►**B**

DECISIONE (PESC) 2019/797 DEL CONSIGLIO

del 17 maggio 2019

concernente misure restrittive contro gli attacchi informatici che minacciano l'Unione o i suoi Stati membri

(GU L 129I del 17.5.2019, pag. 13)

Modificata da:

		Gazzetta ufficiale		
		n.	pag.	data
►**M1**	Decisione (PESC) 2020/651 del Consiglio del 14 maggio 2020	L 153	4	15.5.2020
►**M2**	Decisione (PESC) 2020/1127 del Consiglio del 30 luglio 2020	L 246	12	30.7.2020

Rettificata da:

►**C1** Rettifica, GU L 230 del 17.7.2020, pag. 36 (2019/797)

▼B

DECISIONE (PESC) 2019/797 DEL CONSIGLIO

del 17 maggio 2019

concernente misure restrittive contro gli attacchi informatici che minacciano l'Unione o i suoi Stati membri

Articolo 1

1. La presente decisione si applica agli attacchi informatici con effetti significativi, inclusi tentati attacchi informatici con effetti potenzialmente significativi, che costituiscono una minaccia esterna per l'Unione o i suoi Stati membri.

2. Gli attacchi informatici che costituiscono una minaccia esterna includono quelli che:

a) provengono o sono sferrati dall'esterno dell'Unione;

b) impiegano infrastrutture esterne all'Unione;

c) sono compiuti da una persona fisica o giuridica, un'entità o un organismo stabiliti o operanti al di fuori dell'Unione; o

d) sono commessi con il sostegno, sotto la direzione o sotto il controllo di una persona fisica o giuridica, un'entità o un organismo operanti al di fuori dell'Unione.

3. A tal fine, gli attacchi informatici sono azioni che comportano:

a) accesso a sistemi di informazione;

b) interferenza in sistemi di informazione;

c) interferenza in dati; o

d) intercettazione di dati,

qualora tali azioni non siano debitamente autorizzate dal proprietario o da un altro titolare di diritti sul sistema o sui dati o su parte di essi ovvero non siano consentite a norma del diritto dell'Unione o dello Stato membro interessato.

4. Gli attacchi informatici che costituiscono una minaccia per gli Stati membri comprendono quelli che incidono su sistemi di informazione relativi, tra l'altro, a:

a) infrastrutture critiche, compresi i cavi sottomarini e gli oggetti lanciati nello spazio extratmosferico, essenziali per il mantenimento di funzioni vitali della società o della salute, dell'incolumità, della sicurezza e del benessere economico o sociale della popolazione;

b) servizi necessari per il mantenimento di attività sociali e/o economiche fondamentali, in particolare nei settori dell'energia (energia elettrica, petrolio e gas); trasporti (aerei, ferroviari, per idrovia e stradali); settore bancario; infrastrutture dei mercati finanziari; settore sanitario (prestatori di assistenza sanitaria, ospedali e cliniche private);

▼B

fornitura e distribuzione di acqua potabile; infrastrutture digitali, e qualsiasi altro settore che sia essenziale per lo Stato membro interessato;

c) funzioni statali essenziali, in particolare nei settori della difesa, della governance e del funzionamento di istituzioni, anche per elezioni pubbliche o per la procedura elettorale, del funzionamento di infrastrutture economiche e civili, della sicurezza interna e delle relazioni esterne, anche attraverso missioni diplomatiche;

d) conservazione o trattamento di informazioni classificate; o

e) squadre di pronto intervento governative.

5. Gli attacchi informatici, che costituiscono una minaccia per l'Unione, comprendono quelli sferrati contro le sue istituzioni, i suoi organi e organismi, le sue delegazioni presso paesi terzi o organizzazioni internazionali, le sue operazioni e missioni di politica di sicurezza e di difesa comune (PSDC) e i suoi rappresentanti speciali.

6. Ove ritenuto necessario ai fini del conseguimento degli obiettivi della PESC enunciati nelle pertinenti disposizioni dell'articolo 21 del trattato sull'Unione europea, è possibile applicare misure restrittive a norma della presente decisione anche in risposta ad attacchi informatici con effetti significativi nei confronti di Stati terzi o organizzazioni internazionali.

Articolo 2

Ai fini della presente decisione si applicano le seguenti definizioni:

a) «sistemi di informazione»: dispositivo o gruppo di dispositivi interconnessi o collegati, uno o più dei quali eseguono, in base ad un programma, un trattamento automatico di dati digitali, nonché i dati digitali conservati, trattati, estratti o trasmessi da tale dispositivo o gruppo di dispositivi ai fini del loro funzionamento, del loro uso, della loro protezione e della loro manutenzione;

b) «interferenza in un sistema di informazione»: il fatto di ostacolare o interrompere il funzionamento di un sistema di informazione inserendo, trasmettendo, danneggiando, cancellando, deteriorando, alterando, sopprimendo o rendendo inaccessibili dati digitali;

c) «interferenza in dati»: il fatto di cancellare, danneggiare, deteriorare, alterare o sopprimere dati digitali contenuti in un sistema di informazione o di rendere tali dati inaccessibili; comprende inoltre il furto di dati, fondi, risorse economiche o proprietà intellettuale;

d) «intercettazione di dati»: il fatto di intercettare, tramite strumenti tecnici, trasmissioni non pubbliche di dati digitali verso, da o all'interno di un sistema di informazione, incluse le emissioni elettromagnetiche provenienti da un sistema di informazione contenente tali dati digitali.

▼B

Articolo 3

I fattori che determinano se un attacco informatico ha effetti significativi di cui all'articolo 1, paragrafo 1, comprendono:

a) portata, entità, impatto o gravità delle turbative causate, anche per quanto riguarda le attività economiche e sociali, i servizi essenziali, le funzioni statali essenziali, l'ordine pubblico o la sicurezza pubblica;

b) numero di persone fisiche o giuridiche, entità o organismi interessati;

c) numero di Stati membri interessati;

d) importo della perdita economica causata per esempio mediante furti su larga scala di fondi, risorse economiche o proprietà intellettuale;

e) vantaggio economico ottenuto dall'autore dell'atto per se stesso o per terzi;

f) quantità o natura dei dati oggetto del furto o entità delle violazioni dei dati; o

g) natura dei dati sensibili sotto il profilo commerciale cui si è avuto accesso.

Articolo 4

1. Gli Stati membri adottano le misure necessarie per impedire l'ingresso o il transito nello loro territorio di:

a) persone fisiche responsabili di attacchi informatici o tentati attacchi informatici;

b) persone fisiche che forniscono sostegno finanziario, tecnico o materiale per attacchi informatici o tentati attacchi informatici, o che sono altrimenti coinvolti in tali attacchi o tentati attacchi, anche pianificandoli, preparandoli, partecipandovi, dirigendoli, assistendoli o incoraggiandoli, oppure agevolandoli per azione o omissione;

c) persone fisiche associate a persone di cui alle lettere a) e b);

elencate nell'allegato.

2. Il paragrafo 1 non obbliga gli Stati membri a vietare ai loro cittadini l'ingresso nel proprio territorio.

3. Il paragrafo 1 lascia impregiudicate le situazioni in cui uno Stato membro sia vincolato da un obbligo derivante dal diritto internazionale, segnatamente:

a) in qualità di paese che ospita un'organizzazione intergovernativa internazionale;

b) in qualità di paese che ospita una conferenza internazionale convocata dalle Nazioni Unite o sotto gli auspici di questa organizzazione;

c) in virtù di un accordo multilaterale che conferisce privilegi e immunità; o

d) in virtù del trattato di conciliazione del 1929 (Patti Lateranensi) concluso tra la Santa Sede (Stato della Città del Vaticano) e l'Italia.

▼B

4. Il paragrafo 3 è considerato di applicazione anche qualora uno Stato membro ospiti l'Organizzazione per la sicurezza e la cooperazione in Europa (OSCE).

5. Il Consiglio è debitamente informato in ciascuna delle situazioni in cui uno Stato membro concede una deroga a norma del paragrafo 3 o 4.

6. Gli Stati membri possono concedere deroghe alle misure stabilite a norma del paragrafo 1 allorquando il viaggio è giustificato da ragioni umanitarie urgenti o dall'esigenza di partecipare a riunioni intergovernative o a riunioni promosse o ospitate dall'Unione o ospitate da uno Stato membro che esercita la presidenza di turno dell'OSCE, in cui si conduce un dialogo politico che promuove direttamente gli obiettivi politici delle misure restrittive, compresa la sicurezza e la stabilità nel ciberspazio.

7. Gli Stati membri possono anche concedere deroghe alle misure stabilite a norma del paragrafo 1 quando l'ingresso o il transito è necessario per l'espletamento di un procedimento giudiziario.

8. Uno Stato membro che intenda concedere le deroghe di cui al paragrafo 6 o 7 presenta al riguardo una notifica scritta al Consiglio. La deroga si considera concessa a meno che, entro due giorni lavorativi dalla ricezione della notifica della deroga proposta, vi sia un'obiezione scritta di uno o più membri del Consiglio. Se uno o più membri del Consiglio sollevano obiezioni, il Consiglio, deliberando a maggioranza qualificata, può decidere di concedere la deroga proposta.

9. Qualora uno Stato membro autorizzi, a norma dei paragrafi 3, 4, 6, 7 o 8, l'ingresso o il transito nel suo territorio delle persone elencate nell'allegato, l'autorizzazione è strettamente limitata ai fini per i quali è concessa e alle persone direttamente interessate.

Articolo 5

1. Sono congelati tutti i fondi e le risorse economiche appartenenti a, posseduti, detenuti o controllati da:

a) persone fisiche o giuridiche, entità o organismi che sono responsabili di attacchi informatici o tentati attacchi informatici;

b) persone fisiche o giuridiche, entità o organismi che forniscono sostegno finanziario, tecnico o materiale per attacchi informatici o tentati attacchi informatici, o che sono altrimenti coinvolti in tali attacchi o tentati attacchi, anche pianificandoli, preparandoli, partecipandovi, dirigendoli, assistendoli o incoraggiandoli, oppure agevolandoli per azione o omissione;

c) persone fisiche o giuridiche, entità o organismi associati a persone fisiche o giuridiche, entità o organismi di cui alle lettere a) e b);

elencati nell'allegato.

▼B

2. Non sono messi a disposizione delle persone fisiche o giuridiche, delle entità e degli organismi elencati nell'allegato, direttamente o indirettamente, fondi o risorse economiche, né sono destinati a loro vantaggio.

3. In deroga ai paragrafi 1 e 2, le autorità competenti degli Stati membri possono autorizzare lo svincolo di taluni fondi o risorse economiche congelati o la messa a disposizione di taluni fondi o risorse economiche, alle condizioni che ritengono appropriate, dopo aver accertato che i fondi o le risorse economiche in questione sono:

a) ►C1 necessari per soddisfare le esigenze di base delle persone fisiche o giuridiche, delle entità o degli organismi elencati nell'allegato ◄ e dei familiari a loro carico, compresi i pagamenti relativi a generi alimentari, locazioni o ipoteche, medicinali e cure mediche, imposte, premi assicurativi e utenza di servizi pubblici;

b) destinati esclusivamente al pagamento di onorari ragionevoli o al rimborso delle spese sostenute per la prestazione di servizi legali;

c) destinati esclusivamente al pagamento di diritti o spese connessi alla normale gestione o alla custodia dei fondi o delle risorse economiche congelati;

d) necessari per coprire spese straordinarie, a condizione che la pertinente autorità competente abbia notificato alle autorità competenti degli altri Stati membri e alla Commissione, almeno due settimane prima dell'autorizzazione, i motivi per i quali ritiene che debba essere concessa una determinata autorizzazione; o

e) pagabili su o da un conto di una missione diplomatica o consolare o di un'organizzazione internazionale che gode di immunità in conformità del diritto internazionale, nella misura in cui tali pagamenti servono per scopi ufficiali della missione diplomatica o consolare o dell'organizzazione internazionale.

Lo Stato membro interessato informa gli altri Stati membri e la Commissione di ogni autorizzazione concessa ai sensi del presente paragrafo.

4. In deroga al paragrafo 1, le autorità competenti degli Stati membri possono autorizzare lo svincolo di taluni fondi o risorse economiche congelati a condizione che:

a) i fondi o le risorse economiche siano oggetto di una decisione arbitrale emessa anteriormente alla data dell'inserimento della persona fisica o giuridica, dell'entità o dell'organismo di cui al paragrafo 1 nell'elenco figurante nell'allegato, o siano oggetto di una decisione giudiziaria o amministrativa emessa nell'Unione, o di una decisione giudiziaria esecutiva nello Stato membro interessato, prima o dopo tale data;

▼B

b) i fondi o le risorse economiche siano usati esclusivamente per soddisfare i crediti garantiti da tale decisione o siano riconosciuti validi dalla stessa, entro i limiti fissati dalle leggi e dai regolamenti applicabili che disciplinano i diritti dei creditori;

c) la decisione non vada a favore di una persona fisica o giuridica, di un'entità o di un organismo elencati nell'allegato; e

d) il riconoscimento della decisione non sia contrario all'ordine pubblico dello Stato membro interessato.

Lo Stato membro interessato informa gli altri Stati membri e la Commissione di ogni autorizzazione concessa ai sensi del presente paragrafo.

5. Il paragrafo 1 non osta a che una persona fisica o giuridica, un'entità o un organismo elencati nell'allegato effettuino un pagamento dovuto nell'ambito di un contratto concluso prima della data in cui la persona fisica o giuridica, l'entità o l'organismo sono stati inseriti nell'allegato, purché lo Stato membro interessato abbia determinato che il pagamento non è percepito, direttamente o indirettamente, da una persona fisica o giuridica, da un'entità o da un organismo di cui al paragrafo 1.

6. Il paragrafo 2 non si applica al versamento sui conti congelati di:

a) interessi o altri profitti dovuti su detti conti;

b) pagamenti dovuti nel quadro di contratti, accordi o obblighi conclusi o sorti anteriormente alla data in cui tali conti sono stati assoggettati alle misure di cui ai paragrafi 1 e 2; o

c) pagamenti dovuti nel quadro di decisioni giudiziarie, amministrative o arbitrali emesse nell'Unione o esecutive nello Stato membro interessato,

purché tali interessi, altri profitti e pagamenti continuino a essere soggetti alle misure di cui al paragrafo 1.

Articolo 6

1. Il Consiglio, deliberando all'unanimità su proposta di uno Stato membro o dell'alto rappresentante dell'Unione per gli affari esteri e la politica di sicurezza, predispone e modifica l'elenco riportato nell'allegato.

2. Il Consiglio trasmette la decisione di cui al paragrafo 1, compresi i motivi dell'inserimento nell'elenco, alla persona fisica o giuridica, all'entità o all'organismo interessati direttamente, se l'indirizzo è noto, o mediante la pubblicazione di un avviso, offrendo a tale persona fisica o giuridica, entità o organismo la possibilità di presentare osservazioni.

3. Qualora siano presentate osservazioni o siano addotte nuove prove sostanziali, il Consiglio riesamina la decisione di cui al paragrafo 1 e ne informa di conseguenza la persona fisica o giuridica, l'entità o l'organismo interessati.

▼B

Articolo 7

1. L'allegato include i motivi dell'inserimento nell'elenco delle persone fisiche e giuridiche, delle entità e degli organismi di cui agli articoli 4 e 5.

2. Nell'allegato figurano, ove disponibili, le informazioni necessarie per identificare le persone fisiche o giuridiche, le entità o gli organismi interessati. Per le persone fisiche, tali informazioni possono includere: i nomi e gli pseudonimi; la data e il luogo di nascita; la cittadinanza; i numeri del passaporto e della carta d'identità; il sesso; l'indirizzo, se noto; e la funzione o professione. Per le persone giuridiche, le entità o gli organismi, tali informazioni possono comprendere le denominazioni, la data e il luogo di registrazione, il numero di registrazione e la sede di attività.

Articolo 8

Non è soddisfatta alcuna richiesta in relazione a contratti o operazioni sulla cui esecuzione hanno inciso, direttamente o indirettamente, integralmente o in parte, le misure istituite ai sensi della presente decisione, comprese richieste di indennizzo o richieste analoghe, per esempio richieste di compensazione o richieste nel quadro di una garanzia, in particolare richieste volte a ottenere la proroga o il pagamento di una garanzia o di una controgaranzia, in particolare di una garanzia o controgaranzia finanziaria, indipendentemente dalla sua forma, se la richiesta è presentata da:

a) persone fisiche o giuridiche, entità o organismi designati elencati nell'allegato;

b) qualsiasi persona fisica o giuridica, entità o organismo che agisca per tramite o per conto di una persona fisica o giuridica, un'entità o un organismo di cui alla lettera a).

Articolo 9

Per massimizzare l'impatto delle misure stabilite dalla presente decisione, l'Unione incoraggia i paesi terzi ad adottare misure restrittive analoghe a quelle previste nella presente decisione.

▼M1

Articolo 10

La presente decisione si applica fino al 18 maggio 2021 ed è costantemente riesaminata. È prorogata o modificata, a seconda del caso, se il Consiglio ritiene che i suoi obiettivi non siano stati raggiunti.

▼B

Articolo 11

La presente decisione entra in vigore il giorno successivo alla pubblicazione nella *Gazzetta ufficiale dell'Unione europea*.

▼B

ALLEGATO

Elenco delle persone fisiche e giuridiche, delle entità e degli organismi di cui agli articoli 4 e 5

▼M2

A. Persone fisiche

	Nome	Informazioni identificative	Motivi	Data di inserimento nell'elenco
1.	GAO Qiang	Luogo di nascita: Shandong Province, Cina Indirizzo: Room 1102, Guanfu Mansion, 46 Xinkai Road, Hedong District, Tianjin, Cina Cittadinanza: cinese Sesso: maschile	Gao Qiang è coinvolto nella campagna «Operation Cloud Hopper», una serie di attacchi informatici con effetti significativi che proviene dall'esterno dell'Unione e costituisce una minaccia esterna per l'Unione o i suoi Stati membri e di attacchi informatici con effetti significativi nei confronti di Stati terzi. La campagna «Operation Cloud Hopper» ha preso di mira i sistemi di informazione di imprese multinazionali in sei continenti, tra cui imprese situate nell'Unione, e ha ottenuto l'accesso non autorizzato a dati sensibili sotto il profilo commerciale, causando perdite economiche significative. Il soggetto noto pubblicamente come «APT10» («Advanced Persistent Threat 10») (alias «Red Apollo», «CVNX», «Stone Panda», «MenuPass» e «Potassium») ha condotto la campagna «Operation Cloud Hopper». Gao Qiang può essere collegato all'APT10, anche attraverso la sua associazione con l'infrastruttura di comando e controllo di APT10. Inoltre, Huaying Haitai, un'entità designata per il fatto di fornire sostegno e agevolare la campagna «Operation Cloud Hopper», ha impiegato Gao Qiang. Quest'ultimo ha legami con Zhang Shilong, la cui designazione è altresì connessa alla campagna «Operation Cloud Hopper». Gao Qiang è pertanto associato sia a Huaying Haitai che a Zhang Shilong.	30.7.2020
2.	ZHANG Shilong	Indirizzo: Hedong, Yuyang Road No 121, Tianjin, Cina Cittadinanza: cinese Sesso: maschile	Zhang Shilong è coinvolto nella campagna «Operation Cloud Hopper», una serie di attacchi informatici con effetti significativi che proviene dall'esterno dell'Unione e costituisce una minaccia esterna per l'Unione o i suoi Stati membri e di attacchi informatici con effetti significativi nei confronti di Stati terzi.	30.7.2020

▼M2

	Nome	Informazioni identificative	Motivi	Data di inserimento nell'elenco
			La campagna «Operation Cloud Hopper» ha preso di mira i sistemi di informazione di imprese multinazionali in sei continenti, tra cui imprese situate nell'Unione, e ha ottenuto l'accesso non autorizzato a dati sensibili sotto il profilo commerciale, causando perdite economiche significative. Il soggetto noto pubblicamente come «APT10» («Advanced Persistent Threat 10») (alias «Red Apollo», «CVNX», «Stone Panda», «MenuPass» e «Potassium») ha condotto la campagna «Operation Cloud Hopper». Zhang Shilong può essere collegato all'APT10, anche attraverso il malware che ha sviluppato e testato in relazione agli attacchi informatici condotti dall'APT10. Inoltre, Huaying Haitai, un'entità designata per il fatto di fornire sostegno e agevolare la campagna «Operation Cloud Hopper», ha impiegato Zhang Shilong. Quest'ultimo ha legami con Gao Qiang, la cui designazione è altresì connessa alla campagna «Operation Cloud Hopper». Zhang Shilong è pertanto associato sia a Huaying Haitai che a Gao Qiang.	
3.	Alexey Valeryevich MININ	Алексей Валерьевич МИНИН Data di nascita: 27 maggio 1972 Luogo di nascita: Perm Oblast, RSFS russa (ora Federazione russa) Passaporto n.: 120017582 Rilasciato da: ministero degli Affari esteri della Federazione russa Validità: dal 17 aprile 2017 al 17 aprile 2022 Luogo: Mosca, Federazione russa Cittadinanza: russa Sesso: maschile	Alexey Minin ha partecipato a un tentativo di attacco informatico con effetti potenzialmente significativi contro l'Organizzazione per la proibizione delle armi chimiche (OPCW) nei Paesi Bassi. In qualità di agente di supporto dell'intelligence della direzione principale dello Stato maggiore delle forze armate della Federazione russa (GU/GRU), Alexey Minin faceva parte di una squadra di quattro agenti dell'intelligence militare russa che hanno cercato di ottenere un accesso non autorizzato alla rete Wi-Fi dell'OPCW all'Aia (Paesi Bassi) nell'aprile 2018. Il tentativo di attacco informatico era finalizzato a ottenere un accesso abusivo alla rete Wi-Fi dell'OPCW, che, in caso di successo, avrebbe compromesso la sicurezza della rete e i lavori di indagine dell'OPCW in corso. Il Servizio di intelligence e sicurezza militare dei Paesi Bassi (*Militaire Inlichtingen- en Veiligheidsdienst*— MIVD) ha sventato il tentativo di attacco informatico, impedendo in tal modo gravi danni all'OPCW.	30.7.2020

▼M2

	Nome	Informazioni identificative	Motivi	Data di inserimento nell'elenco
4.	Aleksei Sergeyvich MORENETS	Алексей Сергеевич МОРЕНЕЦ Data di nascita: 31 luglio 1977 Luogo di nascita: Murmanskaya Oblast, RSFS russa (ora Federazione russa) Passaporto n.: 100135556 Rrilasciato da: ministero degli Affari esteri della Federazione russa Validità: dal 17 aprile 2017 al 17 aprile 2022 Luogo: Mosca, Federazione russa Cittadinanza: russa Sesso: maschile	Aleksei Morenets ha partecipato a un tentativo di attacco informatico con effetti potenzialmente significativi contro l'Organizzazione per la proibizione delle armi chimiche (OPCW) nei Paesi Bassi. In qualità di operatore informatico della direzione principale dello Stato maggiore delle forze armate della Federazione russa (GU/GRU), Aleksei Morenets faceva parte di una squadra di quattro agenti dell'intelligence militare russa che hanno cercato di ottenere un accesso non autorizzato alla rete Wi-Fi dell'OPCW all'Aia (Paesi Bassi) nell'aprile 2018. Il tentativo di attacco informatico era finalizzato a ottenere un accesso abusivo alla rete Wi-Fi dell'OPCW, che, in caso di successo, avrebbe compromesso la sicurezza della rete e i lavori di indagine dell'OPCW in corso. Il Servizio di intelligence e sicurezza militare dei Paesi Bassi (*Militaire Inlichtingen- en Veiligheidsdienst*— MIVD) ha sventato il tentativo di attacco informatico, impedendo in tal modo gravi danni all'OPCW.	30.7.2020
5.	Evgenii Mikhaylovich MORENETS	Евгений Михайлович СЕРЕБРЯКОВ Data di nascita: 26 luglio 1981 Luogo di nascita: Kursk, RSFS russa (ora Federazione russa) Passaporto n.: 100135555 R ilasciato dal ministero degli Affari esteri della Federazione russa Validità: dal 17 aprile 2017 al 17 aprile 2022 Luogo: Mosca, Federazione russa Cittadinanza: russa Sesso: maschile	Evgenii Serebriakov ha partecipato a un tentativo di attacco informatico con effetti potenzialmente significativi contro l'Organizzazione per la proibizione delle armi chimiche (OPCW) nei Paesi Bassi. In qualità di operatore informatico della direzione principale dello Stato maggiore delle forze armate della Federazione russa (GU/GRU), Evgenii Serebriakov faceva parte di una squadra di quattro agenti dell'intelligence militare russa che hanno cercato di ottenere un accesso non autorizzato alla rete Wi-Fi dell'OPCW all'Aia (Paesi Bassi) nell'aprile 2018. Il tentativo di attacco informatico era finalizzato a ottenere un accesso abusivo alla rete Wi-Fi dell'OPCW, che, in caso di successo, avrebbe compromesso la sicurezza della rete e i lavori di indagine dell'OPCW in corso. Il Servizio di intelligence e sicurezza militare dei Paesi Bassi (*Militaire Inlichtingen- en Veiligheidsdienst*— MIVD) ha sventato il tentativo di attacco informatico, impedendo in tal modo gravi danni all'OPCW.	30.7.2020

▼M2

	Nome	Informazioni identificative	Motivi	Data di inserimento nell'elenco
6.	Oleg Mikhaylovich SOTNIKOV	Олег Михайлович СОТНИКОВ Data di nascita: 24 agosto 1972 Luogo di nascita: Ulyanovsk, RSFS russa (ora Federazione russa) Passaporto n.: 120018866 Rilasciato dal ministero degli Affari esteri della Federazione russa Validità: dal 17 aprile 2017 al 17 aprile 2022 Luogo: Mosca, Federazione russa Cittadinanza: russa Sesso: maschile	Oleg Sotnikov ha partecipato a un tentativo di attacco informatico con effetti potenzialmente significativi contro l'Organizzazione per la proibizione delle armi chimiche (OPCW) nei Paesi Bassi. In qualità di agente di supporto dell'intelligence della direzione principale dello Stato maggiore delle forze armate della Federazione russa (GU/GRU), Oleg Sotnikov faceva parte di una squadra di quattro agenti dell'intelligence militare russa che hanno cercato di ottenere un accesso non autorizzato alla rete Wi-Fi dell'OPCW all'Aia (Paesi Bassi) nell'aprile 2018. Il tentativo di attacco informatico era finalizzato a ottenere un accesso abusivo alla rete Wi-Fi dell'OPCW, che, in caso di successo, avrebbe compromesso la sicurezza della rete e i lavori di indagine dell'OPCW in corso. Il Servizio di intelligence e sicurezza militare dei Paesi Bassi (*Militaire Inlichtingen- en Veiligheidsdienst*— MIVD) ha sventato il tentativo di attacco informatico, impedendo in tal modo gravi danni all'OPCW.	30.7.2020

B. Persone giuridiche, entità e organismi

	Nome	Informazioni identificative	Motivi	Data di inserimento nell'elenco
1.	Tianjin Huaying Haitai Science and Technology Development Co. Ltd (Huaying Haitai)	Alias: Haitai Technology Development Co. Ltd Ubicazione: Tianjin, Cina	Huaying Haitai ha fornito sostegno finanziario, tecnico o materiale e ha agevolato la campagna «Operation Cloud Hopper», una serie di attacchi informatici con effetti significativi, che proviene dall'esterno dell'Unione e costituisce una minaccia esterna per l'Unione o i suoi Stati membri e di attacchi informatici con effetti significativi nei confronti di Stati terzi.	30.7.2020

▼M2

	Nome	Informazioni identificative	Motivi	Data di inserimento nell'elenco
			La campagna «Operation Cloud Hopper» ha preso di mira i sistemi di informazione di imprese multinazionali in sei continenti, tra cui imprese situate nell'Unione, e ha ottenuto l'accesso non autorizzato a dati sensibili sotto il profilo commerciale, causando perdite economiche significative. Il soggetto noto pubblicamente come «APT10» («Advanced Persistent Threat 10») (alias «Red Apollo», «CVNX», «Stone Panda», «MenuPass» e «Potassium») ha condotto la campagna «Operation Cloud Hopper». Huaying Haitai può essere collegata all'APT10. Inoltre, Huaying Haitai impiegava Gao Qiang e Zhang Shilong, entrambi designati in relazione alla campagna «Operation Cloud Hopper». Huaying Haitai è pertanto associata sia a Gao Qiang che a Zhang Shilong.	
2.	Chosun Expo	Alias: Chosen Expo; Korea Export Joint Venture Ubicazione: RPDC	Chosun Expo ha fornito sostegno finanziario, tecnico o materiale e ha agevolato una serie di attacchi informatici con effetti significativi, che proviene dall'esterno dell'Unione e costituisce una minaccia esterna per l'Unione o i suoi Stati membri e di attacchi informatici con effetti significativi nei confronti di Stati terzi, compresi gli attacchi informatici pubblicamente noti come «WannaCry» e gli attacchi informatici contro l'autorità di vigilanza finanziaria polacca e Sony Pictures Entertainment, nonché il furto informatico alla Bangladesh Bank e il tentativo di furto informatico alla Vietnam Tien Phong Bank. «WannaCry» ha causato perturbazioni a sistemi informatici in diverse parti del mondo compromettendo i sistemi di informazione con ransomware e bloccando l'accesso ai dati. Ha colpito i sistemi di informazione di imprese nell'Unione, compresi quelli relativi ai servizi necessari per il mantenimento di servizi e attività economiche essenziali all'interno degli Stati membri. L'attacco «WannaCry» è stato effettuato dal soggetto noto pubblicamente come «APT38» («Advanced Persistent Threat 38») o «Lazarus Group». Chosun Expo può essere collegata all'APT38/Lazarus Group, anche attraverso i conti utilizzati per gli attacchi informatici.	30.7.2020

▼M2

	Nome	Informazioni identificative	Motivi	Data di inserimento nell'elenco
3.	Centro principale per le tecnologie speciali (GTsST), direzione principale dello Stato maggiore delle forze armate della Federazione russa (GU/GRU)	Indirizzo: 22 Kirova Street, Mosca, Federazione russa	Il Centro principale per le tecnologie speciali (GTsST), direzione principale dello Stato maggiore delle forze armate della Federazione russa (GU/GRU), noto anche come unità 74455, è responsabile di attacchi informatici con effetti significativi che provengono dall'esterno dell'Unione e costituiscono una minaccia esterna per l'Unione o i suoi Stati membri e di attacchi informatici con effetti significativi nei confronti di Stati terzi, compresi gli attacchi informatici pubblicamente noti come «NotPetya» o «EternalPetya» nel giugno 2017 e gli attacchi informatici diretti a una rete elettrica ucraina nell'inverno del 2015 e del 2016. «NotPetya» o «EternalPetya» ha reso i dati inaccessibili a diverse imprese nell'Unione, in Europa in generale e nel resto del mondo, compromettendo i computer con ransomware e bloccando l'accesso ai dati e causando così, tra l'altro, perdite economiche significative. L'attacco informatico a una rete elettrica ucraina ha fatto sì che parti della stessa rimanessero spente durante l'inverno. Il soggetto pubblicamente noto come «Sandworm» (alias «Sandworm Team», «BlackEnergy Group», «Voodoo Bear», «Quedagh», «Olympic Destoyer» e Telebot), che è anche all'origine dell'attacco alla rete elettrica ucraina, è responsabile di «NotPetya» o «EternalPetya». Il Centro principale per le tecnologie speciali, direzione principale dello Stato maggiore delle forze armate della Federazione russa, ha un ruolo attivo nelle attività informatiche intraprese da Sandworm e può essere collegato a Sandworm.	30.7.2020