2026/589

16.3.2026

NÕUKOGU RAKENDUSMÄÄRUS (EL) 2026/589,

16. märts 2026,

millega rakendatakse määrust (EL) 2019/796 piiravate meetmete kohta, millega takistada liitu või selle liikmesriike ähvardavaid küberrünnakuid

EUROOPA LIIDU NÕUKOGU,

võttes arvesse Euroopa Liidu toimimise lepingut,

võttes arvesse nõukogu 17. mai 2019. aasta määrust (EL) 2019/796 piiravate meetmete kohta, millega takistada liitu või selle liikmesriike ähvardavaid küberrünnakuid, [1] eriti selle artikli 13 lõiget 1,

võttes arvesse liidu välisasjade ja julgeolekupoliitika kõrge esindaja ettepanekut

ning arvestades järgmist:

(1) Nõukogu võttis 17. mail 2019 vastu määruse (EL) 2019/796.

(2) Osana liidu kestvast, kohandatud ja kooskõlastatud tegevusest püsivate küberohtude põhjustajate vastu tuleks määruse (EL) 2019/796 I lisas esitatud nende füüsiliste ja juriidiliste isikute, üksuste ja asutuste loetellu, kelle suhtes kohaldatakse piiravaid meetmeid, kanda kaks füüsilist isikut ja kolm üksust. Need füüsilised isikud ja üksused vastutavad selliste märkimisväärse mõjuga küberrünnete eest, mis kujutavad endast liidule või selle liikmesriikidele välist ohtu, või on nende küberrünnetega seotud.

(3) Määruse (EL) 2019/796 I lisa tuleks seetõttu vastavalt muuta,

ON VASTU VÕTNUD KÄESOLEVA MÄÄRUSE:

Artikkel 1

Määruse (EL) 2019/796 I lisa muudetakse vastavalt käesoleva määruse lisale.

Artikkel 2

Käesolev määrus jõustub *Euroopa Liidu Teatajas* avaldamise päeval.

Käesolev määrus on tervikuna siduv ja vahetult kohaldatav kõikides liikmesriikides.

Brüssel, 16. märts 2026

Nõukogu nimel

eesistuja

K. KALLAS

[1] ELT L 129 I, 17.5.2019, lk 1, ELI: http://data.europa.eu/eli/reg/2019/796/oj.

LISA

Määruse (EL) 2019/796 I lisa muudetakse järgmiselt.

1) Jaotisse „A. Füüsilised isikud“ lisatakse järgmised kanded.

	Nimi	Tuvastamisandmed	Põhjused	Loetellu kandmise kuupäev
„18.	CHEN Cheng	陈诚 (kirjapilt hiina keeles) Teise nimega: Jesse Chen lengmo I3n6m0 Sünniaeg: 20.10.1984 Sünnikoht: Yancheng, Jiangsu, Hiina Kodakondsus: Hiina Sugu: mees	Chen Cheng on Hiina ärimees, äriühingu Anxun Information Technology Co. Ltd. kaasasutaja ja üks peadirektoritest. Ta on ka nimetatud äriühingu Sichuani filiaali seaduslik esindaja. Anxun Information Technology Co. Ltd., mida tuntakse ka nime i-Soon all, on Hiina Rahvavabariigis asuv äriühing, mis pakub tasulisi häkkimisteenuseid („hacking-for-hire“). Anxun Information Technology Co. Ltd. on rünnanud liikmesriikide elutähtsaid taristuid ja riigi põhifunktsioone ning pääsenud juurde salastatud teabele ja müünud seda. Lisaks on Anxun Information Technology Co. Ltd. rünnanud mitme kolmanda riigi valitsust, ohustades seeläbi liidu ühise välis- ja julgeolekupoliitika (ÜVJP) eesmärke, mis on sätestatud Euroopa Liidu lepingu artikli 21 lõike 2 punktides a–c. Anxun Information Technology Co. Ltd. saab osutatud teenustest olulist majanduslikku kasu. Seega vastutab Anxun Information Technology Co. Ltd. märkimisväärse mõjuga küberrünnete eest, mis kujutavad välist ohtu liidule ja selle liikmesriikidele ning kolmandatele riikidele. Sellel ametikohal vastutab Chen Cheng märkimisväärse mõjuga küberrünnete eest, mis kujutavad välist ohtu liikmesriikidele, ning kolmandate riikide vastu suunatud märkimisväärse mõjuga küberrünnete eest, ning on nende rünnetega seotud.	16.3.2026

	Nimi	Tuvastamisandmed	Põhjused	Loetellu kandmise kuupäev
19.	WU Heibo	吴海波 (kirjapilt hiina keeles) Teise nimega: shutdown shutd0wn Sünnikoht: Hiina Kodakondsus: Hiina Sugu: mees	Wu Haibo on Hiina ärimees, äriühingu Anxun Information Technology Co. Ltd. kaasasutaja ja üks peadirektoritest. Ta on ka äriühingu Anxun Information Technology Co. Ltd. („emaettevõtja“) Shanghai filiaali seaduslik esindaja, esimees ja peadirektor. Lisaks tegutseb ta kõnealuse äriühingu Sichuani filiaali seadusliku esindajana. Anxun Information Technology Co. Ltd., mida tuntakse ka nime i-Soon all, on Hiina Rahvavabariigis asuv äriühing, mis pakub tasulisi häkkimisteenuseid. Anxun Information Technology Co. Ltd. on rünnanud liikmesriikide elutähtsaid taristuid ja riigi põhifunktsioone ning pääsenud juurde salastatud teabele ja müünud seda. Lisaks on Anxun Information Technology Co. Ltd. rünnanud mitme kolmanda riigi valitsust, ohustades seeläbi liidu ühise välis- ja julgeolekupoliitika (ÜVJP) eesmärke, mis on sätestatud Euroopa Liidu lepingu artikli 21 lõike 2 punktides a–c. Anxun Information Technology Co. Ltd. saab osutatud teenustest olulist majanduslikku kasu. Seega vastutab Anxun Information Technology Co. Ltd. märkimisväärse mõjuga küberrünnete eest, mis kujutavad välist ohtu liikmesriikidele, ning kolmandate riikide vastu suunatud rünnete eest. Wu Haibo oli seotud liikmesriikide vastaste märkimisväärse mõjuga küberründekatsete juhtimise ja neile õhutamisega. Sellel ametikohal vastutab ta märkimisväärse mõjuga küberrünnete eest, mis kujutavad välist ohtu liikmesriikidele, ning kolmandate riikide vastaste märkimisväärse mõjuga küberrünnete eest, ning on nende rünnetega seotud.	16.3.2026“

2) Jaotisse „B. Juriidilised isikud, üksused ja asutused“ lisatakse järgmised kanded.

	Nimi	Tuvastamisandmed	Põhjused	Loetellu kandmise kuupäev
„5.	Integrity Technology Group	永信至诚科技集团股份有限公司 (kirjapilt hiina keeles) Teise nimega: Beijing Integrity Technology Company Limited, Yongxin Zhicheng Technology Group Company Limited Aadress: Fenghao East Road, Room 103, Building 6, No. 9, Beijing Haidian District, China Registreerimiskoht: Peking, Hiina Registreerimise kuupäev: 2.9.2010 Ühtne sotsiaalkrediidi number: 91110108562135265P	Integrity Technology Group on Hiina Rahvavabariigis asuv küberturvalisuse ettevõte, mis hõlbustas Advanced Persistent Threat Flax Typhooniga seotud küberründeid. Nimetatud küberrühm kasutas Integrity Technology Groupi tooteid ja tehnoloogiat arvutivõrkude ärakasutamisega seotud tegevuses. Sellest ajast alates on Integrity Technology Groupi tooteid kasutatud esemevõrgu seadmete kahjustamiseks ja neile juurdepääsuks liikmesriikides, mujal Euroopa riikides ja kogu maailmas. Aastatel 2022 ja 2023 tungis Flax Typhoon Integrity Technology Groupi toodete abil vähemalt 65 600 esemevõrgu seadmesse kuues liikmesriigis. Seega kasutati Integrity Technology Groupi kaubanduslikke tooteid ja kaubandustaristut pidevalt nii liikmesriikide kui ka kolmandate riikide vastastes küberrünnetes. Mõjutades digitaristuga seotud infosüsteeme, pakub Integrity Technology Group seega tehnilist ja materiaalset tuge märkimisväärse mõjuga küberrünnetele, mis kujutavad välist ohtu liikmesriikidele ja kolmandatele riikidele.	16.3.2026

	Nimi	Tuvastamisandmed	Põhjused	Loetellu kandmise kuupäev
6.	Emennet Pasargad	Teise nimega: Anzu Team, Holy Souls, Aria Sepehr Ayandehsazan, Haywire Kitten Registreerimiskoht: Teheran, Iraan Registreerimisnumber: 554267 Peamine tegevuskoht: Teheran, Iraan	Emennet Pasargad on Iraani kübervaldkonna osaleja (äriühing), kes on rünnanud paljusid üksusi, eelkõige liikmesriikides ja Ameerika Ühendriikides (USA). Emennet Pasargad, kes tegutses varjunime „Anzu Team“ all, ründas Rootsi digitaristut ja kahjustas Rootsi SMS-teenust, mõjutades suurt hulka inimesi. Lisaks pääses üksus varjunime Holy Souls all tegutsedes juurde Prantsuse satiiriajakirja Charlie Hebdo abonentide andmebaasile ja reklaamis seda müügiks pimeveebis. Emennet Pasargad kahjustas Pariisi olümpiamängude ajal reklaamtahvleid ja kuvas nendel desinformatsioonikampaaniaid. Emennet Pasargad püüdis ka sekkuda USA 2020. aasta presidendivalimistesse, ohustades demokraatiat ja õigusriiki, hankides USA konfidentsiaalset valijateavet ja tungis loata USA meediaettevõtte arvutivõrku. Emennet Pasargad vastutab seega märkimisväärse mõjuga küberrünnete eest, mis kujutavad välist ohtu liikmesriikidele, ning kolmanda riigi vastu suunatud märkimisväärse mõjuga küberrünnete eest.	16.3.2026

	Nimi	Tuvastamisandmed	Põhjused	Loetellu kandmise kuupäev
7.	Anxun Information Technology Co. Ltd.	安洵信息技术有限公司 (kirjapilt hiina keeles) Teise nimega: i-soon Aadress: Room 1002, Qiangqiang Building, No. 1318 Qixin Road, Minhang District, Shanghai Ühtne sotsiaalkrediidi number: 91510105332025597A (Sichuani filiaal) Ühtne sotsiaalkrediidi number: 91310116561906136G (Shanghai filiaal) Veebisait: i-soon.net, isoon.net, i-soon.com.cn, isoonren.com, isoon.win Telefoninumbrid: +862161119992, +8605645893417, +8613761671735, +864000665915 E-post: shutdown@163.com, isoon2015@126.com, tao_tingting@i-soon.net, li_ping@i-soon.net	Anxun Information Technology Co. Ltd. on Hiina Rahvavabariigis asuv äriühing, mis pakub tasulisi häkkimisteenuseid. Ta on rünnanud liikmesriikide elutähtsaid taristuid ja elutähtsaid riigifunktsioone ning pääsenud juurde salastatud teabele ja müünud seda. Lisaks on Anxun Information Technology Co. Ltd. rünnanud mitme kolmanda riigi valitsusi, ohustades seeläbi liidu ühise välis- ja julgeolekupoliitika (ÜVJP) eesmärke, mis on sätestatud Euroopa Liidu lepingu artikli 21 lõike 2 punktides a–c. Anxun Information Technology Co. Ltd. saab osutatud teenustest olulist majanduslikku kasu. Seega vastutab Anxun Information Technology Co. Ltd. märkimisväärse mõjuga küberrünnete eest, mis kujutavad välist ohtu liikmesriikidele, ning kolmandate riikide vastu suunatud märkimisväärse mõjuga küberrünnete eest.	16.3.2026“