DEĊIŻJONI TAL-KUNSILL (PESK) 2020/1127

tat-30 ta' Lulju 2020

li temenda d-Deċiżjoni (PESK) 2019/797 dwar miżuri restrittivi kontra attakki ċibernetiċi li jheddu lill-Unjoni jew l-Istati Membri tagħha

IL-KUNSILL TAL-UNJONI EWROPEA,

Wara li kkunsidra t-Trattat dwar l-Unjoni Ewropea, u b'mod partikolari l-Artikolu 29 tiegħu,

Wara li kkunsidra l-proposta mir-Rappreżentant Għoli tal-Unjoni għall-Affarijiet Barranin u l-Politika ta' Sigurtà,

Billi:

(1) Fis-17 ta' Mejju 2019, il-Kunsill adotta d-Deċiżjoni (PESK) 2019/797 ([1]).

(2) Il-miżuri restrittivi mmirati kontra l-attakki ċibernetiċi b'effett sinifikanti li jikkostitwixxu theddida esterna għall-Unjoni jew għall-Istati Membri tagħha huma fost il-miżuri inklużi fil-qafas tal-Unjoni għal rispons diplomatiku konġunt għal attivitajiet ċibernetiċi malizzjużi (is-sett ta' għodod taċ-ċiberdiplomazija) u huma strument vitali biex attivitajiet bħal dawn jiġu skoraġġuti u jingħata rispons għalihom. Il-miżuri restrittivi jistgħu wkoll jiġu applikati b'rispons għal attakki ċibernetiċi b'effett sinifikanti kontra Stati terzi jew organizzazzjonijiet internazzjonali, fejn jitqiesu meħtieġa biex jintlaħqu l-objettivi tal-politika esterna u ta' sigurtà komuni stipulati fid-dispożizzjonijiet rilevanti tal-Artikolu 21 tat-Trattat dwar l-Unjoni Ewropea.

(3) Fis-16 ta' April 2018, il-Kunsill adotta konklużjonijiet li fihom ikkundanna bil-qawwa l-użu malizzjuż tat-teknoloġiji tal-informazzjoni u tal-komunikazzjoni, inkluż fl-attakki ċibernetiċi magħrufa pubblikament bħala "WannaCry" u "NotPetya", li kkawżaw ħsara u telf ekonomiku sinifikanti fl-Unjoni u lil hinn minnha. Fl-4 ta' Ottubru 2018 il-Presidenti tal-Kunsill Ewropew u tal-Kummissjoni Ewropea u r-Rappreżentant Għoli tal-Unjoni għall-Affarijiet Barranin u l-Politika ta' Sigurtà (ir-"Rappreżentant Għoli") esprimew f'dikjarazzjoni konġunta tħassib serju dwar tentattiv ta' attakk ċibernetiku maħsub li jdgħajjef l-integrità tal-Organizzazzjoni għall-Projbizzjoni ta' Armi Kimiċi (OPCW) fin-Netherlands, att aggressiv li wera disprezz lejn l-għan solenni tal-OPCW.F'dikjarazzjoni li għamel f'isem l-Unjoni fit-12 ta' April 2019, ir-Rappreżentant Għoli ħeġġeġ lill-atturi biex ma jibqgħux iwettqu attivitajiet ċibernetiċi malizzjużi maħsuba biex idgħajfu l-integrità, is-sigurtà u l-kompetittività ekonomika tal-Unjoni, inkluż atti ta' serq ta' proprjetà intellettwali ffaċilitat miċ-ċibernetika. Fost dan is-serq iffaċilitat miċ-ċibernetika hemm dak imwettaq mill-attur magħruf pubblikament bħala 'APT10' ('Advanced Persistent Threat 10').

(4) F'dan il-kuntest, u bħala prevenzjoni, skoraġġiment, deterrent u rispons għal imġiba malizzjuża kontinwa u dejjem tiżdied fiċ-ċiberspazju, jenħtieġ li sitt persuni fiżiċi u tliet entitajiet jew korpi jiġu inklużi fil-lista tal-persuni fiżiċi u ġuridiċi, entitajiet u korpi soġġetti għal miżuri restrittivi stabbilita fl-Anness għad-Deċiżjoni (PESK) 2019/797. Dawk il-persuni u entitajiet jew korpi huma responsabbli, ipprovdew appoġġ jew kienu involuti, jew iffaċilitaw, attakki ċibernetiċi jew tentattivi ta' attakki ċibernetiċi, inkluż it-tentattiv ta' attakk ċibernetiku kontra l-OPCW u l-attakki ċibernetiċi magħrufa pubblikament bħala "WannaCry" u "NotPetya", kif ukoll l-"Operation Cloud Hopper".

(5) Għalhekk jenħtieġ li d-Deċiżjoni (PESK) 2019/797 tiġi emendata skont dan,

ADOTTA DIN ID-DEĊIŻJONI:

Artikolu 1

L-Anness għad-Deċiżjoni (PESK) 2019/797 huwa emendat f'konformità mal-Anness għal din id-Deċiżjoni.

([1]) Deċiżjoni tal-Kunsill (PESK) 2019/797 tas-17 ta' Mejju 2019 dwar miżuri restrittivi kontra attakki ċibernetiċi li jheddu lill-Unjoni jew l-Istati Membri tagħha (ĠU L 129 I, 17.5.2019, p. 13).

Artikolu 2

Din id-Deċiżjoni għandha tidħol fis-seħħ fid-data tal-pubblikazzjoni tagħha f'*Il-Ġurnal Uffiċjali tal-Unjoni Ewropea*.

Magħmul fi Brussell, it-30 ta' Lulju 2020.

Għall-Kunsill
Il-President
M. ROTH

ANNESS

Il-persuni u l-entitajiet jew il-korpi li ġejjin jiżdiedu mal-lista ta' persuni fiżiċi u ġuridiċi, entitajiet u korpi li tinsab fl-Anness għad-Deċiżjoni (PESK) 2019/797:

"A. Persuni fiżiċi

	Isem	Informazzjoni identifikattiva	Raġunijiet	Data tal-elenkar
1.	GAO Qiang	Post tat-twelid: Provinċja ta' Shandong, iċ-Ċina Indirizz: Room 1102, Guanfu Mansion, 46 Xinkai Road, Hedong District, Tianjin, China Nazzjonalità: Ċiniża Sess: raġel	Gao Qianq huwa involut fl-'Operation Cloud Hopper', sensiela ta' attakki ċibernetiċi b'effett sinifikanti li joriġinaw minn barra l-Unjoni u li jikkostitwixxu theddida esterna għall- Unjoni jew l-Istati Membri tagħha, u ta' attakki ċibernetiċi b'effett sinifikanti kontra Stati terzi. L-'Operation Cloud Hopper' kellha fil-mira tagħha s-sistemi ta' informazzjoni ta' kumpanniji multinazzjonali f'sitt kontinenti, inkluż kumpanniji li jinsabu fl- Unjoni, u kisbet aċċess mhux awtorizzat għal data kummerċjali sensittiva, b'riżultat ta' telf ekonomiku sinifikanti. L-attur magħruf pubblikament bħala 'APT10' ('Advanced Persistent Threat 10' (magħruf ukoll bħala 'Red Apollo', 'CVNX', 'Stone Panda', 'MenuPass' u 'Potassium') wettaq l-'Operation Cloud Hopper'. Gao Qianq jista' jkollu rabtiet ma' APT10, inkluż permezz tal-assoċjazzjoni tiegħu mal-infrastruttura ta' kmand u kontroll ta' APT10. Barra minn hekk, Huaying Haitai, entità dežinjata li tipprovdi appoġġ u li tiffaċilita l-'Operation Cloud Hopper', impjegat lil Gao Qiang. Huwa għandu rabtiet ma' Zhang Shilong, li huwa wkoll iddežinjat b'konnessjoni mal-'Operation Cloud Hopper'. Gao Qiang huwa għalhekk assoċjat kemm ma' Huaying Haitai kif ukoll ma' Zhang Shilong.	30.7.2020
2.	ZHANG Shilong	Indirizz: Hedong, Yuyang Road No 121, Tianjin, China Nazzjonalità: Ċiniża Sess: raġel	Zhang Shilong huwa involut fl-'Operation Cloud Hopper', sensiela ta' attakki ċibernetiċi b'effett sinifikanti li joriġinaw minn barra l-Unjoni u li jikkostitwixxu theddida esterna għall-Unjoni jew l-Istati Membri tagħha, u ta' attakki ċibernetiċi b'effett sinifikanti kontra Stati terzi. L-'Operation Cloud Hopper' kellha fil-mira tagħha s-sistemi ta' informazzjoni ta' kumpanniji multinazzjonali f'sitt kontinenti, inkluż kumpanniji li jinsabu fl- Unjoni, u kisbet aċċess mhux awtorizzat għal data kummerċjali sensittiva, b'riżultat ta' telf ekonomiku sinifikanti. L-attur magħruf pubblikament bħala 'APT10' ('Advanced Persistent Threat 10') (magħruf ukoll bħala 'Red Apollo', 'CVNX', 'Stone Panda', 'MenuPass' u 'Potassium') wettaq l-'Operation Cloud Hopper'.	30.7.2020

			Zhang Shilong jista' jkollu rabtiet ma' APT10, inkluż permezz tal-malware li żviluppa u ttestja b'konnessjoni mal-attakki ċibernetiċi mwettqa minn APT10. Barra minn hekk, Huaying Haitai, entità ddeżinjata li tipprovdi appoġġ u tiffaċilita l-'Operation Cloud Hopper', impjegat lil Zhang Shilong. Huwa għandu rabtiet ma' Gao Qiang, li huwa wkoll iddeżinjat b'konnessjoni mal-'Operation Cloud Hopper'. Għalhekk Zhang Shilong huwa assoċjat kemm ma' Huaying Haitai kif ukoll ma' Gao Qiang.	
3.	Alexey Valeryevich MININ	Алексей Валерьевич МИНИН Data tat-twelid: 27 ta' Mejju 1972 Post tat-twelid: Perm Oblast, ir-Repubblika Soċjalista Federattiva Sovjetika Russa (illum il-Federazzjoni Russa) Numru tal-passaport: 120017582 Maħruġ minn: Ministeru tal-Affarijiet Barranin tal-Federazzjoni Russa Validità: mis-17 ta' April 2017 sas-17 ta' April 2022 Post: Moska, Federazzjoni Russa Nazzjonalità: Russa Sess: raġel	Alexey Minin ħa sehem fit-tentattiv ta' attakk ċibernetiku b'effett potenzjalment sinifikanti kontra l-Organizzazzjoni għall-Projbizzjoni ta' Armi Kimiċi (OPCW) fin-Netherlands. Bħala uffiċjal ta' appoġġ għall-intelligence umana tad-Direttorat Ewlieni tal-Istat Maġġur tal-Forzi Armati tal-Federazzjoni Russa (GU/GRU), Alexey Minin kien parti minn tim ta' erba' uffiċjali tal-intelligence militari Russa li f'April 2018 ippruvaw jiksbu aċċess mhux awtorizzat għan-network tal-WiFi tal-OPCW f'The Hague, in-Netherlands. L-għan tat-tentattiv ta' attakk ċibernetiku kien il-hacking tan-network tal-WiFi tal-OPCW, li kieku rnexxa kien jikkompromietti s-sigurtà tan-network u l-ħidma investigattiva li għaddejja tal-OPCW. Is-Servizz tas-Sigurtà u tal-Intelligence tad-Difiża tan-Netherlands (DISS) (Militaire Inlichtingen- en Veiligheidsdienst – MIVD) ħarbat dan it-tentattiv ta' attakk ċibernetiku, u b'hekk ipprevjena li ssir ħsara gravi lill-OPCW.	30.7.2020
4.	Aleksei Sergeyvich MORENETS	Алексей Сергеевич МОРЕНЕЦ Data tat-twelid: 31 ta' Lulju 1977 Post tat-twelid: Murmanskaya Oblast, ir-Repubblika Soċjalista Federattiva Sovjetika Russa (illum il-Federazzjoni Russa) Numru tal-passaport: 100135556 Maħruġ minn: Ministeru tal-Affarijiet Barranin tal-Federazzjoni Russa Validità: mis-17 ta' April 2017 sas-17 ta' April 2022 Post: Moska, Federazzjoni Russa Nazzjonalità: Russa Sess: raġel	Aleksei Morenets ħa sehem fit-tentattiv ta' attakk ċibernetiku b'effett potenzjalment sinifikanti kontra l-Organizzazzjoni għall-Projbizzjoni ta' Armi Kimiċi (OPCW) fin-Netherlands. Bħala uffiċjal taċ-ċibernetika għad-Direttorat Ewlieni tal-Istat Maġġur tal-Forzi Armati tal-Federazzjoni Russa (GU/GRU), Aleksei Morenets kien parti minn tim ta' erba' uffiċjali tal-intelligence militari Russa li f'April 2018 ippruvaw jiksbu aċċess mhux awtorizzat għan-network tal-WiFi tal-OPCW f'The Hague, in-Netherlands. L-għan tat-tentattiv ta' attakk ċibernetiku kien il-hacking tan-network tal-WiFi tal-OPCW, li kieku rnexxa kien jikkompromietti s-sigurtà tan-network u l-ħidma investigattiva li għaddejja tal-OPCW. Is-Servizz tas-Sigurtà u tal-Intelligence tad-Difiża tan-Netherlands (DISS) (Militaire Inlichtingen- en Veiligheidsdienst – MIVD) ħarbat dan it-tentattiv ta' attakk ċibernetiku, u b'hekk ipprevjena li ssir ħsara gravi lill-OPCW.	30.7.2020

5.	Evgenii Mikhaylovich SEREBRIAKOV	Евгений Михайлович СЕРЕБРЯКОВ Data tat-twelid: 26 ta' Lulju 1981 Post tat-twelid: Kursk, ir-Repubblika Soċjalista Federattiva Sovjetika Russa (illum il-Federazzjoni Russa) Numru tal-passaport: 100135555 Maħruġ minn: Ministeru tal-Affarijiet Barranin tal-Federazzjoni Russa Validità: mis-17 ta' April 2017 sas-17 ta' April 2022 Post: Moska, Federazzjoni Russa Nazzjonalità: Russa Sess: raġel	Evgenii Serebriakov ħa sehem fit-tentattiv ta' attakk ċibernetiku b'effett potenzjalment sinifikanti kontra l-Organizzazzjoni għall-Projbizzjoni ta' Armi Kimiċi (OPCW) fin-Netherlands. Bħala uffiċjal taċ-ċibernetika għad-Direttorat Ewlieni tal-Istat Maġġur tal-Forzi Armati tal-Federazzjoni Russa (GU/GRU), Evgenii Serebriakov kien parti minn tim ta' erba' uffiċjali tal-intelligence militari Russa li f'April 2018 ippruvaw jiksbu aċċess mhux awtorizzat għan-network tal-WiFi tal-OPCW f'The Hague, in-Netherlands. L-għan tat-tentattiv ta' attakk ċibernetiku kien il-hacking tan-network tal-WiFi tal-OPCW, li kieku rnexxa kien jikkompromietti s-sigurtà tan-network u l-ħidma investigattiva li għaddejja tal-OPCW. Is-Servizz tas-Sigurtà u tal-Intelligence tad-Difiża tan-Netherlands (DISS) (Militaire Inlichtingen- en Veiligheidsdienst – MIVD) ħarbat dan it-tentattiv ta' attakk ċibernetiku, u b'hekk ipprevjena li ssir ħsara gravi lill-OPCW.	30.7.2020
6.	Oleg Mikhaylovich SOTNIKOV	Олег Михайлович СОТНИКОВ Data tat-twelid: 24 ta' Awwissu 1972 Post tat-twelid: Ulyanovsk, ir-Repubblika Soċjalista Federattiva Sovjetika Russa (illum il-Federazzjoni Russa) Numru tal-passaport: 120018866 Maħruġ minn: Ministeru tal-Affarijiet Barranin tal-Federazzjoni Russa Validità: mis-17 ta' April 2017 sas-17 ta' April 2022 Post: Moska, Federazzjoni Russa Nazzjonalità: Russa Sess: raġel	Oleg Sotnikov ħa sehem fit-tentattiv ta' attakk ċibernetiku b'effett potenzjalment sinifikanti kontra l-Organizzazzjoni għall-Projbizzjoni ta' Armi Kimiċi (OPCW) fin-Netherlands. Bħala uffiċjal ta' appoġġ għall-intelligence umana tad-Direttorat Ewlieni tal-Istat Maġġur tal-Forzi Armati tal-Federazzjoni Russa (GU/GRU), Oleg Sotnikov kien parti minn tim ta' erba' uffiċjali tal-intelligence militari Russa li f'April 2018 ippruvaw jiksbu aċċess mhux awtorizzat għan-network tal-WiFi tal-OPCW f'The Hague, in-Netherlands. L-għan tat-tentattiv ta' attakk ċibernetiku kien il-hacking tan-network tal-WiFi tal-OPCW, li kieku rnexxa kien jikkompromietti s-sigurtà tan-network u l-ħidma investigattiva li għaddejja tal-OPCW. Is-Servizz tas-Sigurtà u tal-Intelligence tad-Difiża tan-Netherlands (DISS) (Militaire Inlichtingen- en Veiligheidsdienst – MIVD) ħarbat dan it-tentattiv ta' attakk ċibernetiku, u b'hekk ipprevjena li ssir ħsara gravi lill-OPCW.	30.7.2020

B. Persuni ġuridiċi, entitajiet u korpi

	Isem	Informazzjoni identifikattiva	Raġunijiet	Data tal-elenkar
1.	Tianjin Huaying Haitai Science and Technology Development Co. Ltd (Huaying Haitai)	Magħrufa wkoll bħala: Haitai Technology Development Co. Ltd Post: Tianjin, iċ-Ċina	Huaying Haitai pprovdiet appoġġ finanzjarju, tekniku jew materjali, u ffaċilitat, l-'Operation Cloud Hopper', sensiela ta' attakki ċibernetiċi b'effett sinifikanti li joriġinaw minn barra l-Unjoni u jikkostitwixxu theddida esterna għall- Unjoni jew għall-Istati Membri tagħha, u ta' attakki ċibernetiċi b'effett sinifikanti kontra Stati terzi.	30.7.2020

			L-‘Operation Cloud Hopper’ kellha fil-mira tagħha s-sistemi ta’ informazzjoni ta’ kumpanniji multinazzjonali f’sitt kontinenti, inkluż kumpanniji li jinsabu fl- Unjoni, u kisbet aċċess mhux awtorizzat għal data kummerċjali sensittiva, b’riżultat ta’ telf ekonomiku sinifikanti. L-attur magħruf pubblikament bħala ‘APT10’ (‘Advanced Persistent Threat 10’) (magħruf ukoll bħala ‘Red Apollo’, ‘CVNX’, ‘Stone Panda’, ‘MenuPass’ u ‘Potassium’) wettaq l-‘Operation Cloud Hopper’. Huaying Haitai jista’ jkollha rabtiet ma’ APT10. Barra minn hekk, Huaying Haitai impjegat lil Gao Qiang u Zhang Shilong, li t-tnejn huma dežinjati b’rabta mal-‘Operation Cloud Hopper’. Għaldaqstant, Huaying Haitai hija assoċjata ma’ Gao Qiang u Zhang Shilong.	
2.	Chosun Expo	Magħrufa wkoll bħala: Chosen Expo; Korea Export Joint Venture Post: RDPK	Chosun Expo pprovdiet appoġġ finanzjarju, tekniku jew materjali, u ffaċilitat, sensiela ta’ attakki ċibernetiċi b’effett sinifikanti li joriġinaw minn barra l-Unjoni u jikkostitwixxu theddida esterna għall- Unjoni jew għall-Istati Membri tagħha, u ta’ attakki ċibernetiċi b’effett sinifikanti kontra Stati terzi, inkluż l-attakki ċibernetiċi magħrufa pubblikament bħala ‘WannaCry’ u l-attakki ċibernetiċi kontra l-Awtorità Pollakka tas-Superviżjoni Finanzjarja u Sony Pictures Entertainment, kif ukoll serq ċibernetiku mill-Bangladesh Bank u tentattiv ta’ serq ċibernetiku mill-Vietnam Tien Phong Bank. ‘WannaCry’ fixkel is-sistemi tal-informazzjoni madwar id-dinja permezz ta’ ransomware mmirat lejn is-sistemi ta’ informazzjoni u billi waqqaf l-aċċess għad-data. Huwa affettwa s-sistemi tal-informazzjoni ta’ kumpanniji fl-Unjoni, inkluż sistemi ta’ informazzjoni marbuta ma’ servizzi meħtieġa għaż-żamma ta’ servizzi essenzjali u attivitajiet ekonomiċi fl-Istati Membri. L-attur magħruf pubblikament bħala ‘APT38’ (‘Advanced Persistent Threat 38’) jew il-‘Lazarus Group’ wettaq ‘WannaCry’. Chosun Expo jista’ jkollha rabtiet ma’ APT38/il-Lazarus Group, inkluż permezz tal-kontijiet użati għall-attakki ċibernetiċi.	30.7.2020
3.	Main Centre for Special Technologies (iċ-Ċentru Ewlieni għat-Teknoloġiji Speċjali) (GTsST) tad-Direttorat Ewlieni tal-Istat Maġġur tal-Forzi Armati tal-Federazzjoni Russa (GU/GRU)	22 Kirova Street, Moscow, Russian Federation	Iċ-Ċentru Ewlieni għat-Teknoloġiji Speċjali (GTsST) tad-Direttorat Ewlieni tal-Istat Maġġur tal-Forzi Armati tal-Federazzjoni Russa (GU/GRU), magħruf ukoll bin-numru tal-posta militari tiegħu 74455, huwa responsabbli għal attakki ċibernetiċi b’effett sinifikanti li joriġinaw minn barra l-Unjoni u li jikkostitwixxu theddida esterna għall- Unjoni jew għall-Istati Membri tagħha, u għal attakki ċibernetiċi b’effett sinifikanti kontra Stati terzi, inkluż l-attakki ċibernetiċi magħrufa pubblikament bħala ‘NotPetya’ jew ‘EternalPetya’ f’Ġunju 2017 u l-attakki ċibernetiċi diretti kontra l-grilja tal-enerġija Ukrena fix-xitwa tal-2015 u l-2016.	30.7.2020”.

			'NotPetya' jew 'EternalPetya' rendew id-data inaċċessibbli f'għadd ta' kumpanniji fl- Unjoni, fl-Ewropa inġenerali u madwar id-dinja, billi attakkaw kompjuters b'ransomware u waqqfu l-aċċess għad-data, b'riżultat ta' telf ekonomiku sinifikanti, fost l-oħrajn. L-attakk ċibernetiku fuq il-grilja tal-enerġija Ukrena wassal biex partijiet minnha ntfew matul ix-xitwa. L-attur magħruf pubblikament bħala Sandworm (magħruf ukoll bħala 'Sandworm Team', 'BlackEnergy Group', 'Voodoo Bear', 'Quedagh', 'Olympic Destroyer' u 'Telebots'), li huwa wkoll responsabbli għall-attakk fuq il-grilja tal-enerġija Ukrena, wettaq 'NotPetya' jew 'EternalPetya'. Iċ-Ċentru Ewlieni għat-Teknoloġiji Speċjali tad-Direttorat Ewlieni tal-Istat Maġġur tal-Forzi Armati tal-Federazzjoni Russa jaqdi rwol attiv fl-attivitajiet ċibernetiċi mwettqa minn Sandworm u jista' jkollu rabtiet ma' Sandworm.	