►**B**

REGOLAMENTO (UE) 2019/796 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. 1)

Modificato da:

		Gazzetta ufficiale		
		n.	pag.	data
►**M1**	Regolamento di esecuzione (UE) 2020/1125 del Consiglio del 30 luglio 2020	L 246	4	30.7.2020
►**M2**	Regolamento di esecuzione (UE) 2020/1536 del Consiglio del 22 ottobre 2020	L 351I	1	22.10.2020
►**M3**	Regolamento di esecuzione (UE) 2020/1744 del Consiglio del 20 novembre 2020	L 393	1	23.11.2020
►**M4**	Regolamento di esecuzione (UE) 2022/595 della Commissione dell'11 aprile 2022	L 114	60	12.4.2022
►**M5**	Regolamento (UE) 2023/2694 del Consiglio del 27 novembre 2023	L 2694	1	28.11.2023
►**M6**	Regolamento di esecuzione (UE) 2024/1390 del Consiglio del 17 maggio 2024	L 1390	1	17.5.2024
►**M7**	Regolamento di esecuzione (UE) 2024/1778 del Consiglio del 24 giugno 2024	L 1778	1	24.6.2024
►**M8**	Regolamento di esecuzione (UE) 2024/2465 della Commissione del 10 settembre 2024	L 2465	1	12.9.2024
►**M9**	Regolamento di esecuzione (UE) 2025/173 del Consiglio del 27 gennaio 2025	L 173	1	27.1.2025
►**M10**	Regolamento di esecuzione (UE) 2025/886 del Consiglio del 12 maggio 2025	L 886	1	13.5.2025
►**M11**	Regolamento di esecuzione (UE) 2026/589 del Consiglio del 16 marzo 2026	L 589	1	16.3.2026

Rettificato da:

►**C1** Rettifica, GU L 230 del 17.7.2020, pag. 37 (2019/796)

►**C2** Rettifica, GU L 90397 del 9.7.2024, pag. 1 (2024/1778)

▼B

REGOLAMENTO (UE) 2019/796 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. Il presente regolamento si applica agli attacchi informatici con effetti significativi, inclusi i 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,

se tali azioni non sono debitamente autorizzate dal proprietario o da un altro titolare di diritti sul sistema o sui dati o su parte di essi ovvero non sono 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); fornitura e distribuzione di acqua potabile; infrastrutture digitali, e qualsiasi altro settore che sia essenziale per lo Stato membro interessato;

▼B

c) funzioni statali essenziali, in particolare nei settori della difesa, della *governance* e del funzionamento di istituzioni, anche per elezioni pubbliche o 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 politica estera e di sicurezza comune (PESC) nelle pertinenti disposizioni dell'articolo 21 del trattato sull'Unione europea, è possibile applicare misure restrittive ai sensi del presente regolamento possono anche in risposta ad attacchi informatici con effetti significativi nei confronti di Stati terzi od organizzazioni internazionali.

7. Ai fini del presente regolamento 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 a 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.

8. Ai fini del presente regolamento si applicano le seguenti definizioni aggiuntive:

a) «richiesta»: qualsiasi richiesta, sotto forma contenziosa o meno, presentata anteriormente o posteriormente alla data di entrata in vigore del presente regolamento, derivante da un contratto o da un'operazione o a essi collegata, e in particolare:

   i) una richiesta volta a ottenere l'adempimento di un obbligo derivante da un contratto o da un'operazione o a essi collegata;

   ii) una richiesta volta a ottenere la proroga o il pagamento di una garanzia o di una controgaranzia finanziaria, indipendentemente dalla sua forma;

   iii) una richiesta di compensazione relativa a un contratto o a un'operazione;

   iv) una domanda riconvenzionale;

▼B

v) una richiesta volta a ottenere, anche mediante *exequatur*, il riconoscimento o l'esecuzione di una sentenza, di un lodo arbitrale o di una decisione equivalente, indipendentemente dal luogo in cui sono stati pronunciati;

b) «contratto o operazione»: qualsiasi operazione, indipendentemente dalla sua forma e dal diritto a essa applicabile, che comprenda uno o più contratti o obblighi analoghi stipulati fra le stesse parti o fra parti diverse; a tal fine il termine «contratto» include qualsiasi forma di garanzia, in particolare una garanzia o controgaranzia finanziaria, e qualsiasi credito, anche giuridicamente indipendente, nonché qualsiasi clausola annessa derivante da siffatta operazione o a essa correlata;

c) «autorità competenti»: le autorità competenti degli Stati membri i cui siti web sono elencati nell'allegato II;

d) «risorse economiche»: attività di ogni tipo, materiali o immateriali, mobili o immobili, che non sono fondi ma che possono essere utilizzate per ottenere fondi, beni o servizi;

e) «congelamento di risorse economiche»: il divieto di utilizzare risorse economiche per ottenere fondi, beni o servizi in qualsiasi modo, anche attraverso, tra gli altri, la vendita, la locazione o le ipoteche;

f) «congelamento di fondi»: il divieto di movimentazione, trasferimento, modifica, utilizzo o gestione dei fondi o di accesso a essi così da modificarne il volume, l'importo, la collocazione, la proprietà, il possesso, la natura o la destinazione o qualsiasi altro cambiamento che consenta l'uso dei fondi, compresa la gestione di portafoglio;

g) «fondi»: tutte le attività e i benefici finanziari di qualsiasi natura, compresi, tra gli altri:

i) contanti, assegni, cambiali, vaglia postali e altri strumenti di pagamento;

ii) depositi presso istituti finanziari o altre entità, saldi sui conti, debiti e obblighi;

iii) titoli negoziati a livello pubblico e privato e strumenti di debito, tra cui azioni, certificati azionari, titolo a reddito fisso, pagherò, warrant, obbligazioni e contratti derivati;

iv) interessi, dividendi o altri redditi generati dalle attività;

v) credito, diritto di compensazione, garanzie, fideiussioni o altri impegni finanziari;

vi) lettere di credito, polizze di carico e atti di cessione; e

vii) documenti da cui risulti un interesse riguardante capitali o risorse finanziarie;

▼B

h) «territorio dell'Unione»: i territori degli Stati membri cui si applica il trattato, alle condizioni ivi stabilite, compreso lo spazio aereo.

Articolo 2

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 3

1. Sono congelati tutti i fondi e le risorse economiche appartenenti a, posseduti, detenuti o controllati da una qualsiasi delle persone fisiche o giuridiche, delle entità o degli organismi elencati nell'allegato I.

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

3. Nell'allegato I figurano i seguenti soggetti, quali identificati dal Consiglio a norma dell'articolo 5, paragrafo 1, della decisione (PESC) 2019/797:

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, o agevolandoli per azione o omissione;

c) persone fisiche o giuridiche, entità o organismi associati alle persone fisiche o giuridiche, alle entità o agli organismi di cui alle lettere a) e b) del presente paragrafo.

▼B

Articolo 4

1. In deroga all'articolo 3, paragrafo 1, 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 I ◄ e dei familiari a loro carico, compresi i pagamenti relativi a generi alimentari, locazioni o ipoteche, medicinali e cure mediche, imposte, premi assicurativi e utenze 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.

2. Lo Stato membro interessato informa gli altri Stati membri e la Commissione di ogni autorizzazione concessa ai sensi del paragrafo 1 entro due settimane dall'autorizzazione.

▼M5

Articolo 4 bis

1. L'articolo 3, paragrafi 1 e 2, non si applica alla messa a disposizione dei fondi o delle risorse economiche necessari a garantire l'inoltro tempestivo di assistenza umanitaria o sostenere altre attività a sostegno dei bisogni umani fondamentali laddove l'aiuto sia prestato e l'altra attività sia svolta:

a) dall'Organizzazione delle Nazioni Unite, anche per il tramite dei suoi programmi, fondi e altre entità e organismi, e dalle sue agenzie specializzate e organizzazioni collegate;

b) da organizzazioni internazionali;

c) da organizzazioni umanitarie aventi status di osservatore presso l'Assemblea generale delle Nazioni Unite e dai membri di tali organizzazioni umanitarie;

d) da organizzazioni non governative finanziate a livello bilaterale o multilaterale che partecipano ai piani di risposta umanitaria delle Nazioni Unite, ai piani di risposta per i rifugiati, ad altri appelli delle Nazioni Unite o a cluster umanitari coordinati dall'Ufficio delle Nazioni Unite per il coordinamento degli affari umanitari;

▼M5

e) da organizzazioni e agenzie alle quali l'Unione ha rilasciato il certificato di partenariato umanitario o che sono certificate o riconosciute da uno Stato membro conformemente alle procedure nazionali;

f) da agenzie specializzate degli Stati membri; o

g) da membri del personale, beneficiari di sovvenzioni, affiliate o partner esecutivi dei soggetti di cui alle lettere da a) a f), fintantoché e nella misura in cui agiscono in tale veste.

2. Fatto salvo il paragrafo 1, e in deroga all'articolo 3, 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 stabilito che la fornitura di tali fondi o risorse economiche è necessaria per l'inoltro tempestivo di assistenza umanitaria o per sostenere altre attività a sostegno del soddisfacimento dei bisogni umani fondamentali.

3. In assenza di una decisione sfavorevole, di una richiesta di informazioni o di una comunicazione di un termine ulteriore da parte della pertinente autorità competente entro cinque giorni lavorativi dalla data di ricevimento della domanda di autorizzazione ai sensi del paragrafo 2, tale autorizzazione si considera concessa.

4. Lo Stato membro interessato informa gli altri Stati membri e la Commissione di tutte le autorizzazioni rilasciate a norma dei paragrafi 2 e 3 entro quattro settimane dal rilascio di tale autorizzazione.

▼B

Articolo 5

1. In deroga all'articolo 3, 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 all'articolo 4 nell'elenco figurante nell'allegato I, 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) 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 I; e

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

▼B

2. Lo Stato membro interessato informa gli altri Stati membri e la Commissione di ogni autorizzazione concessa ai sensi del paragrafo 1 entro due settimane dall'autorizzazione.

Articolo 6

1. In deroga all'articolo 3, paragrafo 1, e purché un pagamento da parte di una persona fisica o giuridica, di un'entità o di un organismo di cui all'allegato I sia dovuto in forza di un contratto o di un accordo concluso o di un'obbligazione sorta per la persona fisica o giuridica, l'entità o l'organismo in questione prima della data di inserimento di tale persona fisica o giuridica, entità od organismo nell'allegato I, le autorità competenti degli Stati membri possono autorizzare, alle condizioni che ritengono appropriate, lo svincolo di taluni fondi o risorse economiche congelati purché l'autorità competente interessata abbia accertato che:

a) i fondi o le risorse economiche saranno usati per un pagamento da una persona fisica o giuridica, da un'entità o da un organismo di cui all'allegato I; e

b) il pagamento non viola l'articolo 3, paragrafo 2.

2. Lo Stato membro interessato informa gli altri Stati membri e la Commissione di ogni autorizzazione concessa ai sensi del paragrafo 1 entro due settimane dall'autorizzazione.

Articolo 7

1. L'articolo 3, paragrafo 2, non osta a che gli enti finanziari o creditizi accreditino sui conti congelati fondi trasferiti da terzi verso i conti di una persona fisica o giuridica, un'entità o un organismo che figura nell'elenco, purché tali versamenti siano anch'essi congelati. L'ente finanziario o creditizio informa senza indugio l'autorità competente pertinente in merito a tali operazioni.

2. L'articolo 3, 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 la persona fisica o giuridica, l'entità o l'organismo di cui all'articolo 4, paragrafo 1, sono stati inseriti nell'allegato I; o

c) pagamenti dovuti nel quadro di decisioni giudiziarie, amministrative o arbitrali emesse in uno Stato membro o esecutive nello Stato membro interessato,

purché tali interessi, altri profitti e pagamenti continuino a essere soggetti alle misure di cui all'articolo 3, paragrafo 1.

Articolo 8

1. Fatte salve le norme applicabili in materia di relazioni, riservatezza e segreto professionale, le persone fisiche e giuridiche, le entità e gli organismi sono tenuti a:

▼B

a) fornire immediatamente qualsiasi informazione atta a facilitare il rispetto del presente regolamento, quali le informazioni relative ai conti e agli importi congelati a norma dell'articolo 3, paragrafo 1, all'autorità competente dello Stato membro in cui risiedono o sono situati, e a trasmettere tali informazioni, direttamente o attraverso lo Stato membro, alla Commissione; e

b) collaborare con l'autorità competente alla verifica delle informazioni di cui alla lettera a).

2. Le ulteriori informazioni ricevute direttamente dalla Commissione sono messe a disposizione degli Stati membri.

3. Le informazioni fornite o ricevute ai sensi del presente articolo sono utilizzate unicamente per i fini gli scopi per i quali sono state fornite o ricevute.

Articolo 9

È vietato partecipare, consapevolmente e deliberatamente, ad attività aventi l'obiettivo o l'effetto di eludere le misure di cui all'articolo 3.

Articolo 10

1. Il congelamento di fondi e risorse economiche o il rifiuto di rendere disponibili fondi o risorse economiche, se effettuato ritenendo in buona fede che tale azione sia conforme al presente regolamento, non comporta alcun genere di responsabilità per la persona fisica o giuridica, l'entità o l'organismo che lo attua, né per i suoi dirigenti o dipendenti, a meno che non si dimostri che i fondi e le risorse economiche sono stati congelati o trattenuti in seguito a negligenza.

2. Le azioni compiute da persone fisiche o giuridiche, entità o organismi non comportano alcun genere di responsabilità a loro carico se questi non sapevano, e non avevano alcun motivo ragionevole di sospettare, che le loro azioni avrebbero violato le misure previste dal presente regolamento.

Articolo 11

1. 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 del presente regolamento, comprese richieste di indennizzo o richieste analoghe, per esempio richieste di compensazione o richieste nell'ambito 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 I;

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).

2. In ogni procedura volta al soddisfacimento di una richiesta, l'onere della prova che il soddisfacimento della richiesta non è vietato dal paragrafo 1 incombe alla persona fisica o giuridica, all'entità o all'organismo che richiede il soddisfacimento di tale richiesta.

3. Il presente articolo lascia impregiudicato il diritto delle persone fisiche o giuridiche, delle entità e degli organismi di cui al paragrafo 1 al controllo giurisdizionale della legittimità dell'inadempimento degli obblighi contrattuali a norma del presente regolamento.

▼B

Articolo 12

1. La Commissione e gli Stati membri si informano reciprocamente delle misure adottate ai sensi del presente regolamento e condividono qualsiasi altra informazione pertinente a loro disposizione riguardante il presente regolamento, in particolare le informazioni riguardanti:

a) i fondi congelati a norma dell'articolo 4 e le autorizzazioni concesse a norma degli articoli da 4, 5 e 6; e

b) i problemi di violazione e di applicazione delle norme e le sentenze pronunciate dagli organi giurisdizionali nazionali.

2. Gli Stati membri comunicano immediatamente agli altri Stati membri e alla Commissione tutte le altre informazioni pertinenti in loro possesso tali da pregiudicare l'effettiva attuazione del presente regolamento.

Articolo 13

1. Qualora decida di applicare a una persona fisica o giuridica, a un'entità o a un organismo le misure di cui all'articolo 3, il Consiglio modifica di conseguenza l'allegato I.

2. Il Consiglio comunica la decisione di cui al paragrafo 1, compresi i motivi dell'inserimento in elenco, alla persona fisica o giuridica, all'entità o all'organismo interessato, direttamente, se l'indirizzo è noto, o attraverso la pubblicazione di un avviso, dando loro la possibilità di formulare osservazioni.

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

4. L'elenco di cui all'allegato I è riesaminato periodicamente e almeno ogni 12 mesi.

5. La Commissione ha il potere di modificare l'allegato II sulla base delle informazioni fornite dagli Stati membri.

Articolo 14

1. L'allegato I indica i motivi dell'inserimento nell'elenco delle persone fisiche o giuridiche, delle entità o degli organismi interessati.

2. L'allegato I contiene, 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 15

1. Gli Stati membri stabiliscono le norme sulle sanzioni applicabili alle violazioni delle disposizioni del presente regolamento e adottano tutte le misure necessarie per garantirne l'attuazione. Le sanzioni previste sono effettive, proporzionate e dissuasive.

▼B

2. Gli Stati membri comunicano senza indugio alla Commissione le norme di cui al paragrafo 1 dopo l'entrata in vigore del presente regolamento, come pure ogni successiva modifica che le riguardi.

Articolo 16

1. La Commissione tratta i dati personali per svolgere i propri compiti a norma del presente regolamento. Tali compiti comprendono:

a) l'aggiunta del contenuto dell'allegato I nell'elenco elettronico consolidato delle persone, dei gruppi e delle entità oggetto di sanzioni finanziarie dell'Unione e nella mappa interattiva delle sanzioni, entrambi pubblicamente disponibili;

b) il trattamento delle informazioni relative all'impatto delle misure contemplate dal presente regolamento, come il valore dei fondi congelati e le informazioni sulle autorizzazioni rilasciate dalle autorità competenti.

2. Ai fini del presente regolamento, il servizio della Commissione indicato nell'allegato II è designato come «titolare del trattamento» per la Commissione ai sensi dell'articolo 3, punto 8), del regolamento (UE) 2018/1725, per garantire che le persone fisiche interessate possano esercitare i loro diritti a norma dello stesso.

Articolo 17

1. Gli Stati membri designano le autorità competenti di cui al presente regolamento e le identificano sui siti web elencati nell'allegato II. Gli Stati membri comunicano alla Commissione le eventuali modifiche degli indirizzi dei loro siti web elencati nell'allegato II.

2. Gli Stati membri notificano senza indugio alla Commissione le proprie autorità competenti, compresi gli estremi delle stesse, dopo l'entrata in vigore del presente regolamento e informano la Commissione di ogni eventuale successiva modifica.

3. Laddove il presente regolamento imponga di notificare, informare o comunicare in altro modo con la Commissione, l'indirizzo e gli altri estremi da usare per queste comunicazioni sono quelli indicati nell'allegato II.

Articolo 18

Il presente regolamento si applica:

a) nel territorio dell'Unione, compreso il suo spazio aereo;

b) a bordo di tutti gli aeromobili o i natanti sotto la giurisdizione di uno Stato membro;

c) a qualsiasi persona fisica cittadina di uno Stato membro che si trovi all'interno o all'esterno del territorio dell'Unione;

d) a qualsiasi persona giuridica, entità od organismo che si trovi all'interno o all'esterno del territorio dell'Unione e sia registrata/o o costituita/o conformemente al diritto di uno Stato membro;

e) a qualsiasi persona giuridica, entità od organismo relativamente ad attività economiche esercitate, interamente o parzialmente, all'interno dell'Unione.

▼B

Articolo 19

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

Il presente regolamento è obbligatorio in tutti i suoi elementi e direttamente applicabile in ciascuno degli Stati membri.

▼B

ALLEGATO I

Elenco delle persone fisiche e giuridiche, delle entità e degli organismi di cui all'articolo 3

▼M1

A. Persone fisiche

	Nome	Informazioni identificative	Motivi	Data di inserimento nell'elenco
▼M3				
1.	GAO Qiang	Data di nascita: 4 ottobre 1983 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	Data di nascita: 10 settembre 1981 Luogo di nascita: Cina 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. 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.	30.7.2020

▼M3

	Nome	Informazioni identificative	Motivi	Data di inserimento nell'elenco
			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.	

▼M10

3.	Alexey Valeryevich MININ	Алексей Валерьевич МИНИН Data di nascita: 27.5.1972 Luogo di nascita: oblast di Perm, RSFS russa (ora Federazione russa) N. di passaporto: 120017582 Rilasciato da: ministero degli Affari esteri della Federazione russa Validità: dal 17.4.2017 al 17.4.2022 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 e ad attacchi informatici con effetti significativi contro Stati terzi. 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) ha sventato il tentativo di attacco informatico, impedendo in tal modo gravi danni all'OPCW. Un grand jury nel distretto occidentale della Pennsylvania (Stati Uniti d'America) ha accusato Alexey Minin, in quanto agente del GRU russo, di pirateria informatica, frode telematica, furto aggravato d'identità e riciclaggio. Il GRU continua a condurre attacchi informatici contro l'Unione o i suoi Stati membri. In qualità di membro del GRU, Alexey Minin è pertanto coinvolto in attacchi informatici con effetti significativi, inclusi i tentati attacchi informatici con effetti potenzialmente significativi, che costituiscono una minaccia esterna per l'Unione o i suoi Stati membri.	30.7.2020

▼M10

	Nome	Informazioni identificative	Motivi	Data di inserimento nell'elenco
4.	Aleksei Sergeyvich MORENETS	Алексей Сергеевич МОРЕНЕЦ Data di nascita: 31.7.1977 Luogo di nascita: oblast di Murmanskaya, RSFS russa (ora Federazione russa) N. di passaporto: 100135556 Rilasciato da: ministero degli Affari esteri della Federazione russa Validità: dal 17.4.2017 al 17.4.2022 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 e ad attacchi informatici con effetti significativi contro Stati terzi. 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) ha sventato il tentativo di attacco informatico, impedendo in tal modo gravi danni all'OPCW. Un grand jury nel distretto occidentale della Pennsylvania (Stati Uniti d'America) ha accusato Aleksei Morenets, in quanto assegnato all'unità militare 26165, di pirateria informatica, frode telematica, furto aggravato d'identità e riciclaggio. Il GRU continua a condurre attacchi informatici contro l'Unione o i suoi Stati membri. In qualità di membro del GRU, Aleksei Morenets è pertanto coinvolto in attacchi informatici con effetti significativi, inclusi i tentati attacchi informatici con effetti potenzialmente significativi, che costituiscono una minaccia esterna per l'Unione o i suoi Stati membri.	30.7.2020
5.	Evgenii Mikhaylovich SEREBRIAKOV	Евгений Михайлович СЕРЕБРЯКОВ Data di nascita: 26.7.1981 Luogo di nascita: Kursk, RSFS russa (ora Federazione russa) N. di passaporto: 100135555 Rilasciato da: ministero degli Affari esteri della Federazione russa Validità: dal 17.4.2017 al 17.4.2022 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 e ad attacchi informatici con effetti significativi contro Stati terzi. 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) ha sventato il tentativo di attacco informatico, impedendo in tal modo gravi danni all'OPCW. Dalla primavera del 2022 Evgenii Serebriakov guida «Sandworm» (alias «Sandworm Team», «BlackEnergy Group», «Voodoo Bear», «Quedagh», «Olympic Destroyer» e «Telebots»), un soggetto e un gruppo di pirateria informatica affiliato all'unità 74455 della direzione principale dell'intelligence russa. Sandworm ha sferrato attacchi informatici contro l'Ucraina, compresi organismi pubblici ucraini, a seguito della guerra di aggressione della Russia nei confronti dell'Ucraina. Il GRU continua a condurre attacchi informatici contro l'Unione o i suoi Stati membri. In qualità di membro del GRU, Evgenii Serebriakov è pertanto coinvolto in attacchi informatici con effetti significativi, inclusi i tentati attacchi informatici con effetti potenzialmente significativi, che costituiscono una minaccia esterna per l'Unione o i suoi Stati membri.	30.7.2020

▼M10

	Nome	Informazioni identificative	Motivi	Data di inserimento nell'elenco
6.	Oleg Mikhaylovich SOTNIKOV	Олег Михайлович СОТНИКОВ Data di nascita: 24.8.1972 Luogo di nascita: Ulyanovsk, RSFS russa (ora Federazione russa) N. di passaporto: 120018866 Rilasciato da: ministero degli Affari esteri della Federazione russa Validità: dal 17.4.2017 al 17.4.2022 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 e ad attacchi informatici con effetti significativi contro Stati terzi. 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) ha sventato il tentativo di attacco informatico, impedendo in tal modo gravi danni all'OPCW. Un grand jury nel distretto occidentale della Pennsylvania (Stati Uniti d'America) ha accusato Oleg Sotnikov, in quanto agente del GRU russo, di pirateria informatica, frode telematica, furto aggravato d'identità e riciclaggio. Il GRU continua a condurre attacchi informatici contro l'Unione o i suoi Stati membri. In qualità di membro del GRU, Oleg Sotnikov è pertanto coinvolto in attacchi informatici con effetti significativi, inclusi i tentati attacchi informatici con effetti potenzialmente significativi, che costituiscono una minaccia esterna per l'Unione o i suoi Stati membri.	30.7.2020
7.	Dmitry Sergeyevich BADIN	Дмитрий Сергеевич БАДИН Data di nascita: 15.11.1990 Luogo di nascita: Kursk, RSFS russa (ora Federazione russa) Cittadinanza: russa Sesso: maschile	Dmitry Badin ha partecipato a un attacco informatico con effetti significativi contro il parlamento federale tedesco (Deutscher Bundestag) e ad attacchi informatici con effetti significativi contro Stati terzi. In qualità di agente dell'intelligence militare dell'85° Centro principale per i servizi speciali (GTsSS), direzione principale dello Stato maggiore delle forze armate della Federazione russa (GU/GRU), Dmitry Badin faceva parte di una squadra di agenti dell'intelligence militare russa che ha condotto un attacco informatico contro il parlamento federale tedesco tra aprile e maggio 2015. Tale attacco ha colpito il sistema informatico del parlamento, compromettendone il funzionamento per diversi giorni. È stato sottratto un ingente volume di dati e sono stati violati gli account di posta elettronica di diversi parlamentari, nonché quello dell'ex cancelliera Angela Merkel. Un grand jury nel distretto occidentale della Pennsylvania (Stati Uniti d'America) ha accusato Dmitry Badin, in quanto assegnato all'unità militare 26165, di pirateria informatica, frode telematica, furto aggravato d'identità e riciclaggio. Il GRU continua a condurre attacchi informatici contro l'Unione o i suoi Stati membri. In qualità di membro del GRU, Dmitry Badin è pertanto coinvolto in attacchi informatici con effetti significativi, inclusi i tentati attacchi informatici con effetti potenzialmente significativi, che costituiscono una minaccia esterna per l'Unione o i suoi Stati membri.	22.10.2020

▼M10

	Nome	Informazioni identificative	Motivi	Data di inserimento nell'elenco
8.	Igor Olegovich KOSTYUKOV	Игорь Олегович КОСТЮКОВ Data di nascita: 21.2.1961 Cittadinanza: russa Sesso: maschile	Igor Kostyukov è l'attuale capo della direzione principale dello Stato maggiore delle forze armate della Federazione russa (GU/GRU), presso cui ha precedentemente svolto le funzioni di primo vicecapo. Tra le unità sotto il suo comando vi è l'85° Centro principale per i servizi speciali (GTsSS), (alias «unità militare 26165», «APT28», «Fancy Bear», «Sofacy Group», «Pawn Storm», «Strontium»). In tale veste, Igor Kostyukov è responsabile degli attacchi informatici condotti dal GTsSS, tra cui quelli con effetti significativi che costituiscono una minaccia esterna per l'Unione o i suoi Stati membri. In particolare, agenti dell'intelligence militare del GTsSS hanno partecipato all'attacco informatico contro il parlamento federale tedesco (Deutscher Bundestag) tra aprile e maggio 2015, nonché al tentativo di attacco informatico finalizzato a ottenere un accesso abusivo alla rete Wi-Fi dell'Organizzazione per la proibizione delle armi chimiche (OPCW) nei Paesi Bassi nell'aprile 2018. L'attacco informatico ai danni del parlamento federale tedesco ha colpito il sistema informatico del parlamento, compromettendone il funzionamento per diversi giorni. È stato sottratto un ingente volume di dati e sono stati violati gli account di posta elettronica di diversi parlamentari, nonché quello dell'ex cancelliera Angela Merkel. Il GRU continua a condurre attacchi informatici contro l'Unione o i suoi Stati membri. In qualità di membro del GRU, Igor Kostyukov è pertanto coinvolto in attacchi informatici con effetti significativi, inclusi i tentati attacchi informatici con effetti potenzialmente significativi, che costituiscono una minaccia esterna per l'Unione o i suoi Stati membri.	22.10.2020
▼M7 9.	Ruslan Aleksandrovich PERETYATKO	Руслан Александрович ПЕРЕТЯТЬКО Data di nascita: 3.8.1985 Cittadinanza: russa Sesso: maschile	Ruslan PERETYATKO ha preso parte ad attacchi informatici con effetti significativi che costituiscono una minaccia esterna per l'Unione o i suoi Stati membri. ►C2 Ruslan PERETYATKO fa parte del «Callisto Group», gruppo di agenti dell'intelligence russa che conduce operazioni informatiche contro Stati membri dell'UE e Stati terzi. ◄ Callisto Group (alias «Seaborgium», «Star Blizzard», «ColdRiver», «TA446») ha avviato campagne pluriennali di phishing utilizzate per rubare credenziali e dati di account. Inoltre, Callisto Group è responsabile di campagne mirate a persone singole e a funzioni statali essenziali, anche nei settori della difesa e delle relazioni esterne. Pertanto, Ruslan PERETYATKO è coinvolto in attacchi informatici con effetti significativi che costituiscono una minaccia esterna per l'Unione o i suoi Stati membri.	24.6.2024

▼M7

	Nome	Informazioni identificative	Motivi	Data di inserimento nell'elenco
10.	Andrey Stanislavovich KORINETS	Андрей Станиславович КОРИНЕЦ Data di nascita: 18.5.1987 Luogo di nascita: città di Syktyvkar, Russia Cittadinanza: russa Sesso: maschile	Andrey Stanislavovich KORINETS ha preso parte ad attacchi informatici con effetti significativi che costituiscono una minaccia esterna per l'Unione o i suoi Stati membri. Andrey Stanislavovich KORINETS è un agente di «Center 18» del Servizio federale di sicurezza (FSB) della Federazione russa. ►C2 Andrey Stanislavovich KORINETS fa parte del «Callisto Group», gruppo di agenti dell'intelligence russa che conduce operazioni informatiche contro Stati membri dell'UE e Stati terzi. ◄ Callisto Group (alias «Seaborgium», «Star Blizzard», «ColdRiver», «TA446») ha avviato campagne pluriennali di phishing utilizzate per rubare credenziali e dati di account. Inoltre, Callisto Group è responsabile di campagne mirate a persone singole e a funzioni statali essenziali, anche nei settori della difesa e delle relazioni esterne. Pertanto, Andrey Stanislavovich KORINETS è coinvolto in attacchi informatici con effetti significativi che costituiscono una minaccia esterna per l'Unione o i suoi Stati membri.	24.6.2024
11.	Oleksandr SKLIANKO	Александр СКЛЯНКО (grafia russa) Олександр СКЛЯНКО (grafia ucraina) Data di nascita: 5.8.1973 Passaporto: EC 867868, rilasciato il 27.11.1998 (Ucraina) Sesso: maschile	Oleksandr SKLIANKO ha preso parte ad attacchi informatici con effetti significativi contro Stati membri dell'UE come pure ad attacchi informatici con effetti significativi contro Stati terzi. Oleksandr SKLIANKO fa parte del gruppo di hacker Armageddon, sostenuto dal Servizio federale di sicurezza (FSB) della Federazione russa, che ha compiuto vari attacchi informatici con effetti significativi sul governo dell'Ucraina e sugli Stati membri dell'UE e loro funzionari governativi, anche utilizzando email di phishing e campagne di malware. Pertanto, Oleksandr SKLIANKO è coinvolto in attacchi informatici con effetti significativi contro Stati terzi come pure in attacchi informatici con effetti significativi che costituiscono una minaccia esterna per l'Unione o i suoi Stati membri.	24.6.2024

▼M7

	Nome	Informazioni identificative	Motivi	Data di inserimento nell'elenco
12.	Mykola CHERNYKH	Николай ЧЕРНЫХ (grafia russa) Микола ЧЕРНИХ (grafia ucraina) Data di nascita: 12.10.1978 Passaporto: EC 922162, rilasciato il 20.1.1999 (Ucraina) Sesso: maschile	Mykola CHERNYKH ha preso parte ad attacchi informatici con effetti significativi contro Stati membri dell'UE come pure ad attacchi informatici con effetti significativi contro Stati terzi. Mykola CHERNYKH fa parte del gruppo di hacker Armageddon, sostenuto dal Servizio federale di sicurezza (FSB) della Federazione russa, che ha compiuto vari attacchi informatici con effetti significativi sul governo dell'Ucraina e sugli Stati membri dell'UE e loro funzionari governativi, anche utilizzando email di phishing e campagne di malware. In qualità di ex dipendente del servizio di sicurezza dell'Ucraina, è accusato in Ucraina di tradimento e di interferenza non autorizzata nel funzionamento di macchine da calcolo elettroniche e di sistemi automatizzati. Pertanto, Mykola CHERNYKH è coinvolto in attacchi informatici con effetti significativi che costituiscono una minaccia esterna per l'Unione o i suoi Stati membri.	24.6.2024
13.	Mikhail Mikhailovich TSAREV	Михаил Михайлович ЦАРЕВ Data di nascita: 20.4.1989 Luogo di nascita: Serpukhov, Federazione russa Cittadinanza: russa Indirizzo: Serpukhov Sesso: maschile	Mikhail Mikhailovich TSAREV ha preso parte ad attacchi informatici con effetti significativi che costituiscono una minaccia esterna per gli Stati membri dell'UE. Mikhail Mikhailovich TSAREV, noto anche con i soprannomi online «Mango», «Alexander Grachev», «Super Misha», «Ivanov Mixail», «Misha Krutysha» e «Nikita Andreevich Tsarev», svolge un ruolo chiave nell'impiego di programmi malware «Conti» e «Trickbot» ed è coinvolto nel gruppo di minaccia «Wizard Spider» con sede in Russia. I programmi malware Conti e Trickbot sono stati creati e sviluppati dal «Wizard Spider». Wizard Spider ha condotto campagne di ransomware in diversi settori, tra cui servizi essenziali come la sanità e il settore bancario. Il gruppo ha infettato computer in tutto il mondo e i suoi malware sono stati sviluppati in una serie di malware altamente modulari. Le campagne di Wizard Spider, che utilizzano malware quali Conti, Ryuk e TrickBot, sono responsabili di rilevanti danni economici nell'Unione europea. Pertanto, Mikhail Mikhailovich TSAREV è coinvolto in attacchi informatici con effetti significativi che costituiscono una minaccia esterna per l'Unione o i suoi Stati membri.	24.6.2024

▼M7

	Nome	Informazioni identificative	Motivi	Data di inserimento nell'elenco
14.	Maksim Sergeevich GALOCHKIN	Максим Сергеевич ГАЛОЧКИН Data di nascita: 19.5.1982 Luogo di nascita: Abakan, Federazione russa Cittadinanza: russa Sesso: maschile	Maksim Galochkin ha preso parte ad attacchi informatici con effetti significativi che costituiscono una minaccia esterna per gli Stati membri dell'UE. Maksim Galochkin è noto anche con i soprannomi online «Benalen», «Bentley», «Volhvb», «volhvb», «manuel», «Max17» e «Crypt». Galochkin svolge un ruolo chiave nell'impiego di programmi malware TrickBot e Conti ed è coinvolto nel gruppo di minaccia «Wizard Spider». Ha guidato un gruppo di tester, con responsabilità per lo sviluppo, la supervisione e l'attuazione di test per il programma malware TrickBot, creato e impiegato da «Wizard Spider». Wizard Spider ha condotto campagne di ransomware in diversi settori, tra cui servizi essenziali come la sanità e il settore bancario. Il gruppo ha infettato computer in tutto il mondo e i suoi malware sono stati sviluppati in una serie di malware altamente modulari. Le campagne di Wizard Spider che utilizzano malware quali Conti, Ryuk e TrickBot, sono responsabili di rilevanti danni economici nell'Unione europea. Pertanto, Maksim Galochkin è coinvolto in attacchi informatici con effetti significativi che costituiscono una minaccia esterna per l'Unione o i suoi Stati membri.	24.6.2024

▼M9

15.	Nikolay Alexandrovich KORCHAGIN	Николай Александрович Корчагин Data di nascita: 16.9.1997 Cittadinanza: russa Sesso: maschile Entità associata: direzione principale dello Stato maggiore delle forze armate della Federazione russa	Nikolay Korchagin è coinvolto in attacchi informatici con effetti significativi e ne è responsabile in quanto ha svolto attività di intelligence dirette contro l'Estonia ottenendo accesso illegalmente a un sistema informatico. Nikolay Korchagin è un ufficiale dell'unità militare 29155 della direzione principale dello Stato maggiore delle forze armate della Federazione russa (GRU). In tale ruolo è coinvolto in attacchi informatici contro sistemi computerizzati, intesi a raccogliere, dai sistemi di dati di diverse istituzioni, informazioni che in modo indipendente o combinato forniscono una panoramica della politica di sicurezza informatica dell'Estonia, delle capacità informatiche dello Stato, dei dati personali sensibili e di altri dati sensibili, al fine di utilizzare i dati per minacciare la sicurezza dell'Estonia. Gli attacchi interessano pertanto la conservazione di informazioni classificate, ed è responsabile di tali attacchi. Gli attacchi hanno riguardato alleati e partner dell'Estonia. Nikolay Korchagin è pertanto coinvolto in attacchi informatici con effetti significativi che costituiscono una minaccia esterna per uno Stato membro, e ne è responsabile.	27.1.2025

▼M9

	Nome	Informazioni identificative	Motivi	Data di inserimento nell'elenco
16.	Vitaly SHEVCHENKO	Виталий Шевченко Data di nascita: 1.9.1997 Cittadinanza: russa Sesso: maschile Entità associata: direzione principale dello Stato maggiore delle forze armate della Federazione russa	Vitaly Shevchenko è coinvolto in attacchi informatici con effetti significativi e ne è responsabile in quanto ha svolto attività di intelligence dirette contro l'Estonia ottenendo accesso illegalmente a un sistema informatico. Vitaly Shevchenko è un ufficiale dell'unità militare 29155 della direzione principale dello Stato maggiore delle forze armate della Federazione russa (GRU). In tale ruolo è coinvolto in attacchi informatici contro sistemi computerizzati, intesi a raccogliere, dai sistemi di dati di diverse istituzioni, informazioni che in modo indipendente o combinato forniscono una panoramica della politica di sicurezza informatica dell'Estonia, delle capacità informatiche dello Stato, dei dati personali sensibili e di altri dati sensibili, al fine di utilizzare i dati per minacciare la sicurezza dell'Estonia. Gli attacchi interessano pertanto la conservazione di informazioni classificate, ed è responsabile di tali attacchi. Gli attacchi hanno riguardato alleati e partner dell'Estonia. Vitaly Shevchenko è pertanto coinvolto in attacchi informatici con effetti significativi che costituiscono una minaccia esterna per uno Stato membro, e ne è responsabile.	27.1.2025
17.	Yuriy Fedorovich DENISOV	Юрий Федорович Денисов Data di nascita: 17.6.1980 Cittadinanza: russa Sesso: maschile Entità associata: direzione principale dello Stato maggiore delle forze armate della Federazione russa	Yuriy Denisov è coinvolto in attacchi informatici con effetti significativi e ne è responsabile in quanto ha svolto attività di intelligence dirette contro l'Estonia ottenendo accesso illegalmente a un sistema informatico. Yuriy Denisov è un ufficiale dell'unità militare 29155 della direzione principale dello Stato maggiore delle forze armate della Federazione russa (GRU). In tale ruolo è coinvolto in attacchi informatici contro sistemi computerizzati, intesi a raccogliere, dai sistemi di dati di diverse istituzioni, informazioni che in modo indipendente o combinato forniscono una panoramica della politica di sicurezza informatica dell'Estonia, delle capacità informatiche dello Stato, dei dati personali sensibili e di altri dati sensibili, al fine di utilizzare i dati per minacciare la sicurezza dell'Estonia. Gli attacchi interessano pertanto la conservazione di informazioni classificate, ed è responsabile di tali attacchi. Gli attacchi hanno riguardato alleati e partner dell'Estonia. Yuriy Denisov è pertanto coinvolto in attacchi informatici con effetti significativi che costituiscono una minaccia esterna per uno Stato membro, e ne è responsabile.	27.1.2025

▼M1

	Nome	Informazioni identificative	Motivi	Data di inserimento nell'elenco
▼M11				
18.	CHEN Cheng	陈诚 (grafia cinese) Pseudonimi: Jesse Chen lengmo l3n6m0 Data di nascita: 20.10.1984 Luogo di nascita: Yancheng, Jiangsu, Cina Cittadinanza: cinese Sesso: maschile	Chen Cheng è un uomo d'affari cinese, cofondatore e uno dei direttori generali (direttore operativo) di Anxun Information Technology Co. Ltd. È anche rappresentante legale della filiale di tale società del Sichuan di tale società. Anxun Information Technology Co. Ltd., nota anche come i-Soon, è una società con sede nella Repubblica popolare cinese che offre servizi di «hacking-for-hire» (hackeraggio su commissione). Anxun Information Technology Co. Ltd. ha preso di mira infrastrutture critiche e funzioni statali essenziali degli Stati membri, ha avuto accesso a informazioni classificate e le ha vendute. Anxun Information Technology Co. Ltd. ha inoltre attaccato governi di vari Stati terzi, costituendo una minaccia per gli obiettivi della politica estera e di sicurezza comune (PESC) dell'Unione, come stabilito nell'articolo 21, paragrafo 2, lettere da a) a c), del trattato sull'Unione europea. Anxun Information Technology Co. Ltd. trae un importante vantaggio economico dai servizi forniti. Anxun Information Technology Co. Ltd è pertanto responsabile di attacchi informatici con effetti significativi che costituiscono una minaccia esterna per l'Unione e i suoi Stati membri e di attacchi informatici con effetti significativi nei confronti di Stati terzi. In tale veste, Chen Cheng è responsabile di attacchi informatici con effetti significativi che costituiscono una minaccia esterna per gli Stati membri, nonché di attacchi informatici con effetti significativi nei confronti di Stati terzi, e vi è coinvolto.	16.3.2026
19.	WU Haibo	吴海波 (grafia cinese) Pseudonimi: shutdown shutd0wn Luogo di nascita: Cina Cittadinanza: cinese Sesso: maschile	Wu Haibo è un uomo d'affari cinese, cofondatore e uno dei direttori generali (direttore operativo) di Anxun Information Technology Co. Ltd. È anche rappresentante legale, presidente e direttore generale della filiale di Shanghai («società madre») di Anxun Information Technology Co. Ltd. Inoltre agisce inoltre in qualità di rappresentante legale della filiale del Sichuan di tale società. Anxun Information Technology Co. Ltd., nota anche come i-Soon, è una società con sede nella Repubblica popolare cinese che offre servizi di «hacking-for-hire» (hackeraggio su commissione). Anxun Information Technology Co. Ltd. ha preso di mira infrastrutture critiche e funzioni statali essenziali degli Stati membri, ha avuto accesso a informazioni classificate e le ha vendute. Anxun Information Technology Co. Ltd ha inoltre attaccato governi di vari Stati terzi, costituendo una minaccia per gli obiettivi della politica estera e di sicurezza comune (PESC) dell'Unione, come stabilito nell'articolo 21, paragrafo 2, lettere da a) a c), del trattato sull'Unione europea..	16.3.2026

▼M11

	Nome	Informazioni identificative	Motivi	Data di inserimento nell'elenco
			Anxun Information Technology Co. Ltd trae un importante vantaggio economico dai servizi forniti. Anxun Information Technology Co. Ltd è pertanto responsabile di attacchi informatici con effetti significativi che costituiscono una minaccia esterna per gli Stati membri e di attacchi informatici con effetti significativi nei confronti di Stati terzi. Wu Haibo è stato coinvolto nella direzione e nell'incoraggiamento di tentati attacchi informatici con effetti significativi nei confronti degli Stati membri. In tale veste, è responsabile di attacchi informatici con effetti significativi che costituiscono una minaccia esterna per gli Stati membri, nonché di attacchi informatici con effetti significativi nei confronti di Stati terzi, e vi è coinvolto.	

▼M1

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. 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.	30.7.2020
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.	30.7.2020

▼M1

	Nome	Informazioni identificative	Motivi	Data di inserimento nell'elenco
			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.	
▼M6 3.	Main Centre for Special Technologies (GTsST) of the Main Directorate of the General Staff of the Armed Forces of the Russian Federation (GU/GRU)	Indirizzo: 22 Kirova Street, Moscow, Russian Federation	Il Main Centre for Special Technologies (GTsST) of the Main Directorate of the General Staff of the Armed Forces of the Russian Federation (GU/GRU) (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 coinvolto in 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 in 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 Destroyer» e «Telebots»), che è anche all'origine dell'attacco alla rete elettrica ucraina, è responsabile di «NotPetya» o «EternalPetya». Sandworm ha sferrato attacchi informatici contro l'Ucraina, comprese agenzie governative ucraine e infrastrutture critiche ucraine, a seguito della guerra di aggressione della Russia nei confronti dell'Ucraina. Tali attacchi informatici comprendono campagne di phishing mirato (spear phishing), attacchi malware e ransomware. 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

▼M6

	Nome	Informazioni identificative	Motivi	Data di inserimento nell'elenco
4.	85th Main Centre for Special Services (GTsSS) of the Main Directorate of the General Staff of the Armed Forces of the Russian Federation (GU/GRU)	Indirizzo: Komsomol'skiy Prospekt, 20, Moscow, 119146, Russian Federation	L'85th Main Centre for Special Services (GTsSS) of the Main Directorate of the General Staff of the Armed Forces of the Russian Federation (GU/GRU) (85° Centro principale per i servizi speciali (GTsSS), direzione principale dello Stato maggiore delle forze armate della Federazione russa (GU/GRU)], (alias «unità militare 26165», alias: «APT28», «Fancy Bear», «Sofacy Group», «Pawn Storm» e «Strontium»), è coinvolto in attacchi informatici con effetti significativi che costituiscono una minaccia esterna per l'Unione o i suoi Stati membri e in attacchi informatici con effetti significativi nei confronti di Stati terzi. In particolare, agenti dell'intelligence militare del GTsSS hanno partecipato all'attacco informatico ai danni del parlamento federale tedesco (*Deutscher Bundestag*) tra aprile e maggio 2015, nonché al tentativo di attacco informatico finalizzato a ottenere un accesso abusivo alla rete Wi-Fi dell'Organizzazione per la proibizione delle armi chimiche (OPCW) nei Paesi Bassi nell'aprile 2018. L'attacco informatico ai danni del parlamento federale tedesco ha colpito il sistema informatico del parlamento, compromettendone il funzionamento per diversi giorni. È stato sottratto un ingente volume di dati e sono stati violati gli account di posta elettronica di diversi parlamentari, nonché quello dell'ex cancelliera Angela Merkel. A seguito della guerra di aggressione della Russia nei confronti dell'Ucraina, il GTsSS ha sferrato attacchi informatici (attacchi di phishing mirato e attacchi basati su malware) contro l'Ucraina.	22.10.2020
▼M11				
5.	Integrity Technology Group	永信至诚科技集团股份有限公司 (grafia cinese) Pseudonimo: Beijing Integrity Technology Company Limited, Yongxin Zhicheng Technology Group Company Limited Indirizzo: Fenghao East Road, Room 103, Building 6, No. 9, Beijing Haidian District, China Luogo di registrazione: Beijing, China Data di registrazione: 2.9.2010 Codice unificato di credito sociale: 91110108562135265P	Integrity Technology Group è un'impresa di cibersicurezza con sede nella Repubblica popolare cinese che ha agevolato attacchi informatici legati alla minaccia mirata e persistente (*Advanced Persistent Threat* – APT) Flax Typhoon. Tale minaccia APT ha utilizzato i prodotti e la tecnologia di Integrity Technology Group per realizzare le sue attività di sfruttamento delle reti informatiche. Da allora, i prodotti di Integrity Technology Group sono utilizzati per compromettere i dispositivi dell'internet delle cose negli Stati membri, nonché in paesi in tutta Europa e nel mondo, e per accedervi. Tra il 2022 e il 2023 Flax Typhoon ha avuto accesso ad almeno 65 600 dispositivi dell'internet delle cose in sei Stati membri utilizzando i prodotti di Integrity Technology. Pertanto, i prodotti e le infrastrutture commerciali di Integrity Technology Group sono stati utilizzati regolarmente per attacchi informatici nei confronti di Stati membri e Stati terzi. Di conseguenza, colpendo i sistemi di informazione relativi alle infrastrutture digitali, Integrity Technology Group fornisce sostegno tecnico e materiale per attacchi informatici con effetti significativi che costituiscono una minaccia esterna per gli Stati membri e gli Stati terzi.	16.3.2026

▼M11

	Nome	Informazioni identificative	Motivi	Data di inserimento nell'elenco
6.	Emennet Pasargad	Pseudonimo: Anzu Team, Holy Souls, Aria Sepehr Ayandehsazan, Haywire Kitten Luogo di registrazione: Tehran, Iran Numero di registrazione: 554267 Sede principale: Tehran, Iran	Emennet Pasargad è un attore informatico iraniano (società) che ha preso di mira numerose entità, in particolare negli Stati membri e negli Stati Uniti. Emennet Pasargard, che opera con lo pseudonimo «Anzu Team», ha preso di mira l'infrastruttura digitale in Svezia e ha compromesso un servizio di SMS svedese, con conseguenze per un gran numero di persone. Inoltre, agendo con lo pseudonimo «Holy Souls», l'entità ha compromesso la banca dati degli abbonati della rivista satirica francese Charlie Hebdo mettendola in vendita sul dark web. Emennet Pasargad ha compromesso i cartelloni pubblicitari durante i Giochi olimpici di Parigi diffondendo campagne di disinformazione. Emennet Pasargad ha inoltre tentato di interferire con le elezioni presidenziali statunitensi del 2020, minacciando la democrazia e lo Stato di diritto, ottenendo informazioni riservate sugli elettori statunitensi e un accesso non autorizzato alla rete informatica di una società statunitense che opera nel settore dei media. Emennet Pasargad è pertanto responsabile di attacchi informatici con effetti significativi che costituiscono una minaccia esterna per gli Stati membri e di attacchi informatici con effetti significativi nei confronti di uno Stato terzo.	16.3.2026
7.	Anxun Information Technology Co. Ltd	安洵信息技术有限公司 (grafia cinese) Pseudonimo: i-Soon Indirizzo: Room 1002, Qiangqiang Building, No. 1318 Qixin Road, Minhang District, Shanghai Codice unificato di credito sociale: 91510105332025597A (filiale del Sichuan) Codice unificato di credito sociale: 91310116561906136G (filiale di Shanghai) Sito web: i-soon.net, isoon.net, i-soon.com.cn, isoonren.com, isoon.win Numeri di telefono: 16.3.2026862161119992, 16.3.20268605645893417, 16.3.20268613761671735, 16.3.2026864000665915 E-mail: shutdown@163.com, isoon2015@126.com, tao_tingting@i-soon.net, li_ping@i-soon.net	Anxun Information Technology Co. Ltd. è una società con sede nella Repubblica popolare cinese che offre servizi di «hacking-for-hire» (hackeraggio su commissione). Ha preso di mira infrastrutture critiche e funzioni statali essenziali degli Stati membri, ha avuto accesso a informazioni classificate e le ha vendute. Anxun Information Technology Co. Ltd. ha inoltre attaccato governi di vari Stati terzi, costituendo una minaccia per gli obiettivi della politica estera e di sicurezza comune (PESC) dell'Unione, come stabilito nell'articolo 21, paragrafo 2, lettere da a) a c), del trattato sull'Unione europea.. Anxun Information Technology Co. Ltd. trae un importante vantaggio economico dai servizi forniti. Anxun Information Technology Co. Ltd. è pertanto responsabile di attacchi informatici con effetti significativi che costituiscono una minaccia esterna per gli Stati membri e di attacchi informatici con effetti significativi nei confronti di Stati terzi.	16.3.2026

▼B

ALLEGATO II

Siti web contenenti informazioni sulle autorità competenti e l'indirizzo per le notifiche alla Commissione

▼M8

BELGIO

https://diplomatie.belgium.be/en/policy/policy_areas/peace_and_security/sanctions

BULGARIA

https://www.mfa.bg/en/EU-sanctions

CECHIA

www.financnianalytickyurad.cz/mezinarodni-sankce.html

DANIMARCA

https://um.dk/udenrigspolitik/sanktioner/ansvarlige-myndigheder

GERMANIA

https://www.bmwi.de/Redaktion/DE/Artikel/Aussenwirtschaft/embargos-aussenwirtschaftsrecht.html

ESTONIA

https://vm.ee/sanktsioonid-ekspordi-ja-relvastuskontroll/rahvusvahelised-sanktsioonid

IRLANDA

https://www.dfa.ie/our-role-policies/ireland-in-the-eu/eu-restrictive-measures/

GRECIA

http://www.mfa.gr/en/foreign-policy/global-issues/international-sanctions.html

SPAGNA

https://www.exteriores.gob.es/es/PoliticaExterior/Paginas/SancionesInternacionales.aspx

FRANCIA

http://www.diplomatie.gouv.fr/fr/autorites-sanctions/

CROAZIA

https://mvep.gov.hr/vanjska-politika/medjunarodne-mjere-ogranicavanja/22955

ITALIA

https://www.esteri.it/it/politica-estera-e-cooperazione-allo-sviluppo/politica_europea/misure_deroghe/

CIPRO

https://mfa.gov.cy/themes/

LETTONIA

https://www.fid.gov.lv/en

LITUANIA

https://www.urm.lt/en/lithuania-in-the-region-and-the-world/lithuanias-security-policy/international-sanctions/997

LUSSEMBURGO

https://maee.gouvernement.lu/fr/directions-du-ministere/affaires-europeennes/organisations-economiques-int/mesures-restrictives.html

UNGHERIA

https://kormany.hu/kulgazdasagi-es-kulugyminiszterium/ensz-eu-szankcios-tajekoztato

▼**M8**

MALTA

https://smb.gov.mt/

PAESI BASSI

https://www.rijksoverheid.nl/onderwerpen/internationale-sancties

AUSTRIA

https://www.bmeia.gv.at/themen/aussenpolitik/europa/eu-sanktionen-nationale-behoerden/

POLONIA

https://www.gov.pl/web/dyplomacja/sankcje-miedzynarodowe

https://www.gov.pl/web/diplomacy/international-sanctions

PORTOGALLO

https://portaldiplomatico.mne.gov.pt/politica-externa/medidas-restritivas

ROMANIA

http://www.mae.ro/node/1548

SLOVENIA

http://www.mzz.gov.si/si/omejevalni_ukrepi

SLOVACCHIA

https://www.mzv.sk/europske_zalezitosti/europske_politiky-sankcie_eu

FINLANDIA

https://um.fi/pakotteet

SVEZIA

https://www.regeringen.se/sanktioner

Indirizzo per le notifiche alla Commissione europea:

Commissione europea
Direzione generale della Stabilità finanziaria, dei servizi finanziari e dell'Unione dei mercati dei capitali (DG FISMA)
Rue de Spa 2/Spastraat 2
1049 Bruxelles/Brussel (Belgio)
E-mail: relex-sanctions@ec.europa.eu