Rada
Evropské unie

Brusel 18. října 2023
(OR. en)

14394/23

COSI 181
CRIMORG 139
ENFOPOL 433
CT 156
COTER 186
AVIATION 194
JAI 1334

PRŮVODNÍ POZNÁMKA

Odesílatel:	Martine DEPREZOVÁ, ředitelka, za generální tajemnici Evropské komise
Datum přijetí:	18. října 2023
Příjemce:	Thérèse BLANCHETOVÁ, generální tajemnice Rady Evropské unie
Č. dok. Komise:	COM(2023) 659 final
Předmět:	SDĚLENÍ KOMISE RADĚ A EVROPSKÉMU PARLAMENTU o boji proti potenciálním hrozbám, které představují drony

Delegace naleznou v příloze dokument COM(2023) 659 final.

Příloha: COM(2023) 659 final

EVROPSKÁ
KOMISE

V Bruselu dne 18.10.2023
COM(2023) 659 final

SDĚLENÍ KOMISE RADĚ A EVROPSKÉMU PARLAMENTU

o boji proti potenciálním hrozbám, které představují drony

I. ÚVOD

Toto sdělení stanoví politiku EU v oblasti boje proti potenciálním hrozbám ze strany nespolupracujících bezpilotních systémů (UAS), obecně známých jako „drony“. Je součástí širšího protidronového balíčku, který zahrnuje rovněž dvě příručky, jež poskytují praktické pokyny ke klíčovým technickým aspektům této politiky. Tento balíček byl oznámen jako stěžejní opatření v rámci sdělení Komise *„Strategie pro drony 2.0 pro inteligentní a udržitelný ekosystém bezpilotních letadel v Evropě“*[1]. Toto sdělení reaguje na potřebu: i) poskytnout komplexní a harmonizovaný politický rámec; ii) dosáhnout jednotného chápání použitelných postupů, aby bylo možné čelit neustále se vyvíjejícím hrozbám, které mohou drony představovat, a iii) zohlednit rychlý vývoj technologií.

A. Doplnění rámce EU týkajícího se dronů

Legitimní využívání dronů je klíčovou součástí cesty k souběžné zelené a digitální transformaci, jak je stanoveno ve strategii EU pro drony 2.0. Drony hrají důležitou úlohu zejména v oblasti dopravy, obrany, obchodu a služeb. Počet dronů používaných v EU v nadcházejících letech velmi pravděpodobně výrazně vzroste a značně se zlepší jejich rychlost, obratnost, maximální dolet, možnosti užitečného zatížení, přesnost senzorů a využití umělé inteligence. Tento vývoj s sebou přinese širší škálu legitimních a zákonných způsobů využití dronů. Aby však bylo možné tohoto potenciálu využít, je nutné zabývat se potenciální hrozbou, kterou mohou představovat nespolupracující drony. Nespolupracující dron je třeba definovat podle povahy nespolupráce: může jít o trestný čin, protiprávní jednání (úmyslné porušení předpisů) nebo neodborné zacházení (neznalost, nedbalost).

Toto sdělení se zabývá hrozbami, které představují drony určené pro civilní použití, a snaží se řešit hrozby, které tyto drony představují v civilním prostředí. Ačkoli drony určené pro obranné účely nejsou předmětem tohoto sdělení, několik vzájemných vazeb s oblastí obrany zde existuje. Tyto vazby zahrnují potenciální využívání menších dronů určených pro obranné účely pachateli trestné činnosti nebo teroristy, jakož i synergie mezi protidronovými technologiemi. Drony určené pro obranné účely by mohly využívat stejný vzdušný prostor jako civilní drony a v těchto případech je třeba, aby je příslušné orgány dokázaly identifikovat pro účely informovanosti o situaci.

Oblast působnosti tohoto sdělení se týká konkrétně *boje proti* potenciálním hrozbám, které drony představují. Jeho cílem proto není pokrýt širší rozměr úlohy dronů v oblasti vnitřní bezpečnosti, konkrétně jejich využití pro prosazování práva, veřejnou bezpečnost nebo veřejné zabezpečení.

Za potírání hrozeb, které nespolupracující drony představují, odpovídají především orgány členských států. Členské státy však také využívají opatření na úrovni EU, která umožňují užší spolupráci a koordinaci různých prostředků a nástrojů za tímto účelem využívaných. Proto toto sdělení podporuje různé činnosti související s budováním komunit a sdílením informací. Rovněž podporuje členské státy poskytováním pokynů, školení, financování a provozních postupů.

Potenciálně nebezpečné incidenty související s drony jsou stále častější, a to jak v EU, tak i za jejími hranicemi. Je proto důležité usnadnit donucovacím orgánům a jiným orgánům veřejné správy v EU a provozovatelům kritické infrastruktury zavádění fyzických nebo digitálních protidronových řešení. Vytvoření protidronové politiky EU přispěje k posílení postupů pro testování účinnosti dostupných nových

[1] Strategie pro drony 2.0 pro inteligentní a udržitelný ekosystém bezpilotních letadel v Evropě, COM(2022) 652 final ze dne 29. listopadu 2022.

řešení a k usnadnění cíleného využívání výzkumu a inovací v této oblasti. Vypracováním této protidronové politiky Komise pomáhá posílit trh EU s protidronovými řešeními. Tím se otevře cesta k větší strategické autonomii a technologické suverenitě EU, a to i v oblastech kritických technologií. Podpoří se tak evropské kapacity pro vývoj špičkových řešení v oblasti obrany, letectví a civilní bezpečnosti a sníží se závislost na mimoevropských dodavatelích. Bude se přitom vycházet z výsledků posouzení závislostí na kritických technologiích[2] a budou k dispozici další údaje a analýzy. Dále pak: i) budou Komisi poskytnuty informace o využívání kritických technologií a závislosti na mimoevropských dodavatelích a ii) poskytne se spolehlivý přehled o míře závislosti.

Kromě toho je s ohledem na potírání hrozeb, jež nespolupracující drony představují, z pohledu orgánů veřejné správy také důležité: i) mít zavedeny jasné a harmonizované rámce a postupy; ii) poskytnout zodpovědným veřejným a soukromým zúčastněným stranám jasnou pravomoc zasáhnout proti nespolupracujícím dronům a iii) usnadnit spolupráci mezi zúčastněnými stranami, které nejsou vždy zvyklé pracovat společně (donucovací orgány, orgány civilního letectví, hospodářské subjekty, výrobci, provozovatelé mobilních sítí). Toto sdělení předkládá opatření, jejichž cílem je: i) dosáhnout jednotného chápání použitelných postupů při řešení hrozeb, které drony představují, a ii) určit možné potřeby, pokud jde o harmonizaci regulačních opatření.

B. Řešení aktuální a rychle se vyvíjející hrozby

Jak strategie bezpečnostní unie EU[3], tak i Protiteroristická agenda[4] zdůrazňují, že hrozba nespolupracujících dronů je v Evropě vážným problémem.

Rychle se rozvíjející schopnosti dronů představují rostoucí bezpečnostní riziko. V posledních letech byly odhaleny úmysly a faktické pokusy týkající se využití dronů k teroristickým útokům[5]. Byly také zaznamenány případy podezřelých dronů v okolí kritické infrastruktury, jako jsou energetická zařízení, letiště a přístavy, což naznačuje možné zneužití dronů k nepřátelskému sběru informací. Drony využívají zločinci zabývající se pašováním přes hranice nebo slouží k usnadnění jiných nezákonných operací, včetně obchodu s drogami. Drony mohou být dále zdrojem kybernetických rizik, například pokud jsou používány k digitálnímu průzkumu. Hrozby, které drony představují, nejsou pouze technickým problémem. V současné době lze většinu dronů určených pro civilní účely odhalit a identifikovat, ale stále je velmi obtížné proti nim zasáhnout nebo je zneškodnit (tj. převzít nad nimi kontrolu, bezpečně s nimi přistát nebo je sestřelit), často kvůli chybějícímu zákonnému oprávnění. To platí zejména v případě soukromých provozovatelů kritické infrastruktury. Boj proti hrozbám, které drony představují, by proto měl být zohledněn v budoucích posouzeních rizik podle směrnice o odolnosti kritických subjektů[6].

Při pohledu na incidenty v zemích poblíž EU a v jiných částech světa je přehled hrozeb ještě názornější. Ukázalo se, že drony jsou nákladově efektivní a účinnou platformou dvojího užití, která posílila obranné

[2] Interní hloubkové posouzení autonomních systémů provedené Komisí v roce 2022.

[3] Strategie bezpečnostní unie EU, COM(2020) 605 final ze dne 24. července 2020.

[4] Protiteroristická agenda pro EU: předvídání, prevence, ochrana a reakce, COM(2020) 795 final ze dne 9. prosince 2020.

[5] Mezi příklady patří: i) případ inspirovaného džihádisty, který byl v říjnu 2022 odsouzen španělským soudem za to, že plánoval zaútočit na stadion během významného fotbalového zápasu pomocí dronu vybaveného výbušninami, a ii) případ belgického občana, který byl odsouzen za pokus o bombový útok na věznici za použití dronů.

[6] Směrnice (EU) 2022/2557 ze dne 14. prosince 2022 o odolnosti kritických subjektů (Úř. věst. L 333, 27.12.2022, s. 164).

inovace ve válce Ruska proti Ukrajině. Používání dronů určených pro civilní účely k ničivým útokům i v jiných ozbrojených konfliktech (např. v Jemenu nebo Sýrii) je jevem, který může mít důsledky pro vnitřní bezpečnost EU. To, jakým způsobem teroristické skupiny operují, a lepší dovednosti při používání běžně dostupných dronů jsou faktory, které by mohly představovat hrozbu, jež by se mohla dostat až k našim hranicím. Totéž platí pro používání dronů k pokusům o cílené vraždy[7].

Protidronová řešení však nejsou nutná pouze proti cílenému nepřátelskému využívání. Jsou potřebná také k předcházení incidentům způsobeným nedbalostí nebo neopatrností. Většina uživatelů dronů v EU (zejména licencovaní profesionální dálkově řídící piloti nebo organizovaní rekreační piloti) stávající pravidla, předpisy a technická omezení dodržuje. Za mnoho nebezpečných incidentů s drony v EU jsou nicméně zodpovědní neznalí, neopatrní uživatelé dronů a uživatelé dronů, kteří se dopouštějí trestné činnosti. Obzvláště zranitelné vůči takovým narušením jsou velké veřejné akce a některá kritická odvětví, jako je letecká doprava. Nezákonné používání dronů může navíc narušit osobní bezpečnost a právo na soukromí občanů, zejména pokud jsou drony provozovány v obytných oblastech.

C. Udržení kroku s technologickým vývojem

K ochraně naší společnosti před škodlivými a nespolupracujícími drony je zapotřebí přístup k cenově dostupným a spolehlivým protiopatřením, která umožňují flexibilní řešení. Řešení se obvykle zabývají třemi aspekty: detekcí, sledováním a identifikací, přičemž orgány veřejné správy se zajímají i o další dva aspekty: neutralizaci a forenzní hledisko.

V oblasti obrany i civilní bezpečnosti se již vyvíjejí a testují inovativní protidronová řešení. Jejich vstup na trh a jejich přijetí ze strany koncových uživatelů mohou být usnadněny zastřešujícím rámcem EU pro obranu proti dronům, jak je prosazován v tomto sdělení. Vzhledem k vysoké rozmanitosti možných operačních scénářů a prostředí však není možné k provádění protidronových opatření zaujmout standardizovaný přístup, který by vyhovoval všem.

Protidronová opatření je proto třeba přizpůsobit různým potřebám a různým provozním prostředím. Z pohledu orgánů odpovědných za vnitřní bezpečnost mohou nastat situace, kdy je upřednostňovanou a jedinou možností úplné fyzické zničení dronu, například s cílem zabránit bezprostředně hrozícímu útoku na osoby nebo infrastrukturu. V jiných případech, jako je využití pro trestnou činnost nebo nepřátelské shromažďování informací, je naopak žádoucí zajistit si kontrolu nad dronem, aby mohl přistát a zároveň zůstal co nejvíce neporušený, a aby tak bylo možné optimální forenzní vyšetření. K tomu patří i potřeba sofistikovaných kybernetických řešení pro přebírání kontroly nad operačními systémy dronů.

Jedním z technologických trendů, které je třeba sledovat a aktivně využívat, je vývoj senzorů pro přesnější detekci dronů. Stávající schopnosti senzorů lze dále rozvíjet nejen k detekci dronu, ale také k vyhodnocení hrozby, kterou představuje, pomocí analýzy letového vzoru, detekce užitečného zatížení a detekce vybavení. Senzory a detekční systémy musí být schopny přizpůsobit se měnícím se podobám a schopnostem dronů (rychlost, obratnost, schopnost rozmisťovat návnady atd.). Schopnost orgánů veřejné správy a soukromých provozovatelů kritické infrastruktury analyzovat údaje z těchto senzorů bude nabývat na významu. Svou roli bude hrát i umělá inteligence, například při automatickém generování výstrah, výpočtu rizik, předvídání tras nebo odhadování míst přistání. Nové trendy na trzích s drony je proto třeba průběžně sledovat a zapracovávat do protidronových řešení. Sledování tohoto technologického vývoje by mělo

[7] Jako příklad lze uvést neúspěšný pokus o vraždu venezuelského prezidenta či mexické drogové kartely využívající drony proti zástupcům jiných zločineckých organizací.

orgánům v EU umožnit určit priority pro investice a podpořit vývoj, který nejlépe vyhovuje operativním potřebám vyjádřeným donucovacími orgány členských států a soukromými subjekty.

Pokud jde o zasahování proti dronům a jejich neutralizaci, je třeba dále testovat technologie, které by byly vhodné v různých prostředích a scénářích. V oblasti obrany byla nalezena řešení, která umožňují fyzicky zničit nebo zcela zachytit dron, který je ve vzduchu, a tím omezit vznik úlomků, které by mohly vést ke zranění osob nebo poškození objektů. Patří sem například směrové vyzařování energie v podobě vysokoenergetických laserů, jakož i použití výkonných radiofrekvenčních systémů a systémů pro zachycení do sítí a také digitálních nástrojů pro získání kontroly nad nespolupracujícími drony.

Pro prosazování práva a vyšetřování by bylo obzvláště užitečné mít možnost zneškodnit dron, který představuje hrozbu, převzetím kontroly nad jeho řídicím systémem a bezpečným přistáním s ním, což by orgánům a vyšetřovatelům umožnilo co nejlepší přístup k potenciálním fyzickým a digitálním důkazům. Proto by měla být k dispozici široká škála různých řešení, která by byla ověřena pro různé účely a sloužila by oblasti vnitřní bezpečnosti. Je proto nezbytné podporovat skutečné tržní a inovační prostředí zabývající se protidronovými řešeními, která slouží potřebám civilní bezpečnosti. V opačném případě vývoj protidronových řešení pravděpodobně neudrží krok s rostoucím počtem a schopnostmi samotných dronů. Je rovněž nezbytné tento trh strukturovat a segmentovat s cílem pomoci příslušným orgánům identifikovat taková řešení, která nejlépe vyhovují jejich potřebám.

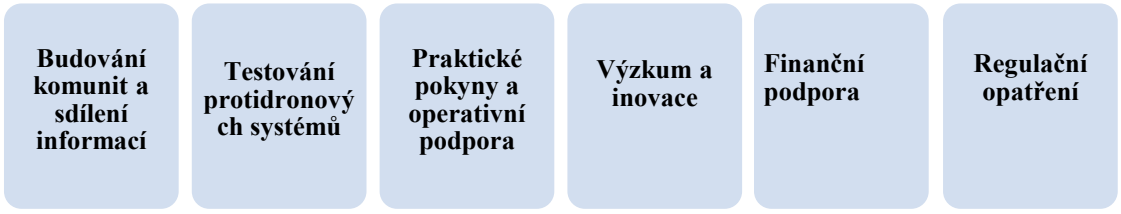
Kromě toho je důležité sledovat také systémy zaměřené proti protidronovým systémům, které využívají pachatelé trestné činnosti. Systémy zaměřené proti protidronovým systémům jsou zařízení, která jsou buď nesena dronem, nebo vysílána ze země a jsou určena k tomu, aby bránila specifickým protidronovým opatřením.

Mnoho protidronových systémů je také vyvíjeno pro obranné účely. Ačkoli se liší v požadavcích, často mají společné vlastnosti a technologie se systémy určenými pro civilní účely, což vede k potřebě úzké spolupráce s oblastí obrany.

Toto vyvíjející se technologické prostředí rovněž vyžaduje konzistentní a průběžně aktualizovaný regulační rámec pro používání protidronových systémů.

II. FORMULOVÁNÍ PROTIDRONOVÉ POLITIKY EU

Komise spolupracuje s členskými státy a dalšími zúčastněnými stranami na řešení potenciální hrozby, kterou představují drony, od roku 2016, kdy se konal první seminář EU o obraně proti dronům. Od té doby byla zavedena celá řada iniciativ, které usnadňují budování komunit, sdílení informací, rozvoj osvědčených postupů a účelové financování projektů. Na základě diskusí s odborníky z členských států bude Komise tyto probíhající iniciativy nadále podporovat a zároveň bude dále rozvíjet a integrovat nové oblasti činnosti s cílem vypracovat plnohodnotnou protidronovou politiku EU. Tato činnost bude sestávat z těchto šesti klíčových aktivit:



A. Budování komunit a sdílení informací

Na protidronových řešeních nyní na úrovni EU pracuje celá řada různých sítí a aktérů. Je proto třeba zefektivnit a vést jejich budoucí činnost z politického, technického a provozního hlediska s cílem: i) vybudovat fungující komunity zúčastněných stran; ii) zajistit účinné sdílení informací a osvědčených postupů a iii) zamezit překrývání práce.

Komise bude podporovat stávající iniciativy na technické úrovni a zároveň zřídí **skupinu odborníků Komise pro obranu proti dronům**, která bude poskytovat poradenství na politické úrovni. Tato skupina odborníků bude moci poskytovat strategické podklady pro různé politiky na úrovni EU, které mají význam pro protidronové činnosti, například v oblasti vnitřní bezpečnosti, správy hranic nebo odolnosti kritické infrastruktury. Za tímto účelem bude odborná skupina spolupracovat s dalšími odbornými skupinami a případně s příslušnými pracovními skupinami Rady.

Na téma protidronových řešení a politik se pravidelně konají semináře a setkání odborníků. Účastní se jich tvůrci politik, techničtí odborníci a výzkumní pracovníci z Komise, členských států, dalších institucí EU, agentur EU, projektů financovaných EU, mezinárodních organizací a partnerských zemí. Výsledkem těchto činností je trvalé zapojení všech zúčastněných stran, což významně usnadňuje jejich operativní a praktickou spolupráci. Za tímto účelem Komise zřídila **informační středisko pro obranu proti UAS**[8], které má v současné době více než 300 členů. Tato online platforma je pravidelně aktualizována a obsahuje různé zdroje informací, například výsledky příslušných projektů financovaných EU, prezentace, zprávy a pololetní zpravodaj.

Další důležitá část budování komunit a sdílení informací, zejména pro operativní potřeby donucovacích orgánů, probíhá v rámci **evropských sítí pro vymáhání práva** financovaných z prostředků EU. Vlastní činnost zaměřenou na boj proti hrozbám, které drony představují, zahájily například všechny následující sítě: evropská síť technologických služeb pro vymáhání práva (ENLETS), síť EU pro jednotky policie a pohraniční stráže na letištích (AIRPOL), síť zvláštních zásahových jednotek EU (ATLAS) a bezpečnostní síť EU pro vysoce rizikové veřejné prostory. Nově vytvořená pracovní skupina pro sítě pro vymáhání práva, která je iniciativou GŘ HOME zaměřenou na podporu spolupráce mezi policejními sítěmi a která je financována Komisí[9], zefektivní probíhající činnosti v oblasti obrany proti dronům v rámci specializované pracovní podskupiny.

Evropská agentura pro bezpečnost letectví (EASA) vypracovala nezávazné pokyny, které pomáhají orgánům a letištím připravit se na incidenty s drony, reagovat na ně a zotavit se z nich[10]. V zájmu posílení informovaných podpůrných činností a tvorby politik na úrovni EU je nezbytné mít spolehlivou a podrobnou výměnu informací o incidentech týkajících se dronů v EU, a to nad rámec výměn, které již probíhají v konkrétních kritických oblastech, jako jsou letiště. Při plném respektování důvěrnosti vyšetřování existuje významný potenciál pro zlepšení sdílení informací o: i) metodách používaných provozovateli nespolupracujících dronů; ii) konkrétních vzorcích ohrožení a iii) zjištěných potenciálních rizicích. S cílem usnadnit a harmonizovat sdílení těchto informací o incidentech sdílela Komise s členskými státy šablonu pro podávání zpráv o incidentech s drony. V zájmu dalšího zvýšení kvality a četnosti sdílení informací

---

[8] Za využití platformy EU CIRCABC, která je podporována programem ISA² Evropské komise, jenž prosazuje řešení interoperability pro evropské orgány veřejné správy.

[9] (Neformální) pracovní skupina pro sítě pro vymáhání práva (Law Enforcement Network Working Group – LENWG), jíž předsedá Komise, se poprvé sešla 20. března 2023 s cílem podpořit lepší spolupráci mezi sítěmi financovanými z prostředků GŘ HOME. Po dvanáctiměsíčním hodnotícím období by se pracovní skupina LENWG mohla přeměnit na řádnou expertní skupinu Komise.

[10] Agentura Evropské unie pro bezpečnost letectví (EASA) zveřejnila v březnu 2021 soubor pokynů pro řízení incidentů s drony na letištích: *Drone Incident Management at Aerodromes*.

Komise prozkoumá možnost zřízení **digitální platformy obsahující informace o incidentech s drony**, kterou by mohly využívat příslušné orgány veřejné správy. Mohla by sloužit k řádné identifikaci a shromažďování významných bezpečnostních incidentů týkajících se dronů v EU. To by mohlo zahrnovat i kybernetický rozměr, neboť drony se používají nejen k vizuálnímu, ale také k digitálnímu průzkumu. Tato platforma by byla v souladu se stávajícími oznamovacími povinnostmi podle nařízení (EU) č. 376/2014[11] a nezdvojovala by stávající úsilí.

Komise bude rovněž organizovat pravidelná utajovaná setkání ve vhodném formátu, aby podpořila výměnu zkušeností získaných z incidentů.

Klíčová opatření pro budování komunit a sdílení informací

- **Komise zřídí skupinu odborníků složenou z odborníků z členských států a dalších zúčastněných stran, která se bude zabývat činnostmi v oblasti obrany proti dronům.**
- **Komise prozkoumá možnost vytvoření digitální platformy obsahující informace o incidentech s drony.**
- **Komise bude pořádat pravidelná setkání s cílem usnadnit mezi členskými státy výměnu utajovaných informací o závažných bezpečnostních incidentech týkajících se použití dronů.**

B. Testování protidronových systémů: hledání a testování řešení

Členské státy a místní orgány si mohou vybrat ze široké škály komerčních kybernetických i nekybernetických protidronových řešení, která jsou na trhu k dispozici. Tato volba je náročná, zejména pro místní subjekty, které nemají dostatečné technické možnosti. Komise bude orgánům členských států pomáhat při správném výběru z hlediska jejich operativních potřeb poskytováním poradenství a pokynů prostřednictvím specializované skupiny odborníků pro obranu proti dronům a činností Společného výzkumného střediska Komise (JRC).

Činnosti zaměřené na testování protidronových systémů byly na úrovni EU zahájeny v roce 2019. Jejich cílem je vypracovat společnou metodiku hodnocení systémů, které mohou využívat donucovací orgány a další orgány veřejné správy k odhalování, sledování a identifikaci potenciálně škodlivých dronů. Ústředním pilířem těchto aktivit je projekt „Courageous“[12] (2021–2024), který je financován z unijního Fondu pro vnitřní bezpečnost – policie (ISF–policie). Projekt Courageous vede belgická Královská vojenská akademie a jeho úkolem je: i) identifikovat příslušné standardní scénáře pro testování protidronových systémů; ii) vypracovat funkční a výkonnostní požadavky a iii) vyvinout metodiku testování. V rámci projektu se rovněž testuje výkonnost senzorů a integrovaných systémů. Výsledky projektu se průběžně sdílejí s členskými státy i vybranými partnerskými zeměmi a mezinárodními organizacemi. Po dokončení projektu Komise a konsorcium Courageous předloží členským státům možnosti, jak zajistit udržitelnost projektu, a doporučí **metodiku pro testovací protidronová zařízení** v členských státech.

Technologie relevantní pro oblast protidronových systémů se rychle vyvíjí. Proto je nutné kromě testovacích činností neustále sledovat trendy, aby bylo možné odhalit jak nejslibnější řešení, tak případné nové výzvy pro vývoj protidronových systémů. Za účelem provádění tohoto sledování a odhalování těchto nových výzev vybudovalo JRC potřebné kapacity. To je užitečné pro členské státy a zároveň tak lze získat

[11] Nařízení Evropského parlamentu a Rady (EU) č. 376/2014 ze dne 3. dubna 2014 o hlášení událostí v civilním letectví, analýze těchto hlášení a navazujících opatřeních.

[12] https://courageous-isf.eu/

cenné podněty pro testovací iniciativy na úrovni EU. Informace budou sdíleny prostřednictvím vhodných kanálů, zejména prostřednictvím odborné skupiny.

Jedním z nástrojů harmonizace technologických řešení je normalizace. V rámci projektu Courageous bylo vypracováno konkrétní poradenství týkající se předběžné normalizace, na jehož základě lze dále posoudit proveditelnost a potřebu zahájení normalizačních procesů. Na úrovni EU bylo dosaženo značného pokroku ve vývoji dobrovolných požadavků na výkonnost detekčních zařízení mimo letectví (např. pro rentgenové přístroje a detektory kovů[13]). Komise nyní společně s odborníky z členských států a průmyslu vypracuje také **dobrovolné požadavky na výkonnost** protidronových systémů, v příslušných případech soudržně s ustanoveními aktu o kybernetické bezpečnosti[14]. Střednědobým cílem by mělo zůstat zavedení procesu certifikace protidronových systémů. V případě potřeby budou zváženy i hybridní civilní/obranné normy.

Dalším klíčovým prvkem je normalizace a certifikace kybernetické bezpečnosti protidronových systémů, zejména pokud je poskytují dodavatelé ze zemí mimo EU. V této fázi přetrvává nejistota ohledně toho, jak dobře jsou chráněny údaje, které shromažďují některé detekční systémy. Kromě toho je důležité v co největší možné míře zabránit hackerským útokům na protidronové systémy a jejich zneužití zajištěním kybernetické odolnosti jejich součástí.

V září 2022 přijala Komise návrh nařízení o kybernetické odolnosti[15], jehož cílem je vypracovat obecná pravidla kybernetické bezpečnosti pro produkty s digitálními součástmi (jak hardwarovými, tak softwarovými), které vstupují na jednotný trh. Cílem navrhovaného nového nařízení je zavést povinné požadavky na kybernetickou bezpečnost těchto produktů. Tyto požadavky budou zahrnovat zajištění kybernetické bezpečnosti standardně a již od návrhu, jakož i požadavky na řešení zranitelnosti. Podle návrhu Komise by se na dronové systémy, které nejsou vyvinuty výhradně pro účely národní bezpečnosti nebo pro vojenské účely a které dosud nebyly certifikovány v souladu s nařízením (EU) 2018/1139, tato nová pravidla vztahovala jako na produkty s digitálními prvky, s výjimkou těch, které byly vyvinuty výhradně pro účely národní bezpečnosti nebo obrany.

Klíčové činnosti pro testování protidronových systémů

- **Na základě výsledků projektu Courageous začne Komise pracovat na zavedení harmonizované metodiky testování protidronových systémů.**
- **Společné výzkumné středisko vypracuje výroční zprávu o technickém vývoji v oblasti protidronové technologie.**
- **Komise ve spolupráci s příslušnými odbornými skupinami, jako jsou evropské sítě pro vymáhání práva ENLETS, HRSN, AIRPOL, vypracuje soubor dobrovolných požadavků na výkonnost protidronových systémů.**

[13] Doporučení Komise o dobrovolných požadavcích na výkonnost rentgenových zařízení používaných ve veřejných prostorách (C(2022) 4179 final).

[14] Nařízení Evropského parlamentu a Rady (EU) 2019/881 ze dne 17. dubna 2019 o agentuře ENISA a o certifikaci kybernetické bezpečnosti informačních a komunikačních technologií.

[15] Návrh nařízení Evropského parlamentu a Rady o horizontálních požadavcích na kybernetickou bezpečnost produktů s digitálními prvky a o změně nařízení (EU) 2019/1020 (COM(2022) 454 final).

C. Praktické pokyny a operativní podpora

Potírání hrozeb, které představují nespolupracující drony, již bylo označeno za prioritu v řadě publikací Společného výzkumného střediska, například v pokynech zaměřených na ochranu obvodu budov[16] a ve specializované studii o výbušných nálož přenášených drony[17]. Nedávná publikace[18] o konceptu bezpečnosti již od fáze návrhu navíc zdůrazňuje význam začlenění přiměřených, vhodných a multifunkčních ochranných opatření na základě promyšleného přístupu od samého počátku plánovací fáze a fáze návrhu projektu, včetně opatření proti případným útokům využívajícím drony.

Příručka agentury EASA o *řízení incidentů s drony na letištích* dále poskytuje návod, jak vytvořit vhodná opatření a postupy, které podporují systém reakce na incidenty na letištích, který je rychlý, účinný a přiměřený. Tímto způsobem se lze vyhnout pozastavením letového provozu nebo uzavření vzdušného prostoru či vzletových a přistávacích drah nebo je omezit na minimum, přičemž uzavření letiště by zůstalo krajním řešením. Agentura EASA při své práci zohledňuje pokyny Mezinárodní organizace pro civilní letectví týkající se ochrany letectví před protiprávními činy[19].

JRC vypracovalo dvě nové příručky:

- ***Ochrana proti bezpilotním systémům:*** *Příručka o ochraně kritické infrastruktury a veřejného prostoru proti UAS – pětifázový přístup pro zúčastněné strany systému C-UAS*

- ***Ochrana proti bezpilotním systémům:*** *Příručka o posouzení rizik bezpilotních systémů a zásadách fyzického zabezpečení budov a pozemků.*

V oblasti **školení** byl v rámci projektu DroneWISE[20] financovaného z prostředků EU pro zásahové složky v první linii vytvořen balíček strategií řízení, kontroly a koordinace obrany proti dronům. V rámci projektu vzniklo také 10 vzdělávacích modulů, příručka a online školicí portál. Tyto vzdělávací moduly byly začleněny do osnov CEPOL, Agentury Evropské unie pro vzdělávání a výcvik v oblasti prosazování práva. Dalším projektem ISF, který se věnoval školení v oblasti obrany proti dronům, byl projekt Skyfall. Dostupnou nabídku školení je třeba dále rozšířit na soukromé poskytovatele bezpečnostních služeb, zejména na ty, kteří jsou odpovědní za ochranu kritické infrastruktury.

Program Komise **pro poradce EU pro ochranu bezpečnosti (EU PSA)**[21] obsahuje oddíl věnovaný činnostem v oblasti obrany proti dronům, který nabízí: i) konkrétní posouzení zranitelnosti vysoce rizikových zařízení a infrastruktury; ii) praktické rady, jak se vypořádat s hrozbou dronů, a iii) praktické rady, jak se vypořádat s nasazením zařízení pro detekci dronů během vysoce rizikových událostí. Komise

---

[16] Karlos, V. a Larcher, M., *Guideline – Building Perimeter Protection* (Obecný pokyn – ochrana obvodu budovy), EUR 30346 EN, Úřad pro publikace Evropské unie, Lucemburk, 2020.

[17] Hrozbu, kterou představují bezpilotní systémy využívající výbušniny, zkoumalo JRC v rámci studie: Larcher M., Karlos V., Valsamos G., Solomos G.: *Scenario study: drones carrying explosives* (Situační studie: drony přepravující výbušniny), JRC107683, 2018.

[18] Evropská komise, *Security by Design: Protection of public spaces from terrorist attacks* (Bezpečnost již od návrhu: Ochrana veřejných prostor před teroristickými útoky), JRC131172, 2022.

[19] Příručka ICAO pro ochranu civilního letectví před protiprávními činy (dokument Doc 8973 – Restricted) pomáhá členským státům při provádění přílohy 17 Chicagské úmluvy tím, že poskytuje návod, jak uplatňovat její standardy a doporučené postupy (SARP) Příručka pro ochranu civilního letectví před protiprávními činy.

[20] https://dronewise-project.eu/

[21] https://home-affairs.ec.europa.eu/policies/internal-security/counter-terrorism-and-radicalisation/protection/eu-protective-security-advisors-eu-psa_en

prozkoumá potřebu vytvoření rezervy EU pro vybavení proti dronům, kterou by členské státy měly k dispozici na podporu při rozsáhlých událostech.

Ke zvýšení operační připravenosti v různých oblastech vnitřní bezpečnosti přispívají rovněž **cvičení**, jako jsou ta, která jsou pořádána na úrovni EU v rámci sítě pro vymáhání práva. V případě potřeby bude Komise spolupracovat s příslušnými sítěmi, aby do budoucích cvičení zahrnula prvky obrany proti dronům. To přispěje k dalšímu rozšíření znalostí a výměně osvědčených postupů s využitím různých řešení. Jedním z požadavků na účinnou reakci na hrozby, které drony představují, je spolehlivá a bezpečná komunikace mezi různými orgány. Proto bude boj proti hrozbám, které mohou drony představovat, součástí plánování budoucích cvičení, která budou prováděna v rámci přípravného projektu BroadEU.Net financovaného z prostředků EU a která budou testovat základ budoucího kritického komunikačního systému EU[22]. Kromě toho by se mohla konat společná cvičení s odborníky na kybernetickou bezpečnost a bezpečnost dronů, zaměřená na kybernetická rizika, která drony představují, jakož i na digitální řešení k neutralizaci dronů.

Klíčová opatření pro praktické pokyny a operativní podporu

- **Společné výzkumné středisko vydá v rámci protidronového balíčku dvě příručky.**
- **Komise ve spolupráci s příslušnými agenturami podpoří rozšíření stávajícího školení v oblasti obrany proti dronům na soukromý bezpečnostní sektor.**
- **Komise ve spolupráci se sítěmi pro vymáhání práva zahrne do plánování cvičení také složky týkající se obrany proti dronům.**

D. Výzkum a inovace

EU nadále financuje svůj program pro výzkum v otázkách bezpečnosti v rámci programu **Horizont Evropa (2021–2027)**[23]. Tento program pro výzkum v otázkách bezpečnosti představuje zhruba 50 % celkových veřejných finančních prostředků investovaných v EU a jejích členských státech do oblasti bezpečnosti. Tento výzkum v oblasti bezpečnosti, který strategicky přispívá k různým prioritám bezpečnostní politiky EU, se již začal zabývat také hrozbami, které představují drony. Mezi nejvýznamnější příklady patří projekt ALADDIN, který poskytuje řešení pro detekci a neutralizaci dronů ve vyhrazených oblastech[24], nebo projekt 7SHIELD, který se zabýval vývojem protidronových řešení pro pozemní segmenty kritické vesmírné infrastruktury. V rámci projektu ALFA se také podařilo vyvinout systém pro detekci a sledování dronů používaných k pašování[25]. Tyto výzkumné a inovační iniciativy mohou pokračovat v rámci programu Horizont Evropa, mohou být schváleny nebo je lze doplnit o činnosti prováděné v rámci ISF–policie.

V budoucnu Komise umožní systematičtější výměnu výsledků příslušných projektů s příslušnými zúčastněnými stranami, mimo jiné prostřednictvím Společenství pro evropský výzkum a inovace v oblasti bezpečnosti[26]. Díky tomu by se dále posílila výměna konkrétních údajů. Rovněž by to umožnilo zefektivnit

[22] Kritický komunikační systém EU poskytne bezpečnou širokopásmovou infrastrukturu, která zajistí přeshraniční interoperabilitu komunikačních systémů používaných orgány pro vymáhání práva a zásahovými složkami reagujícími na mimořádné události v schengenském prostoru.

[23] Až do konce roku 2020 byly výzkum a inovace v oblasti bezpečnosti financovány v rámci programu Horizont 2020 a sedmého rámcového programu.

[24] https://cordis.europa.eu/project/id/740859

[25] Z projektu ALFA rovněž vychází projekt ISF Courageous a jeho testovací činnosti.

[26] Společenství pro evropský výzkum a inovace v oblasti bezpečnosti (CERIS) sdružuje zúčastněné strany z oblasti bezpečnostního výzkumu, od tvůrců politik, koncových uživatelů, akademické obce a průmyslu až po civilní

shromažďování požadavků uživatelů a sdělování těchto požadavků průmyslovým odvětvím s cílem řídit inovace. Systematická výměna výsledků projektů navíc napomůže strukturovanému dialogu s členskými státy a zúčastněnými stranami s cílem určit slibné technologie, nástroje a řešení, které by mohly být využity skupinou orgánů členských států. V této souvislosti Komise společně s členskými státy[27] posoudí možnost: i) vytvoření samostatného výzkumného tématu týkajícího se protidronových řešení v budoucích pracovních programech programu Horizont Evropa a ii) podpory konkrétních inovativních systémů prostřednictvím zadávání veřejných zakázek v předobchodní fázi[28]. To je plně v souladu s přístupem založeným na schopnostech, který je podrobně popsán v pracovním dokumentu útvarů Komise „Posílení bezpečnosti prostřednictvím výzkumu a inovací“[29].

Zásadní význam má posílení synergií v oblasti protidronových řešení mezi evropským civilně-bezpečnostním, obranným a kosmickým průmyslem. Cílem by měla být podpora synergií v oblasti dronových a protidronových technologií mezi těmito třemi odvětvími[30]. V praxi posílení těchto synergií znamená, že obranné projekty mohou využívat inovativního vývoje v civilní oblasti, zatímco civilní letectví může těžit z vývoje v oblasti obrany.

Evropský obranný fond a předcházející programy podněcují a podporují přeshraniční výzkum a vývoj v oblasti obrany založený na spolupráci. Evropský obranný fond doplňuje a posiluje snahy členských států a podporuje spolupráci mezi společnostmi a výzkumnými subjekty ze všech členských států EU bez ohledu na jejich velikost. Předchůdci Evropského obranného fondu již financovaly protidronové projekty v rámci výzkumu a vývoje v oblasti obrany.

Pracovní program Evropského obranného fondu na rok 2023 obsahuje opatření na rozvoj obrany proti dronům[31] s orientačním rozpočtem 43 milionů EUR. Cílem tohoto opatření je vyvinout hardwarové nebo softwarové moduly pro komplexní mobilní řešení pro obranu proti široké škále dronů, včetně rojů.

Hlavním očekávaným výsledkem podpory Evropského obranného fondu v oblasti obrany proti dronům v letech 2021–2027 je vytvoření prototypu protidronového řešení, které povede k možnému budoucímu společnému zadávání veřejných zakázek na úrovni EU. Technologické výzvy v oblasti protidronových systémů jsou řešeny prostřednictvím Programu EU pro inovace v oblasti obrany (EUDIS). Kromě toho program EUDIS obsahuje složku pro inkubátory dvojího použití, které mají podpořit lepší spolupráci mezi civilní a obrannou oblastí a urychlit technologické zrání a přizpůsobení.

Dalším klíčovým pilířem pro inovace, konkrétně pro aplikovaný výzkum věnující se tomu, jak čelit hrozbám, které mohou drony představovat, je činnost Společného výzkumného střediska. V rámci projektu Drone C-UAS Společného výzkumného střediska přezkoumá středisko technologie aktivních a pasivních

bezpečnost: https://home-affairs.ec.europa.eu/networks/ceris-community-european-research-and-innovation-security_en

[27] Ve složení programového výboru v rámci programu Horizont Evropa „Civilní bezpečnost pro společnost“.

[28] Zadávání veřejných zakázek v předobchodní fázi je přístup k zadávání veřejných zakázek na služby výzkumu a vývoje, který byl popsán ve sdělení o zadávání veřejných zakázek v předobchodní fázi (KOM(2007) 799 v konečném znění) ze dne 14. prosince 2007. Jde o důležitý nástroj pro stimulaci inovací, neboť veřejnému sektoru umožňuje řídit vývoj nových řešení podle svých potřeb.

[29] Pracovní dokument útvarů Komise „Posílení bezpečnosti prostřednictvím výzkumu a inovací“, SWD(2021) 422 final ze dne 15. prosince 2021.

[30] SWD(2022) 362 ze dne 10. listopadu 2022. Jak je popsáno ve zprávě o pokroku při provádění akčního plánu pro synergie mezi civilním, obranným a kosmickým průmyslem v rámci akce 9.

[31] Prováděcí rozhodnutí Komise C(2023) 2296 ze dne 29. března 2023 o financování Evropského obranného fondu zřízeného nařízením Evropského parlamentu a Rady (EU) 2021/697 a o přijetí pracovního programu na rok 2023 – část II.

protiopatření a způsoby, jakými lze tyto technologie využít k zajištění bezpečnosti veřejných prostor a kritické infrastruktury.

Za tímto účelem a jako první krok vytvoří Společné výzkumné středisko **živou laboratoř**, která bude zkoumat protidronové technologie a způsob, jakým lze tyto technologie použít v reálném prostředí. V rámci provozu laboratoře bude probíhat plánování, příprava a realizace řešení. Laboratoř se bude rovněž zabývat detekcí, sledováním, identifikací a neutralizací a dále integrací zúčastněných stran a procesů. Rozsah provádění živé laboratoře bude zahrnovat integraci se systémy řízení provozu bezpilotních letadel a letadel s posádkou, především se vzdušným prostorem U-space[32]. Živá laboratoř bude rovněž zkoumat, jakým způsobem lze ke zlepšení celkové výkonnosti protidronových řešení využít strojové učení a umělou inteligenci.

Ve střednědobém horizontu se tato živá laboratoř Společného výzkumného střediska rozvine v **centrum excelence pro obranu proti dronům**.

Prioritní opatření pro maximální využití výzkumu a inovací

- **Komise a členské státy rozhodnou o tom, jakým budoucím potřebám nových protidronových řešení se budou věnovat příslušné evropské výzkumné a inovační programy, zejména program Horizont Evropa.**
- **Komise a členské státy určí seznam slibných protidronových řešení a posoudí proveditelnost zadávání zakázek na některá z těchto řešení v předobchodní fázi.**
- **Komise určí nápady, technologie a řešení, které mají být začleněny do rozvoje obranných schopností, a podpoří projekty, jejichž cílem je šířit tyto nápady, technologie a řešení do civilních odvětví.**
- **V rámci dalšího vývoje živé laboratoře zřídí Společné výzkumné středisko Centrum excelence pro obranu proti dronům.**

E. Finanční podpora

Komise bude i nadále poskytovat finanční podporu příslušným činnostem v oblasti obrany proti dronům, především prostřednictvím ISF, ale také v rámci Nástroje pro finanční podporu správy hranic a vízové politiky (BMVI) a programu Horizont Evropa (pro činnosti související s výzkumem a inovacemi).

Tematický nástroj ISF podpoří: i) evropské sítě pro vymáhání práva; ii) související činnosti Společného výzkumného střediska; iii) novou skupinu odborníků pro obranu proti dronům a iv) vytvoření platformy pro výměnu informací. Již nyní Komise financuje projekty zaměřené na zkušební provoz a schvalování systémů pro odhalování a lokalizaci dronů, které nelegálně překračují vnější hranice EU. Tyto projekty vycházejí z výsledků předchozích výzkumných projektů financovaných z prostředků EU[33].

[32] Prováděcí nařízení Komise (EU) 2021/664 o regulačním rámci pro vzdušný prostor U-space. Pojem „vzdušný prostor U-space“ se používá pro popis řízení provozu bezpilotních letadel s cílem zajistit bezpečnou interakci s ostatními subjekty využívajícími stejný prostor v městských oblastech a na jakýchkoli jiných místech.

[33] Příkladem mohou být projekty financované v rámci specifických akcí nástroje BMVI, které se týkají: i) inovací pro námořní/pobřežní a/nebo pozemní hranice a ii) agentury Frontex. Některé projekty financované v rámci specifické akce týkající se inovací pro námořní/pobřežní a/nebo pozemní hranice se zaměřují na zkušební provoz inovativních technologií sledování. Existuje také specifická akce na nákup a zpřístupnění zařízení, které mohou evropské pohraniční orgány nasadit za účelem odhalování a lokalizace dronů, které překračují hranice v souvislosti s

V rámci tematického nástroje ISF Komise v první polovině roku 2024 zahájí **výzvu k podávání návrhů** zaměřenou konkrétně na podporu zavádění protidronových řešení s vysokým potenciálem využití.

Členské státy budou podporovány v tom, aby toto sdělení prováděly a využívaly výsledky výzkumu protidronových řešení financovaného z prostředků EU prostřednictvím svých programů ISF.

Klíčová opatření pro finanční podporu

- **Komise vyhlásí výzvu k podávání návrhů na protidronová řešení v rámci pracovních programů tematického nástroje ISF na období 2026–2027.**
- **Členské státy budou vybízeny k tomu, aby plně využívaly svých programů ISF na období 2021–2027 s cílem určit a zavést účinná protidronová řešení.**

F. Zkoumání regulačních opatření

Ačkoli je v EU legální používání dronů regulováno, na úrovni EU v současné době neexistují žádné konkrétní protidronové předpisy, které by stanovovaly společný harmonizovaný rámec pro orgány členských států, provozovatele a výrobce. Nezávazné pokyny EASA, které se týkají incidentů s drony na letištích (zmíněné výše v tomto sdělení), byly sice odvětvím přijaty příznivě, avšak vzhledem k jejich poradní povaze a omezenému rozsahu nepostačují ke zmírnění hrozby, kterou nespolupracující drony představují. Vzhledem k tomu, že potřeba účinně bránit neoprávněnému používání dronů neustále roste, bude Komise v úzké spolupráci s odborníky z členských států dále analyzovat budoucí potřebu legislativních či nelegislativních opatření. Za tímto účelem Komise zahájí specializovanou mapovací studii s cílem vytvořit stávající regulační prostředí. Tato mapovací studie by měla rovněž zohlednit rámec organizace ICAO a její vývoj a také by měla přihlédnout k tomu, že pravidla pro boj proti potenciálním hrozbám, které drony představují, by neměla nepřiměřeně bránit legitimnímu provozu, včetně činností organizovaných rekreačních pilotů.

Letiště v EU se řídí podrobnými a ucelenými bezpečnostními pravidly, která se vztahují i na hrozbu ze strany dronů. S cílem zajistit větší odolnost leteckých úřadů a letišť vůči rizikům, která drony představují, a v souladu s přístupem založeným na důkazech Komise ve spolupráci s členskými státy **v rámci posouzení bezpečnostních rizik určí případná další zranitelná místa v ochraně proti nespolupracujícím dronům, která mohou vyžadovat změny právních předpisů**.

V této souvislosti je zapotřebí vést s průmyslovým odvětvím a výrobci dronů strukturovaný dialog o bezpečnostních opatřeních již od návrhu (např. robustní systémy proti fingování (spoofingu), omezení funkčních možností, sdílení komunikačních protokolů a aktualizace protidronových databází).

nezákonnou nebo trestnou činností. Tato specifická akce umožní členským státům zajistit dva protidronové systémy. Přidanou hodnotou EU je, že na žádost agentury Frontex v rámci každoročních dvoustranných jednání musí být technické zařízení pořízené v rámci specifických akcí poskytnuto agentuře Frontex na dobu až čtyř měsíců ročně, aby je mohla využívat při svých společných operacích.

Klíčová opatření pro zkoumání regulačních opatření

- **Komise zahájí mapovací studii s cílem určit regulační potřeby a možnosti harmonizace právních předpisů a postupů členských států.**
- **V souladu s přístupem založeným na důkazech provede Komise v souvislosti s drony posouzení rizik v oblasti ochrany letectví před protiprávními činy, aby zjistila případná další zranitelná místa letišť, která by mohla vyžadovat změny právních předpisů.**
- **Komise povede strukturovaný dialog s průmyslovým odvětvím o nutnosti a povaze případných dalších zvláštních opatření týkajících se bezpečnosti dronů.**

III. DALŠÍ POSTUP

S cílem zajistit, aby rychlý technologický vývoj a rostoucí počet dronů nevedly k nekontrolovanému nárůstu hrozeb, které představují nespolupracující drony, je nutné posílit spolupráci na úrovni EU na základě ucelené protidronové politiky EU popsané v tomto sdělení. Za tímto účelem budou pokračovat stávající činnosti na úrovni EU a budou doplněny souborem klíčových opatření uvedených v tomto sdělení, která budou prováděna v nadcházejících letech.

Činnosti uvedené v tomto sdělení se budou týkat období do roku 2030. Do roku 2027 proběhne v rámci odborné skupiny hodnocení v polovině období a nejpozději do roku 2030 se plánuje úplná revize protidronového programu EU.