



## Secretariat UNNPR

**De la:** sanctiuni.internationale@onpcsb.ro  
**Trimis:** Tuesday, March 24, 2026 2:36 PM  
**Către:** secretariat@unnpr.ro  
**Subiect:** Regim atacuri cibernetice: noi listări

Bună ziua,

În conformitate cu prevederile art. 5 alin. (1) din *OUG nr. 202/2008 privind punerea în aplicare a sancțiunilor internaționale*, cu modificările și completările ulterioare, vă transmitem spre publicare următoarele acte prin care se modifică regimuri sancționatorii internaționale, pentru postarea lor pe site-ul dvs. și, după caz, pentru comunicarea acestora către entitățile raportoare, în vederea îndeplinirii obligației de asigurare a publicității:

- [Regulamentul de punere în aplicare \(UE\) 2026/589 al Consiliului din 16 martie 2026 privind punerea în aplicare a Regulamentului \(UE\) 2019/796 privind măsuri restrictive împotriva atacurilor cibernetice care reprezintă o amenințare la adresa Uniunii sau a statelor sale membre](#)
- [Decizia \(PESC\) 2026/588 a Consiliului din 16 martie 2026 de modificare a Deciziei \(PESC\) 2019/797 privind măsuri restrictive împotriva atacurilor cibernetice care reprezintă o amenințare la adresa Uniunii sau a statelor sale membre](#)

Vă informăm că, la data de 16.03.2026, au fost adoptate actele normative sus menționate cu privire la regimul de măsuri restrictive împotriva atacurilor cibernetice care reprezintă o amenințare la adresa Uniunii sau a statelor sale membre, având ca efect listarea a 2 persoane și 3 entități și pot fi regăsite accesând link-urile menționate anterior.

Cu stimă,



**Oficiul Național de Prevenire și Combatere a Spălării Banilor**  
**FIU România**

Adresa: Bd.Tudor Vladimirescu nr.22, Clădirea Green Gate, Et.7, Sector 5, București

Tel. +40 213 155 207

[www.onpcsb.ro](http://www.onpcsb.ro)

[onpcsb@onpcsb.ro](mailto:onpcsb@onpcsb.ro)



2026/589

16.3.2026

**REGULAMENTUL DE PUNERE ÎN APLICARE (UE) 2026/589 AL CONSILIULUI**

**din 16 martie 2026**

**privind punerea în aplicare a Regulamentului (UE) 2019/796 privind măsuri restrictive împotriva atacurilor cibernetice care reprezintă o amenințare la adresa Uniunii sau a statelor sale membre**

CONSILIUL UNIUNII EUROPENE,

având în vedere Tratatul privind funcționarea Uniunii Europene,

având în vedere Regulamentul (UE) 2019/796 al Consiliului din 17 mai 2019 privind măsuri restrictive împotriva atacurilor cibernetice care reprezintă o amenințare la adresa Uniunii sau a statelor sale membre <sup>(1)</sup>, în special articolul 13 alineatul (1),

având în vedere propunerea Înalțului Reprezentant al Uniunii pentru afaceri externe și politica de securitate,

întrucât:

- (1) La 17 mai 2019, Consiliul a adoptat Regulamentul (UE) 2019/796.
- (2) Ca parte a acțiunii susținute, adaptate și coordonate a Uniunii împotriva entităților care reprezintă amenințări cibernetice persistente, două persoane fizice și trei entități ar trebui să fie incluse pe lista persoanelor fizice și juridice, a entităților și a organismelor cărora li se aplică măsurile restrictive prevăzută în anexa I la Regulamentul (UE) 2019/796. Respectivele persoane fizice și entități sunt răspunzătoare pentru atacuri cibernetice cu un efect semnificativ care constituie o amenințare externă la adresa Uniunii sau a statelor sale membre sau sunt implicate în astfel de atacuri.
- (3) Prin urmare, anexa I la Regulamentul (UE) 2019/796 ar trebui să fie modificată în consecință,

**ADOPTĂ PREZENTUL REGULAMENT:**

*Articolul 1*

Anexa I la Regulamentul (UE) 2019/796 se modifică în conformitate cu anexa la prezentul regulament.

*Articolul 2*

Prezentul regulament intră în vigoare la data publicării în *Jurnalul Oficial al Uniunii Europene*.

Prezentul regulament este obligatoriu în toate elementele sale și se aplică direct în toate statele membre.

Adoptat la Bruxelles, 16 martie 2026.

*Pentru Consiliu*

*Președintele*

K. KALLAS

(<sup>1</sup>) JO-L 129 I, 17.5.2019, p. 1, ELI: <http://data.europa.eu/eli/reg/2019/796/oj>.

## ANEXĂ

Anexa I la Regulamentul (UE) 2019/796 se modifică după cum urmează:

1. în secțiunea „A. Persoane fizice” se adaugă următoarele rubrici:

	Nume	Informații de identificare	Motive	Data includerii pe listă
„18.	CHEN Cheng	陈诚 (ortografia chineză) Alias: Jesse Chen lengmo l3n6m0 Data nașterii: 20.10.1984 Locul nașterii: Yancheng, Jiangsu, China Cetățenia: chineză Sexul: masculin	Chen Cheng este un om de afaceri chinez, cofondator și unul dintre directorii generali (director general administrativ) ai Anxun Information Technology Co. Ltd. De asemenea, este reprezentant legal al sucursalei din Sichuan a respectivei societăți. Anxun Information Technology Co. Ltd., cunoscută și sub denumirea i-Soon, este o societate cu sediul în Republica Populară Chineză (RPC) care oferă servicii de tip «hacking-for-hire». Anxun Information Technology Co. Ltd. a vizat infrastructura critică și funcțiile critice ale statului din statele membre și a accesat și vândut informații clasificate. În plus, Anxun Information Technology Co. Ltd. a atacat guverne din diferite	16.3.2026

			<p>state terțe, ceea ce reprezintă o amenințare la adresa obiectivelor Uniunii în materie de politică externă și de securitate comună (PESC), astfel cum se prevede la articolul 21 alineatul (2) literele (a)-(c) din Tratatul privind Uniunea Europeană.</p> <p>Anxun Information Technology Co. Ltd. obține un beneficiu economic important din serviciile furnizate.</p> <p>Prin urmare, Anxun Information Technology Co. Ltd. este responsabilă de atacuri cibernetice cu un efect semnificativ care constituie o amenințare externă la adresa statelor membre ale Uniunii, precum și de atacuri la adresa statelor terțe.</p> <p>În calitatea respectivă, Chen Cheng este responsabil de atacuri cibernetice cu efecte semnificative care reprezintă o amenințare externă la adresa statelor membre, precum și de atacuri cibernetice cu efecte semnificative împotriva unor state terțe și este implicat în astfel de atacuri.</p>	
19.	WU Haibo	<p>吴海波 (ortografia chineză)</p> <p>Alias: shutdown shutd0wn</p> <p>Locul nașterii: China</p> <p>Cetățenia: chineză</p> <p>Sexul: masculin</p>	<p>Wu Haibo este un om de afaceri chinez, cofondator și unul dintre directorii generali (director general administrativ) ai Anxun Information Technology Co. Ltd. De asemenea, este reprezentant legal, președinte și director</p>	16.3.2026”;

general al sucursalei din Shanghai («societatea mamă») a Anxun Information Technology Co. Ltd. De asemenea, acționează și în calitate de reprezentant legal al sucursalei din Sichuan al respectivei societăți.

Anxun Information Technology Co. Ltd., cunoscută și sub denumirea i-Soon, este o societate cu sediul în Republica Populară Chineză (RPC) care oferă servicii de tip «hacking-for-hire». Anxun Information Technology Co. Ltd. a vizat infrastructura critică și funcțiile critice ale statului din statele membre și a accesat și vândut informații clasificate. În plus, Anxun Information Technology Co. Ltd. a atacat guverne din diferite state terțe, ceea ce reprezintă o amenințare la adresa obiectivelor Uniunii în materie de politică externă și de securitate comună (PESC), astfel cum se prevede la articolul 21 alineatul (2) literele (a)-(c) din Tratatul privind Uniunea Europeană.

Anxun Information Technology Co. Ltd. obține un beneficiu economic important din serviciile furnizate.

Prin urmare, Anxun Information Technology Co. Ltd. este responsabilă de atacuri cibernetice cu un efect semnificativ care

		<p>constituie o amenințare externă la adresa statelor membre, precum și de atacuri la adresa statelor terțe.</p> <p>Wu Haibo a fost implicat în conducerea și încurajarea tentativelor de atacuri cibernetice cu efecte semnificative asupra statelor membre.</p> <p>În calitatea respectivă, el este responsabil de atacuri cibernetice cu efecte semnificative care reprezintă o amenințare externă la adresa statelor membre, precum și de atacuri cibernetice cu efecte semnificative împotriva unor state terțe și este implicat în astfel de atacuri.</p>
--	--	---

2. în secțiunea „B. Persoane juridice, entități și organisme” se adaugă următoarele rubrici:

	Denumire	Informații de identificare	Motive	Data includerii pe listă
„5.	Integrity Technology Group	<p>永信至诚科技集团股份有限公司 (ortografia chineză)</p> <p>Alias:</p> <p>Beijing Integrity Technology Company Limited, Yongxin Zhicheng Technology Group Company Limited</p> <p>Adresa: Fenghao East Road, Room 103, Building 6, No. 9, Beijing Haidian District, China</p> <p>Locul înregistrării: Beijing, China</p> <p>Data înregistrării: 2.9.2010</p> <p>Codul unificat de credit social: 91110108562135265P</p>	<p>Integrity Technology Group este o întreprindere din domeniul securității cibernetice, cu sediul în Republica Populară Chineză (RPC), care a facilitat atacuri cibernetice legate de Advanced Persistent Threat – (APT) Flax Typhoon. Respectiva APT a utilizat produsele și tehnologia Integrity Technology Group pentru a-și desfășura activitățile de exploatare a rețelelor informatice. De atunci, produsele</p>	16.3.2026

			<p>Integrity Technology Group au fost utilizate pentru a compromite și a accesa dispozitive din internetul obiectelor în statele membre, cât și în țări din întreaga Europă și la nivel global. Între 2022 și 2023, Flax Typhoon a accesat cel puțin 65 600 de dispozitive din internetul obiectelor în șase state membre prin utilizarea produselor Integrity Technology Group.</p> <p>Prin urmare, produsele comerciale și infrastructura Integrity Technology Group au fost utilizate în mod curent în atacurile cibernetice împotriva statelor membre, precum și a statelor terțe. În consecință, prin afectarea sistemelor informatice legate de infrastructura digitală, Integrity Technology Group oferă sprijin tehnic și material pentru atacurile cibernetice cu un efect semnificativ care constituie o amenințare externă la adresa statelor membre și a statelor terțe.</p>	
6.	Emennet Pasargad	<p>Alias: Anzu Team, Holy Souls, Aria Sepehr Ayandehsazan, Haywire Kitten Locul înregistrării: Teheran, Iran Număr de înregistrare: 554267 Locul principal de desfășurare a activității: Teheran, Iran</p>	<p>Emennet Pasargad este un actor cibernetic iranian (societate) care a vizat numeroase entități, în special în statele membre, precum și în Statele Unite (SUA).</p>	16.3.2026

Emennet Pasargad, care acționează sub denumirea «Anzu Team», a vizat infrastructura digitală din Suedia și a compromis un serviciu SMS suedez, afectând un număr mare de persoane. În plus, acționând sub denumirea «Holy Souls», entitatea a compromis baza de date a abonaților revistei satirice franceze Charlie Hebdo și a oferit-o spre vânzare pe dark web.

Emennet Pasargad a compromis panourile publicitare în timpul Jocurilor Olimpice de la Paris și a afișat campanii de dezinformare.

Emennet Pasargad a încercat, de asemenea, să intervină în alegerile prezidențiale din SUA în 2020, amenințând democrația și statul de drept, obținând informații confidențiale despre alegătorii americani și obținând acces neautorizat la rețeaua informatică a unei societăți mass-media din SUA.

Prin urmare, Emennet Pasargad este responsabil de atacuri cibernetice cu efecte semnificative care reprezintă o amenințare externă la adresa statelor membre, precum și de atacuri cibernetice cu

			efecte semnificative împotriva unui stat terț.	
7.	Anxun Information Technology Co. Ltd.	<p>安洵信息技术有限公司 (ortografia chineză)</p> <p>Alias: i-Soon</p> <p>Adresa: Room 1002, Qiangqiang Building, No. 1318 Qixin Road, Minhang District, Shanghai</p> <p>Codul unificat de credit social: 91510105332025597A (sucursala din Sichuan)</p> <p>Codul unificat de credit social: 91310116561906136G (sucursala din Shanghai)</p> <p>Site web: i-soon.net, isoon.net, i-soon.com.cn, isoonren.com, isoon.win</p> <p>Numere de telefon: +862161119992, +8605645893417, +8613761671735, +864000665915</p> <p>E-mail: shutdown@163.com, isoon2015@126.com, tao_tingting@i-soon.net, li_ping@i-soon.net.</p>	<p>Anxun Information Technology Co. Ltd. este o societate cu sediul în Republica Populară Chineză care oferă servicii de tip «hacking-for-hire». Aceasta a vizat infrastructura critică și funcțiile critice ale statului din statele membre și a accesat și vândut informații clasificate. În plus, Anxun Information Technology Co. Ltd. a atacat guverne din diferite state terțe, ceea ce reprezintă o amenințare la adresa obiectivelor Uniunii în materie de politică externă și de securitate comună (PESC), astfel cum se prevede la articolul 21 alineatul (2) literele (a)-(c) din Tratatul privind Uniunea Europeană. Anxun Information Technology Co. Ltd. obține un beneficiu economic important din serviciile furnizate.</p> <p>Prin urmare, Anxun Information Technology Co. Ltd. este responsabilă de atacuri cibernetice cu efecte semnificative care reprezintă o amenințare externă la adresa statelor membre, precum și de atacuri cibernetice cu efecte semnificative</p>	16.3.2026”.

			împotriva unor state terțe.	
--	--	--	--------------------------------	--

ELI: [http://data.europa.eu/eli/reg\\_impl/2026/589/oj](http://data.europa.eu/eli/reg_impl/2026/589/oj)

ISSN 1977-0782 (electronic edition)



2026/588

16.3.2026

**DECIZIA (PESC) 2026/588 A CONSILIULUI**

**din 16 martie 2026**

**de modificare a Deciziei (PESC) 2019/797 privind măsuri restrictive împotriva atacurilor cibernetice care reprezintă o amenințare la adresa Uniunii sau a statelor sale membre**

CONSILIUL UNIUNII EUROPENE,

având în vedere Tratatul privind Uniunea Europeană, în special articolul 29,

având în vedere propunerea Înalțului Reprezentant al Uniunii pentru afaceri externe și politica de securitate,

întrucât:

- (1) La 17 mai 2019, Consiliul a adoptat Decizia (PESC) 2019/797 <sup>(1)</sup>.
- (2) Ca parte a acțiunii susținute, adaptate și coordonate a Uniunii împotriva entităților care reprezintă amenințări cibernetice persistente, două persoane fizice și trei entități ar trebui să fie incluse pe lista persoanelor fizice și juridice, a entităților și a organismelor cărora li se aplică măsurile restrictive prevăzută în anexa la Decizia (PESC) 2019/797. Persoanele și entitățile respective sunt răspunzătoare pentru atacuri cibernetice cu un efect semnificativ care constituie o amenințare externă la adresa Uniunii sau a statelor sale membre sau sunt implicate în astfel de atacuri.
- (3) Prin urmare, Decizia (PESC) 2019/797 ar trebui să fie modificată în consecință,

ADOPTĂ PREZENTA DECIZIE:

*Articolul 1*

Anexa la Decizia (PESC) 2019/797 se modifică în conformitate cu anexa la prezenta decizie.

*Articolul 2*

Prezenta decizie intră în vigoare la data publicării în *Jurnalul Oficial al Uniunii Europene*.

Adoptată la Bruxelles, 16 martie 2026.

*Pentru Consiliu*  
*Președintele*  
K. KALLAS

(<sup>1</sup>) Decizia (PESC) 2019/797 a Consiliului din 17 mai 2019 privind măsuri restrictive împotriva atacurilor cibernetice care reprezintă o amenințare la adresa Uniunii sau a statelor sale membre (JO L 129 I, 17.5.2019, p. 13, ELI: <http://data.europa.eu/eli/dec/2019/797/oj>).

## ANEXĂ

Anexa la Decizia (PESC) 2019/797 se modifică după cum urmează:

1. În secțiunea „A. Persoane fizice” se adaugă următoarele rubrici:

	Nume	Informații de identificare	Motive	Data includerii pe listă
„18.	CHEN Cheng	陈诚 (ortografia chineză) Alias: Jesse Chen Jengmo J3n6m0 Data nașterii: 20.10.1984 Locul nașterii: Yancheng, Jiangsu, China Cetățenia: chineză Sexul: masculin	Chen Cheng este un om de afaceri chinez, cofondator și unul dintre directorii generali (director general administrativ) ai Anxun Information Technology Co. Ltd. De asemenea, este reprezentant legal al sucursalei din Sichuan a respectivei societăți. Anxun Information Technology Co. Ltd., cunoscută și sub denumirea i-Soon, este o societate cu sediul în Republica Populară Chineză (RPC) care oferă servicii de tip «hacking-for-hire». Anxun Information Technology Co. Ltd. a vizat infrastructura critică și funcțiile critice ale statului din statele membre și a accesat și vândut informații clasificate. În plus, Anxun Information Technology Co. Ltd. a atacat guverne din diferite state terțe, ceea ce reprezintă o amenințare la adresa obiectivelor Uniunii în materie de politică externă și de securitate comună (PESC), astfel cum se prevede la articolul 21	16.3.2026

			<p>alineatul (2) literele (a)-(c) din Tratatul privind Uniunea Europeană.</p> <p>Anxun Information Technology Co. Ltd. obține un beneficiu economic important din serviciile furnizate.</p> <p>Prin urmare, Anxun Information Technology Co. Ltd. este responsabilă de atacuri cibernetice cu un efect semnificativ care constituie o amenințare externă la adresa statelor membre ale Uniunii, precum și de atacuri la adresa statelor terțe.</p> <p>În calitatea respectivă, Chen Cheng este responsabil de atacuri cibernetice cu efecte semnificative care reprezintă o amenințare externă la adresa statelor membre, precum și de atacuri cibernetice cu efecte semnificative împotriva unor state terțe și este implicat în astfel de atacuri.</p>	
19.	WU Haibo	<p>吴海波 (ortografia chineză)</p> <p>Alias: shutdown shutd0wn</p> <p>Locul nașterii: China</p> <p>Cetățenia: chineză</p> <p>Sexul: masculin</p>	<p>Wu Haibo este un om de afaceri chinez, cofondator și unul dintre directorii generali (director general administrativ) ai Anxun Information Technology Co. Ltd. De asemenea, este reprezentant legal, președinte și director general al sucursalei din Shanghai («societatea mamă») a Anxun Information Technology Co. Ltd. De asemenea, acționează și în calitate de reprezentant legal al</p>	16.3.2026”

sucursalei din Sichuan al  
respectivei societăți.

Anxun Information  
Technology Co. Ltd.,  
cunoscută și sub denumirea  
Xi-Soon, este o societate cu  
sediul în Republica  
Populară Chineză (RPC)  
care oferă servicii de tip  
«hacking-for-hire». Anxun  
Information Technology  
Co. Ltd. a vizat  
infrastructura critică și  
funcțiile critice ale statului  
din statele membre și  
a accesat și vândut  
informații clasificate. În  
plus, Anxun Information  
Technology Co. Ltd.

a atacat guverne din diferite  
state terțe, ceea ce  
reprezintă o amenințare la  
adresa obiectivelor Uniunii  
în materie de politică  
externă și de securitate  
comună (PESC), astfel cum  
se prevede la articolul 21  
alineatul (2) literele (a)-(c)  
din Tratatul privind  
Uniunea Europeană.

Anxun Information  
Technology Co. Ltd. obține  
un beneficiu economic  
important din serviciile  
furnizate.

Prin urmare, Anxun  
Information Technology  
Co. Ltd. este responsabilă  
de atacuri cibernetice cu un  
efect semnificativ care  
constituie o amenințare  
externă la adresa statelor  
membre, precum și de  
atacuri la adresa statelor  
terțe.

		<p>Wu Haibo a fost implicat în conducerea și încurajarea tentativelor de atacuri cibernetice cu efecte semnificative asupra statelor membre.</p> <p>În calitate respectivă, el este responsabil de atacuri cibernetice cu efecte semnificative care reprezintă o amenințare externă la adresa statelor membre, precum și de atacuri cibernetice cu efecte semnificative împotriva unor state terțe și este implicat în astfel de atacuri.</p>
--	--	---

2. În secțiunea „B. Persoane juridice, entități și organisme” se adaugă următoarele rubrici:

	Denumire	Informații de identificare	Motive	Data includerii pe listă
„5.	Integrity Technology Group	<p>永信至诚科技集团股份有限公司 (ortografia chineză)</p> <p>Alias: Beijing Integrity Technology Company Limited, Yongxin Zhicheng Technology Group Company Limited</p> <p>Adresa: Fenghao East Road, Room 103, Building 6, No. 9, Beijing Haidian District, China</p> <p>Locul înregistrării: Beijing, China</p> <p>Data înregistrării: 2.9.2010</p> <p>Codul unificat de credit social: 91110108562135265P</p>	<p>Integrity Technology Group este o întreprindere din domeniul securității cibernetice, cu sediul în Republica Populară Chineză (RPC), care a facilitat atacuri cibernetice legate de Advanced Persistent Threat – (APT) Flax Typhoon. Respectiva APT a utilizat produsele și tehnologia Integrity Technology Group pentru a-și desfășura activitățile de exploatare a rețelelor informatice. De atunci, produsele Integrity Technology Group au fost utilizate pentru a compromite și a accesa dispozitive din internetul obiectelor în statele membre, cât și în</p>	16.3.2026

			<p>tări din întreaga Europă și la nivel global.</p> <p>Între 2022 și 2023, Flax Typhoon a accesat cel puțin 65 600 de dispozitive din internetul obiectelor în șase state membre prin utilizarea produselor Integrity Technology Group.</p> <p>Prin urmare, produsele comerciale și infrastructura Integrity Technology Group au fost utilizate în mod curent în atacurile cibernetice împotriva statelor membre, precum și a statelor terțe. În consecință, prin afectarea sistemelor informatice legate de infrastructura digitală, Integrity Technology Group oferă sprijin tehnic și material pentru atacurile cibernetice cu un efect semnificativ care constituie o amenințare externă la adresa statelor membre și a statelor terțe.</p>	
6.	Emennet Pasargad	<p>Alias: Anzu Team, Holy Souls, Aria Sepehr Ayandehsazan, Haywire Kitten</p> <p>Locul înregistrării: Teheran, Iran</p> <p>Număr de înregistrare: 554267</p> <p>Locul principal de desfășurare a activității: Teheran, Iran</p>	<p>Emennet Pasargad este un actor cibernetic iranian (societate) care a vizat numeroase entități, în special în statele membre, precum și în Statele Unite (SUA).</p> <p>Emennet Pasargad, care acționează sub denumirea «Anzu Team», a vizat infrastructura digitală</p>	16.3.2026

			<p>din Suedia și a compromis un serviciu SMS suedez, afectând un număr mare de persoane. În plus, acționând sub denumirea «Holy Souls», entitatea a compromis baza de date a abonaților revistei satirice franceze Charlie Hebdo și a oferit-o spre vânzare pe dark web. Emennet Pasargard a compromis panourile publicitare în timpul Jocurilor Olimpice de la Paris și a afișat campanii de dezinformare. Emennet Pasargad a încercat, de asemenea, să intervină în alegerile prezidențiale din SUA în 2020, amenințând democrația și statul de drept, obținând informații confidențiale despre alegătorii americani și obținând acces neautorizat la rețeaua informatică a unei societăți mass-media din SUA. Prin urmare, Emennet Pasargad este responsabil de atacuri cibernetice cu efecte semnificative care reprezintă o amenințare externă la adresa statelor membre, precum și de atacuri cibernetice cu efecte semnificative împotriva unui stat terț.</p>	
7.	Anxun Information	安洵信息技术有限公司 (ortografia chineză)	Anxun Information Technology Co. Ltd. este o societate cu sediul	16.3.2026”

<p>Technology Co. Ltd.</p>	<p>Alias: i-Soon</p> <p>Adresa: Room 1002, Qiangqiang Building, No. 1318 Qixin Road, Minhang District, Shanghai</p> <p>Codul unificat de credit social: 91510105332025597A (sucursala din Sichuan)</p> <p>Codul unificat de credit social: 91310116561906136G (sucursala din Shanghai)</p> <p>Site web: i-soon.net, isoon.net, i-soon.com.cn, isoonren.com, isoon.win</p> <p>Numere de telefon: +862161119992, +8605645893417, +8613761671735, +864000665915</p> <p>E-mail: shutdown@163.com, isoon2015@126.com, tao_tingting@i-soon.net, li_ping@i-soon.net</p>	<p>în Republica Populară Chineză care oferă servicii de tip «hacking-for-hire». Aceasta a vizat infrastructura critică și funcțiile critice ale statului din statele membre și a accesat și vândut informații clasificate. În plus, Anxun Information Technology Co. Ltd. a atacat guverne din diferite state terțe, ceea ce reprezintă o amenințare la adresa obiectivelor Uniunii în materie de politică externă și de securitate comună (PESC), astfel cum se prevede la articolul 21 alineatul (2) literele (a)-(c) din Tratatul privind Uniunea Europeană. Anxun Information Technology Co. Ltd. obține un beneficiu economic important din serviciile furnizate.</p> <p>Prin urmare, Anxun Information Technology Co. Ltd. este responsabilă de atacuri cibernetice cu efecte semnificative care reprezintă o amenințare externă la adresa statelor membre, precum și de atacuri cibernetice cu efecte semnificative împotriva unor state terțe.</p>
----------------------------	--	--