BESCHLUSS (GASP) 2020/1127 DES RATES

vom 30. Juli 2020

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 („Cyber Diplomacy Toolbox“) und sind ein wichtiges Instrument, um von solchen Aktivitäten abzuschrecken und darauf zu reagieren. Restriktive Maßnahmen können auch zur Reaktion auf gegen Drittstaaten oder internationale Organisationen gerichtete Cyberangriffe mit erheblichen Auswirkungen angewendet werden, sofern dies für notwendig erachtet wird, um die in den einschlägigen Bestimmungen des Artikels 21 des Vertrags über die Europäische Union festgelegten gemeinsamen außen- und sicherheitspolitischen Ziele zu erreichen.

(3) Der Rat hat am 16. April 2018 Schlussfolgerungen angenommen, in denen er die böswillige Nutzung von Informations- und Kommunikationstechnologien, einschließlich im Fall von als „WannaCry“ und „NotPetya“ bekannten Cyberangriffen, die beträchtlichen Schaden und wirtschaftlichen Verlust in und außerhalb der Union angerichtet haben, entschieden verurteilt hat. Der Präsident des Europäischen Rates und der Präsident der Europäischen Kommission sowie der Hohe Vertreter der Union für Außen- und Sicherheitspolitik (im Folgenden „Hoher Vertreter“) äußerten am 4. Oktober 2018 in einer gemeinsamen Erklärung ernste Bedenken über einen versuchten Cyberangriff zur Untergrabung der Integrität der Organisation für das Verbot chemischer Waffen (OVCW) in den Niederlanden; es handelte sich um einen aggressiven Akt, in dem Verachtung für das hohe Ziel der OVCW zum Ausdruck gebracht wurde. In einer Erklärung im Namen der Union vom 12. April 2019 forderte der Hohe Vertreter die Täter nachdrücklich auf, böswillige Cyberaktivitäten zu unterlassen, die darauf abzielen, die Integrität, Sicherheit und wirtschaftliche Wettbewerbsfähigkeit der Union zu untergraben; dazu gehört auch der Cyberdiebstahl von geistigem Eigentum. Zu solchen Cyberdiebstählen zählen auch diejenigen, die von dem als „APT10“ („Advance Persistent Threat 10“) bekannten Täter verübt wurden.

(4) In diesem Zusammenhang und um fortgesetzte und zunehmende böswillige Handlungen im Cyberraum zu verhindern, von ihnen abzuschrecken und auf sie zu reagieren, sollten sechs natürliche Personen und drei Organisationen bzw. Einrichtungen 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, Organisationen und Einrichtungen sind verantwortlich für Cyberangriffe oder versuchte Cyberangriffe — darunter der versuchte Cyberangriff gegen die OVCW und die als „WannaCry“ und „NotPetya“ bekannten Cyberangriffe sowie „Operation Cloud Hopper“ — oder haben diese unterstützt oder waren daran beteiligt oder haben diese erleichtert.

(5) 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.

([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).

Artikel 2

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

Geschehen zu Brüssel am 30. Juli 2020.

Im Namen des Rates
Der Präsident
M. ROTH

ANHANG

Die folgenden Personen und Organisationen bzw. Einrichtungen werden in die Liste der natürlichen und juristischen Personen, Organisationen und Einrichtungen im Anhang des Beschlusses (GASP) 2019/797 aufgenommen:

„A. Natürliche Personen

	Name	Angaben zur Identität	Gründe	Datum der Aufnahme in die Liste
1.	GAO Qiang	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. „Operation Cloud Hopper“ zielte auf die Informationssysteme multinationaler Unternehmen auf sechs Kontinenten, darunter Unternehmen mit Sitz in der Union, und verschaffte sich unbefugt Zugang zu sensiblen Geschäftsinformationen, wodurch erhebliche wirtschaftliche Verluste entstanden. Verübt wurde „Operation Cloud Hopper“ von dem als „APT10“ („Advanced Persistent Threat 10“) (alias „Red Apollo“, „CVNX“, „Stone Panda“, „MenuPass“ und „Potassium“) bekannten Täter. 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	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. „Operation Cloud Hopper“ zielte auf die Informationssysteme multinationaler Unternehmen auf sechs Kontinenten, darunter Unternehmen mit Sitz in der Union, und verschaffte sich unbefugt Zugang zu sensiblen Geschäftsinformationen, wodurch erhebliche wirtschaftliche Verluste entstanden. Verübt wurde „Operation Cloud Hopper“ von dem als „APT10“ („Advanced Persistent Threat 10“) (alias „Red Apollo“, „CVNX“, „Stone Panda“, „MenuPass“ und „Potassium“) bekannten Täter.	30.7.2020

			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.	
3.	Alexey Valeryevich MININ	Алексей Валерьевич МИНИН Geburtsdatum: 27. Mai 1972 Geburtsort: Oblast Perm, Russische SFSR (jetzt Russische Föderation) Reisepass-Nr.: 120017582, ausgestellt vom Außenministerium der Russischen Föderation, gültig vom 17. April 2017 bis zum 17. April 2022 Ort: Moskau, Russische Föderation Staatsangehörigkeit: russisch Geschlecht: männlich	Alexey Minin hat an einem versuchten Cyberangriff auf die Organisation für das Verbot chemischer Waffen (OVCW) in den Niederlanden mit potenziell erheblichen Auswirkungen teilgenommen. 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 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 — MIVD) hat den versuchten Cyberangriff abgewehrt und damit die OVCW vor einem schwerem Schaden bewahrt.	30.7.2020
4.	Aleksei Sergeyvich MORENETS	Алексей Сергеевич МОРЕНЕЦ Geburtsdatum: 31. Juli 1977 Geburtsort: Oblast Murmansk, Russische SFSR (jetzt Russische Föderation) Reisepass-Nr.: 100135556, ausgestellt vom Außenministerium der Russischen Föderation, gültig vom 17. April 2017 bis zum 17. April 2022 Ort: Moskau, Russische Föderation Staatsangehörigkeit: russisch Geschlecht: männlich	Aleksei Morenets hat an einem versuchten Cyberangriff auf die Organisation für das Verbot chemischer Waffen (OVCW) in den Niederlanden mit potenziell erheblichen Auswirkungen teilgenommen. 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 — MIVD) hat den versuchten Cyberangriff abgewehrt und damit die OVCW vor einem schwerem Schaden bewahrt.	30.7.2020

5.	Evgenii Mikhaylovich SEREBRIAKOV	Евгений Михайлович СЕРЕБРЯКОВ Geburtsdatum: 26. Juli 1981 Geburtsort: Kursk, Russische SFSR (jetzt Russische Föderation) Reisepass-Nr.: 100135555, ausgestellt vom Außenministerium der Russischen Föderation, gültig vom 17. April 2017 bis zum 17. April 2022 Ort: Moskau, Russische Föderation Staatsangehörigkeit: russisch Geschlecht: männlich	Evgenii Serebriakov hat an einem versuchten Cyberangriff auf die Organisation für das Verbot chemischer Waffen (OVCW) in den Niederlanden mit potenziell erheblichen Auswirkungen teilgenommen. 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 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 — MIVD) hat den versuchten Cyberangriff abgewehrt und damit die OVCW vor einem schwerem Schaden bewahrt.	30.7.2020
6.	Oleg Mikhaylovich SOTNIKOV	Олег Михайлович СОТНИКОВ Geburtsdatum: 24. August 1972 Geburtsort: Uljanowsk, Russische SFSR (jetzt Russische Föderation) Reisepass-Nr.: 120018866, ausgestellt vom Außenministerium der Russischen Föderation, gültig vom 17. April 2017 bis zum 17. April 2022 Ort: Moskau, Russische Föderation Staatsangehörigkeit: russisch Geschlecht: männlich	Oleg Sotnikov hat an einem versuchten Cyberangriff auf die Organisation für das Verbot chemischer Waffen (OVCW) in den Niederlanden mit potenziell erheblichen Auswirkungen teilgenommen. 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 — MIVD) hat den versuchten Cyberangriff abgewehrt und damit die OVCW vor einem schwerem Schaden bewahrt.	30.7.2020

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.	30.7.2020

			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.	
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 versuchter Cyberdiebstahl bei der Vietnam Tien Phong Bank. „WannaCry“ hat Störungen in Informationssystemen auf der ganzen Welt 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.	30.7.2020
3.	Hauptzentrum für Spezialtechnologien (GTsST) der Hauptdirektion des Generalstabs der Streitkräfte der Russischen Föderation (GU/GRU)	Adresse: 22 Kirova Street, Moscow, Russian Federation	Das Hauptzentrum für Spezialtechnologien (GTsST) der Hauptdirektion des Generalstabs der Streitkräfte der Russischen Föderation (GU/GRU), auch unter seiner Feldpostnummer 74455 bekannt, ist verantwortlich für Cyberangriffe mit erheblichen Auswirkungen, die von außerhalb der Union ausgehen und eine externe Bedrohung für die Union bzw. ihre Mitgliedstaaten darstellen und für Cyberangriffe 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.	30.7.2020“

			„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. Das Hauptzentrum für Spezialtechnologien der Hauptdirektion des Generalstabs der Streitkräfte der Russischen Föderation spielt eine aktive Rolle bei den Cyberaktivitäten von „Sandworm“ und kann mit „Sandworm“ in Verbindung gebracht werden.	