

Posouzení návrhu programu

Strategická podpora rozvoje bezpečnostního výzkumu ČR 2026–2031 (IMPAKT 2)

Poskytovatel účelové podpory v rámci programu: Ministerstvo vnitra.

ÚVOD

Bezpečnostní situace ve světě se v posledních letech bohužel významnou měrou zhoršuje, situace v ČR je sice relativně stabilní, ale existují hrozby a rizika, které mohou ovlivnit národní bezpečnost, včetně bezpečnosti kritické infrastruktury. Hrozby jsou velmi různorodé a mohou pocházet jak z vnějších, tak vnitřních zdrojů. Lze konstatovat, že vzhledem k současnému geopolitickému napětí, rostoucímu vlivu širokého spektra kybernetických útoků a i hybridních hrozeb, lze Českou republiku vnímat jako zranitelnou vůči bezpečnostním rizikům.

Jako hlavní hrozby a rizika lze např. uvést:

Kybernetické útoky, které mohou být považovány za jednu z největších hrozeb zejména pro kritickou infrastrukturu (sektoru energetiky, vodovodních a kanalizačních systémů, dopravy a zdravotní péče). Útoky mohou být prováděny jak státními aktéry, tak i privátními hackery a jejich skupinami. Útoky mohou cílit jak na destabilizaci, špionáž, vydírání nebo způsobení přímých škod. Kybernetické útoky probíhají téměř neustále, jak na vládní instituce, bankovní sektor a podniky, a mohou vést k úniku citlivých dat nebo paralyzování klíčových systémů.

Vliv geopolitického napětí, které je vyvoláno nejen konflikty na Ukrajině a na Blízkém východě. Oba mají globální dopady a vliv na Českou republiku, a to jak přímo (například v podobě přílivu migrantů nebo protiprávních aktivit), tak i nepřímo (ekonomické sankce, energetická krize, vlivy na dodávky surovin).

Terorismus a radikalizace - přestože prozatím nejsou teroristické útoky v ČR běžné, rostoucí polarizace společnosti a příliv radikalizovaných jedinců mohou zvýšit riziko násilných činů. Přítomnost extremistických skupin nebo jednotlivců se může projevat ve formě výzev k násilí vůči státním institucím nebo minoritním skupinám.

Hrozby z vnitřních zdrojů, rizikem může být i vnitřní destabilizace, například prostřednictvím dezinformací, politické polarizace nebo organizovaných protestů, které by mohly narušit veřejný pořádek. Dezinformační kampaně mohou oslabit důvěru občanů v instituce a vládu, což by mohlo vést k sociálním a politickým nepokojům.

Hrozby spojené s přírodními katastrofami (např. povodně, sucho, vichřice) a klimatickými změnami mohou mít také negativní vliv na infrastrukturu a její odolnost. Změny klimatu mohou ovlivnit stabilitu dodávek energie, vody, výrobu potravin a dalších základních potřeb.

Růst migrace, zejména z válkou zasažených oblastí, přináší nejen humanitární výzvy, ale také možné bezpečnostní hrozby v podobě nelegální migrace, organizovaného zločinu nebo potenciálního teroristického infiltrátu. To vyžaduje zvýšenou pozornost a kontrolu hranic.

Na tyto nastíněné hrozby, jejichž výčet není úplný, je nutno reagovat v rámci zvyšování odolnosti kritické infrastruktury a přípravy bezpečnostních složek, budování bezpečného veřejného prostoru, nebo environmentální bezpečnosti.

Jedním z velmi významných nástrojů pro řešení nastíněných rizik je i dlouhodobě etablovaný Bezpečnostní výzkum ČR, který přináší inovativní řešení pro zvyšování odolnosti a ochrany kritické infrastruktury, zefektivnění postupů bezpečnostních složek i celého IZS, i přínos k rozvoji efektivních bezpečnostních politik a strategií.

A) nastavení cílů programu

Zaměření Programu IMPAKT 2 vychází ze strategických dokumentů v oblasti bezpečnostní politiky a národních strategických dokumentů v oblasti výzkumu, vývoje a inovací. Jedná se především o Meziresortní koncepcí podpory bezpečnostního výzkumu ČR 2017–2023 s výhledem do roku 2030, která formulovala prioritizované věcné vymezení bezpečnostního výzkumu. V tomto věcném vymezení se předpokládá zacílení prostředků z programů Ministerstva vnitra na tzv. výhradní témata bezpečnostního výzkumu zaměřená na plnění prioritních cílů celého systému podpory bezpečnostního výzkumu. Jde především o oblast „efektivní zásah“, který rozvíjí schopnosti včas identifikovat hrozící nebezpečí nebo probíhající incident, zorientovat se v situaci a v nejkratším možném čase adekvátně a koordinovaně reagovat v jeho průběhu i po jeho skončení v souladu se svou systémovou funkcí. K tomu je všestranně připraven a vybaven vhodnými prostředky, včetně vlastní ochrany, které vždy splňují přísné nároky na funkci v náročných podmínkách a zároveň nesnižují úroveň pozornosti, či jinak nezatěžují fyzické či kognitivní kapacity jedince. Za druhou hlavní oblast lze považovat „adaptabilní bezpečnostní systém“, kde se jedná o prediktivní analýzu, soustavnou analýzu rizik, modelování, simulaci a evaluaci. Bezpečnostní systém z nich těží a promítá jejich závěry do regulace i plánování na všech rozhodovacích úrovních. Jednotlivé bezpečnostní složky a součásti bezpečnostního systému optimalizují vlastní plány, postupy, řídicí procesy a náklady tak, aby byly vždy schopné plnit své úkoly v požadované kvalitě a rozsahu, a tyto aspekty aktivně maximalizovat učením se ze zkušeností. Jejich směřování probíhá proaktivně, v prostředí, kde kritická rozhodnutí podporují přesné, důvěryhodné a precizně analyticky zpracované informace z maximálního možného spektra relevantních zdrojů.

Svým tematickým vymezením Program navazuje na vysoce participativní proces tvorby Národních priorit orientovaného výzkumu, vývoje a inovací, který byl realizován v roce 2024.

Zaměření Programu také navazuje na Národní výzkumnou a inovační strategii pro inteligentní specializaci České republiky 2021–2027 (Národní RIS3 strategie). Svým zacílením na koncentraci výzkumných kapacit, integraci výzkumných témat a agend a současně důrazem na rozvoj mezinárodní spolupráce přispívá k realizaci strategického cíle Zvýšení kvality veřejného výzkumu (klíčová oblast změn – Veřejný výzkum a vývoj) a jeho komponenty B1 – Zvýšení kvality a společenské relevance veřejného výzkumu.

Program IMPAKT 2 svým tematickým zaměřením také navazuje na vymezení prioritní oblasti 6 – Bezpečná společnost Národních priorit orientovaného výzkumu, experimentálního vývoje a inovací, zejména na vymezení oblastí 1. Bezpečnost občanů, 2. Bezpečnost kritických infrastruktur a zdrojů a 3. Krizové řízení a bezpečnostní politika.

Hlavní cíl programu IMPAKT 2 je jasně definován jako soustředěná mobilizace potenciálu akademického a veřejného výzkumného sektoru v oblastech spolupráce a koordinace výzkumných agend výzkumných organizací, mezinárodní spolupráce a rozvoje lidských zdrojů (institucionálního zázemí) pro rozvoj bezpečnostního výzkumu, která přispěje k vytvoření prostředí pro synergickou a dlouhodobou výzkumnou podporu bezpečnostního systému ČR.

Program se dělí na 3 podprogramy, které jsou odlišného charakteru, mezi kterými, ale i ve vztahu k iniciativám již existujícím v národním výzkumném prostředí, existují synergické efekty.

Podprogram 1 – Centra spolupráce v bezpečnostním výzkumu. Cílem je posílení znalostní a výzkumnou základnu bezpečnostního systému prostřednictvím vytvoření Center spolupráce v bezpečnostním výzkumu, která zajistí integraci a koordinaci výzkumných aktivit v prioritních

oblastech napříč výzkumnou komunitou, efektivní šíření znalostí a technologií mezi výzkumnou komunitou a koncovými uživateli a dlouhodobý rozvoj odborných kapacit a aplikovaných znalostí v klíčových oblastech, které odpovídají dlouhodobým potřebám bezpečnostního systému.

Podprogram 2 – Internacionalizace bezpečnostního výzkumu. Cílem je rozvoj mezinárodní spolupráce v oblasti bezpečnostního výzkumu za účelem získání a sdílení klíčových poznatků a posílení globální konkurenceschopnosti domácí výzkumné komunity. Zahrnuje podporu projektových iniciativ a pracovišť při realizaci mezinárodních projektů v klíčových oblastech bezpečnostního výzkumu, rozvoj spolupráce ve vysoce specializovaných tématech relevantních pro bezpečnostní systém, prohlubování vztahů mezi českými vědeckými institucemi a zahraničními partnery za účelem dlouhodobé spolupráce a sdílení know-how.

Podprogram 3 – Lidské zdroje pro bezpečnostní výzkum. Cílem je mobilizovat lidský potenciál nezbytný pro rozvoj bezpečnostního výzkumu, podpoření iniciativ zaměřených na profesní růst a dlouhodobý rozvoj odborné způsobilosti v oblasti bezpečnostního výzkumu, stimulaci kariérního rozvoje mladých (začínajících) výzkumníků a výzkumnic, vytvoření podmínek pro návrat výzkumníků a výzkumnic do bezpečnostního výzkumu po kariérní přestávce, vytvoření podmínek pro návrat a další kariérní rozvoj výzkumníků a výzkumnic ze zahraničních výzkumných organizací.

Rozdělení na specifické podprogramy, z nichž každý má svůj cíl, specifické podporované aktivity, výstupy, výsledky a dopady, bude naplňovat intervenční logiku Programu.

Cíle Programu jsou definovány konkrétně, jsou konsistentní, měřitelné dle stanovených indikátorů a reálné.

B) synergie s jinými programy

Program IMPAKT 2 navazuje na zkušenosti z realizace svého předchůdce Programu IMPAKT 1 a přináší významné změny parametrů směrem ke stabilizaci podpořených týmů s důrazem na rozvoj udržitelnosti. Je součástí portfolia programů na podporu bezpečnostního výzkumu a je komplementární k institucionální podpoře na dlouhodobý koncepční rozvoj výzkumných organizací.

Program bude vytvářet potřebné a unikátní synergické efekty s dalšími programy Bezpečnostního výzkumu, jedná se především o:

Program Otevřené výzvy v bezpečnostním výzkumu 2023–2029 (OPSEC) je páteřním programem portfolia programových nástrojů účelové podpory bezpečnostního výzkumu. Jeho hlavním cílem je systematicky podněcovat a rozvíjet zájem výzkumné a inovační sféry o zapojení do řešení bezpečnostních výzev pro moderní společnost a tvořit tak základnu pro rozvoj konkurenceschopných bezpečnostních inovací.

Program bezpečnostního výzkumu pro potřeby státu 2022–2027 (SecPro) je realizován zadáváním jednotlivých veřejných zakázek na služby ve výzkumu a experimentálním vývoji. Jeho posláním je zajištění výzkumných potřeb státu (resp. orgánů státní správy, bezpečnostních a záchranných sborů) v oblasti bezpečnosti, v souladu s inovačními a rozvojovými prioritami, jak je vymezují platné strategické a koncepční materiály bezpečnostní politiky, které shrnuje Meziresortní koncepce podpory bezpečnostního výzkumu.

Program bezpečnostního výzkumu ČR 2021–2026: vývoj, testování a evaluace nových bezpečnostních technologií (SECTECH) podporuje vývojové, testovací a evaluační aktivity v oblasti bezpečnosti státu a jeho občanů v souladu s charakteristickými potřebami bezpečnostního systému. Jeho cílem je prostřednictvím mobilizace potenciálu podnikového sektoru, zejm. začínajících, malých a středních podniků, k participaci na vývoji a transferu nových bezpečnostních technologií podpořit dosažení technologické a technické úrovně, která umožní jednotlivým složkám bezpečnostního systému ČR získávat, osvojovat si, udržovat a rozvíjet specifické schopnosti pro zajištění bezpečnosti státu a jeho občanů.

Žádný z podprogramů Programu IMPAKT 2 nemá v ČR přímý ekvivalent, ve kterém by hrozily překryvy nebo neefektivní přístupy. Jedním z důvodů je i požadavek na úzké propojení s praxí bezpečnostního systému a jeho specializovaných požadavků v různém časovém horizontu. Ukazuje se, že se kolem programů Ministerstva vnitra dlouhodobě vytváří specializovaná komunita s omezenými možnostmi podpory z jiných zdrojů. Jakkoliv jsou tyto týmy relativně úspěšné i v programech EU, jde stále především o míru specializace jejich činnosti, a tedy omezenou širokou dostupnost relevantních nástrojů podpory. Program IMPAKT 2 proto aspiruje právě na posílení možností specializovaných pracovišť k vlastnímu rozvoji bez nutnosti opouštět zájmovou sféru témat relevantních pro konečné uživatele.

Situaci v EU lze považovat za obdobnou z hlediska pokrytí bezpečnostně relevantních témat z relativně užšího programu SecureSocieties (v současnosti tzv. Cluster 3), který se svými prioritami s potřebami českého bezpečnostního výzkumu překrývá jen částečně. Kapitola SecureSocieties mezi jednotlivými Rámcovými programy od svého zařazení v roce 2006 a pod různými názvy soustavně roste v objemu finančního zajištění. Vedle této specializované části jsou ale relevantní projekty podporovány napříč řadou dalších nástrojů. Obdobně jako je tomu v ČR, specializovanou část řídí a kontroluje DG HOME, zatímco ostatní části (např. ICT nebo Health) jsou řízeny z jiných organizačních jednotek Evropské komise. Přesto, opět obdobně jako v ČR, má i specializovaná část evropského bezpečnostního výzkumu nadresortní charakter, který kombinuje široké spektrum potřeb a požadavků evropské bezpečnostní politiky.

V rámci EU podporuje bezpečnostní výzkum i řada členských států. Velká Británie, podobně jako USA, poskytuje podporu na úzce vymezená témata, spojená s potřebami bezpečnostního systému, cestou specializované agentury (*Home Office*, po organizačních změnách se zapojením *Defense Science and Technology Laboratories*, které supluje roli organizací financovaných v ČR institucionální podporou). Podobnou cestu volilo i Švédsko, kde se bezpečnostnímu výzkumu věnuje Agentura pro zvládání mimořádných událostí. Mezi další státy se samostatným bezpečnostním výzkumem lze zařadit Nizozemsko, Francii, Itálii, Finsko, Německo a Rakousko. Tyto státy tvoří také skupinu prioritních zemí pro cílení mezinárodní spolupráce v bezpečnostním výzkumu na evropské úrovni.

Program je s ostatními programy podpory MV komplementární. K duplicitě s jinými programy BV nedochází. V systému podpory bezpečnostního výzkumu program doplňuje ostatní programové nástroje, realizovaných formou veřejné soutěže/zakázky.

C) zkušenosti z předchozích programů

Program reflektuje dlouhodobé zkušenosti poskytovatele s programy Bezpečnostního výzkumu, z poslední doby se jedná zejména o:

Program IMPAKT 1, který vnáší do portfolia podpory bezpečnostního výzkumu možnost rozvoje schopností výzkumné sféry v oblastech, které mají pro bezpečnostní výzkum dlouhodobě strategický význam. Hlavní část podpory se zaměřuje na projekty, které vykazují klíčový operační význam v kontextu současného stavu bezpečnostního systému.

Program bezpečnostního výzkumu ČR 2021–2026: vývoj, testování a evaluace nových bezpečnostních technologií (SECTECH) přináší do portfolia schopnost podpořit projekty, které vynikají vývojovou povahou a značným důrazem na testování a evaluaci v reálných podmínkách, s cílem dotažení budoucího nového produktu a jeho funkčních vlastností. Zacílení na oblasti strategického významu a oblasti s vysokým potenciálem umožňuje vysokou přidanou hodnotu v oblasti bezpečnosti u podpořených výsledků, s využitím nejnovějších dostupných technologií.

Program Otevřené výzvy v bezpečnostním výzkumu 2023–2029 (OPSEC) hraje v portfoliu poskytovatele klíčovou roli. Podporuje také rozvoj aplikací relativně nižší úrovně vyspělosti v technických oblastech s vysokým potenciálem a dává dále prostor pro dílčí projekty netechnické povahy.

Program bezpečnostního výzkumu pro potřeby státu 2022–2027 (SECPRO) slouží k zajištění výzkumných potřeb státu (resp. orgánů státní správy, bezpečnostních a záchranných sborů) v oblasti bezpečnosti, v souladu s inovačními a rozvojovými prioritami.

V rámci programu institucionální podpory cílí Ministerstvo vnitra pozornost především na aktivity jako např. udržitelnost schopností a infrastruktury, internacionalizace výzkumu a vývoje, veřejná komunikace a prezentace výsledků.

Ve snaze maximálního zamezení možným duplicitám v poskytování podpory dochází mezi tematicky nejbližšími poskytovateli ke kooperaci, a k zastoupení jednotlivých poskytovatelů v odborných poradních orgánech napříč ostatními poskytovateli. Stejně tak jako má svého nominanta v Radě programu IMPAKT Ministerstvo školství, mládeže a tělovýchovy nebo například Technologická agentura ČR, tak i Ministerstvo vnitra je členem odborných poradních orgánů jiných poskytovatelů (například Ministerstvo obrany, Ministerstvo dopravy, Technologická agentura ČR).

V předchozím programu IMPAKT 1 byl identifikován významný převis poptávky, v rámci celkem 4 veřejných soutěží bylo podpořeno jen 33 % z celkového objemu požadavku finančních prostředků, zbývající část návrhů nebyla podpořena z důvodu nedoporučení návrhů projektů k podpoře odborným poradním orgánem nebo z důvodu nedostatku financí. Všechny podpořené projekty v programu IMPAKT 1 byly relevantní z hlediska vazby na strategické dokumenty ve výzkumu, vývoji a inovacích jako jsou Národní priority orientovaného výzkumu, experimentálního vývoje a inovací, Národní výzkumná a inovační strategie pro inteligenční specializaci České republiky a Národní politika výzkumu, vývoje a inovací České republiky. Obdobně každý projekt splňoval vazbu na výše uvedené dokumenty a přispěl tak k naplnění v nich definovaných cílů.

Z dosud získaných ohlasů příjemců podpory i uživatelů výsledků bezpečnostního výzkumu vyplývá, že program IMPAKT 1 bude oběma stranami pozitivně hodnocen. I to je jedním z důvodů, proč je předkládán IMPAKT 2. Mj. se také osvědčilo zacílení programu pouze na výzkumné organizace.

Členění podobného typu programů na podprogramy bylo také přínosné, a proto pokračuje navazující program se třemi podprogramy popsány výše.

Poskytovatel průběžně vyhodnocuje informace získané z přihlášek do veřejných soutěží (tj. zda informace byly dostatečné ke správnému rozhodnutí o ne/poskytnutí účelové podpory

nebo zda také nejsou pro příjemce zbytečně zatěžující bez větší přidané hodnoty v následném procesu). Pozornost je také věnována výběru vhodných oponentů, kritéria výběru jsou po každé soutěži vyhodnocována a jsou činěna opatření pro další veřejné soutěže, aby výběr nezávislých oponentů byl efektivní s maximálním přínosem pro rozhodnutí o ne/udělení podpory.

Kontinuálně poskytovatel sleduje i v rámci řešení podpořených projektů jednotlivé procesy, ve kterých může dojít ke zlepšení. Například věcné kontroly jsou přizpůsobovány charakteristice jednotlivých projektů, resp. podprogramů (za respektu všech zákonných aspektů). Další oblastí se snahou poskytovatele o minimální zátěž příjemce a zefektivnění procesu změnových řízení.

Program tak navazuje na analýzu minulých zkušeností, současného stavu, potřeba požadavků na systém bezpečnostního výzkumu kladených a jeho významných specifik.

D) způsob postupného hodnocení programu

Realizace projektů, kterým byla poskytnuta účelová podpora z Programu, bude monitorována prostřednictvím průběžných a závěrečných zpráv vypracovaných příjemcem podle pokynů poskytovatele. Monitoring řešení projektu poskytovatelem bude probíhat za účasti členů Rady. Kontrolu a věcné zhodnocení plnění cílů projektu provede poskytovatel v souladu s § 13 odst. 1 a 2 zákona č. 130/2002 Sb. Poskytovatel zároveň provádí finanční kontrolu podle § 13 odst. 3 zákona č. 130/2002 Sb. a souvisejících právních předpisů. U Podprogramu 1 bude v průběhu realizace projektu u každého podpořeného projektu provedeno podrobné průběžné hodnocení plnění cílů a aktivit projektů a dosahování jeho výstupů.

Monitorování a hodnocení průběhu a splnění cílů Programu bude provedeno v souladu s Metodikou 2025+ a principy pro hodnocení programů účelové podpory platnými v době hodnocení Programu, případně podmínkami stanovenými poskytovatelem.

Průběh Programu a jeho jednotlivých podprogramů bude poskytovatelem kontinuálně monitorován na základě sady kvantitativních monitorovacích ukazatelů. Monitorovací ukazatele sledují počet a strukturální charakteristiky projektů a příjemců (resp. podpořených subjektů) a čerpání finančních prostředků Programu. Hodnoty těchto ukazatelů budou získávány z periodických a závěrečných zpráv o realizaci projektu, které budou předkládat příjemci podpory, a z IS VaVal.

V průběhu realizace Programu bude provedeno průběžné hodnocení Programu poskytovatelem, dále pak hodnocení ukončeného Programu a hodnocení jeho dopadů.

Průběžné hodnocení Programu bude nabývat především formativní podoby a bude provedeno na dvou úrovních – úrovni veřejných soutěží a úrovni podprogramů. Hodnocení na úrovni veřejných soutěží bude spočívat v evaluaci každé ukončené veřejné soutěže. Kromě průběžného sledování charakteristik poptávky po podpoře, a to z hlediska oborového, tematického a institucionálního rozložení, úspěšnosti a podílu udělené na podpoře, se zaměří také na zhodnocení relevance a funkčnosti. Hodnocení na úrovni podprogramů bude provedeno odlišně, u Podprogramu 1 po ukončení průběžného hodnocení projektů podpořených v první veřejné soutěži a ukončení druhé veřejné soutěže s cílem poskytnutí informací pro rozhodnutí, zda v pokračovat s podporou prostřednictvím podobně koncipovaného programu, a tvorbu návazných nástrojů podpory. U Podprogramu 2 a 3 po

ukončení druhé veřejné soutěže a před vyhlášením třetí veřejné soutěže, s cílem získání informací pro efektivní zaměření třetí veřejné soutěže tak, aby byly splněny cíle podprogramů, a dále získání podkladů pro zaměření případného návazného programu.

Průběžné hodnocení provede poskytovatel (případně ve spolupráci s externím subjektem). Zaměří se na zjištění úrovně naplňování cíle, účelu a aktivit podprogramů a Programu, souladu implementace podprogramů a Programu s jeho intervenční logikou.

Hodnocení ukončeného Programu bude realizováno do 18 měsíců po ukončení Programu. Zaměří se na zhodnocení všech realizovaných aktivit, výstupů a výsledků Programu a vyhodnocení naplnění cílů Programu. Hodnocení provede nezávislý externí subjekt.

Hodnocení dopadů Programu bude uskutečněno po 3 letech od ukončení Programu. Zaměří se na zhodnocení dopadů, jejich rozsahu a trvalosti na úrovni jednotlivých podprogramů i celého Programu. Provedou jej nezávislí externí hodnotitelé ve spolupráci s poskytovatelem.

Průběžné hodnocení, hodnocení ukončeného Programu a hodnocení dopadů budou založeny na kvantitativních a kvalitativních indikátorech, které uvádí v příloha 2 Programu. Pro zjištění hodnot indikátorů budou využity zejména informace z průběžných a závěrečných zpráv o řešení projektů, IS VaVal, zpráv o implementaci projektů předkládané příjemci, interní databáze a archivy poskytovatele, dotazníková šetření a strukturované rozhovory.

Zpracovaný rámec evaluační strategie a monitoringu v návrh Programu je odpovídající, přehledný, plně realizovatelný a kvalitně zpracovaný.

E) očekávané výsledky a dopady programu

U Podprogramu 1 jsou očekávány výsledky - posílení koordinace výzkumných agend a aktivit výzkumných organizací sdružených v jednotlivých Centrech spolupráce v bezpečnostním výzkumu a následné zvýšení efektivity a excelence prováděných aktivit ve výzkumu a vývoji, efektivnější přenos poznatků bezpečnostního výzkumu dosažených v Centrech spolupráce v bezpečnostním výzkumu (resp. sdružených výzkumných organizacích) do aplikačního sektoru (sdružených v radě uživatelů), identifikace a rozvoj nových směrů a oborů výzkumu dle potřeb bezpečnostního systému (aplikačního sektoru).

Dopady - pomoc dlouhodobě etablovat schopnosti výzkumné podpory bezpečnostního systému a stabilizovat spolupráci vzájemně se doplňujících organizací, aniž by docházelo k nadbytečné institucionalizaci nebo zdvojování aktivit. Dopady podprogramu lze spatřovat zejména v konsolidaci výzkumné základny pro bezpečnostní výzkum a její orientace na klíčové priority bezpečnostního systému, dosažení excelence a zvýšení aplikovatelnosti poznatků bezpečnostního výzkumu, zlepšení koordinace a synergického působení výzkumných aktivit napříč institucemi, vyšším využívání poznatků VaV v bezpečnostním systému ČR.

Pro Podprogram 2 jsou očekávány výsledky - zvýšení účasti českých výzkumných týmů v mezinárodních programech a zejména programech podpory bezpečnostního výzkumu, zapojení do mezinárodních výzkumných sítí prostřednictvím nových partnerství mezi českými a zahraničními výzkumnými organizacemi, zapojení českých výzkumných organizací do zahraničních vědeckých společností, platforem či klastrů.

Dopady - přispívá k posílení zahraničních vztahů klíčových výzkumných týmů s úzkou bezpečnostní specializací a posílení často existujících vazeb jednotlivých výzkumníků, do podoby institucionální komunikace a spolupráce. Dopady lze charakterizovat jako zvýšení mezinárodní viditelnosti domácího bezpečnostního výzkumu a výzkumných organizací věnujících se bezpečnostnímu výzkumu, diverzifikace finančních zdrojů na podporu bezpečnostního výzkumu se zvýšením objemu podpory ze zahraničních programů, získání přístupu k zahraničním technologiím a know-how.

U Podprogramu 3 jsou očekávány výsledky - zvýšení počtu juniorních výzkumníků a výzkumnic v bezpečnostním výzkumu, zlepšení podmínek pro návrat výzkumnic po kariérní přestávce – odstranění bariér pro jejich opětovné zapojení do výzkumných a vývojových aktivit, návrat zahraničních výzkumníků do ČR, vytvoření atraktivních podmínek pro jejich uplatnění v domácích výzkumných organizacích, posílení mezinárodní mobility výzkumníků a výzkumnic.

Dopady - prohloubení zájmu výzkumníků o bezpečnostní výzkum a nápomoc vyšší participaci zejména juniorních výzkumníků/výzkumnic a výzkumnic po kariérní přestávce v aktivitách bezpečnostního výzkumu. Je očekáváno především zajištění generační obnovy v oblasti bezpečnostního výzkumu, zvýšení diverzity a rovnosti příležitostí v rámci výzkumných týmů, dlouhodobá stabilizace lidských kapacit v bezpečnostním výzkumu, zvýšení excelence, resp. odborné kvality výzkumníků schopných realizovat špičkový výzkum v ČR.

Na úrovni celého Programu jsou očekávány dopady - zvýšení excelence a globální konkurenceschopnosti výzkumných pracovišť věnujících se bezpečnostnímu výzkumu, zajištění dlouhodobé udržitelnosti odborných kapacit v bezpečnostním výzkumu ČR, včetně posílení mezinárodního renomé domácích výzkumných organizací v oblasti bezpečnostního výzkumu.

Představené cíle a dopady jsou plně v souladu s výše uvedenými hlavními strategickými dokumenty.

Výstupy Programu budou přímé efekty podpořených/realizovaných aktivit Programu, kterých bude dosaženo s využitím vstupů Programu. V Programu budou rozlišovány vědecké výstupy a věcné výstupy. Vědecké výstupy odpovídají klasifikaci a definicím výsledků uvedeným v Metodice 2025+ a užívaným v RIV (tj. jde o formální výsledky). Jejich spektrum je dostatečně široké a odpovídá multidisciplinaritě Programu.

Některé z typů výsledků budou uznatelné, pouze pokud splňují předpoklady - ustanovení § 3 zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, a svým věcným zaměřením spadají do některé z oblastí vymezených nařízením vlády č. 522/2005 Sb., kterým se stanoví seznam utajovaných informací, ve znění pozdějších předpisů, v celém jeho rozsahu a takový ochranný režim vyžádá konečný uživatel, nebo ustanovení § 27 zákona č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon) a ochranu v režimu zvláštní skutečnosti vyžádá konečný uživatel.

To je zcela pochopitelné u výsledků H_{konc} , H_{pub} , N_{map} , V_{souhrn} , a O , diskutabilní je to u výsledků typu R a S a dle názoru posuzovatele zcela nevhodné u výsledků N_{met} . Zde je potřebné doporučit vyřazení těchto výsledků z výčtu restrikcí.

F) rizika spojená s realizací programu

Dokumentace Programu zahrnuje také komplexní analýzu rizik spojených s jeho realizací. V tabulkách jsou zaznamenána rizika, která by mohla zamezit nebo omezit dosažení vytyčených cílů. Rizika jsou rozdělena na skupin rizik politických, ekonomických, společenských, technických, legislativních a environmentálních (analýza PESTLE). Žádné environmentální riziko nebylo identifikováno. V analýze byla využita pětistupňová škála hodnocení pravděpodobnosti a dopadu.

V kategoriích rizik společenských, technických a legislativních se nachází pouze rizika s nízkým významem. V textu je uvedeno, že *„tři ze čtyř uvedených politických rizik lze označit za rizika středního významu a dvě ekonomická rizika mají význam vysoký.“*, tabulka politických rizik obsahuje ale pouze tři rizika.

Byly stanoveny referenční hodnoty úrovně rizik a v relaci na kategorizaci významu rizik byla navržena příslušná eliminační opatření. Rizika jsou identifikována zodpovědně a eliminační opatření reálná. Komplexní reflexe rizik nasvědčuje na systematické úsilí poskytovatele v této oblasti a znalost prostředí.

Závěr:

Bezpečnostní situace ve světě se v posledních letech bohužel významnou měrou zhoršuje, situace v ČR je sice relativně stabilní, ale existují hrozby a rizika, které mohou ovlivnit národní bezpečnost, včetně bezpečnosti kritické infrastruktury. Hrozby jsou velmi různorodé a mohou pocházet jak z vnějších, tak vnitřních zdrojů. Lze konstatovat, že vzhledem k současnému geopolitickému napětí, rostoucímu vlivu širokého spektra kybernetických útoků a i hybridních hrozeb, lze Českou republiku vnímat jako zranitelnou vůči bezpečnostním rizikům. Na tyto hrozby je nutno reagovat v rámci zvyšování odolnosti kritické infrastruktury a přípravy bezpečnostních složek, budování bezpečného veřejného prostoru, nebo environmentální bezpečnosti. Jedním z velmi významných nástrojů pro řešení možných rizik v této oblasti je i dlouhodobě etablovaný Bezpečnostní výzkum ČR, který přináší inovativní řešení pro zvyšování odolnosti a ochrany kritické infrastruktury, zefektivnění postupů bezpečnostních složek i celého IZS i přínos k rozvoji efektivních bezpečnostních politik a strategií.

Program reaguje adekvátně na společenské potřeby, plynoucí z analýzy aktuálního situace a rizik bezpečnostní oblasti.

Program IMPAKT 2 navazuje na zkušenosti z realizace svého předchůdce Programu IMPAKT 1 a přináší změny parametrů směrem ke stabilizaci podpořených týmů s důrazem na rozvoj udržitelnosti. Je součástí portfolia programů na podporu bezpečnostního výzkumu a je komplementární k institucionální podpoře na dlouhodobý koncepční rozvoj výzkumných organizací. Program bude vytvářet potřebné a unikátní synergické efekty s dalšími programy Bezpečnostního výzkumu, jedná se především o Program Otevřené výzvy v bezpečnostním výzkumu 2023–2029 (OPSEC), Program bezpečnostního výzkumu pro potřeby státu 2022–2027 (SecPro), Program bezpečnostního výzkumu ČR 2021–2026: vývoj, testování a evaluace nových bezpečnostních technologií (SECTECH). Žádný z připravovaných podprogramů Programu IMPAKT 2 nemá v ČR přímý ekvivalent, ve kterém by hrozily překryvy nebo neefektivní přístupy.

Program reflektuje dlouhodobé zkušenosti poskytovatele s programy Bezpečnostního výzkumu,

Členění podobného typu programů v minulosti na podprogramy bylo přínosné, a proto pokračuje IMPAKT 2 se třemi podprogramy. Poskytovatel sleduje i v rámci řešení podpořených projektů jednotlivé procesy, ve kterých může dojít ke zlepšení. Program navazuje na analýzu minulých zkušeností, současného stavu, potřeb a požadavků na systém Bezpečnostního výzkumu kladených a zohledňuje jeho významná specifika.

Na úrovni celého Programu je očekáváno zvýšení excelence a globální konkurenceschopnosti výzkumných pracovišť věnujících se bezpečnostnímu výzkumu, zajištění dlouhodobé udržitelnosti odborných kapacit v bezpečnostním výzkumu ČR, včetně posílení mezinárodního renomé domácích výzkumných organizací v oblasti bezpečnostního výzkumu.

Zpracovaný rámec evaluační strategie a monitoringu v návrh Programu je odpovídající, přehledný, plně realizovatelný a kvalitně zpracovaný. Navřené způsoby a zvolené metody hodnocení mají potenciál pro objektivní zhodnocení Programu.

Analýza řešené problematiky je zpracována vysoce fundovaně a vyčerpávajícím způsobem.

Představené cíle a dopady jsou plně v souladu s výše uvedenými hlavními strategickými dokumenty (Meziresortní koncepce podpory bezpečnostního výzkumu ČR 2017–2023 s výhledem do roku 2030, Národní RIS3 strategie, a další). Cíle Programu vycházejí

z komplexní analýzy bezpečnostní problematiky a potřeb bezpečnostní komunity. Navržené cíle jsou dostatečně ambiciózní a jejich dosažení je plně reálné.

Zpracovaný rámec evaluační strategie a monitoringu v návrhu Programu je odpovídající, přehledný, plně realizovatelný a kvalitně zpracovaný.

Výstupy Programu budou přímé efekty podpořených/realizovaných aktivit Programu. Vědecké výstupy odpovídají klasifikaci a definicím výsledků uvedeným v Metodice 2025+ a užívaným v RIV. Jejich spektrum je dostatečně široké a odpovídá multidisciplinaritě Programu, je definován odpovídající počet výsledků, včetně způsobu jejich využití

Některé z typů výsledků budou uznatelné, pouze pokud splňují předpoklady - ustanovení § 3 zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, a svým věcným zaměřením spadají do některé z oblastí vymezených nařízením vlády č. 522/2005 Sb., kterým se stanoví seznam utajovaných informací, ve znění pozdějších předpisů, v celém jeho rozsahu a takový ochranný režim vyžádá konečný uživatel, nebo ustanovení § 27 zákona č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon) a ochranu v režimu zvláštní skutečnosti vyžádá konečný uživatel.

To je zcela pochopitelné u výsledků H_{konc} , H_{pub} , N_{map} , V_{souhrn} , a O , diskutabilní je to u výsledků typu R a S a dle názoru posuzovatele zcela nevhodné u výsledků N_{met} . Zde je potřebné doporučit vyřazení těchto výsledků z výčtu restrikcí.

Dokumentace Programu zahrnuje také komplexní analýzu rizik spojených s jeho realizací. V tabulkách jsou zaznamenána rizika, která by mohla zamezit nebo omezit dosažení vytyčených cílů. Rizika jsou rozdělena na skupin rizik politických, ekonomických, společenských, technických, legislativních a environmentálních (analýza PESTLE). V analýze byla využita pětistupňová škála hodnocení pravděpodobnosti a dopadu.

Byly stanoveny referenční hodnoty úrovně rizik a v relaci na kategorizaci významu rizik byla navržena příslušná eliminační opatření. Rizika jsou identifikována zodpovědně a eliminační opatření reálná. Komplexní reflexe rizik nasvědčuje na systematické úsilí poskytovatele v této oblasti a znalost prostředí. Rizika spojená s realizací Programu jsou definována vyčerpávajícím způsobem a indikátory jsou vhodně zvoleny, včetně jejich počáteční hodnoty.

Závěrem lze konstatovat, že Program je kvalitně připraven, plně životaschopný a pro uživatelskou komunitu žádoucí.



RNDr. Marek Kotrlý, Ph.D.