



Rada
Evropské unie

Brusel 14. května 2019
(OR. en)

7299/19

LIMITE

CORLX 106
CFSP/PESC 191
RELEX 235
CYBER 81
JAI 264
FIN 216

PRÁVNÍ PŘEDPISY A JINÉ AKTY

Předmět: ROZHODNUTÍ RADY o omezujících opatřeních proti kybernetickým útokům ohrožujícím Unii nebo její členské státy

ROZHODNUTÍ RADY (SZBP) 2019/...

ze dne...

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

RADA EVROPSKÉ UNIE,

s ohledem na Smlouvu o Evropské unii, a zejména na článek 29 této smlouvy,

s ohledem na návrh vysoké představitelky Unie pro zahraniční věci a bezpečnostní politiku,

vzhledem k těmto důvodům:

- (1) Dne 19. června 2017 přijala Rada závěry Rady o rámci pro společnou diplomatickou reakci na nepřátelské činnosti v kyberprostoru („soubor nástrojů pro diplomacii v oblasti kybernetiky“), v nichž vyjádřila znepokojení nad zvyšující se schopností a odhodláním státních i nestátních subjektů sledovat své cíle prostřednictvím nepřátelských činností v kyberprostoru a potvrdila, že se zvyšuje potřeba chránit integritu a bezpečnost Unie, jejích členských států a jejích občanů proti kybernetickým hrozbám a nepřátelským činnostem v kyberprostoru.
- (2) Rada zdůraznila, že je-li dáno jasně najevo, jaké důsledky společná diplomatická reakce Unie na nepřátelské činnosti v kyberprostoru pravděpodobně bude mít, ovlivní se tím chování potenciálních agresorů v kyberprostoru a posílí bezpečnost Unie i jejích členských států. Rada rovněž potvrdila, že opatření v rámci společné zahraniční a bezpečnostní politiky (SZBP) přijatá na základě příslušných ustanovení Smluv a zahrnující v nutných případech i opatření omezující jsou z hlediska rámce pro společnou diplomatickou reakci Unie na nepřátelské činnosti v kyberprostoru vhodná a měla by podporovat spolupráci, usnadňovat zmírňování bezprostředních i dlouhodobých hrozeb a dlouhodobě ovlivňovat chování potenciálních agresorů.

- (3) Dne 11. října 2017 schválil Politický a bezpečnostní výbor prováděcí pokyny pro soubor nástrojů pro diplomacii v oblasti kybernetiky. Tyto prováděcí pokyny se týkají pěti kategorií opatření, včetně omezujících opatření, v rámci souboru nástrojů pro diplomacii v oblasti kybernetiky, jakož i postupu, jak tato opatření uplatnit.
- (4) V závěrech o nepřátelské činnosti v kyberprostoru, přijatých dne 16. dubna 2018, Rada důrazně odsoudila nepřátelské využívání informačních a komunikačních technologií a zdůraznila, že používání informačních a komunikačních technologií pro účely nepřátelských aktů je nepřijatelné, neboť jeho důsledkem je narušování stability, bezpečnosti a výhod, jež internet a informační a komunikační technologie skýtají. Rada připomněla, že soubor nástrojů pro diplomacii v oblasti kybernetiky přispívá k předcházení konfliktům, ke spolupráci v kyberprostoru a k jeho stabilitě, neboť vymezuje opatření v rámci SZBP, jichž lze k předcházení nepřátelským aktivitám v kyberprostoru a k reakci na ně využívat, a to včetně opatření omezujících. Uvedla, že Unie bude i v budoucnu důrazně prosazovat postoj, podle něhož je stávající mezinárodní právo právem rozhodným pro kyberprostor, a zdůraznila, že dodržování mezinárodního práva, zejména pak Charty Organizace spojených národů, má zásadní význam pro zachování míru a stability. Rada rovněž zdůraznila, že pro páchaní činů, jež představují porušení mezinárodního práva a jež využívají informační a komunikační technologie, jednotlivé státy nesmějí využívat ani prostředníků a že by měly usilovat o zajištění toho, aby takové činy z jejich vlastního území nepáchali nestátní aktéři, jak bylo uvedeno ve zprávě skupin vládních odborníků OSN pro rozvoj v oblasti informací a telekomunikací v kontextu mezinárodní bezpečnosti za rok 2015.

- (5) Evropská rada přijala dne 28. června 2018 závěry, v nichž zdůraznila, že je třeba posílit schopnosti zaměřené na boj proti hrozbám v oblasti kybernetické bezpečnosti majícím původ mimo Unii. Evropská rada vyzvala orgány i členské státy, aby zavedly opatření uvedená ve společném sdělení Komise a vysoké představitelky Unie pro zahraniční věci a bezpečnostní politiku ze dne 13. června 2018 nazvaném „Zvýšení odolnosti a posílení schopností reakce na hybridní hrozby“, včetně praktického využívání souboru nástrojů pro diplomacii v oblasti kybernetiky.
- (6) Evropská rada přijala dne 18. října 2018 závěry, v nichž vyzývá k tomu, aby v návaznosti na závěry Rady z 19. června 2017 pokročila práce věnovaná schopnosti odrazovat od kybernetických útoků a reagovat na ně prostřednictvím omezujících opatření Unie.
- (7) V uvedeném kontextu stanoví toto rozhodnutí rámec pro cílená omezující opatření pro odrazování od kybernetických útoků s významným dopadem, které představují vnější hrozbu pro Unii a její členské státy, a pro reakci na ně. Tam, kde je to považováno za nezbytné k dosažení cílů SZBP v příslušných ustanoveních článku 21 Smlouvy o Evropské unii, umožňuje toto rozhodnutí rovněž uplatňovat omezující opatření v rámci reakce na kybernetické útoky s významným dopadem na třetí země nebo mezinárodní organizace.

- (8) Mají-li mít cílená omezující opatření odrazující a odstrašující účinek, měla by se zaměřovat na kybernetické útoky spadající do oblasti působnosti tohoto rozhodnutí, jež jsou prováděny úmyslně.
- (9) Cílená omezující opatření by měla být odlišována od přičtení odpovědnosti třetímu státu za kybernetické útoky. Uplatnění cílených omezujících opatření nepředstavuje přičtení odpovědnosti v uvedeném smyslu, neboť se jedná o svrchované politické rozhodnutí přijímané případ od případu. Každý členský stát může učinit vlastní rozhodnutí, zda přičte odpovědnost třetímu státu za kybernetické útoky.
- (10) K provedení některých opatření je nezbytná další činnost Unie,

PŘIJALA TOTO ROZHODNUTÍ:

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); bankovníctví; 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;
 - 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 zneprístupněním;
- c) „zasahováním do údajů“ vymazání, poškození, znehodnocení, pozměnění nebo potlačení digitálních údajů v informačním systému nebo zneprístupnění 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;

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 povinnostmi 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.
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 mezinárodních 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 nevznesou písemně námitku do dvou pracovních dnů od obdržení oznámení o navrhované výjimce. Pokud jeden nebo více členů Rady vznesou 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.

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) nezbytné pro uspokojení základních potřeb fyzických osob 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 nálezů, 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) 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 něž 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.

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.

Článek 10

Toto rozhodnutí se použije do ... [jeden rok od vstupu tohoto rozhodnutí v platnost]. Toto rozhodnutí je průběžně přezkoumáváno. Bude-li mít Rada za to, že jeho cílů nebylo dosaženo, odpovídajícím způsobem prodlouží jeho použitelnost nebo je změní.

Článek 11

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

V ... dne ...

Za Radu

předseda nebo předsedkyně

PŘÍLOHA

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

[...]
