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

▼M2

	Name	Angaben zur Identität	Gründe	Datum der Aufnahme in die Liste
			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

	Name	Angaben zur Identität	Gründe	Datum der Aufnahme in die Liste
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 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 Generalstabs der Streitkräfte der Russischen Föderation spielt eine aktive Rolle bei den Cyberaktivitäten von ‚Sandworm' und kann mit ‚Sandworm' in Verbindung gebracht werden.	30.7.2020

ELI: http://data.europa.eu/eli/dec/2024/1391/oj
ABl. L vom 17.5.2024

	Name	Angaben zur Identität	Gründe	Datum der Aufnahme in die Liste
4.	85. Hauptzentrum für Spezialdienste (GTsST) der Hauptdirektion des Generalstabs der Streitkräfte der Russischen Föderation (GU/GRU)	Adresse: Komsomol'skiy Prospekt, 20, Moskau, 119146, Russische Föderation	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. 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. 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. Im Zuge des Angriffskrieg Russlands gegen die Ukraine wurden durch das GTsST Cyberangriffe (Spear-Phishing-Angriffe und Angriffe mit Schadsoftware) gegen die Ukraine verübt.	22.10.2020