# ROZHODNUTÍ RADY (SZBP) 2021/1026

## ze dne 21. června 2021

## na podporu programu Organizace pro zákaz chemických zbraní (OPCW) zaměřeného na kybernetickou bezpečnost a odolnost a zabezpečení informací v rámci provádění strategie EU proti šíření zbraní hromadného ničení

RADA EVROPSKÉ UNIE,

s ohledem na Smlouvu o Evropské unii, a zejména na čl. 28 odst. 1 a čl. 31 odst. 1 této smlouvy,

s ohledem na návrh vysokého představitele Unie pro zahraniční věci a bezpečnostní politiku,

vzhledem k těmto důvodům:

(1) Dne 12. prosince 2003 přijala Evropská rada strategii EU proti šíření zbraní hromadného ničení (dále jen „strategie EU"), jejíž kapitola III obsahuje seznam opatření pro boj proti tomuto šíření.

(2) Strategie EU zdůrazňuje klíčovou úlohu Úmluvy o zákazu vývoje, výroby, hromadění zásob a použití chemických zbraní a jejich zničení (dále jen „úmluva") a Organizace pro zákaz chemických zbraní (OPCW) při vytváření světa bez chemických zbraní. Cíle této strategie EU doplňují cíle sledované OPCW v souvislosti s její odpovědností za provádění úmluvy.

(3) Dne 22. listopadu 2004 přijala Rada společnou akci 2004/797/SZBP ([1]) na podporu činnosti OPCW. Po skončení její platnosti následovala společná akce Rady 2005/913/SZBP ([2]) a po ní společná akce Rady 2007/185/SZBP ([3]).

Po uvedené společné akci následovala rozhodnutí Rady 2009/569/SZBP ([4]), 2012/166/SZBP ([5]), 2013/726/SZBP ([6]), (SZBP) 2015/259 ([7]), (SZBP) 2017/2302 ([8]), (SZBP) 2017/2303 ([9]) a (SZBP) 2019/538 ([10]).

([1]) Společná akce Rady 2004/797/SZBP ze dne 22. listopadu 2004 na podporu činnosti Organizace pro zákaz chemických zbraní (OPCW) v rámci provádění strategie EU proti šíření zbraní hromadného ničení (Úř. věst. L 349, 25.11.2004, s. 63).

([2]) Společná akce Rady 2005/913/SZBP ze dne 12. prosince 2005 na podporu činnosti Organizace pro zákaz chemických zbraní (OPCW) v rámci provádění strategie EU proti šíření zbraní hromadného ničení (Úř. věst. L 331, 17.12.2005, s. 34).

([3]) Společná akce Rady 2007/185/SZBP ze dne 19. března 2007 na podporu činnosti Organizace pro zákaz chemických zbraní (OPCW) v rámci provádění strategie EU proti šíření zbraní hromadného ničení (Úř. věst. L 85, 27.3.2007, s. 10).

([4]) Rozhodnutí Rady 2009/569/SZBP ze dne 27. července 2009 na podporu činnosti Organizace pro zákaz chemických zbraní (OPCW) v rámci provádění strategie EU proti šíření zbraní hromadného ničení (Úř. věst. L 197, 29.7.2009, s. 96).

([5]) Rozhodnutí Rady 2012/166/SZBP ze dne 23. března 2012 na podporu činnosti Organizace pro zákaz chemických zbraní (OPCW) v rámci provádění strategie EU proti šíření zbraní hromadného ničení (Úř. věst. L 87, 24.3.2012, s. 49).

([6]) Rozhodnutí Rady 2013/726/SZBP ze dne 9. prosince 2013 na podporu rezoluce Rady bezpečnosti OSN č. 2118 (2013) a rozhodnutí Výkonné rady Organizace pro zákaz chemických zbraní (OPCW) č. EC-M-33/Dec 1 v rámci provádění strategie EU proti šíření zbraní hromadného ničení (Úř. věst. L 329, 10.12.2013, s. 41).

([7]) Rozhodnutí Rady (SZBP) 2015/259 ze dne 17. února 2015 na podporu činnosti Organizace pro zákaz chemických zbraní (OPCW) v rámci provádění strategie EU proti šíření zbraní hromadného ničení (Úř. věst. L 43, 18.2.2015, s. 14).

([8]) Rozhodnutí Rady (SZBP) 2017/2302 ze dne 12. prosince 2017 na podporu činnosti Organizace pro zákaz chemických zbraní (OPCW) s cílem napomáhat při provádění sanačních a dekontaminačních operací v bývalém skladu chemických zbraní v Libyi v rámci provádění strategie EU proti šíření zbraní hromadného ničení (Úř. věst. L 329, 13.12.2017, s. 49).

([9]) Rozhodnutí Rady (SZBP) 2017/2303 ze dne 12. prosince 2017 na podporu pokračujícího provádění rezoluce Rady bezpečnosti OSN č. 2118 (2013) a rozhodnutí Výkonné rady Organizace pro zákaz chemických zbraní (OPCW) č. EC-M-33/DEC.1 o zničení syrských chemických zbraní v rámci provádění strategie EU proti šíření zbraní hromadného ničení (Úř. věst. L 329, 13.12.2017, s. 55).

([10]) Rozhodnutí Rady (SZBP) 2019/538 ze dne 1. dubna 2019 na podporu činnosti Organizace pro zákaz chemických zbraní (OPCW) v rámci provádění strategie EU proti šíření zbraní hromadného ničení (Úř. věst. L 93, 2.4.2019, s. 3).

(4) V souvislosti s aktivním prováděním kapitoly III strategie EU je nutné, aby Unie tuto intenzivní a cílenou pomoc OPCW nadále poskytovala.

(5) Je třeba, aby Unie dále podporovala program OPCW pro kybernetickou bezpečnost a odolnost a zabezpečení informací, jehož cílem je posílit schopnost OPCW zachovat náležitou úroveň kybernetické bezpečnosti a odolnosti při řešení současných a vznikajících výzev souvisejících s kybernetickou bezpečností,

PŘIJALA TOTO ROZHODNUTÍ:

*Článek 1*

1. Za účelem okamžitého a praktického provádění některých součástí strategie EU Unie podporuje projekt OPCW s těmito cíli:

— modernizovat infrastrukturu IKT v souladu s rámcem OPCW pro zachování kontinuity institucionální činnosti, se silným důrazem na odolnost, a

— zajistit řízení privilegovaného přístupu, správu fyzických, logických a kryptografických informací a oddělení všech strategických sítí OPCW a sítí jejích misí.

2. V souvislosti s odstavcem 1 se za činnosti projektu OPCW podporované Unií, které jsou v souladu s opatřeními stanovenými v kapitole III strategie EU, považují:

— zprovoznění prostředí napomáhajícího ke stávajícímu úsilí v oblasti kybernetické bezpečnosti a odolnosti v rámci operací OPCW prováděných na více místech,

— navržení individualizovaného řešení pro integraci a konfiguraci systémů umístěných v prostorách i v cloudu s IKT systémy OPCW a řešeními v oblasti řízení privilegovaného přístupu a

— zahájení a testování řešení v oblasti řízení privilegovaného přístupu.

3. Podrobný popis činností OPCW podporovaných Unií podle odstavce 2 je uveden v příloze.

*Článek 2*

1. Za provádění tohoto rozhodnutí odpovídá vysoký představitel Unie pro zahraniční věci a bezpečnostní politiku (dále jen „vysoký představitel“).

2. Technické provádění projektu uvedeného v článku 1 vykonává technický sekretariát OPCW (dále jen „technický sekretariát“). Tento úkol plní pod dohledem vysokého představitele, jenž za něj nese odpovědnost. Za tímto účelem uzavře vysoký představitel s technickým sekretariátem nezbytná ujednání.

*Článek 3*

1. Finanční referenční částka na provádění projektu uvedeného v článku 1 činí EUR 2 151 823.

2. Výdaje financované částkou stanovenou v odstavci 1 jsou spravovány v souladu s postupy a pravidly, kterými se řídí souhrnný rozpočet Unie.

3. Komise dohlíží na řádnou správu výdajů uvedených v odstavci 2. Za tímto účelem uzavře s technickým sekretariátem potřebnou dohodu. Tato dohoda stanoví, že technický sekretariát zajistí viditelnost příspěvku Unie úměrně jeho velikosti a stanoví opatření, která usnadní rozvoj součinnosti a zabrání zdvojování činností.

4. Komise usiluje o uzavření dohody uvedené v odstavci 3 co nejdříve po vstupu tohoto rozhodnutí v platnost. Informuje Radu o veškerých obtížích v tomto procesu a o dni uzavření uvedené dohody.

*Článek 4*

Vysoký představitel podává Radě zprávy o provádění tohoto rozhodnutí na základě pravidelných zpráv vypracovávaných technickým sekretariátem. Na základě těchto zpráv vysokého představitele provádí Rada hodnocení. Komise poskytne informace o finančních aspektech projektu uvedeného v článku 1.

*Článek 5*

1. Toto rozhodnutí vstupuje v platnost dnem přijetí.

2. Toto rozhodnutí pozbývá platnosti 24 měsíců ode dne uzavření dohody uvedené v čl. 3 odst. 3. Pozbývá však platnosti šest měsíců po svém vstupu v platnost, nebude-li do té doby uvedená dohoda uzavřena.

V Lucemburku dne 21. června 2021.

*Za Radu*
*předseda*
J. BORRELL FONTELLES

*PŘÍLOHA*

**PROJEKTOVÝ DOKUMENT**

1. Souvislosti

OPCW je povinna udržovat infrastrukturu, která umožňuje suverenitu v oblasti informací přiměřenou stupni utajení pro privilegovaný přístup, vhodným postupům pro nakládání s informacemi a existujícím hrozbám a která je současně nadále schopna poskytovat ochranu proti nově vznikajícím rizikům. OPCW nadále neustále čelí závažným a nově vznikajícím rizikům, pokud jde o kybernetickou bezpečnost a kybernetickou odolnost. Je terčem velmi schopných a motivovaných aktérů, kteří mají k dispozici četné zdroje. Cílem častých útoků těchto aktérů je i nadále důvěrnost a integrita aktiv OPCW v oblasti informací a infrastruktury. Má-li se reagovat na obavy, které byly prohloubeny uvedenými nedávnými kybernetickými útoky, stávajícími politickými úvahami a krizí způsobenou onemocněním COVID-19, a současně zohlednit jedinečné požadavky vyplývající z povahy činnosti OPCW, jejímž účelem je plnění mandátu úmluvy CWC, je jasné, že jsou zapotřebí zásadní investice do technických schopností.

V rámci zvláštního fondu OPCW pro kybernetickou bezpečnost, kontinuitu činností, fyzickou bezpečnost infrastruktury vypracovala OPCW svůj program pro kybernetickou bezpečnost a odolnost a zabezpečení informací (dále jen „program OPCW“), který obsahuje 47 činností zaměřených na řešení výzev v oblasti kybernetické bezpečnosti. Program OPCW je sladěn s osvědčenými postupy, které prosazují subjekty, jako je Agentura Evropské unie pro bezpečnost sítí a informací (ENISA), nebo využívá koncepce související s evropskou směrnicí o bezpečnosti sítí a informací v oblasti telekomunikací a obrany. Program OPCW celkově zahrnuje tyto tematické oblasti: sítě podléhající utajení a sítě nepodléhající utajení; politika a správa; odhalování a reakce; provoz a údržba a telekomunikace. Program OPCW je v zásadě navržen tak, aby OPCW umožnil omezit příležitosti k tomu, aby útočníci podporovaní některým státem anebo mající k dispozici četné zdroje dosáhli svých cílů, a zmírnit rizika vyplývající z vnějších i vnitřních hrozeb z lidské i technické stránky. Podpora Unie je strukturována jako projekt sestávající ze tří činností, které odpovídají dvěma ze 47 činností programu OPCW.

2. Účel projektu

Obecným účelem projektu je zajistit schopnost sekretariátu OPCW zachovat odpovídající úroveň kybernetické bezpečnosti a odolnosti při řešení současných a nově vznikajících výzev souvisejících s ochranou kybernetické bezpečnosti v ústředí OPCW i jejích pomocných zařízeních a umožnit plnění mandátu OPCW a účinné provádění úmluvy.

3. Cíle

— Modernizovat infrastrukturu IKT v souladu s rámcem OPCW pro zachování kontinuity institucionální činnosti, a to se silným důrazem na odolnost.

— Zajistit řízení privilegovaného přístupu, stejně jako správu fyzických, logických a kryptografických informací a oddělení všech strategických sítí a sítí misí.

4. Výsledky

Očekávané výsledky, k nimž má projekt přispět, jsou následující:

— Vybavení IKT a související služby zajistí velmi vysokou spolehlivost systému (hybridní/geografická redundance) a usnadní zvýšenou dostupnost systémů IKT a souvisejících služeb na podporu kontinuity činnosti.

— Možnost, aby jakýkoli jednotlivý faktor či osoba mohly nepříznivě ovlivnit důvěrnost a integritu informací či systémů v rámci OPCW, bude omezena na minimum.

5. Činnosti

5.1. Činnost 1 – zprovoznění prostředí napomáhajícího ke stávajícímu úsilí v oblasti kybernetické bezpečnosti a odolnosti v rámci operací OPCW prováděných na více místech

Účelem této činnosti je vytvořit prostředí napomáhající k bezproblémovému zahájení plánování kontinuity činnosti OPCW, pokud jde o kybernetickou bezpečnost a odolnost. K dosažení tohoto cíle je zapotřebí modernizace infrastruktury – restrukturalizace a archivace za účelem kontinuity činnosti OPCW v rámci všech operací prováděných na více místech. Rovněž je třeba dále usnadnit a umožnit integraci řízení privilegovaného přístupu do procesů plánování a reakce v oblasti kontinuity činnosti.

5.2. Činnost 2 – Navržení individualizovaného řešení pro integraci a konfiguraci systémů umístěných v prostorách i v cloudu s IKT systémy OPCW a řešeními v oblasti řízení privilegovaného přístupu

Účelem této činnosti je transformovat toto příznivé prostředí do individualizovaného návrhu pro integraci a konfiguraci systémů umístěných v prostorách i v cloudu s IKT systémy OPCW a řešeními v oblasti řízení privilegovaného přístupu. Očekává se, že se tak zvýší účinnost infrastruktury systémů IKT a tento krok povede k navržení integrovaného systému v oblasti řízení privilegovaného přístupu pro kritická aktiva, který je schopen odrazovat a odhalovat a je sladěn s přiměřenými schopnostmi pro zjišťování hrozeb.

5.3. Činnost 3 – Zahájení a testování řešení v oblasti řízení privilegovaného přístupu

Tato činnost je založena na zavedené infrastruktuře a řešeních v oblasti řízení privilegovaného přístupu, která jsou navržena tak, aby integrace a konfigurace přešly od teorie k praxi. Systémy je třeba zmapovat, profilovat a začlenit do stávajících systémů a zohlednit přitom související politické a lidské faktory. Poté se důkladným testováním ověří a zaručí spolehlivost systému (veškeré nové systémy mají silné ověřování pro uživatele i zařízení, vhodné utajení informací a jejich ochranu a pokročilé systémy pro prevenci ztráty dat) při provádění a v průběhu času, což sekretariátu OPCW umožní zjistit a řešit nedostatky v co největší míře.

6. Doba trvání

Celková odhadovaná doba provádění a završení činností financovaných v rámci projektu by měla být 24 měsíců.

7. Příjemci

Příjemci projektu budou zaměstnanci technického sekretariátu OPCW, orgány odpovědné za tvorbu politik, pomocné orgány a zúčastněné strany úmluvy, včetně států, které jsou jejími stranami.

8. Zviditelnění EU

OPCW přijme veškerá vhodná opatření, aby při zohlednění opodstatněných bezpečnostních kritérií zveřejnila skutečnost, že tento projekt byl financován Unií.