►**B**

NAŘÍZENÍ RADY (EU) 2019/796

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. 1)

Ve znění:

		Úřední věstník		
		Č.	Strana	Datum
►**M1**	Prováděcí nařízení Rady (EU) 2020/1125 ze dne 30. července 2020	L 246	4	30.7.2020
►**M2**	Prováděcí nařízení Rady (EU) 2020/1536 ze dne 22. října 2020	L 351 I	1	22.10.2020
►**M3**	Prováděcí nařízení Rady (EU) 2020/1744 ze dne 20. listopadu 2020	L 393	1	23.11.2020
►**M4**	Prováděcí nařízení Komise (EU) 2022/595 ze dne 11. dubna 2022	L 114	60	12.4.2022

Opraveno:

►**C1** Oprava, Úř. věst. L 230, 17.7.2020, s. 37 (2019/796)

▼B

NAŘÍZENÍ RADY (EU) 2019/796

ze dne 17. května 2019,

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

Článek 1

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

▼B

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 společné zahraniční a bezpečnostní politiky (SZBP) v příslušných ustanoveních článku 21 Smlouvy o Evropské unii, mohou být omezující opatření podle tohoto nařízení rovněž použita v rámci reakce na kybernetické útoky s významným dopadem na třetí země nebo mezinárodní organizace.

7. Pro účely tohoto nařízení 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, 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.

8. Pro účely tohoto nařízení se dále rozumí:

a) „nárokem“ jakýkoli nárok, uplatňovaný právní cestou či nikoli, jenž vznikl přede dnem nebo po dni vstupu tohoto nařízení v platnost na základě smlouvy nebo transakce nebo v souvislosti s nimi, a zejména:

   i) nárok na plnění závazku vyplývajícího ze smlouvy nebo transakce nebo s nimi spojeného;

   ii) nárok na prodloužení doby platnosti nebo na vyplacení dluhopisů, finančních záruk nebo příslibu odškodnění v jakékoli formě;

   iii) nárok na náhradu škody související se smlouvou nebo transakcí;

   iv) protinárok;

▼B

v) nárok na uznání nebo vymáhání, včetně využití doložky vykonatelnosti, rozsudku či rozhodčího nálezu nebo jiného rovnocenného rozhodnutí bez ohledu na místo vydání;

b) „smlouvou nebo transakcí“ jakákoli transakce bez ohledu na její formu a použitelné právo a bez ohledu na to, zda zahrnuje jednu nebo více smluv nebo podobných závazků uzavřených mezi týmiž nebo různými stranami; v tomto smyslu se „smlouvou“ rozumějí též dluhopisy, záruky nebo přísliby odškodnění, zejména finanční záruky nebo přísliby finančního odškodnění, a úvěry, ať už jsou právně nezávislé, či nikoli, a jakákoli související ujednání vyplývající z dané transakce nebo s ní související;

c) „příslušnými orgány“ příslušné orgány členských států uvedené na internetových stránkách, jejichž seznam je uveden v příloze II;

d) „hospodářskými zdroji“ aktiva všeho druhu, hmotná nebo nehmotná, movitá či nemovitá, která nejsou finančními prostředky, ale lze je použít k získání finančních prostředků, zboží nebo služeb;

e) „zmrazením hospodářských zdrojů“ zabránění jejich použití k získání finančních prostředků, zboží nebo služeb jakýmkoli způsobem, zejména prodejem, pronájmem nebo zastavením;

f) „zmrazením finančních prostředků“ zabránění jakémukoli pohybu, převodu, přeměně nebo použití finančních prostředků, přístupu k nim nebo zacházení s nimi jakýmkoli způsobem, který by vedl k jakékoli změně jejich objemu, výše, umístění, vlastnictví, držby, povahy, určení nebo k jiné změně, která by umožnila použití těchto prostředků, včetně správy portfolia;

g) „finančními prostředky“ finanční aktiva a výnosy všeho druhu, mimo jiné:

i) peníze v hotovosti, šeky, peněžní pohledávky, směnky, peněžní příkazy a jiné platební nástroje;

ii) vklady u finančních institucí a jiných subjektů, zůstatky na účtech, pohledávky a závazky z pohledávek;

iii) veřejně i soukromě obchodované cenné papíry a dluhové nástroje, včetně akcií a kapitálových podílů, certifikátů zastupujících cenné papíry, dluhopisů, směnek, opčních listů, dlužních úpisů a smluv o derivátových nástrojích;

iv) úroky, dividendy nebo jiné výnosy nebo hodnoty pocházející z aktiv nebo jimi vytvářené;

v) úvěry, práva na započtení, záruky, závazky plnění nebo jiné finanční závazky;

vi) akreditivy, nákladní listy a dodací listy; a

vii) dokumenty prokazující podíl na finančních prostředcích nebo na finančních zdrojích;

▼B

(a) „územím Unie“ území členských států, na která se vztahuje Smlouva za podmínek v ní stanovených, včetně jejich vzdušného prostoru.

Článek 2

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 či 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 3

1. Zmrazují se veškeré finanční prostředky a hospodářské zdroje, které patří fyzickým nebo právnickým osobám, subjektům či orgánům zařazeným na seznam uvedený v příloze I nebo které jsou jimi vlastněny, drženy či ovládány.

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

3. V příloze I jsou uvedeny, jak určila Rada v souladu s čl. 5 odst. 1 rozhodnutí (SZBP) 2019/797:

a) fyzické nebo právnické osoby, subjekty či orgány nesoucí odpovědnost za kybernetické útoky nebo za pokus o ně;

b) fyzické nebo právnické osoby, subjekty nebo orgány, 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) fyzické nebo právnické osoby, subjekty nebo orgány spojené s fyzickými nebo právnickými osobami, subjekty nebo orgány uvedenými v písmenech a) a b) tohoto odstavce.

▼B

Článek 4

1. Odchylně od článku 3 mohou příslušné orgány členských států povolit za podmínek, které považují za vhodné, uvolnění některých zmrazených finančních prostředků nebo hospodářských zdrojů nebo zpřístupnění některých zmrazených finančních prostředků nebo hospodářských zdrojů, pokud rozhodnou o tom, že dotyčné 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 I ◄ 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) určeny výlučně k úhradě přiměřených honorářů za odborné výkony či k náhradě výdajů vzniklých v souvislosti s poskytováním právních služeb;

c) určeny výlučně k úhradě poplatků nebo nákladů na běžné vedení nebo správu zmrazených 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.

2. Dotčený členský stát uvědomí ostatní členské státy a Komisi o každém povolení uděleném podle odstavce 1 do dvou týdnů od jeho udělení.

Článek 5

1. Odchylně od čl. 3 odst. 1 mohou příslušné orgány členských států povolit uvolnění některých zmrazených finančních prostředků nebo hospodářských zdrojů, jsou-li splněny tyto podmínky:

a) tyto finanční prostředky nebo hospodářské zdroje jsou předmětem rozhodčího nálezu, který byl vydán přede dnem zařazení fyzické nebo právnické osoby, subjektu či orgánu uvedených v článku 3 na seznam obsažený v příloze I, nebo předmětem soudního či správního rozhodnutí vydaného v Unii nebo soudního rozhodnutí vykonatelného v dotčeném členském státě před tímto dnem či po něm;

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

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

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

▼B

2. Dotčený členský stát uvědomí ostatní členské státy a Komisi o každém povolení uděleném podle odstavce 1 do dvou týdnů od jeho udělení.

Článek 6

1. Odchylně od čl. 3 odst. 1 a v případě, kdy je splatná platba fyzické nebo právnické osoby, subjektu či orgánu zařazených na seznam uvedený v příloze I na základě smlouvy nebo dohody, která byla uzavřena dotčenou fyzickou nebo právnickou osobou, subjektem či orgánem, nebo povinnosti, která dotčené fyzické nebo právnické osobě, subjektu či orgánu vznikla přede dnem, kdy byla tato fyzická nebo právnická osoba, subjekt či orgán zařazena na seznam uvedený v příloze I, mohou příslušné orgány členských států za podmínek, které považují za vhodné, povolit uvolnění některých zmrazených finančních prostředků nebo hospodářských zdrojů, pokud dotčený příslušný orgán shledal, že:

a) finanční prostředky nebo hospodářské zdroje budou použity na platbu provedenou fyzickou nebo právnickou osobou, subjektem či orgánem zařazenými na seznam uvedený v příloze I; a

b) platba není v rozporu s čl. 3 odst. 2.

2. Dotčený členský stát uvědomí ostatní členské státy a Komisi o každém povolení uděleném podle odstavce 1 do dvou týdnů od jeho udělení.

Článek 7

1. Ustanovení čl. 3 odst. 2 nebrání finančním nebo úvěrovým institucím, aby na zmrazené účty připisovaly finanční prostředky, které byly na daný účet fyzické nebo právnické osoby, subjektu či orgánu uvedených na seznamu převedeny třetími stranami, budou-li přírůstky těchto účtů rovněž zmrazeny. Dotčená finanční nebo úvěrová instituce neprodleně uvědomí o každé takové operaci příslušný orgán.

2. Ustanovení čl. 3 odst. 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, kdy byly fyzická nebo právnická osoba, subjekt nebo orgán uvedené v čl. 3 odst. 1 zařazeny na seznam uvedený v příloze I, nebo

c) platby splatné na základě soudních nebo správních rozhodnutí nebo rozhodčích nálezů vydaných v členském státě nebo vykonatelných v dotčeném členském státě;

pokud se na veškeré takové úroky, jiné výnosy a platby nadále vztahují opatření podle čl. 3 odst. 1.

Článek 8

1. Aniž jsou dotčeny platné předpisy o ohlašování, důvěrnosti údajů a profesním tajemství, fyzické a právnické osoby, subjekty a orgány:

▼B

a) neprodleně poskytnou příslušnému orgánu členského státu, ve kterém mají bydliště nebo sídlo, veškeré informace, které mohou usnadnit zajištění souladu s tímto nařízením, jako jsou informace o účtech a částkách zmrazených v souladu s čl. 3 odst. 1, a předají tyto informace přímo nebo prostřednictvím dotčeného členského státu Komisi a

b) spolupracují s příslušným orgánem při ověřování informací uvedených v písmeni a).

2. Veškeré dodatečné informace, které obdrží přímo Komise, se zpřístupní členským státům.

3. Veškeré informace poskytnuté nebo obdržené na základě tohoto článku se použijí pouze pro účely, pro něž byly poskytnuty nebo obdrženy.

Článek 9

Zakazuje se vědomě a úmyslně se účastnit činností, jejichž cílem nebo následkem je obcházení opatření uvedených v článku 3.

Článek 10

1. Zmrazení finančních prostředků a hospodářských zdrojů nebo odmítnutí zpřístupnit finanční prostředky nebo hospodářské zdroje učiněné v dobré víře, že je takové jednání v souladu s tímto nařízením, nezakládá žádnou odpovědnost fyzické nebo právnické osoby, subjektu či orgánu, které je provádějí, ani jejich vedoucích pracovníků či zaměstnanců, ledaže se prokáže, že tyto finanční prostředky a hospodářské zdroje byly zmrazeny nebo zadrženy v důsledku nedbalosti.

2. Jednání fyzických nebo právnických osob, subjektů nebo orgánů nezakládá jejich odpovědnost, pokud nevěděly a neměly žádný důvod se domnívat, že svým jednáním porušují opatření stanovená v tomto nařízení.

Článek 11

1. Nesmí být uspokojen žádný nárok vyplývající ze smlouvy nebo transakce, jejichž plnění nebo uskutečnění je přímo nebo nepřímo, zcela nebo částečně dotčeno opatřeními uloženými tímto nařízením, a to včetně náhrady škody nebo jiných nároků tohoto druhu, jako je nárok na náhradu škody 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 zařazenými na seznam uvedený v příloze I;

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

2. Ve všech řízeních týkajících se uplatnění nároku nese důkazní břemeno ohledně toho, že uspokojení nároku není zakázáno odstavcem 1, fyzická nebo právnická osoba, subjekt či orgán uplatňující tento nárok.

3. Tímto článkem není dotčeno právo fyzických nebo právnických osob, subjektů a orgánů uvedených v odstavci 1 na soudní přezkum legálnosti neplnění smluvních závazků v souvislosti s tímto nařízením.

▼B

Článek 12

1. Komise a členské státy se navzájem informují o opatřeních přijatých podle tohoto nařízení a sdílejí všechny další důležité informace, které mají k dispozici v souvislosti s tímto nařízením, zejména informace o:

a) finančních prostředcích zmrazených na základě článku 3 a povoleních udělených na základě článků 4, 5 a 6;

b) porušování tohoto nařízení, o problémech s jeho vymáháním a o rozhodnutích vydaných vnitrostátními soudy.

2. Členské státy si poskytují navzájem a poskytují i Komisi veškeré další důležité informace, které mají k dispozici a které by mohly ovlivnit účinné provádění tohoto nařízení.

Článek 13

1. Pokud Rada rozhodne o tom, že se na fyzickou nebo právnickou osobu, subjekt či orgán mají vztahovat opatření uvedená v článku 3, změní odpovídajícím způsobem přílohu I.

2. Rada sdělí rozhodnutí uvedené v odstavci 1 dotčené fyzické nebo právnické osobě, subjektu nebo orgánu, 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.

4. Seznam uvedený v příloze I se pravidelně přezkoumává, a to nejméně každých 12 měsíců.

5. Komise je oprávněna měnit přílohu II na základě informací sdělených členskými státy.

Článek 14

1. V příloze I jsou uvedeny důvody pro zařazení dotčených fyzických nebo právnických osob, subjektů a orgánů na seznam.

2. V příloze I jsou uvedeny dostupné informace nezbytné k identifikaci dotčených fyzických nebo právnických osob, subjektů či 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 15

1. Členské státy stanoví pravidla pro sankce za porušení tohoto nařízení a přijmou veškerá nezbytná opatření pro zajištění jejich uplatňování. Stanovené sankce musí být účinné, přiměřené a odrazující.

▼B

2. Členské státy oznámí Komisi pravidla uvedená v odstavci 1 neprodleně po vstupu tohoto nařízení v platnost a oznámí jí rovněž jakékoli následné změny.

Článek 16

1. Komise za účelem plnění svých úkolů podle tohoto nařízení zpracovává osobní údaje. Mezi tyto úkoly patří:

a) doplnění obsahu přílohy I do veřejně dostupného elektronického konsolidovaného seznamu osob, skupin a subjektů, na něž se vztahují finanční sankce Unie, a do veřejně dostupné interaktivní mapy sankcí;

b) zpracování informací o dopadu opatření tohoto nařízení, jako je hodnota zmrazených finančních prostředků, a informací o povoleních udělených příslušnými orgány.

2. Pro účely tohoto nařízení je útvar Komise uvedený v příloze II určen „správcem“ za Komisi ve smyslu čl. 3 bodu 8 nařízení (EU) 2018/1725 s cílem zajistit, aby dotčené fyzické osoby mohly vykonávat svá práva podle uvedeného nařízení.

Článek 17

1. Členské státy určí příslušné orgány pro účely tohoto nařízení a údaje o nich zveřejní na internetových stránkách, jejichž seznam je v příloze II. Členské státy oznámí Komisi veškeré změny adres svých internetových stránek, jejichž seznam je v příloze II.

2. Členské státy oznámí Komisi své příslušné orgány včetně jejich kontaktních údajů neprodleně po vstupu tohoto nařízení v platnost a oznámí jí rovněž jakékoli následné změny.

3. Pokud se v tomto nařízení ukládá povinnost oznámit určité skutečnosti Komisi, informovat ji nebo s ní jinak komunikovat, použije se pro tyto účely adresa a další kontaktní údaje uvedené v příloze II.

Článek 18

Toto nařízení se použije:

a) na území Unie, včetně jejího vzdušného prostoru;

b) na palubě jakéhokoli letadla nebo plavidla v jurisdikci některého z členských států;

c) na každou fyzickou osobu, která je státním příslušníkem některého členského státu, ať již se nachází na území Unie nebo mimo ně;

d) na každou právnickou osobu, subjekt či orgán zapsaný nebo zřízený podle práva některého členského státu, ať se nacházejí na území Unie, nebo mimo ně;

e) na právnické osoby, subjekty nebo orgány v souvislosti s jakoukoli obchodní činností vykonávanou zcela nebo částečně v Unii.

▼B

Článek 19

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

Toto nařízení je závazné v celém rozsahu a přímo použitelné ve všech členských státech.

▼B

PŘÍLOHA I

Seznam fyzických nebo právnických osob, subjektů a orgánů uvedených v článku 3

▼M1

A. Fyzické osoby

	Jméno	Identifikační údaje	Odůvodnění	Datum zařazení na seznam
▼M3				
1.	GAO Qiang (Kao Čchiang)	Datum narození: 4. října 1983 Místo narození: Provincie Shandong (Šan-tung), 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. „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.	30.7.2020

▼M3

	Jméno	Identifikační údaje	Odůvodnění	Datum zařazení na seznam
			„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.	

▼M1

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
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

▼M1

	Jméno	Identifikační údaje	Odůvodnění	Datum zařazení na seznam
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
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

▼M1

	Jméno	Identifikační údaje	Odůvodnění	Datum zařazení na seznam
▼M2				
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
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

▼M1

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. „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 Čchi-angem a Čang Š’-lungem spojena.	30.7.2020
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.	30.7.2020

▼M1

	Název	Identifikační údaje	Odůvodnění	Datum zařazení na seznam
			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.	
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.	30.7.2020
			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.	

▼M1

	Název	Identifikační údaje	Odůvodnění	Datum zařazení na seznam
▼M2				
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. 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

▼B

PŘÍLOHA II

Internetové stránky pro informace o příslušných orgánech a adresa pro účely oznamování Komisi

▼M4

BELGIE

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

BULHARSKO

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

ČESKO

www.financnianalytickyurad.cz/mezinarodni-sankce.html

DÁNSKO

http://um.dk/da/Udenrigspolitik/folkeretten/sanktioner/

NĚMECKO

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

ESTONSKO

https://vm.ee/et/rahvusvahelised-sanktsioonid

IRSKO

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

ŘECKO

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

ŠPANĚLSKO

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

FRANCIE

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

CHORVATSKO

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

ITÁLIE

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

KYPR

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

LOTYŠSKO

http://www.mfa.gov.lv/en/security/4539

LITVA

http://www.urm.lt/sanctions

LUCEMBURSKO

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

MAĎARSKO

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

▼**M4**

MALTA

https://foreignandeu.gov.mt/en/Government/SMB/Pages/SMB-Home.aspx

NIZOZEMSKO

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

RAKOUSKO

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

POLSKO

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

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

PORTUGALSKO

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

RUMUNSKO

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

SLOVINSKO

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

SLOVENSKO

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

FINSKO

https://um.fi/pakotteet

ŠVÉDSKO

https://www.regeringen.se/sanktioner

Adresa pro účely oznamování Evropské komisi:

European Commission

Directorate-General for Financial Stability, Financial Services and Capital Markets Union (DG FISMA)

Rue de Spa / Spaastraat 2

B-1049 Bruxelles/Brussel, Belgie

E-mail: relex-sanctions@ec.europa.eu