►B

ROZHODNUTÍ RADY (SZBP) 2019/797

ze dne 17. května 2019,

o omezujících opatřeních proti kybernetickým útokům ohrožujícím Unii nebo její členské státy

(Úř. věst. L 129I, 17.5.2019, s. 13)

Ve znění:

		Úřední věstník		
		Č.	Strana	Datum
►M1	Rozhodnutí Rady (SZBP) 2020/651 ze dne 14. května 2020	L 153	4	15.5.2020
►M2	Rozhodnutí Rady (SZBP) 2020/1127 ze dne 30. července 2020	L 246	12	30.7.2020
►M3	Rozhodnutí Rady (SZBP) 2020/1537 ze dne 22. října 2020	L 351I	5	22.10.2020
►M4	Rozhodnutí Rady (SZBP) 2020/1748 ze dne 20. listopadu 2020	L 393	19	23.11.2020

Opraveno:

►C1 Oprava, Úř. věst. L 230, 17.7.2020, s. 36 (2019/797)

▼B

ROZHODNUTÍ RADY (SZBP) 2019/797

ze dne 17. května 2019,

o omezujících opatřeních proti kybernetickým útokům ohrožujícím Unii nebo její členské státy

Článek 1

1. Toto rozhodnutí se použije na kybernetické útoky s významným dopadem, včetně pokusů o kybernetické útoky s potenciálně významným dopadem, které představují vnější hrozbu pro Unii a její členské státy.

2. Kybernetické útoky představující vnější hrozbu zahrnují útoky, které:

a) vznikají nebo jsou prováděny mimo Unii;

b) využívají infrastrukturu mimo Unii;

c) jsou prováděny jakoukoli fyzickou nebo právnickou osobou, subjektem nebo orgánem usazenými nebo působícími mimo Unii; nebo

d) jsou prováděny za podpory, pod vedením nebo pod kontrolou jakékoli fyzické nebo právnické osoby, subjektu nebo orgánu působících mimo Unii.

3. Pro tento účel se kybernetickými útoky rozumí činnosti zahrnující jednu z následujících oblastí:

a) přístup k informačním systémům;

b) zasahování do informačních systémů;

c) zasahování do údajů; nebo

d) zachycování údajů,

pokud tyto činnosti nejsou řádně povoleny majitelem či jiným držitelem práv k systému nebo údajům či jejich části, anebo nejsou povoleny na základě práva Unie či dotyčného členského státu.

4. Kybernetické útoky představující hrozbu pro členské státy zahrnují útoky, které postihují informační systémy týkající se mimo jiné:

a) kritické infrastruktury, včetně podmořských kabelů a předmětů vypuštěných do kosmického prostoru, které mají zásadní význam pro zachování životně důležitých funkcí společnosti nebo zdraví, bezpečnosti a ekonomického nebo sociálního blahobytu občanů;

b) služeb nezbytných pro zachování zásadních společenských nebo hospodářských činností, zejména v odvětví energetiky (elektřina, ropa a zemní plyn); dopravy (letecká, železniční, vodní a silniční); bankovnictví; infrastruktur finančních trhů; zdravotnictví (poskytovatelé zdravotní péče, nemocnice a soukromé kliniky); dodávek

▼B

a rozvodů pitné vody; digitální infrastruktury; nebo jakéhokoli dalšího odvětví, jež má zásadní význam pro dotyčný členský stát;

c) kritických funkcí státu, především v oblasti obrany, správy věcí veřejných a fungování institucí, včetně pořádání veřejných voleb či hlasování, fungování hospodářské a civilní infrastruktury, vnitřní bezpečnosti a vnějších vztahů, a to i prostřednictvím diplomatických misí;

d) uchovávání nebo zpracovávání utajovaných informací; nebo

e) vládních skupin pro reakci na počítačové hrozby.

5. Kybernetické útoky představující hrozbu pro Unii zahrnují útoky, které jsou vedeny proti jejím orgánům, institucím a subjektům, proti jejím delegacím ve třetích zemích nebo mezinárodních organizacích, proti jejím misím a operacím Společné bezpečnostní a obranné politiky (SBOP) a jejím zvláštním zástupcům.

6. Tam, kde je to považováno za nezbytné k dosažení cílů SZBP v příslušných ustanoveních článku 21 Smlouvy o Evropské unii, mohou být omezující opatření podle tohoto rozhodnutí rovněž použita v rámci reakce na kybernetické útoky s významným dopadem na třetí země nebo mezinárodní organizace.

Článek 2

Pro účely tohoto rozhodnutí se rozumí:

a) „informačními systémy“ jakýkoli přístroj nebo skupina vzájemně propojených nebo přidružených přístrojů, z nichž jeden nebo více provádí na základě programu automatické zpracování digitálních údajů, jakož i digitální údaje uložené, zpracované, opětovně vyhledané nebo přenesené tímto přístrojem či skupinou přístrojů za účelem jeho či jejich provozu, použití, ochrany a údržby;

b) „zasahováním do informačních systémů“ narušení nebo přerušení fungování informačního systému vložením digitálních údajů či jejich přenosem, poškozením, vymazáním, znehodnocením, pozměněním nebo potlačením nebo znepřístupněním;

c) „zasahováním do údajů“ vymazání, poškození, znehodnocení, pozměnění nebo potlačení digitálních údajů v informačním systému nebo znepřístupnění takových údajů; zahrnuje rovněž krádež údajů, finančních prostředků, hospodářských zdrojů nebo duševního vlastnictví;

d) „zachycováním údajů“ sledování neveřejných přenosů digitálních údajů do informačního systému, z něj nebo uvnitř něj, prováděné technickými prostředky, a to včetně elektromagnetického záření z informačního systému nesoucího takové digitální údaje;

▼B

Článek 3

Faktory určující, zda má kybernetický útok významný dopad podle čl. 1 odst. 1, mohou mimo jiné zahrnovat:

a) rozsah, míru, dopad nebo závažnost způsobeného narušení, včetně dopadu na hospodářské a společenské činnosti, základní služby, kritické funkce státu, veřejný pořádek či veřejnou bezpečnost;

b) počet zasažených fyzických nebo právnických osob, subjektů nebo orgánů;

c) počet dotčených členských států;

d) výši hospodářské ztráty způsobené například rozsáhlými krádežemi finančních prostředků, hospodářských zdrojů nebo duševního vlastnictví;

e) hospodářský přínos, který získal pachatel pro sebe nebo pro jiné osoby;

f) výši či povahu odcizených údajů nebo míru porušení ochrany údajů; nebo

g) povahu obchodně citlivých údajů, k nimž byl získán přístup.

Článek 4

1. Členské státy přijmou opatření nezbytná k tomu, aby zabránily ve vstupu na své území nebo průjezdu přes své území:

a) fyzickým osobám odpovědným za kybernetické útoky nebo za pokusy o ně;

b) fyzickým osobám, které poskytují finanční, technickou či materiální podporu na kybernetické útoky nebo pokusy o ně nebo jsou do nich jiným způsobem zapojeny, a to včetně plánování, přípravy, účasti, řízení, pomoci či podněcování těchto útoků [nebo jejich napomáhání, ať už aktivně, nebo opomenutím;

c) fyzickým osobám spojeným s osobami uvedenými v písmenech a) a b),

jak jsou zařazeny na seznam uvedený v příloze.

2. Z odstavce 1 nevyplývá pro členské státy povinnost odmítnout vstup na své území svým státním příslušníkům.

3. Odstavcem 1 nejsou dotčeny případy, kdy je členský stát vázán povinností podle mezinárodního práva, zejména:

a) jako hostitelská země mezinárodní mezivládní organizace;

b) jako hostitelská země mezinárodní konference svolané nebo konané pod záštitou Organizace spojených národů;

c) podle mnohostranné dohody o výsadách a imunitách nebo

d) na základě smlouvy o smíru z roku 1929 (Lateránský pakt) uzavřené mezi Svatým stolcem (Vatikánským městským státem) a Itálií.

▼B

4. Odstavec 3 se vztahuje rovněž na případy, kdy je členský stát hostitelskou zemí Organizace pro bezpečnost a spolupráci v Evropě (OBSE).

5. Rada je řádně informována o všech případech, kdy členský stát udělí výjimku podle odstavce 3 nebo 4.

6. Členské státy mohou udělit výjimky z opatření uložených podle odstavce 1, pokud je cesta dotyčné osoby odůvodněna naléhavými humanitárními potřebami nebo účastí na mezivládních zasedáních, včetně zasedání podporovaných nebo pořádaných Unií nebo zasedání pořádaných členským státem vykonávajícím předsednictví OBSE, na nichž je veden politický dialog, který přímo podporuje politické cíle sledované omezujícími opatřeními včetně prosazování bezpečnosti a stability v kyberprostoru.

7. Členské státy také mohou udělit výjimky z opatření uložených podle odstavce 1, pokud je vstup nebo průjezd nezbytný z důvodu soudního řízení.

8. Členský stát, který hodlá udělit výjimky uvedené v odstavci 6 nebo 7, tuto skutečnost oznámí písemně Radě. Výjimka se pokládá za udělenou, pokud jeden nebo více členů Rady nevznese písemně námitku do dvou pracovních dnů od obdržení oznámení o navrhované výjimce. Pokud jeden nebo více členů Rady vznese námitku, může o udělení navrhované výjimky rozhodnout Rada kvalifikovanou většinou.

9. Pokud členský stát povolí podle odstavců 3, 4, 6, 7 nebo 8 osobám zařazeným na seznam uvedený v příloze vstup na své území nebo průjezd přes ně, je toto povolení striktně omezeno na účel, pro který bylo uděleno, a na osoby, jichž se přímo týká.

Článek 5

1. Zmrazují se veškeré finanční prostředky a hospodářské zdroje, které patří:

a) fyzickým nebo právnickým osobám, subjektům nebo orgánům nesoucím odpovědnost za kybernetické útoky nebo za pokusy o ně;

b) fyzickým nebo právnickým osobám, subjektům či orgánům, které poskytují finanční, technickou či materiální podporu na kybernetické útoky nebo pokusy o ně nebo jsou do nich jiným způsobem zapojeny, a to včetně plánování, přípravy, účasti, řízení, pomoci či podněcování těchto útoků nebo jejich napomáhání, ať už aktivně, nebo opomenutím;

c) fyzickým nebo právnickým osobám, subjektům nebo orgánům spojeným s fyzickými nebo právnickými osobami, subjekty nebo orgány uvedenými v písmenech a) a b),

jak jsou zařazeny na seznam uvedený v příloze.

▼B

2. Fyzickým nebo právnickým osobám, subjektům nebo orgánům zařazeným na seznam uvedený v příloze ani v jejich prospěch nesmějí být přímo ani nepřímo zpřístupněny žádné finanční prostředky ani hospodářské zdroje.

3. Odchylně od odstavců 1 a 2 mohou příslušné orgány členských států povolit uvolnění některých zmrazených finančních prostředků nebo hospodářských zdrojů nebo zpřístupnění některých finančních prostředků nebo hospodářských zdrojů za podmínek, které považuje za vhodné, pokud shledají, že tyto finanční prostředky nebo hospodářské zdroje jsou:

a) ►C1 nezbytné pro uspokojení základních potřeb fyzických nebo právnických osob, subjektů nebo orgánů zařazených na seznam uvedený v příloze ◄ a rodinných příslušníků závislých na těchto fyzických osobách, včetně plateb za potraviny, plateb nájemného nebo splátek hypoték, plateb za léky a lékařskou péči a plateb daní, pojistného a poplatků za veřejné služby;

b) určené výlučně k úhradě přiměřených honorářů za odborné výkony nebo k náhradě výdajů vzniklých v souvislosti s poskytováním právních služeb;

c) určené výlučně k úhradě poplatků nebo nákladů na běžné vedení nebo správu zmrazených finančních prostředků nebo hospodářských zdrojů;

d) nezbytné k úhradě mimořádných výdajů, pokud daný příslušný orgán oznámí příslušným orgánům ostatních členských států a Komisi nejméně dva týdny před udělením povolení důvody, proč se domnívá, že by dané povolení mělo být uděleno, nebo

e) určené k platbě na účet nebo z účtu diplomatické mise, konzulárního úřadu nebo mezinárodní organizace požívající výsad podle mezinárodního práva, pokud mají být tyto platby použity pro služební účely této diplomatické mise, konzulárního úřadu nebo mezinárodní organizace.

Dotčený členský stát uvědomí ostatní členské státy a Komisi o každém povolení uděleném podle tohoto odstavce.

4. Odchylně od odstavce 1 mohou příslušné orgány členského státu povolit uvolnění některých zmrazených finančních prostředků nebo hospodářských zdrojů, jsou-li splněny tyto podmínky:

a) finanční prostředky nebo hospodářské zdroje jsou předmětem rozhodčího nálezu, který byl vydán přede dnem zařazení fyzické nebo právnické osoby, subjektu nebo orgánu uvedených v odstavci 1 na seznam obsažený v příloze, nebo předmětem soudního nebo správního rozhodnutí vydaného v Unii nebo soudního rozhodnutí vykonatelného v dotčeném členském státě, před tímto dnem nebo po něm;

▼B

b) finanční prostředky nebo hospodářské zdroje budou použity výlučně k uspokojení nároků zajištěných nebo uznaných za platné takovým nálezem či rozhodnutím, a to v mezích stanovených platnými právními předpisy, kterými se řídí práva osob uplatňujících takové nároky;

c) nález či rozhodnutí není ve prospěch fyzické nebo právnické osoby, subjektu či orgánu zařazeného na seznam uvedený v příloze; a

d) uznání nálezu či rozhodnutí není v rozporu s veřejným pořádkem v dotčeném členském státě.

Dotčený členský stát uvědomí ostatní členské státy a Komisi o každém povolení uděleném podle tohoto odstavce.

5. Odstavec 1 nebrání fyzickým nebo právnickým osobám, subjektům či orgánům zařazeným na seznam uvedený v příloze provést platbu vyplývající ze smlouvy, jež byla uzavřena před jejich zařazením, jestliže dotčený členský stát shledá, že tuto platbu přímo ani nepřímo neobdrží fyzická nebo právnická osoba, subjekt či orgán uvedené v odstavci 1.

6. Odstavec 2 se nepoužije, jsou-li na zmrazené účty připsány:

a) úroky nebo jiné výnosy z těchto účtů;

b) platby splatné na základě smluv, dohod nebo závazků, které byly uzavřeny nebo vznikly přede dnem, od nějž se na tyto účty vztahují opatření podle odstavců 1 a 2, nebo

c) platby splatné na základě soudního či správního rozhodnutí nebo rozhodčího nálezu, které byly vydány v Unii nebo které jsou v dotčeném členském státě vykonatelné,

pokud se na veškeré takové úroky, jiné výnosy a platby nadále vztahují opatření podle odstavce 1.

Článek 6

1. Rada na návrh členského státu nebo vysokého představitele Unie pro zahraniční věci a bezpečnostní politiku jednomyslně rozhoduje o sestavení nebo změně seznamu uvedeného v příloze.

2. Rada sdělí dotčené fyzické nebo právnické osobě, subjektu nebo orgánu své rozhodnutí podle odstavce 1 včetně důvodů jejich zařazení na seznam buď přímo, je-li známa jejich adresa, nebo zveřejněním oznámení, a tím dané fyzické nebo právnické osobě, subjektu nebo orgánu umožní se k věci vyjádřit.

3. Jsou-li předloženy připomínky nebo nové podstatné důkazy, Rada své rozhodnutí podle odstavce 1 přezkoumá a informuje o tom dotčenou fyzickou nebo právnickou osobu, subjekt nebo orgán.

▼B

Článek 7

1. V příloze jsou uvedeny důvody zařazení fyzických a právnických osob, subjektů a orgánů podle článků 4 a 5 na seznam.

2. V příloze jsou uvedeny dostupné informace nezbytné k identifikaci dotčených fyzických nebo právnických osob, subjektů nebo orgánů. V případě fyzických osob mohou tyto informace zahrnovat jména a další používaná jména, datum a místo narození, státní příslušnost, číslo pasu a číslo průkazu totožnosti, pohlaví, adresu, je-li známa, a funkci nebo povolání. V případě právnických osob, subjektů nebo orgánů mohou tyto informace zahrnovat názvy, místo a datum registrace, registrační číslo a místo podnikání.

Článek 8

Nesmí být uspokojen žádný nárok vyplývající ze smlouvy nebo transakce, jejichž plnění nebo uskutečnění bylo přímo nebo nepřímo, zcela nebo částečně dotčeno opatřeními uloženými tímto rozhodnutím, včetně náhrady škody nebo jiných nároků tohoto druhu, jako je nárok na náhradu nebo nárok vyplývající ze záruky, zejména nárok na prodloužení doby platnosti nebo vyplacení dluhopisů, záruk nebo příslibu odškodnění v jakékoli formě, zejména finančních záruk nebo příslibů finančního odškodnění, je-li vznesen:

a) určenými fyzickými nebo právnickými osobami, subjekty či orgány uvedenými na seznamu v příloze;

b) jakoukoli fyzickou nebo právnickou osobou, subjektem nebo orgánem jednajícími prostřednictvím nebo jménem fyzických nebo právnických osob, subjektů nebo orgánů uvedených v písmeni a).

Článek 9

Pro dosažení co největšího účinku opatření stanovených v tomto rozhodnutí podporuje Unie třetí země v přijímání omezujících opatření podobných těm, která jsou stanovena v tomto rozhodnutí.

▼M1

Článek 10

Toto rozhodnutí se použije do 18. května 2021. Toto rozhodnutí je průběžně přezkoumáváno. Bude–li mít Rada za to, že jeho cílů nebylo dosaženo, odpovídajícím způsobem prodlouží jeho použitelnost nebo je změní.

▼B

Článek 11

Toto rozhodnutí vstupuje v platnost prvním dnem po vyhlášení v *Úředním věstníku Evropské unie*.

▼B

PŘÍLOHA

Seznam fyzických a právnických osob, subjektů a orgánů podle článků 4 a 5

▼M2

A. Fyzické osoby

▼M4

	Jméno	Identifikační údaje	Odůvodnění	Datum zařazení na seznam
1.	GAO Qiang (Kao Čchiang)	Datum narození: 4. října 1983 Místo narození: Provincie Shandong (Šantung), Čína Adresa: Room 1102, Guanfu Mansion, 46 Xinkai Road, Hedong District, Tianjin (Tchien-ťin), Čína Státní občanství: čínské Pohlaví: muž	Kao Čchiang je zapojen do „operace Cloud Hopper“, což byla série kybernetických útoků s významným dopadem pocházejících ze zemí mimo Unii a představujících vnější hrozbu pro Unii nebo její členské státy a kybernetických útoků s významným dopadem na třetí státy. „Operace Cloud Hopper“ byla namířena na informační systémy nadnárodních společností na šesti světadílech, včetně společností se sídlem v Unii, a v jejím rámci byl získán neoprávněný přístup k údajům citlivým z obchodního hlediska, což mělo za následek významné ekonomické ztráty. „Operaci Cloud Hopper“ provedl aktér veřejně známý jako „APT10“ („Advanced Persistent Threat 10“) (také znám jako „Red Apollo“, „CVNX“, „Stone Panda“, „MenuPass“ a „Potassium“). Kao Čchiang může být s aktérem APT10 spojen, a to i prostřednictvím svého napojení na řídicí a kontrolní infrastrukturu aktéra APT10. Kromě toho byl Kao Čchiang zaměstnán u společnosti Huaying Haitai, což je subjekt označený z důvodu poskytování podpory pro „operaci Cloud Hopper“ a napomáhání k ní. Má vazby na Čang Š’-lunga, který je v souvislosti s „operací Cloud Hopper“ rovněž označen. Kao Čchiang je proto spojen jak se společností Huaying Haitai, tak i s Čang Š’-lungem.	30. 7. 2020
2.	ZHANG Shilong (Čang Š’-lung)	Datum narození: 10. září 1981 Místo narození: Čína Adresa: Hedong, Yuyang Road No 121, Tianjin (Tchien-ťin), Čína Státní občanství: čínské Pohlaví: muž	Čang Š’-lung je zapojen do „operace Cloud Hopper“, což byla série kybernetických útoků s významným dopadem pocházejících ze zemí mimo Unii a představujících vnější hrozbu pro Unii nebo její členské státy a kybernetických útoků s významným dopadem na třetí státy.	30. 7. 2020

▼M4

	Jméno	Identifikační údaje	Odůvodnění	Datum zařazení na seznam
			„Operace Cloud Hopper“ byla namířena na informační systémy nadnárodních společností na šesti světadílech, včetně společností se sídlem v Unii, a v jejím rámci byl získán neoprávněný přístup k údajům citlivým z obchodního hlediska, což mělo za následek významné ekonomické ztráty. „Operaci Cloud Hopper“ provedl aktér veřejně známý jako „APT10“ („Advanced Persistent Threat 10“) (také znám jako „Red Apollo“, „CVNX“, „Stone Panda“, „MenuPass“ a „Potassium“). Čang Š’-lung může být s aktérem APT10 spojen, a to i prostřednictvím malwaru, který v souvislosti s kybernetickými útoky provedenými aktérem APT10 vyvinul a otestoval. Kromě toho byl Čang Š’-lung zaměstnán u společnosti Huaying Haitai, což je subjekt označený z důvodu poskytování podpory pro „operaci Cloud Hopper“ a napomáhání k ní. Má vazby na Kao Čchianga, který je v souvislosti s „operací Cloud Hopper“ rovněž označen. Čang Š’-lung je proto spojen jak se společností Huaying Haitai, tak i s Kao Čchiangem.	

▼M2

3.	Alexey Valeryevich MININ (Alexej Valerjevič Minin)	Алексей Валерьевич МИНИН Datum narození: 27. května 1972 Místo narození: Permská oblast, Ruská SFSR (nyní Ruská federace) Číslo pasu: 120017582 Vydalo: Ministerstvo zahraničních věcí Ruské federace Platnost: od 17. dubna 2017 do 17. dubna 2022 Místo výkonu zaměstnání: Moskva, Ruská federace Státní občanství: ruské Pohlaví: muž	Alexej Minin se podílel na pokusu o kybernetický útok s potenciálně významným dopadem na Organizaci pro zákaz chemických zbraní (OPCW) v Nizozemsku. Jako důstojník pro podporu zpravodajství lidských zdrojů působící v rámci hlavního ředitelství generálního štábu ozbrojených sil Ruské federace (GU/GRU) byl Alexej Minin součástí týmu čtyř ruských vojenských zpravodajských důstojníků, kteří se v dubnu 2018 pokusili získat neoprávněný přístup do bezdrátové sítě organizace OPCW v Haagu (Nizozemsko). Pokus o kybernetický útok byl zaměřen na „hacking“ do bezdrátové sítě organizace OPCW, který by v případě úspěchu ohrozil bezpečnost sítě a probíhající vyšetřovací činnost této organizace. Nizozemská obranná zpravodajská a bezpečnostní služba (Militaire Inlichtingen- en Veiligheidsdienst – MIVD) pokus o kybernetický útok zmařila, čímž zabránila vážným škodám pro organizaci OPCW.	30. 7. 2020

▼M2

	Jméno	Identifikační údaje	Odůvodnění	Datum zařazení na seznam
4.	Aleksei Sergeyvich MORENETS (Alexej Sergejevič Moreněc)	Алексей Сергеевич МОРЕНЕЦ Datum narození: 31. července 1977 Místo narození: Murmanská oblast, Ruská SFSR (nyní Ruská federace) Číslo pasu: 100135556 Vydalo: Ministerstvo zahraničních věcí Ruské federace Platnost: od 17. dubna 2017 do 17. dubna 2022 Místo výkonu zaměstnání: Moskva, Ruská federace Státní občanství: ruské Pohlaví: muž	Alexej Moreněc se podílel na pokusu o kybernetický útok s potenciálně významným dopadem na Organizaci pro zákaz chemických zbraní (OPCW) v Nizozemsku. Jako pracovník pro kybernetické operace působící v rámci hlavního ředitelství generálního štábu ozbrojených sil Ruské federace (GU/GRU) byl Alexej Moreněc součástí týmu čtyř ruských vojenských zpravodajských důstojníků, kteří se v dubnu 2018 pokusili získat neoprávněný přístup do bezdrátové sítě organizace OPCW v Haagu (Nizozemsko). Pokus o kybernetický útok byl zaměřen na „hacking“ do bezdrátové sítě organizace OPCW, který by v případě úspěchu ohrozil bezpečnost sítě a probíhající vyšetřovací činnost této organizace. Nizozemská obranná zpravodajská a bezpečnostní služba (Militaire Inlichtingen- en Veiligheidsdienst – MIVD) pokus o kybernetický útok zmařila, čímž zabránila vážným škodám pro organizaci OPCW.	30. 7. 2020
5.	Evgenii Mikhaylovich SEREBRIAKOV (Jevgenij Michailovič Serebrjakov)	Евгений Михайлович СЕРЕБРЯКОВ Datum narození: 26. července 1981 Místo narození: Kursk, Ruská SFSR (nyní Ruská federace) Číslo pasu: 100135555, Vydalo: Ministerstvo zahraničních věcí Ruské federace Platnost: od 17. dubna 2017 do 17. dubna 2022 Místo výkonu zaměstnání: Moskva, Ruská federace Státní občanství: ruské Pohlaví: muž	Jevgenij Serebrjakov se podílel na pokusu o kybernetický útok s potenciálně významným dopadem na Organizaci pro zákaz chemických zbraní (OPCW) v Nizozemsku. Jako pracovník pro kybernetické operace působící v rámci hlavního ředitelství generálního štábu ozbrojených sil Ruské federace (GU/GRU) byl Jevgenij Serebrjakov součástí týmu čtyř ruských vojenských zpravodajských důstojníků, kteří se v dubnu 2018 pokusili získat neoprávněný přístup do bezdrátové sítě organizace OPCW v Haagu (Nizozemsko). Pokus o kybernetický útok byl zaměřen na „hacking“ do bezdrátové sítě organizace OPCW, který by v případě úspěchu ohrozil bezpečnost sítě a probíhající vyšetřovací činnost této organizace. Nizozemská obranná zpravodajská a bezpečnostní služba (Militaire Inlichtingen- en Veiligheidsdienst – MIVD) pokus o kybernetický útok zmařila, čímž zabránila vážným škodám pro organizaci OPCW.	30. 7. 2020

▼M2

	Jméno	Identifikační údaje	Odůvodnění	Datum zařazení na seznam
6.	Oleg Mikhaylovich SOTNIKOV (Oleg Michajlovič Sotnikov)	Олег Михайлович СОТНИКОВ Datum narození: 24. srpna 1972 Místo narození: Uljanovsk, Ruská SFSR (nyní Ruská federace) Číslo pasu: 120018866 Vydalo: Ministerstvo zahraničních věcí Ruské federace Platnost. od 17. dubna 2017 do 17. dubna 2022 Místo výkonu zaměstnání: Moskva, Ruská federace Státní občanství: ruské Pohlaví: muž	Oleg Sotnikov se podílel na pokusu o kybernetický útok s potenciálně významným dopadem na Organizaci pro zákaz chemických zbraní (OPCW) v Nizozemsku. Jako důstojník pro podporu zpravodajství lidských zdrojů působící v rámci hlavního ředitelství generálního štábu ozbrojených sil Ruské federace (GU/GRU) byl Oleg Sotnikov součástí týmu čtyř ruských vojenských zpravodajských důstojníků, kteří se v dubnu 2018 pokusili získat neoprávněný přístup do bezdrátové sítě organizace OPCW v Haagu (Nizozemsko). Pokus o kybernetický útok byl zaměřen na „hacking“ do bezdrátové sítě organizace OPCW, který by v případě úspěchu ohrozil bezpečnost sítě a probíhající vyšetřovací činnost této organizace. Nizozemská obranná zpravodajská a bezpečnostní služba (Militaire Inlichtingen- en Veiligheidsdienst – MIVD) pokus o kybernetický útok zmařila, čímž zabránila vážným škodám pro organizaci OPCW.	30. 7. 2020
▼M3 7.	Dmitry Sergeyevich BADIN	Дмитрий Сергеевич БАДИН Datum narození: 15. listopadu 1990 Místo narození: Kursk, Ruská SFSR (nyní Ruská federace) Státní občanství: ruské Pohlaví: muž	Dmitrij Badin se podílel na kybernetickém útoku s významným dopadem namířeném proti německému Spolkovému sněmu (Deutscher Bundestag). Jako vojenský zpravodajský důstojník 85. hlavního střediska pro speciální služby (GTsSS) hlavního ředitelství generálního štábu ozbrojených sil Ruské federace (GU/GRU) byl Dmitrij Badin součástí týmu ruských vojenských zpravodajských důstojníků, který v dubnu a květnu 2015 provedl kybernetický útok na německý Spolkový sněm (Deutscher Bundestag). Uvedený kybernetický útok byl namířen proti informačnímu systému sněmu a na několik dní narušil jeho provoz. Byl při něm odcizen značný objem dat a byly postiženy emailové účty několika poslanců, jakož i kancléřky Angely Merkelové.	22.10.2020

▼M3

	Jméno	Identifikační údaje	Odůvodnění	Datum zařazení na seznam
8.	Igor Olegovich KOSTYUKOV	Игорь Олегович КОСТЮКОВ Datum narození: 21. února 1961 Státní občanství: ruské Pohlaví: muž	Igor Kosťjukov je v současné době vedoucím hlavního ředitelství generálního štábu ozbrojených sil Ruské federace (GU/GRU), kde předtím působil jako první náměstek vedoucího. Jedním z oddělení, která spadala pod jeho vedení, je 85. hlavní středisko pro speciální služby (GTsSS), rovněž známé jako vojenská jednotka 26165 (pracovní přezdívky: APT28, Fancy Bear, Sofacy Group, Pawn Storm a Strontium). Ze své funkce je Igor Kosťjukov odpovědný za kybernetické útoky provedené GTsSS, včetně kybernetických útoků s významným dopadem, které představují vnější hrozbu pro Unii nebo její členské státy. Vojenští zpravodajští důstojníci GTsSS se zejména podíleli na kybernetickém útoku na německý Spolkový sněm (Deutscher Bundestag), k němuž došlo v dubnu a květnu 2015, a na pokusu o kybernetický útok, k němuž došlo v dubnu 2018 a jehož cílem bylo proniknout do bezdrátové sítě Organizace pro zákaz chemických zbraní (OPCW) v Nizozemsku. Kybernetický útok na německý Spolkový sněm byl namířen proti informačnímu systému sněmu a na několik dní narušil jeho provoz. Byl při něm odcizen značný objem dat a byly postiženy emailové účty několika poslanců, jakož i kancléřky Angely Merkelové.	22.10.2020

▼M2

B. Právnické osoby, subjekty a orgány

	Název	Identifikační údaje	Odůvodnění	Datum zařazení na seznam
1.	Tianjin Huaying Haitai Science and Technology Development Co Ltd	Také známa jako: Haitai Technology Development Co. Ltd Místo: Tchien-ťin, Čína	Společnost Huaying Haitai poskytovala finanční, technickou nebo materiální podporu pro „operaci Cloud Hopper“, což byla série kybernetických útoků s významným dopadem pocházejících ze zemí mimo Unii a představujících vnější hrozbu pro Unii nebo její členské státy a kybernetických útoků s významným dopadem na třetí státy, a k této operaci napomáhala.	30. 7. 2020

▼M2

	Název	Identifikační údaje	Odůvodnění	Datum zařazení na seznam
			„Operace Cloud Hopper“ byla namířena na informační systémy nadnárodních společností na šesti světadílech, včetně společností se sídlem v Unii, a v jejím rámci byl získán neoprávněný přístup k údajům citlivým z obchodního hlediska, což mělo za následek významné ekonomické ztráty. „Operaci Cloud Hopper“ provedl aktér veřejně známý jako „APT10“ („Advanced Persistent Threat 10“) (také znám jako „Red Apollo“, „CVNX“, „Stone Panda“, „MenuPass“ a „Potassium“). Společnost Huaying Haitiai může být s aktérem APT10 spojena. Kromě toho společnost Huaying Haitai zaměstnávala Kao Čchianga a Čang Š’-lunga, kteří jsou oba v souvislosti s „operací Cloud Hopper“ označeni. Společnost Huaying Haitia je proto s Kao Čchiangem a Čang Š’-lungem spojena.	
2.	Chosun Expo	Také známa jako: Chosen Expo; Korea Export Joint Venture Místo: KLDR	Společnost Chosun Expo poskytla finanční, technickou nebo materiální podporu pro sérii kybernetických útoků s významným dopadem pocházejících ze zemí mimo Unii a představujících vnější hrozbu pro Unii nebo její členské státy, jakož i s významným dopadem na třetí státy, včetně kybernetických útoků veřejně známých jako „WannaCry“ a kybernetických útoků na polský Úřad pro finanční dozor a společnost Sony Pictures Entertainment, jakož i kybernetické krádeže z banky Bangladesh Bank a pokusu o kybernetickou krádež z banky Vietnam Tien Phong Bank. Kybernetické útoky „WannaCry“ narušily fungování informačních systémů po celém světě tím, že se zaměřily na informační systémy pomocí ransomwaru a zablokovaly přístup k údajům. Měly nepříznivý dopad na informační systémy společností v Unii, včetně informačních systémů týkajících se služeb nezbytných pro udržování základních služeb a hospodářských činností v členských státech. Kybernetické útoky „WannaCry“ provedl aktér veřejně známý jako „APT38“ („Advanced Persistent Threat 38“) a skupina „Lazarus Group“. Společnost Chosun Expo může být na aktéra APT38 nebo skupinu Lazarus Group napojena, a to i prostřednictvím účtů používaných pro kybernetické útoky.	30. 7. 2020

▼M2

	Název	Identifikační údaje	Odůvodnění	Datum zařazení na seznam
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) (Hlavní středisko pro speciální technologie (GTsST) hlavního ředitelství generálního štábu ozbrojených sil Ruské federace (GU/GRU))	Adresa: Ul. Kirova 22, Moskva, Ruská federace	Hlavní středisko pro speciální technologie (GTsST) hlavního ředitelství generálního štábu ozbrojených sil Ruské federace (GU/GRU), známé rovněž pod svým systémovým identifikačním číslem 74455, je odpovědné za kybernetické útoky s významným dopadem pocházející ze zemí mimo Unii a představující vnější hrozbu pro Unii nebo její členské státy a za kybernetické útoky s významným dopadem na třetí státy, včetně kybernetických útoků veřejně známých jako „NotPetya“ nebo „EternalPetya“ provedených v červnu 2017 a kybernetických útoků namířených na ukrajinskou elektrickou rozvodnou síť v zimě 2015 a 2016. Kybernetické útoky „NotPetya“ nebo „EternalPetya“ znemožnily přístup k údajům v řadě společností v Unii, v širší Evropě a po celém světě tím, že se zaměřily na počítače pomocí ransomwaru a zablokovaly přístup k údajům, což mělo mimo jiné za následek významné ekonomické ztráty. Kybernetický útok na ukrajinskou elektrickou rozvodnou síť způsobil, že její části byly během zimy odpojeny. Za útokem na ukrajinskou elektrickou síť, který byl proveden pomocí útoků „NotPetya“ nebo „EternalPetya“, stál aktér veřejně známý jako „Sandworm“ (také znám jako „Sandworm Team“, „BlackEnergy Group“, „Voodoo Bear“, „Quedagh“, „Olympic Destroyer“ a „Telebots“). Hlavní středisko pro speciální technologie v rámci hlavního ředitelství generálního štábu ozbrojených sil Ruské federace se aktivně podílí na kybernetických činnostech prováděných aktérem Sandworm a může být na tohoto aktéra napojeno.“	30. 7. 2020

▼M3

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) (85. hlavní středisko pro speciální služby (GTsSS) hlavního ředitelství generálního štábu ozbrojených sil Ruské federace (GU/GRU))	Adresa: Komsomolskij Prospekt, 20, Moskva, 119146, Ruská federace	85. hlavní středisko pro speciální služby (GTsSS) hlavního ředitelství generálního štábu ozbrojených sil Ruské federace (GU/GRU), které je rovněž známé jako vojenská jednotka 26165 (pracovní přezdívky: APT28, Fancy Bear, Sofacy Group, Pawn Storm, Strontium), je odpovědné za kybernetické útoky s významným dopadem, které představují vnější hrozbu pro Unii nebo její členské státy.	22.10.2020

▼M3

	Název	Identifikační údaje	Odůvodnění	Datum zařazení na seznam
			Vojenští zpravodajští důstojníci GTsSS se zejména podíleli na kybernetickém útoku na německý Spolkový sněm (Deutscher Bundestag), k němuž došlo v dubnu a květnu 2015, a na pokusu o kybernetický útok, k němuž došlo v dubnu 2018 a jehož cílem bylo proniknout do bezdrátové sítě Organizace pro zákaz chemických zbraní (OPCW) v Nizozemsku. Kybernetický útok na německý Spolkový sněm byl namířen proti informačnímu systému sněmu a na několik dní narušil jeho provoz. Byl při něm odcizen značný objem dat a byly postiženy emailové účty několika poslanců, jakož i kancléřky Angely Merkelové.	