solchen Erteilung.

Artikel 5

- (1) Abweichend von Artikel 3 Absatz 1 können die zuständigen Behörden der Mitgliedstaaten die Freigabe bestimmter eingefrorener Gelder oder wirtschaftlicher Ressourcen genehmigen, wenn die nachstehenden Voraussetzungen erfüllt sind:
- a) Die Gelder oder wirtschaftlichen Ressourcen sind Gegenstand einer schiedsgerichtlichen Entscheidung, die vor dem Datum ergangen ist, an dem die in Artikel 3 genannte natürliche oder juristische Person, Organisation oder Einrichtung in Anhang I aufgenommen wurde, oder Gegenstand einer vor oder nach diesem Datum in der Union ergangenen gerichtlichen oder behördlichen Entscheidung oder einer in dem betreffenden Mitgliedstaat vollstreckbaren gerichtlichen Entscheidung;
 - b) die Gelder oder wirtschaftlichen Ressourcen werden im Rahmen der anwendbaren Gesetze und sonstigen Rechtsvorschriften über die Rechte des Gläubigers ausschließlich zur Erfüllung der Forderungen verwendet, die durch eine solche Entscheidung gesichert sind oder deren Bestehen in einer solchen Entscheidung bestätigt worden ist;
 - c) die Entscheidung begünstigt nicht einer in Anhang I aufgeführten natürlichen oder juristischen Person, Organisation oder Einrichtung; und
 - d) die Anerkennung der Entscheidung steht nicht im Widerspruch zur öffentlichen Ordnung des betreffenden Mitgliedstaats.
- (2) Der betreffende Mitgliedstaat unterrichtet die anderen Mitgliedstaaten und die Kommission innerhalb von zwei Wochen über jede nach Absatz 1 erteilte Genehmigung.

Artikel 6

- (1) Abweichend von Artikel 3 Absatz 1 und vorausgesetzt, dass eine Zahlung von einer in Anhang I aufgeführten natürlichen oder juristischen Person, Organisation oder Einrichtung Zahlungen aufgrund eines Vertrags, einer Vereinbarung oder einer Verpflichtung zu leisten ist, der/die vor dem Datum geschlossen bzw. eingegangen wurde, an dem jene natürliche oder juristische Person, Organisation oder Einrichtung in Anhang I

aufgenommen wurde, können die zuständigen Behörden der Mitgliedstaaten die Freigabe bestimmter eingefrorener Gelder oder wirtschaftlicher Ressourcen unter ihnen geeignet erscheinenden Bedingungen genehmigen, wenn die betreffende zuständige Behörde festgestellt hat, dass

- a) die Gelder oder wirtschaftlichen Ressourcen für eine Zahlung von einer in Anhang I aufgeführten natürlichen oder juristischen Person, Organisation oder Einrichtung verwendet werden sollen und
 - b) die Zahlung nicht gegen Artikel 3 Absatz 2 verstößt.
- (2) Der betreffende Mitgliedstaat unterrichtet die anderen Mitgliedstaaten und die Kommission innerhalb von zwei Wochen über jede nach Absatz 1 erteilte Genehmigung.

Artikel 7

- (1) Artikel 3 Absatz 2 hindert Finanz- und Kreditinstitute nicht daran, Gelder, die von Dritten auf das Konto einer in der Liste geführten natürlichen oder juristischen Person, Einrichtung oder Organisation überwiesen werden, auf den eingefrorenen Konten gutzuschreiben, sofern die auf diesen Konten gutgeschriebenen Beträge ebenfalls eingefroren werden. Die Finanz- oder Kreditinstitute setzen unverzüglich die einschlägige zuständige Behörde von solchen Transaktionen in Kenntnis.
- (2) Artikel 3 Absatz 2 gilt nicht für die auf eingefrorenen Konten eingehenden
- a) Zinsen und sonstigen Erträge dieser Konten,
 - b) Zahlungen aufgrund von Verträgen, Vereinbarungen oder Verpflichtungen, die vor dem Datum, an dem die in Artikel 3 Absatz 1 genannte natürliche oder juristische Person, Organisation oder Einrichtung in Anhang I aufgenommen wurde, geschlossen wurden bzw. entstanden sind, oder
 - c) Zahlungen aufgrund von in einem Mitgliedstaat ergangenen oder in dem betreffenden Mitgliedstaat vollstreckbaren gerichtlichen, behördlichen oder schiedsgerichtlichen Entscheidungen,
- sofern diese Zinsen, sonstigen Erträge und Zahlungen weiterhin den Maßnahmen nach Artikel 3 Absatz 1 unterliegen.

Artikel 8

- (1) Unbeschadet der geltenden Vorschriften über die Anzeigepflicht, die Vertraulichkeit und das Berufsgeheimnis müssen natürliche und juristische Personen, Organisationen und Einrichtungen
- a) Informationen, die die Anwendung dieser Verordnung erleichtern, wie etwa Informationen über die nach Artikel 3 Absatz 1 eingefrorenen Konten und Beträge, unverzüglich der zuständigen Behörde des Mitgliedstaats, in dem sie ihren Sitz bzw. Wohnsitz haben, und – direkt oder über den Mitgliedstaat – der Kommission übermitteln und
 - b) mit der zuständigen Behörde bei der Überprüfung dieser Informationen gemäß Buchstabe a zusammenarbeiten.
- (2) Zusätzliche Informationen, die direkt bei der Kommission eingehen, werden den Mitgliedstaaten zur Verfügung gestellt.
- (3) Die gemäß diesem Artikel übermittelten oder erhaltenen Angaben dürfen nur für die Zwecke verwendet werden, für die sie übermittelt oder entgegengenommen wurden.

Artikel 9

Es ist verboten, wissentlich und vorsätzlich an Tätigkeiten teilzunehmen, mit denen die Umgehung der Maßnahmen nach Artikel 3 bezweckt oder bewirkt wird.

Artikel 10

- (1) Natürliche und juristische Personen, Organisationen und Einrichtungen sowie ihre Führungskräfte und Beschäftigten, die im guten Glauben, im Einklang mit dieser Verordnung zu handeln, Gelder oder wirtschaftliche Ressourcen einfrieren oder ihre Zurverfügungstellung ablehnen, können hierfür nicht haftbar gemacht werden, es sei denn, es ist nachgewiesen, dass das Einfrieren oder das Zurückhalten der Gelder oder wirtschaftlichen Ressourcen auf Fahrlässigkeit beruht.
- (2) Natürliche oder juristische Personen, Organisationen oder Einrichtungen können für ihre Handlungen nicht haftbar gemacht werden, wenn sie nicht wussten und vernünftigerweise nicht wissen konnten, dass sie mit ihrem Handeln gegen die in dieser Verordnung festgelegten Maßnahmen verstoßen würden.

Artikel 11

- (1) Ansprüche im Zusammenhang mit Verträgen oder Transaktionen, deren Erfüllung bzw. Durchführung von den mit dieser Verordnung verhängten Maßnahmen unmittelbar oder mittelbar, ganz oder teilweise betroffen ist, einschließlich Schadensersatzansprüchen und sonstigen derartigen Ansprüchen, wie etwa Entschädigungsansprüche oder Garantieansprüche, vor allem Ansprüche auf Verlängerung oder Zahlung einer insbesondere finanziellen Garantie oder Gegengarantie in jeglicher Form, werden nicht erfüllt, sofern sie geltend gemacht werden von
 - a) den benannten, in Anhang I aufgeführten natürlichen oder juristischen Personen, Organisationen oder Einrichtungen,
 - b) natürlichen oder juristischen Personen, Organisationen oder Einrichtungen, die über eine der unter Buchstabe a genannten natürlichen oder juristischen Personen, Organisationen oder Einrichtungen oder in deren Namen handeln.
- (2) In Verfahren zur Durchsetzung eines Anspruchs trägt die natürliche oder juristische Person, Organisation oder Einrichtung, die den Anspruch geltend macht, die Beweislast dafür, dass die Erfüllung des Anspruchs nicht nach Absatz 1 verboten ist.
- (3) Dieser Artikel berührt nicht das Recht der in Absatz 1 genannten natürlichen oder juristischen Personen, Organisationen und Einrichtungen auf gerichtliche Überprüfung der Rechtmäßigkeit der Nichterfüllung vertraglicher Pflichten nach dieser Verordnung.

Artikel 12

- (1) Die Kommission und die Mitgliedstaaten informieren sich untereinander über die nach dieser Verordnung getroffenen Maßnahmen und übermitteln einander ihnen im Zusammenhang mit dieser Verordnung vorliegende sonstige sachdienliche Informationen, insbesondere in Bezug auf
 - a) gemäß Artikel 3 eingefrorene Gelder und gemäß den Artikeln 4, 5 und 6 erteilte Genehmigungen,
 - b) Verstöße, Vollzugsprobleme und Urteile einzelstaatlicher Gerichte.
- (2) Die Mitgliedstaaten übermitteln einander und der Kommission unverzüglich ihnen vorliegende sonstige sachdienliche Informationen, die die wirksame Anwendung dieser Verordnung berühren könnten.

Artikel 13

- (1) Beschließt der Rat, eine natürliche oder juristische Person, Organisation oder Einrichtung den in Artikel 3 genannten Maßnahmen zu unterwerfen, so ändert er Anhang I entsprechend.
- (2) Der Rat setzt die betreffende natürliche oder juristische Person, Organisation oder Einrichtung entweder auf direktem Weg, falls ihre Anschrift bekannt ist, oder durch die Veröffentlichung einer Bekanntmachung von dem Beschluss nach Absatz 1 und den Gründen für die Aufnahme in die Liste in Kenntnis und gibt dieser natürlichen oder juristischen Person, Organisation oder Einrichtung Gelegenheit zur Stellungnahme.
- (3) Wird eine Stellungnahme unterbreitet oder werden stichhaltige neue Beweise vorgelegt, so überprüft der Rat seinen Beschluss nach Absatz 1 und unterrichtet die betreffende natürliche oder juristische Person, Organisation oder Einrichtung entsprechend.
- (4) Die Liste in Anhang I wird regelmäßig, mindestens jedoch alle 12 Monate, überprüft.
- (5) Die Kommission wird ermächtigt, Anhang II auf der Grundlage der durch die Mitgliedstaaten übermittelten Informationen zu ändern.

Artikel 14

- (1) In Anhang I werden die Gründe für die Aufnahme der betreffenden natürlichen und juristischen Personen, Organisationen und Einrichtungen in die Liste angegeben.
- (2) Anhang I enthält die zur Identifizierung der betreffenden natürlichen oder juristischen Personen, Organisationen oder Einrichtungen erforderlichen Angaben, soweit diese verfügbar sind. Bei natürlichen Personen können diese Angaben Namen und Aliasnamen, Geburtsdatum und -ort, Staatsangehörigkeit, Reisepass- und Personalausweisnummern, Geschlecht, Anschrift, soweit bekannt, und Funktion oder Beruf umfassen. Bei juristischen Personen, Organisationen oder Einrichtungen können diese Angaben Namen, Ort und Datum der Registrierung, Registriernummer und Geschäftssitz umfassen.

Artikel 15

- (1) Die Mitgliedstaaten legen fest, welche Sanktionen bei Verstößen gegen Bestimmungen dieser Verordnung zu verhängen sind, und treffen die zu ihrer Durchsetzung erforderlichen Maßnahmen. Die vorgesehenen Sanktionen müssen wirksam, verhältnismäßig und abschreckend sein.

- (2) Die Mitgliedstaaten teilen der Kommission die in Absatz 1 genannten Bestimmungen unverzüglich nach Inkrafttreten dieser Verordnung mit und melden ihr alle Änderungen dieser Bestimmungen.

Artikel 16

- (1) Die Kommission verarbeitet personenbezogene Daten, um ihre Aufgaben nach dieser Verordnung zu erfüllen. Zu diesen Aufgaben gehören
- a) die Aufnahme des Inhalts von Anhang I in die elektronisch verfügbare konsolidierte Liste der Personen, Gruppen und Organisationen, die finanziellen Sanktionen der Union unterliegen, und in die interaktive Weltkarte der Sanktionen, die beide öffentlich zugänglich sind;
 - b) die Verarbeitung von Informationen über die Auswirkungen der in dieser Verordnung vorgesehenen Maßnahmen, z. B. Wert der eingefrorenen Gelder, und von Informationen über die von den zuständigen Behörden erteilten Genehmigungen.
- (2) Für die Zwecke dieser Verordnung wird die in Anhang II angegebene Dienststelle der Kommission zu dem „für die Verarbeitung Verantwortlichen“ der Kommission im Sinne von Artikel 3 Absatz 8 der Verordnung (EU) 2018/1725 bestimmt, um sicherzustellen, dass die betreffenden natürlichen Personen ihre Rechte nach jener Verordnung ausüben können.

Artikel 17

- (1) Die Mitgliedstaaten benennen die in dieser Verordnung genannten zuständigen Behörden und geben sie auf den Websites in Anhang II an. Die Mitgliedstaaten notifizieren der Kommission jede Änderung der Adressen ihrer Websites in Anhang II.
- (2) Die Mitgliedstaaten teilen der Kommission ihre zuständigen Behörden, einschließlich der Kontaktdaten, unverzüglich nach Inkrafttreten dieser Verordnung mit und informieren sie über spätere Änderungen.
- (3) Soweit diese Verordnung eine Mitteilungs-, Informations- oder sonstige Kommunikationspflicht gegenüber der Kommission vorsieht, werden dazu die Anschrift und die anderen Kontaktdaten verwendet, die in Anhang II angegeben sind.

Artikel 18

Diese Verordnung gilt

- a) im Gebiet der Union einschließlich ihres Luftraums,
- b) an Bord der Luftfahrzeuge und Schiffe, die der Hoheitsgewalt der Mitgliedstaaten unterstehen,
- c) für natürliche Personen, die die Staatsangehörigkeit eines Mitgliedstaats besitzen, innerhalb und außerhalb des Gebiets der Union,
- d) für alle nach dem Recht eines Mitgliedstaats gegründeten oder eingetragenen juristischen Personen, Organisationen und Einrichtungen innerhalb und außerhalb des Gebiets der Union,
- e) für juristische Personen, Organisationen und Einrichtungen in Bezug auf Geschäfte, die ganz oder teilweise in der Union getätigt werden.

Artikel 19

Diese Verordnung tritt am Tag nach ihrer Veröffentlichung im *Amtsblatt der Europäischen Union* in Kraft.

Diese Verordnung ist in allen ihren Teilen verbindlich und gilt unmittelbar in jedem Mitgliedstaat.

Geschehen zu Brüssel am 17. Mai 2019.

Im Namen des Rates
Der Präsident
E.O. TEODOROVICI

(¹) ABI. L 129 I vom 17.5.2019, S. 1.

(²) ABI. L, 2025/886, 13.5.2025.

⁽¹⁾ Siehe Seite 13 dieses Amtsblatts.

⁽²⁾ Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz- Grundverordnung) (ABl. L 119 vom 4.5.2016, S. 1).

⁽³⁾ Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates vom 23. Oktober 2018 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe, Einrichtungen und sonstigen Stellen der Union, zum freien Datenverkehr und zur Aufhebung der Verordnung (EG) Nr. 45/2001 und des Beschlusses Nr. 1247/2002/EG (ABl. L 295 vom 21.11.2018, S. 39).

ANHANG I

Liste der natürlichen und juristischen Personen, Organisationen und Einrichtungen gemäß Artikel 3

A. Natürliche Personen

	Name	Angaben zur Identität	Gründe	Datum der Aufnahme in die Liste
1.	GAO Qiang	<p>Geburtsdatum: 4. Oktober 1983</p> <p>Geburtsort: Provinz Shandong, China</p> <p>Anschrift: Room 1102, Guanfu Mansion, 46 Xinkai Road, Hedong District, Tianjin, China</p> <p>Staatsangehörigkeit: chinesisch</p> <p>Geschlecht: männlich</p>	<p>Gao Qiang ist an ‚Operation Cloud Hopper‘ beteiligt, einer Reihe von Cyberangriffen mit erheblichen Auswirkungen, die von außerhalb der Union verübt werden und eine externe Bedrohung für die Union oder ihre Mitgliedstaaten darstellen, und von Cyberangriffen mit erheblichen Auswirkungen auf Drittstaaten.</p> <p>Mit ‚Operation Cloud Hopper‘ wurden Informationssysteme multinationaler Unternehmen auf sechs Kontinenten angegriffen, darunter Unternehmen mit Sitz in der Union, und unbefugt auf sensible Geschäftsdaten zugegriffen, was zu erheblichen wirtschaftlichen Verlusten geführt hat.</p> <p>‚Operation Cloud Hopper‘ wurde von dem als ‚APT10‘ (‚Advanced Persistent Threat 10‘) (alias ‚Red Apollo‘, ‚CVNX‘, ‚Stone Panda‘, ‚MenuPass‘ und ‚Potassium‘) bekannten Täter verübt.</p> <p>Gao Qiang kann mit APT10 in Verbindung gebracht werden, auch aufgrund seiner Verbindungen zur Führungs- und Kontrollinfrastruktur von APT10.</p> <p>Überdies ist er bei Huaying Haitai beschäftigt, einer Organisation, die benannt wurde, weil sie ‚Operation Cloud Hopper‘ unterstützt und ermöglicht. Er unterhält Verbindungen zu Zhang Shilong, der auch im Zusammenhang mit ‚Operation Cloud Hopper‘ benannt wurde. Gao Qiang steht somit sowohl mit Huaying Haitai als auch mit Zhang Shilong in Verbindung.</p>	30.7.2020
2.	ZHANG Shilong	<p>Geburtsdatum: 10. September 1981</p> <p>Geburtsort: China</p> <p>Anschrift: Hedong, Yuyang Road No 121, Tianjin, China</p> <p>Staatsangehörigkeit: chinesisch</p> <p>Geschlecht: männlich</p>	<p>Zhang Shilong ist an ‚Operation Cloud Hopper‘ beteiligt, einer Reihe von Cyberangriffen mit erheblichen Auswirkungen, die von außerhalb der Union verübt werden und eine externe Bedrohung für die Union oder ihre Mitgliedstaaten darstellen, und von Cyberangriffen mit erheblichen Auswirkungen auf Drittstaaten.</p> <p>Mit ‚Operation Cloud Hopper‘ wurden Informationssysteme multinationaler Unternehmen auf sechs Kontinenten angegriffen, darunter Unternehmen mit Sitz in der Union, und unbefugt auf sensible Geschäftsdaten zugegriffen, was zu erheblichen wirtschaftlichen Verlusten geführt hat.</p>	30.7.2020

			<p>„Operation Cloud Hopper“ wurde von dem als „APT10“ („Advanced Persistent Threat 10“) (alias „Red Apollo“, „CVNX“, „Stone Panda“, „MenuPass“ und „Potassium“) bekannten Täter verübt.</p> <p>Zhang Shilong kann mit APT10 in Verbindung gebracht werden, auch über die Schadsoftware, die er im Zusammenhang mit den Cyberangriffen von APT10 entwickelt und getestet hat. Überdies ist er bei Huaying Haitai beschäftigt, einer Organisation, die benannt wurde, weil sie „Operation Cloud Hopper“ unterstützt und ermöglicht. Er unterhält Verbindungen zu Gao Qiang, der auch im Zusammenhang mit „Operation Cloud Hopper“ benannt wurde. Zhang Shilong steht somit sowohl mit Huaying Haitai als auch mit Gao Qiang in Verbindung.</p>	
3.	Alexey Valeryevich MININ	<p>Алексей Валерьевич МИНИН</p> <p>Geburtsdatum: 27.5.1972</p> <p>Geburtsort: Oblast Perm, Russische SFSR (jetzt Russische Föderation)</p> <p>Reisepass-Nr.: 120017582 ausgestellt vom Außenministerium der Russischen Föderation gültig vom 17.4.2017 bis zum 17.4.2022</p> <p>Ort: Moskau, Russische Föderation</p> <p>Staatsangehörigkeit: russisch</p> <p>Geschlecht: männlich</p>	<p>Alexey Minin hat an einem versuchten Cyberangriff auf die Organisation für das Verbot chemischer Waffen (OVCW) in den Niederlanden mit potenziell erheblichen Auswirkungen sowie an Cyberangriffen mit erheblichen Auswirkungen auf Drittstaaten teilgenommen.</p> <p>Als für „human intelligence“ (Aufklärung mit menschlichen Quellen) zuständiger Mitarbeiter der Hauptdirektion des Generalstabs der Streitkräfte der Russischen Föderation (GU/GRU) gehörte Alexey Minin einem Team von vier Beamten des russischen Militärgeheimdienstes an, die im April 2018 versuchten, sich unbefugten Zugang zum WiFi-Netz der OVCW in Den Haag (Niederlande) zu verschaffen. Der versuchte Cyberangriff hatte zum Ziel, in das WiFi-Netz der OVCW einzudringen, was bei Erfolg die Sicherheit des Netzes und die laufenden Untersuchungen der OVCW gefährdet hätte. Der niederländische militärische Nachrichten- und Sicherheitsdienst (Militaire Inlichtingen- en Veiligheidsdienst) hat den versuchten Cyberangriff abgewehrt und damit die OVCW vor einem schweren Schaden bewahrt.</p> <p>Eine Grand Jury des Western District of Pennsylvania (Vereinigte Staaten von Amerika) hat Alexey Minin als Beamter der GRU wegen Computerhackings, Telekommunikationsbetrugs, schweren Identitätsdiebstahls und Geldwäsche angeklagt.</p> <p>Die GRU führt weiterhin aktiv Cyberangriffe gegen die Union oder ihre Mitgliedstaaten durch. Als Mitglied der GRU ist Alexey Minin daher an Cyberangriffen mit erheblichen Auswirkungen beteiligt, einschließlich versuchter Cyberangriffe mit potenziell erheblichen Auswirkungen, die eine</p>	30.7.2020

			externe Bedrohung für die Union oder ihre Mitgliedstaaten darstellen.	
4.	Aleksei Sergeyvich MORENETS	<p>Алексей Сергеевич МОРЕНЕЦ</p> <p>Geburtsdatum: 31.7.1977</p> <p>Geburtsort: Oblast Murmansk, Russische SFSR (jetzt Russische Föderation)</p> <p>Reisepass-Nr.: 100135556 ausgestellt vom Außenministerium der Russischen Föderation gültig vom 17.4.2017 bis zum 17.4.2022</p> <p>Ort: Moskau, Russische Föderation</p> <p>Staatsangehörigkeit: russisch</p> <p>Geschlecht: männlich</p>	<p>Aleksei Morenets hat an einem versuchten Cyberangriff auf die Organisation für das Verbot chemischer Waffen (OVCW) in den Niederlanden mit potenziell erheblichen Auswirkungen sowie an Cyberangriffen mit erheblichen Auswirkungen auf Drittstaaten teilgenommen.</p> <p>Als Cyber-Operator der Hauptdirektion des Generalstabs der Streitkräfte der Russischen Föderation (GU/GRU) gehörte Aleksei Morenets einem Team von vier Beamten des russischen Militärgeheimdienstes an, die im April 2018 versuchten, sich unbefugt Zugang zum WiFi-Netz der OVCW in Den Haag (Niederlande) zu verschaffen. Der versuchte Cyberangriff hatte zum Ziel, in das WiFi-Netz der OVCW einzudringen, was bei Erfolg die Sicherheit des Netzes und die laufenden Untersuchungen der OVCW gefährdet hätte. Der niederländische militärische Nachrichten- und Sicherheitsdienst (Militaire Inlichtingen- en Veiligheidsdienst) hat den versuchten Cyberangriff abgewehrt und damit die OVCW vor einem schweren Schaden bewahrt.</p> <p>Eine Grand Jury des Western District of Pennsylvania (Vereinigte Staaten von Amerika) hat Aleksei Morenets, der der Militäreinheit 26165 zugewiesen ist, wegen Computerhackings, Telekommunikationsbetrugs, schweren Identitätsdiebstahls und Geldwäsche angeklagt.</p> <p>Die GRU führt weiterhin aktiv Cyberangriffe gegen die Union oder ihre Mitgliedstaaten durch. Als Mitglied der GRU ist Aleksei Morenets daher an Cyberangriffen mit erheblichen Auswirkungen beteiligt, einschließlich versuchter Cyberangriffe mit potenziell erheblichen Auswirkungen, die eine externe Bedrohung für die Union oder ihre Mitgliedstaaten darstellen.</p>	30.7.2020
5.	Evgenii Mikhaylovich SEREBRIAKOV	<p>Евгений Михайлович СЕРЕБРЯКОВ</p> <p>Geburtsdatum: 26.7.1981</p> <p>Geburtsort: Kursk, Russische SFSR (jetzt Russische Föderation)</p> <p>Reisepass-Nr.: 100135555 ausgestellt vom Außenministerium der Russischen Föderation gültig vom 17.4.2017</p>	<p>Evgenii Serebriakov hat an einem versuchten Cyberangriff auf die Organisation für das Verbot chemischer Waffen (OVCW) in den Niederlanden mit potenziell erheblichen Auswirkungen sowie an Cyberangriffen mit erheblichen Auswirkungen auf Drittstaaten teilgenommen.</p> <p>Als Cyber-Operator der Hauptdirektion des Generalstabs der Streitkräfte der Russischen Föderation (GU/GRU) gehörte Evgenii Serebriakov einem Team von vier Beamten des russischen Militärgeheimdienstes an, die im April 2018 versuchten, sich unbefugt Zugang zum WiFi-Netz der OVCW in Den Haag (Niederlande) zu</p>	30.7.2020

		<p>bis zum 17.4.2022</p> <p>Ort: Moskau, Russische Föderation</p> <p>Staatsangehörigkeit: russisch</p> <p>Geschlecht: männlich</p>	<p>verschaffen. Der versuchte Cyberangriff hatte zum Ziel, in das WiFi-Netz der OVCW einzudringen, was bei Erfolg die Sicherheit des Netzes und die laufenden Untersuchungen der OVCW gefährdet hätte. Der niederländische militärische Nachrichten- und Sicherheitsdienst (Militaire Inlichtingen- en Veiligheidsdienst) hat den versuchten Cyberangriff abgewehrt und damit die OVCW vor einem schweren Schaden bewahrt.</p> <p>Seit Frühjahr 2022 ist Evgenii Serebriakov Anführer von ‚Sandworm‘ (alias ‚Sandworm Team‘, ‚BlackEnergy Group‘, ‚Voodoo Bear‘, ‚Quedagh‘, ‚Olympic Destroyer‘ und ‚Telebots‘), einer Täter- und Hackergruppe, die mit der Einheit 74455 der Hauptdirektion des russischen Militärgeheimdienstes in Verbindung steht. Sandworm hat im Zuge des Angriffskriegs Russlands gegen die Ukraine Cyberangriffe auf die Ukraine, einschließlich auf ukrainische Regierungsstellen, verübt.</p> <p>Die GRU führt weiterhin aktiv Cyberangriffe gegen die Union oder ihre Mitgliedstaaten durch. Als Mitglied der GRU ist Evgenii Serebriakov daher an Cyberangriffen mit erheblichen Auswirkungen beteiligt, einschließlich versuchter Cyberangriffe mit potenziell erheblichen Auswirkungen, die eine externe Bedrohung für die Union oder ihre Mitgliedstaaten darstellen.</p>	
6.	Oleg Mikhaylovich SOTNIKOV	<p>Олег Михайлович СОТНИКОВ</p> <p>Geburtsdatum: 24.8.1972</p> <p>Geburtsort: Uljanowsk, Russische SFSR (jetzt Russische Föderation)</p> <p>Reisepass-Nr.: 120018866 ausgestellt vom Außenministerium der Russischen Föderation gültig vom 17.4.2017 bis zum 17.4.2022</p> <p>Ort: Moskau, Russische Föderation</p> <p>Staatsangehörigkeit: russisch</p> <p>Geschlecht: männlich</p>	<p>Oleg Sotnikov hat an einem versuchten Cyberangriff auf die Organisation für das Verbot chemischer Waffen (OVCW) in den Niederlanden mit potenziell erheblichen Auswirkungen sowie an Cyberangriffen mit erheblichen Auswirkungen auf Drittstaaten teilgenommen.</p> <p>Als für ‚human intelligence‘ (Aufklärung mit menschlichen Quellen) zuständiger Mitarbeiter der Hauptdirektion des Generalstabs der Streitkräfte der Russischen Föderation (GU/GRU) gehörte Oleg Sotnikov einem Team von vier Beamten des russischen Militärgeheimdienstes an, die im April 2018 versuchten, sich unbefugt Zugang zum WiFi-Netz der OVCW in Den Haag (Niederlande) zu verschaffen. Der versuchte Cyberangriff hatte zum Ziel, in das WiFi-Netz der OVCW einzudringen, was bei Erfolg die Sicherheit des Netzes und die laufenden Untersuchungen der OVCW gefährdet hätte. Der niederländische militärische Nachrichten- und Sicherheitsdienst (Militaire Inlichtingen- en Veiligheidsdienst) hat den versuchten Cyberangriff abgewehrt und damit die OVCW vor einem schweren Schaden bewahrt.</p>	30.7.2020

			<p>Eine Grand Jury des Western District of Pennsylvania (Vereinigte Staaten von Amerika) hat Oleg Sotnikov als Beamter der GRU wegen Computerhackings, Telekommunikationsbetrugs, schweren Identitätsdiebstahls und Geldwäsche angeklagt.</p> <p>Die GRU führt weiterhin aktiv Cyberangriffe gegen die Union oder ihre Mitgliedstaaten durch. Als Mitglied der GRU ist Oleg Sotnikov daher an Cyberangriffen mit erheblichen Auswirkungen beteiligt, einschließlich versuchter Cyberangriffe mit potenziell erheblichen Auswirkungen, die eine externe Bedrohung für die Union oder ihre Mitgliedstaaten darstellen.</p>	
7.	Dmitry Sergejevich BADIN	<p>Дмитрий Сергеевич БАДИН</p> <p>Geburtsdatum: 15.11.1990</p> <p>Geburtsort: Kursk, Russische SFSR (jetzt Russische Föderation)</p> <p>Staatsangehörigkeit: russisch</p> <p>Geschlecht: männlich</p>	<p>Dmitry Badin war an einem Cyberangriff mit erheblichen Auswirkungen gegen den Deutschen Bundestag sowie an Cyberangriffen mit erheblichen Auswirkungen auf Drittstaaten beteiligt.</p> <p>Als Militärgeheimdienstbeamter des 85. Hauptzentrums für Spezialdienste (GTsST) der Hauptdirektion des Generalstabs der Streitkräfte der Russischen Föderation (GU/GRU) war Dmitry Badin Teil eines Teams von Beamten des russischen Militärgeheimdienstes, die im April und Mai 2015 einen Cyberangriff gegen den Deutschen Bundestag durchführten. Dieser Cyberangriff zielte auf das Informationssystem des Parlaments ab und beeinträchtigte dessen Betrieb für mehrere Tage. Es wurde eine beträchtliche Menge an Daten gestohlen, und die E-Mail-Konten mehrerer MdB sowie der ehemaligen Bundeskanzlerin Angela Merkel waren betroffen.</p> <p>Eine Grand Jury des Western District of Pennsylvania (Vereinigte Staaten von Amerika) hat Dmitry Badin, der der Militäreinheit 26165 zugewiesen ist, wegen Computerhackings, Telekommunikationsbetrugs, schweren Identitätsdiebstahls und Geldwäsche angeklagt.</p> <p>Die GRU führt weiterhin aktiv Cyberangriffe gegen die Union oder ihre Mitgliedstaaten durch. Als Mitglied der GRU ist Dmitry Badin daher an Cyberangriffen mit erheblichen Auswirkungen beteiligt, einschließlich versuchter Cyberangriffe mit potenziell erheblichen Auswirkungen, die eine externe Bedrohung für die Union oder ihre Mitgliedstaaten darstellen.</p>	22.10.2020
8.	Igor Olegovich KOSTYUKOV	<p>Игорь Олегович КОСТЮКОВ</p> <p>Geburtsdatum: 21.2.1961</p>	<p>Igor Kostyukov ist derzeit Leiter der Hauptdirektion des Generalstabs der Streitkräfte der Russischen Föderation (GU/GRU), wo er zuvor als Erster Stellvertretender Leiter tätig war. Eine der seiner Befehlsgewalt unterste-</p>	22.10.2020

		<p>Staatsangehörigkeit: russisch</p> <p>Geschlecht: männlich</p>	<p>henden Einheiten ist das 85. Hauptzentrum für Spezialdienste (GTsST), (alias ‚Militäreinheit 26165‘, ‚APT28‘, ‚Fancy Bear‘, ‚Sofacy Group‘, ‚Pawn Storm‘ und ‚Strontium‘).</p> <p>In dieser Eigenschaft ist Igor Kostyukov verantwortlich für vom GTsST durchgeführte Cyberangriffe, einschließlich derjenigen mit erheblichen Auswirkungen, die eine externe Bedrohung für die Union oder ihre Mitgliedstaaten darstellen.</p> <p>Militärgeheimdienstbeamte des GTsST waren insbesondere beteiligt am Cyberangriff gegen den Deutschen Bundestag im April und Mai 2015, und an dem versuchten Cyberangriff vom April 2018 in den Niederlanden mit dem Ziel, sich unbefugt Zugang zum WiFi-Netz der Organisation für das Verbot chemischer Waffen (OVCW) zu verschaffen.</p> <p>Der Cyberangriff gegen den Deutschen Bundestag zielte auf das Informationssystem des Parlaments ab und beeinträchtigte dessen Betrieb für mehrere Tage. Es wurde eine beträchtliche Menge an Daten gestohlen, und die E-Mail-Konten mehrerer MdB sowie der ehemaligen Bundeskanzlerin Angela Merkel waren betroffen.</p> <p>Die GRU führt weiterhin aktiv Cyberangriffe gegen die Union oder ihre Mitgliedstaaten durch. Als Mitglied der GRU ist Igor Kostyukov daher an Cyberangriffen mit erheblichen Auswirkungen beteiligt, einschließlich versuchter Cyberangriffe mit potenziell erheblichen Auswirkungen, die eine externe Bedrohung für die Union oder ihre Mitgliedstaaten darstellen.</p>	
9.	Ruslan Aleksandrovich PERETYATKO	<p>Руслан Александрович ПЕРЕТЯТЪКО</p> <p>Geburtsdatum: 3.8.1985</p> <p>Staatsangehörigkeit: russisch</p> <p>Geschlecht: männlich</p>	<p>Ruslan PERETYATKO war an Cyberangriffen mit erheblichen Auswirkungen beteiligt, die eine externe Bedrohung für die Union oder ihre Mitgliedstaaten darstellen.</p> <p>Ruslan PERETYATKO gehört der ‚Callisto‘-Gruppe an, einer Gruppe von Beamten des russischen Geheimdienstes, die Cyberoperationen gegen Mitgliedstaaten der EU und Drittstaaten durchführt.</p> <p>Die ‚Callisto‘-Gruppe (alias ‚Seaborgium‘, ‚Star Blizzard‘, ‚ColdRiver‘, ‚TA446‘) hat mehrjährige Phishing-Kampagnen gestartet, um Kontozugangsdaten und Daten zu stehlen. Darüber hinaus zeichnet die ‚Callisto‘-Gruppe für Kampagnen verantwortlich, die sich gegen Einzelpersonen und kritische staatliche Funktionen, auch in den Bereichen Verteidigung und Außenbeziehungen, richten.</p> <p>Deshalb ist Ruslan PERETYATKO an Cyberangriffen mit erheblichen Auswirkungen beteiligt, die eine externe</p>	24.6.2024

			Bedrohung für die Union oder ihre Mitgliedstaaten darstellen.	
10.	Andrey Stanislavovich KORINETS	<p>Андрей Станиславович КОРИНЕЦ</p> <p>Geburtsdatum: 18.5.1987</p> <p>Geburtsort: Stadt Syktyvkar, Russland</p> <p>Staatsangehörigkeit: russisch</p> <p>Geschlecht: männlich</p>	<p>Andrey Stanislavovich KORINETS war an Cyberangriffen mit erheblichen Auswirkungen beteiligt, die eine externe Bedrohung für die Union oder ihre Mitgliedstaaten darstellen.</p> <p>Andrey Stanislavovich KORINETS ist Offizier des ‚Center 18‘ des Inlandsgeheimdienstes der Russischen Föderation. Andrey Stanislavovich KORINETS gehört der ‚Callisto-Gruppe‘ an, einer Gruppe von Beamten des russischen Geheimdienstes, die Cyberoperationen gegen Mitgliedstaaten der EU und Drittstaaten durchführt. Die ‚Callisto‘-Gruppe (alias ‚Seaborgium‘, ‚Star Blizzard‘, ‚ColdRiver‘, ‚TA446‘) hat mehrjährige Phishing-Kampagnen gestartet, um Kontozugangsdaten und Daten zu stehlen. Darüber hinaus zeichnet die ‚Callisto‘-Gruppe für Kampagnen verantwortlich, die sich gegen Einzelpersonen und kritische staatliche Funktionen, auch in den Bereichen Verteidigung und Außenbeziehungen, richten. Deshalb ist Andrey Stanislavovich KORINETS an Cyberangriffen mit erheblichen Auswirkungen beteiligt, die eine externe Bedrohung für die Union oder ihre Mitgliedstaaten darstellen.</p>	24.6.2024
11.	Oleksandr SKLIANKO	<p>Александр СКЛЯНКО (russische Schreibweise)</p> <p>Олександр СКЛЯНКО (ukrainische Schreibweise)</p> <p>Geburtsdatum: 5.8.1973</p> <p>Reisepass: EC 867868, ausgestellt am 27.11.1998 (Ukraine)</p> <p>Geschlecht: männlich</p>	<p>Oleksandr SKLIANKO war an Cyberangriffen mit erheblichen Auswirkungen, die gegen Mitgliedstaaten der EU gerichtet waren, sowie an Cyberangriffen mit erheblichen Auswirkungen, die gegen Drittstaaten gerichtet waren, beteiligt.</p> <p>Oleksandr SKLIANKO gehört der ‚Armageddon‘-Hackergruppe an, die vom Inlandsgeheimdienst der Russischen Föderation unterstützt wird und verschiedene Cyberangriffe mit erheblichen Auswirkungen durchgeführt hat, die gegen die Regierung der Ukraine und gegen Mitgliedstaaten der EU und deren Regierungsbeamte gerichtet waren, unter anderem mittels Phishing-E-Mails und Schadsoftware-Kampagnen.</p> <p>Deshalb ist Oleksandr SKLIANKO an Cyberangriffen mit erheblichen Auswirkungen, die gegen Drittstaaten gerichtet sind, sowie an Cyberangriffen mit erheblichen Auswirkungen, die eine externe Bedrohung für die Union oder ihre Mitgliedstaaten darstellen, beteiligt.</p>	24.6.2024
12.	Mykola CHERNYKH	<p>Николай ЧЕРНЫХ (russische Schreibweise)</p>	<p>Mykola CHERNYKH war an Cyberangriffen mit erheblichen Auswirkungen, die gegen Mitgliedstaaten der EU gerichtet waren, sowie an Cyberangriffen mit erheblichen Auswirkungen,</p>	24.6.2024

		<p>Микола ЧЕРНИХ (ukrainische Schreibweise)</p> <p>Geburtsdatum: 12.10.1978</p> <p>Reisepass: EC 922162, ausgestellt am 20.1.1999 (Ukraine)</p> <p>Geschlecht: männlich</p>	<p>die gegen Drittstaaten gerichtet waren, beteiligt.</p> <p>Mykola CHERNYKH gehört der ‚Armageddon‘-Hackergruppe an, die vom Inlandsgeheimdienst der Russischen Föderation unterstützt wird und verschiedene Cyberangriffe mit erheblichen Auswirkungen durchgeführt hat, die gegen die Regierung der Ukraine und gegen Mitgliedstaaten der EU und deren Regierungsbeamte gerichtet waren, unter anderem mittels Phishing-E-Mails und Schadsoftware-Kampagnen.</p> <p>Als ehemaliger Mitarbeiter des Sicherheitsdienstes der Ukraine ist er in der Ukraine des Verrats und des unberechtigten Eingriffs in den Betrieb elektronischer Rechner und automatisierter Systeme angeklagt.</p> <p>Deshalb ist Mykola CHERNYKH an Cyberangriffen mit erheblichen Auswirkungen beteiligt, die eine externe Bedrohung für die Union oder ihre Mitgliedstaaten darstellen.</p>	
13.	Mikhail Mikhailovich TSAREV	<p>Михаил Михайлович ЦАРЕВ</p> <p>Geburtsdatum: 20.4.1989</p> <p>Geburtsort: Serpukhov, Russische Föderation</p> <p>Staatsangehörigkeit: russisch</p> <p>Anschrift: Serpukhov</p> <p>Geschlecht: männlich</p>	<p>Mikhail Mikhailovich TSAREV war an Cyberangriffen mit erheblichen Auswirkungen beteiligt, die eine externe Bedrohung für die Mitgliedstaaten der EU darstellen.</p> <p>Mikhail Mikhailovich TSAREV, auch bekannt unter den Online-Spitznamen ‚Mango‘, ‚Alexander Grachev‘, ‚Super Misha‘, ‚Ivanov Mixail‘, ‚Misha Krutysha‘ und ‚Nikita Andreevich Tsarev‘, ist ein wichtiger Akteur in der Einsetzung der Schadsoftware ‚Conti‘ und ‚Trickbot‘ und ist an der Russland-basierten Bedrohungsgruppe ‚Wizard Spider‘ beteiligt.</p> <p>Die Schadsoftware ‚Conti‘ und ‚Trickbot‘ wurde von ‚Wizard Spider‘ geschaffen und entwickelt wurde. Die Gruppe ‚Wizard Spider‘ hat in verschiedenen Branchen, darunter wesentliche Dienstleistungsbereiche wie die Gesundheitsversorgung und das Bankwesen, Ransomware-Kampagnen durchgeführt. Die Gruppe hat weltweit Computer infiziert und ihre Schadsoftware in eine hochmodulare Schadsoftware-Reihe entwickelt. Von der Gruppe ‚Wizard Spider‘ durchgeführte Kampagnen, bei denen Schadsoftware wie ‚Conti‘, ‚Ryuk‘ und ‚TrickBot‘, eingesetzt wird, sind für erhebliche wirtschaftliche Schäden in der Europäischen Union verantwortlich.</p> <p>Deshalb ist Mikhail Mikhailovich TSAREV an Cyberangriffen mit erheblichen Auswirkungen beteiligt, die eine externe Bedrohung für die Union oder ihre Mitgliedstaaten darstellen.</p>	24.6.2024
14.	Maksim Sergeevich	<p>Максим Сергеевич ГАЛОЧКИН</p>	<p>Maksim Galochkin hat bei Cyberangriffen mit erheblichen Auswirkungen</p>	24.6.2024

	GALOCHKIN	<p>Geburtsdatum: 19.5.1982</p> <p>Geburtsort: Abakan, Russische Föderation</p> <p>Staatsangehörigkeit: russisch</p> <p>Geschlecht: männlich</p>	<p>mitgewirkt, die eine externe Bedrohung für die Mitgliedstaaten der EU darstellen.</p> <p>Maksim Galochkin ist auch bekannt unter den Online-Spitznamen ‚Benalen‘, ‚Bentley‘, ‚Volhvb‘, ‚volhvb‘, ‚manuel‘, ‚Max17‘ und ‚Crypt‘. Galochkin ist ein wichtiger Akteur in der Einsetzung der Schadsoftware ‚TrickBot‘ und ‚Conti‘ und ist an der Russland-basierten Bedrohungsgruppe ‚Wizard Spider‘ beteiligt. Er hat ein Team von Testern geleitet, das mit für die Entwicklung, Überwachung und Durchführung von Tests für die von ‚Wizard Spider‘ geschaffene und eingesetzte TrickBot-Schadsoftware verantwortlich war.</p> <p>‚Wizard Spider‘ hat in verschiedenen Branchen, darunter wesentliche Dienstleistungsbereiche wie die Gesundheitsversorgung und das Bankwesen, Ransomware-Kampagnen durchgeführt. Die Gruppe hat weltweit Computer infiziert und ihre Schadsoftware in eine hochmodulare Schadsoftware-Reihe entwickelt. Von der Gruppe ‚Wizard Spider‘ durchgeführte Kampagnen, bei denen Schadsoftware wie ‚Conti‘, ‚Ryuk‘ und ‚TrickBot‘, eingesetzt wird, sind für erhebliche wirtschaftliche Schäden in der Europäischen Union verantwortlich.</p> <p>Deshalb ist Maksim Galochkin an Cyberangriffen mit erheblichen Auswirkungen beteiligt, die eine externe Bedrohung für die Union oder ihre Mitgliedstaaten darstellen.</p>	
15.	Nikolay Alexandrovich KORCHAGIN	<p>Николай Александрович Корчагин</p> <p>Geburtsdatum: 16.9.1997</p> <p>Staatsangehörigkeit: russisch</p> <p>Geschlecht: männlich</p> <p>Verbundene Organisation: Hauptdirektion des Generalstabs der Streitkräfte der Russischen Föderation</p>	<p>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.</p> <p>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 gewahren, mit dem Ziel, die Daten zu verwenden, um die Sicherheit Estlands zu bedrohen. Die Angriffe betreffen daher die Speicherung von Verschlusssachen. Die Angriffe betreffen Verbündete und Partner Estlands.</p>	27.1.2025

			Somit ist Nikolay Korchagin an Cyberangriffen mit erheblichen Auswirkungen, die eine äußere Bedrohung für einen Mitgliedstaat darstellen, beteiligt und dafür verantwortlich.	
16.	Vitaly SHEVCHENKO	<p>Виталий Шевченко</p> <p>Geburtsdatum: 1.9.1997</p> <p>Staatsangehörigkeit: russisch</p> <p>Geschlecht: männlich</p> <p>Verbundene Organisation: Hauptdirektion des Generalstabs der Streitkräfte der Russischen Föderation</p>	<p>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.</p> <p>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 betreffen 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.</p>	27.1.2025
17.	Yuriy Fedorovich DENISOV	<p>Юрий Федорович Денисов</p> <p>Geburtsdatum: 17.6.1980</p> <p>Staatsangehörigkeit: russisch</p> <p>Geschlecht: männlich</p> <p>Verbundene Organisation: Hauptdirektion des Generalstabs der Streitkräfte der Russischen Föderation</p>	<p>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.</p> <p>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 betreffen Verbündete und Partner Estlands.</p>	27.1.2025

			Somit ist Yuriy Denisov an Cyberangriffen mit erheblichen Auswirkungen, die eine äußere Bedrohung für einen Mitgliedstaat darstellen, beteiligt und dafür verantwortlich.	
--	--	--	---	--

B. Juristische Personen, Organisationen und Einrichtungen

	Name	Angaben zur Identität	Gründe	Datum der Aufnahme in die Liste
1.	Tianjin Huaying Haitai Science and Technology Development Co Ltd (Huaying Haitai)	Aliasname: Haitai Technology Development Co. Ltd Ort: Tianjin, China	Die Huaying Haitai hat die „Operation Cloud Hopper“ finanziell, technisch oder materiell unterstützt; es handelt sich dabei um eine Reihe von Cyberangriffen mit erheblichen Auswirkungen, die von außerhalb der Union ausgehen und eine externe Bedrohung für die Union bzw. ihre Mitgliedstaaten darstellen und von Cyberangriffen mit erheblichen Auswirkungen auf Drittstaaten. Mit der „Operation Cloud Hopper“ wurden Informationssysteme multinationaler Unternehmen auf sechs Kontinenten angegriffen, darunter Unternehmen mit Sitz in der Union, und unbefugt auf sensible Geschäftsdaten zugegriffen, was zu erheblichen wirtschaftlichen Verlusten geführt hat. Die „Operation Cloud Hopper“ wurde von dem als „APT10“ („Advanced Persistent Threat 10“) (alias „Red Apollo“, „CVNX“, „Stone Panda“, „MenuPass“ und „Potassium“) bekannten Täter verübt. Die Huaying Haitai kann mit APT10 in Verbindung gebracht werden. Darüber hinaus waren Gao Qiang und Zhang Shilong bei Huaying Haitai beschäftigt, die beide in Zusammenhang mit der „Operation Cloud Hopper“ gebracht werden. Die Huaying Haitai steht daher in Beziehung zu Gao Qiang und Zhang Shilong.	30.7.2020
2.	Chosun Expo	Aliasname: Chosen Expo; Korea Export Joint Venture Ort: DVRK	Die Chosun Expo hat eine Reihe von Cyberangriffen mit erheblichen Auswirkungen, die von außerhalb der Union ausgehen und eine externe Bedrohung für die Union bzw. ihre Mitgliedstaaten darstellen und von Cyberangriffen mit erheblichen Auswirkungen auf Drittstaaten, finanziell, technisch oder materiell unterstützt; dazu zählen die als „WannaCry“ bekannten Cyberangriffe und Cyberangriffe auf die polnische Finanzaufsichtsbehörde und auf Sony Pictures Entertainment sowie Cyberdiebstahl bei der Bangladesh Bank und verurteilter Cyberdiebstahl bei der Vietnam Tien Phong Bank. „WannaCry“ hat Störungen in Informationssystemen auf der ganzen Welt	30.7.2020

			<p>verursacht, indem Ransomware in Informationssysteme eingeschleust und der Zugriff auf Daten blockiert wurde. Betroffen waren Informationssysteme von Unternehmen in der Union, darunter Informationssysteme in Bezug auf Dienste, die für die Aufrechterhaltung wesentlicher Dienstleistungen und wirtschaftlicher Tätigkeiten in den Mitgliedstaaten erforderlich sind. „WannaCry“ wurde von dem als „APT38“ („Advanced Persistent Threat 38“) bekannten Täter oder der „Lazarus Group“ verübt. Die Chosun Expo kann mit APT38/der Lazarus Group in Verbindung gebracht werden, auch durch die bei den Cyberangriffen benutzten Konten.</p>	
3.	<p>Hauptzentrum für Spezialtechnologien (GTsST) der Hauptdirektion des Generalstabs der Streitkräfte der Russischen Föderation (GU/GRU)</p>	<p>Adresse: 22 Kirova Street, Moscow, Russian Federation</p>	<p>Das Hauptzentrum für Spezialtechnologien (GTsST) der Hauptdirektion des Generalstabs der Streitkräfte der Russischen Föderation (GU/GRU), auch unter seiner Feldpostnummer 74455 bekannt, ist an Cyberangriffen mit erheblichen Auswirkungen beteiligt, die von außerhalb der Union ausgehen und eine externe Bedrohung für die Union bzw. ihre Mitgliedstaaten darstellen, und an Cyberangriffen mit erheblichen Auswirkungen auf Drittstaaten; dazu zählen die als ‚NotPetya‘ oder ‚EternalPetya‘ bekannten Cyberangriffe vom Juni 2017 und die im Winter 2015 und 2016 gegen das ukrainische Stromnetz gerichteten Cyberangriffe. ‚NotPetya‘ und ‚EternalPetya‘ haben in einer Reihe von Unternehmen in der Union, in Europa außerhalb der Union und auf der ganzen Welt Daten unzugänglich gemacht, indem Ransomware in Computer eingeschleust und der Zugriff auf Daten blockiert wurde, was u. a. zu erheblichen wirtschaftlichen Verlusten geführt hat. Der Cyberanschlag auf ein ukrainisches Stromnetz hat dazu geführt, dass Teile des Netzes im Winter abgeschaltet wurden. ‚NotPetya‘ und ‚EternalPetya‘ wurden von dem als ‚Sandworm‘ (alias ‚Sandworm Team‘, ‚BlackEnergy Group‘, ‚Voodoo Bear‘, ‚Quedagh‘, ‚Olympic Destroyer‘ und ‚Telebots‘) bekannten Täter verübt, der auch den Angriff auf das ukrainische Stromnetz ausgeführt hat. Sandworm hat im Zuge des Angriffskriegs Russlands gegen die Ukraine Cyberangriffe auf die Ukraine, einschließlich auf Regierungsstellen und kritische Infrastruktur der Ukraine, verübt. Zu diesen Cyberangriffen gehören Spear-Phishing-Kampagnen und Angriffe mit Schadsoftware und Ransomware. Das Hauptzentrum für Spezialtechnologien der Hauptdirektion des Gene-</p>	30.7.2020

			<p>ralstabs der Streitkräfte der Russischen Föderation spielt eine aktive Rolle bei den Cyberaktivitäten von ‚Sandworm‘ und kann mit ‚Sandworm‘ in Verbindung gebracht werden.</p>	
4.	<p>85. Hauptzentrum für Spezialdienste (GTsST) der Hauptdirektion des Generalstabs der Streitkräfte der Russischen Föderation (GU/GRU)</p>	<p>Anschrift: Komsomol'skiy Prospekt, 20, Moskau, 119146, Russische Föderation</p>	<p>Das 85. Hauptzentrum für Spezialdienste (GTsST) der Hauptdirektion des Generalstabs der Streitkräfte der Russischen Föderation (GU/GRU), (alias ‚Militäreinheit 26165‘, ‚APT28‘, ‚Fancy Bear‘, ‚Sofacy Group‘, ‚Pawn Storm‘ und ‚Strontium‘), ist an Cyberangriffen mit erheblichen Auswirkungen, die eine externe Bedrohung für die Union oder ihre Mitgliedstaaten darstellen, sowie an Cyberangriffen mit erheblichen Auswirkungen auf Drittstaaten beteiligt.</p> <p>Militärgeheimdienstbeamte des GTsST waren insbesondere beteiligt am Cyberangriff gegen den Deutschen Bundestag im April und Mai 2015, und an dem versuchten Cyberangriff vom April 2018 in den Niederlanden mit dem Ziel, sich unbefugten Zugang zum WiFi-Netz der Organisation für das Verbot chemischer Waffen (OVCW) zu verschaffen.</p> <p>Der Cyberangriff gegen den Deutschen Bundestag zielte auf das Informationssystem des Parlaments ab und beeinträchtigte dessen Betrieb für mehrere Tage. Es wurde eine beträchtliche Menge an Daten gestohlen, und die E-Mail-Konten mehrerer MdB sowie der ehemaligen Bundeskanzlerin Angela Merkel waren betroffen.</p> <p>Im Zuge des Angriffskriegs Russlands gegen die Ukraine wurden durch das GTsST Cyberangriffe (Spear-Phishing-Angriffe und Angriffe mit Schadsoftware) gegen die Ukraine verübt.</p>	22.10.2020

ANHANG II

Kontaktdaten der zuständigen Behörden der Mitgliedstaaten
und der Anschrift für Notifikationen an die Europäische Kommission

BELGIEN

https://diplomatie.belgium.be/en/policy/policy_areas/peace_and_security/sanctions

BULGARIEN

<https://www.mfa.bg/en/EU-sanctions>

TSCHECHIEN

<https://fau.gov.cz/en/international-sanctions>

DÄNEMARK

<https://um.dk/udenrigspolitik/sanktioner/ansvarlige-myndigheder>

DEUTSCHLAND

<https://www.bmwi.de/Redaktion/DE/Artikel/Aussenwirtschaft/embargos-aussenwirtschaftsrecht.html>

ESTLAND

<https://vm.ee/en/sanctions-arms-and-export-control/international-sanctions>

IRLAND

<https://www.dfa.ie/our-role/policies/ireland-in-the-eu/eu-restrictive-measures/>

GRIECHENLAND

<http://www.mfa.gr/en/foreign-policy/global-issues/international-sanctions.html>

SPANIEN

<https://www.exteriores.gob.es/en/PolíticaExterior/Paginas/SancionesInternacionales.aspx>

FRANKREICH

<http://www.diplomatie.gouv.fr/fr/autorites-sanctions/>

KROATIEN

<https://mvep.gov.hr/foreign-policy/restrictive-measures/271988>

ITALIEN

https://www.esteri.it/en/politica-estera-e-cooperazione-allo-sviluppo/politica_europea/misure_deroghe/

ZYPERN

<https://mfa.gov.cy/themes/>

LETTLAND

<https://www.fid.gov.lv/en>

LITAUEN

<https://www.urm.lt/en/lithuania-in-the-region-and-the-world/lithuanias-security-policy/international-sanctions/997>

LUXEMBURG

<https://maee.gouvernement.lu/fr/directions-du-ministere/affaires-europeennes/organisations-economiques-int/mesures-restrictives.html>

UNGARN

<https://kormany.hu/kulgazdasagi-es-kulugyminiszterium/ensz-eu-szancios-tajekoztato>

MALTA

<https://smb.gov.mt/>

NIEDERLANDE

<https://www.government.nl/topics/international-sanctions>

ÖSTERREICH

<https://www.bmeia.gv.at/themen/aussenpolitik/europa/eu-sanktionen-nationale-behoerden/>

POLEN

<https://www.gov.pl/web/dyplomacja/sankcje-miedzynarodowe>

<https://www.gov.pl/web/diplomacy/international-sanctions>

PORTUGAL

<https://portaldiplomatico.mne.gov.pt/politica-externa/medidas-restritivas>

RUMÄNIEN

<http://www.mae.ro/en/node/2123>

SLOWENIEN

<https://www.gov.si/en/topics/restrictive-measures/>

SLOWAKEI

<https://www.mzv.sk/en/web/en/diplomacy/international-sanctions>

FINNLAND

<https://um.fi/international-sanctions>

SCHWEDEN

<https://www.government.se/government-policy/foreign-and-security-policy/international-sanctions/>

Anschrift für Notifikationen an die Europäische Kommission:

Europäische Kommission

Generaldirektion Finanzstabilität, Finanzdienstleistungen und Kapitalmarktunion (GD FISMA)

Rue de Spa 2/Spastraat 2

1049 Bruxelles/Brussel, Belgien

E-Mail: relex-sanctions@ec.europa.eu