II

(Rechtsakte ohne Gesetzescharakter)

VERORDNUNGEN

DURCHFÜHRUNGSVERORDNUNG (EU) 2020/1744 DES RATES

vom 20. November 2020

zur Durchführung der Verordnung (EU) 2019/796 über restriktive Maßnahmen gegen Cyberangriffe, die die Union oder ihre Mitgliedstaaten bedrohen

DER RAT DER EUROPÄISCHEN UNION —

gestützt auf den Vertrag über die Arbeitsweise der Europäischen Union,

gestützt auf die Verordnung (EU) 2019/796 des Rates vom 17. Mai 2019 über restriktive Maßnahmen gegen Cyberangriffe, die die Union oder ihre Mitgliedstaaten bedrohen ([1]), insbesondere auf Artikel 13 Absatz 1,

auf Vorschlag des Hohen Vertreters der Union für Außen- und Sicherheitspolitik,

in Erwägung nachstehender Gründe:

(1) Der Rat hat am 17. Mai 2019 die Verordnung (EU) 2019/796 angenommen.

(2) Der Rat hat am 30. Juli 2020 die Durchführungsverordnung (EU) 2020/1125 ([2]) angenommen, mit der sechs natürliche Personen und drei Organisationen oder Einrichtungen in die in Anhang I der Verordnung (EU) 2019/796 enthaltene Liste der natürlichen und juristischen Personen, Organisationen und Einrichtungen, die restriktiven Maßnahmen unterliegen, aufgenommen wurden.

(3) Zu zwei Listeneinträgen zu natürlichen Personen sind aktualisierte Informationen eingegangen.

(4) Die Verordnung (EU) 2019/796 sollte daher entsprechend geändert werden —

HAT FOLGENDE VERORDNUNG ERLASSEN:

Artikel 1

Anhang I der Verordnung (EU) 2019/796 wird gemäß dem Anhang der vorliegenden Verordnung geändert.

Artikel 2

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 20. November 2020.

Im Namen des Rates
Der Präsident
M. ROTH

([1]) ABl. L 129I vom 17.5.2019, S. 1.
([2]) Durchführungsverordnung (EU) 2020/1125 des Rates vom 30. Juli 2020 zur Durchführung der Verordnung (EU) 2019/796 über restriktive Maßnahmen gegen Cyberangriffe, die die Union oder ihre Mitgliedstaaten bedrohen (ABl. L 246 vom 30.7.2020, S. 4).

ANHANG

In Anhang I der Verordnung (EU) 2019/796 erhalten die Einträge 1 und 2 unter der Überschrift „A. Natürliche Personen“ folgende Fassung:

	Name	Angaben zur Identität	Gründe	Datum der Aufnahme in die Liste
„1.	GAO Qiang	Geburtsdatum: 4. Oktober 1983 Geburtsort: Provinz Shandong, China Anschrift: Room 1102, Guanfu Mansion, 46 Xinkai Road, Hedong District, Tianjin, China Staatsangehörigkeit: chinesisch Geschlecht: männlich	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. 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. ‚Operation Cloud Hopper‘ wurde von dem als ‚APT10‘ (‚Advanced Persistent Threat 10‘) (alias ‚Red Apollo‘, ‚CVNX‘, ‚Stone Panda‘, ‚MenuPass‘ und ‚Potassium‘) bekannten Täter verübt. Gao Qiang kann mit APT10 in Verbindung gebracht werden, auch aufgrund seiner Verbindungen zur Führungs- und Kontrollinfrastruktur von APT10. 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.	30.7.2020
2.	ZHANG Shilong	Geburtsdatum: 10. September 1981 Geburtsort: China Anschrift: Hedong, Yuyang Road No 121, Tianjin, China Staatsangehörigkeit: chinesisch Geschlecht: männlich	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. 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. ‚Operation Cloud Hopper‘ wurde von dem als ‚APT10‘ (‚Advanced Persistent Threat 10‘) (alias ‚Red Apollo‘, ‚CVNX‘, ‚Stone Panda‘, ‚MenuPass‘ und ‚Potassium‘) bekannten Täter verübt. 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.	30.7.2020“