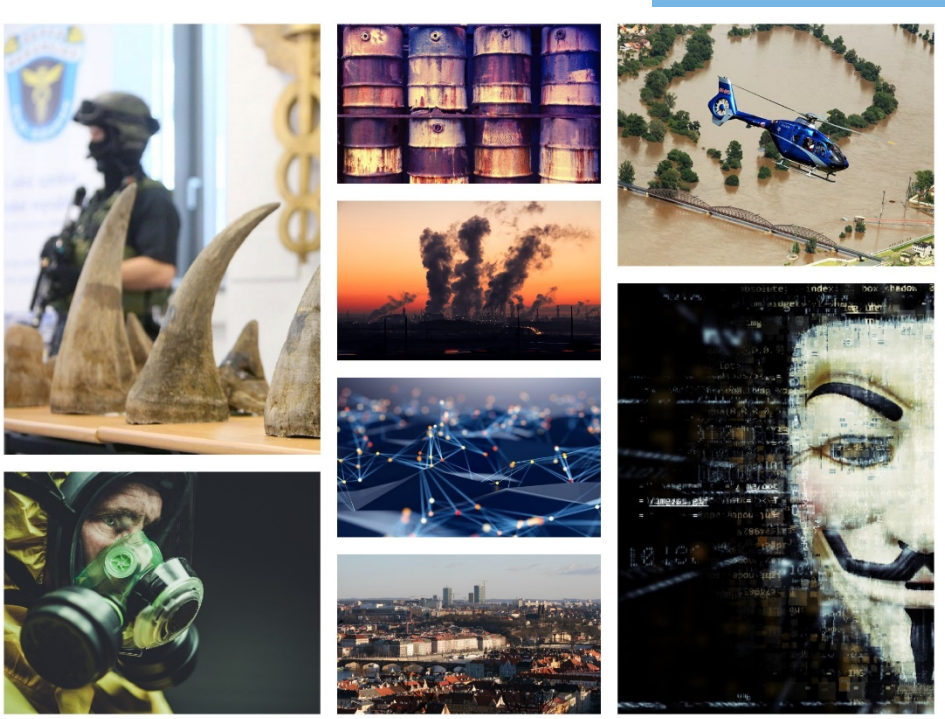
MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

2021

Podkladová studie k návrhu programu Otevřené výzvy v bezpečnostním výzkumu 2022-2027 (OPSEC)



Ludek Moravec

7/11/2021

OBSAH

1 ÚVOD – KONCEPT PROGRAMU SOUTĚŽ 3

Vznik podpory bezpečnostního výzkumu jako konsolidované agendy je v EU spojen s několika tragickými událostmi – s teroristickými útoky v Londýně a Madridu a sérií živelních katastrof krátce po nich. Premisou jejich vzniku bylo a je, že dynamické bezpečnostní prostředí vyžaduje přinejmenším stejně dynamickou schopnost reakce a se zapojením výzkumné a inovační komunity lze tuto dynamiku zásadně posílit. Simultánně reprezentují tyto programy snahu o kultivaci trhu bezpečnostních technologií, který je vysoce specifický a pro zájemce o inovace na tomto poli, vzdor populární percepci, velmi rizikový.

ČR, díky vlastním zkušenostem zejm. se zvládáním přírodních katastrof, tohoto trendu v EU využila a v rámci reformy systému poskytování veřejné podpory na výzkum, vývoj a inovace, stanovila MV gestorem této problematiky s širokou nadresortní působností. Programy veřejných soutěží tvoří z logistických i praktických důvodů dlouhodobě páteř této podpory. Při tom organizace podpory v ČR v jistém smyslu předstihla přinejmenším evropské trendy, ať již ukotvením na věcně odpovědném ministerstvu nebo aktivním zahrnutím kyberbezpečnosti do podporovaného spektra od samého začátku těchto podpor.

Předkládaná třetí generace programu veřejných soutěží stojí na širokých zkušenostech z implementace programů předchozích, včetně řady experimentálních postupů (uživatelské hodnocení, cílená soutěž, evaluace). Ty postupně umožnily „krystalizaci“ center excelence ve veřejné akademické komunitě, cestou koncentrace finančních prostředků z kompetitivních nástrojů.. Spolu s úpravou postupů pro poskytování institucionální podpory docílil poskytovatel také modifikace v roli, kterou v těchto programech hrají státní/resortní specializované výzkumné organizace. Ta se postupem času změnila z významných příjemců na specializované dodavatele/moderátory v projektech ostatních VO. Postupně také roste komunita zapojených podniků všech velikostí, zejm. ale malých a středních a vzájemné propojování právě s několika stěžejními vysokoškolskými pracovišti.

Bezpečnostní výzkum se díky těmto programům etabloval jako hlavní nebo jediný zdroj podpory pro kyberbezpečnost, CBRN, forenzní vědy nebo aplikace v některých často zmiňovaných silných oborech české vědy, jako AI nebo nanotechnologie. V kyberbezpečnosti lze zmínit projekt KYPO (FI MUNI), který je základem pro celou řadu dalších vývojových aktivit, ale slouží také přípravě vládních i podnikových profesionálů na kybernetické incidenty. Přímo tím zásadně ovlivňuje bezpečnost ČR. V CBRN lze hovořit o celé řadě laboratorních nebo testovacích metod, které krom přímého uplatnění bývají často předmětem mezinárodní výměny a spolupráce a vstupují tedy i do sféry vědecké diplomacie. Ve forenzních oborech se nabízí patentovaná metoda rozeznávání půdních fází, v AI potom řečové technologie, široce používané policejními sbory doma i v zahraničí a v nanotechnologiích např. nanovlákenné prostředky osobní ochrany, připravené speciálně se zohledněním požadavků bezpečnostních a záchranných sborů, komercionalizované a úspěšně používané v ČR i v zahraničí.

U třetí generace programu se poskytovatel snaží akcentovat dobrou praxi z minula a úzce ji svázat s prioritami bezpečnostní politiky, aniž by došlo k narušení jiných vlastností programu, jako je multidisciplinarita, oborová i tematická otevřenost.

1.1 CHARAKTERISTIKY TRHU BEZPEČNOSTNÍCH TECHNOLOGIÍ

Efektivní rozvoj inovací v bezpečnostním sektoru je prakticky závislý na veřejné podpoře. Jde totiž o **natolik specifický tržní segment, že rizika vlastní investice do vývoje dedikované bezpečnostní**

technologie jsou pro podnik v ČR prakticky prohibitivní. Tomu odpovídá i dnešní situace, kde drtivou většinu technologií pro tento sektor produkují hráči mimo tento segment jako doplněk svého portfolia a v těchto případech jde o relativně jednoduché a univerzálnější technologie, nebo jde o zcivilněné technologie vojenské či opačně, sekuritizované technologie z jiných oblastí civilního života.

Tato situace má několik strukturálních důvodů. Především jsou vnitřní bezpečnost a krizová připravenost velmi malé a extrémně specifické trhy v národním kontextu. V tom mezinárodním jde o trhy extrémně fragmentované. Vzdor populární představě jsou totiž konkrétní požadavky na velmi podobné technologie velmi odlišné mezi jednotlivými sbory, ale také mezi stejnými sbory v různých zemích. Zkrátka není policie jako policie a každá z nich se řídí zcela jinou legislativou, pravidly i taktikou. Situace v kyberbezpečnosti nebo v krizovém řízení je sice méně komplikovaná, přesto obdobně nelehká. Rizikovost investice do těchto technologií je tak zesílená specializovanými požadavky konečných uživatelů a nutností pochopit specifika prostředí, ve kterém jsou dané technologie nasazovány, a to zvlášť u každého potenciálního zákazníka. Obvykle také nejde o zákazníky, zaměřené na objemové nákupy.[1]

Druhým klíčovým důvodem pro rizikovost investice, a tedy nutnost státní ingerence, je absence strategického plánování schopností, známá z obranného sektoru. Zatímco směřování obranného sektoru lze relativně směřovat na základě analýzy tzv. nedostatků ve schopnostech ve vztahu *k očekávaným scénářům ozbrojených konfliktů* nebo nasazování sil, není situace ve vnitřní bezpečnosti tak přehledná. Význam tohoto faktoru se sice opět liší oblast od oblasti, nicméně kdekoliv bezpečnostní systém naráží na sociogenní hrozby, je dlouhodobý strategický odhad kapacit málo reálný. Na druhou stranu ale není, při zohlednění limitních možností, dostatečně využívaný. Bezpečnostní a záchranné sbory jsou z podstaty vlastní odpovědnosti poměrně konzervativní a silně preferují pěstování schopností již ověřených nad snahou o získávání schopností nových. Zdánlivá podobnost mezi bezpečnostním a obranným sektorem zde tedy zcela neplatí, přestože existuje několik témat, kde dochází k významným a využitelným překryvům.

Cesta k bezpečnostním inovacím je tedy nejen trnitá, ale také „klikatá“. **Aktivní oponenti velmi rychle využívají obecných technologických trendů a proliferace technologií, zatímco bezpečnostní systém v reakci musí budovat velmi specializované nástroje, neboť jsou na jeho činnost kladeny výrazně jiné společenské, etické, ale také právní požadavky**. Pro tržního aktéra je tato situace extrémně nevýhodná a z hlediska investice do vývoje produktu nesmírně riziková. Fragmentace a minimální mezinárodní standardizace v tomto smyslu problém ještě prohlubují, protože nepřináší perspektivu zásadního zisku v případě, že bude vývoj úspěšný.[2]

Naproti tomu ale v akademické i soukromé sféře existuje řada aktérů, kteří mohou efektivně přispět k plnění potřeb bezpečnostního systému a k zachycení trendů, které bezpečnost ovlivňují. **Je však nutné je k tomu motivovat a efektivně s nimi komunikovat – v tom je role státu a podpory bezpečnostního výzkumu, vývoje a inovací zcela klíčová a nezastupitelná.**

V mezinárodním srovnání je v tomto směru důležité zmínit zásadní rozdíl mezi EU a USA – kolébkou bezpečnostních a obranných inovací. Uvedené problémy a rizika spojená s firemní specializací na

[1] Určitou výjimku představují vozidla nebo uniformy, tam ale dochází právě k sekuritizaci civilních sériových technologií, někdy k uvedenému zcivilnění vojenského vybavení.

[2] Příkladem budiž evropské PCP projekty v oblasti chytrých uniforem pro HZS, kde byly výsledky dosaženy v kvalitě daleko nad očekávání, ovšem ke splnění opcí na pořízení nikdy nedošlo, zejm. kvůli znovuobjeveným rozdílům ve standardech, požadavcích a legislativě a zároveň obecné neochotě zavádět natolik novátorskou technologii

tento sektor totiž v USA do značné míry neplatí, nebo se je daří skrze programové iniciativy omezovat.

1.2 KONTEXT OBDOBNÝCH PROGRAMŮ V MEZINÁRODNÍM PROSTŘEDÍ

Z mezinárodních zkušeností plyne jedno zásadní poučení – motorem bezpečnostních inovací jsou právě programy jejich podpory. Trh sám reaguje na bezpečnostní trendy jen velmi pozvolna a zpravidla s výrazně větším zpožděním, než je žádoucí, a to vše při limitech uvedených výše. V mnoha případech, zejm. ve vztahu k trendům poslední dekády, jsou bezpečnostní systémy závislé na in-house vývoji nebo složitých úpravách v zásadě ne zcela vhodných komerčních systémů (nebo na jejich drahých modifikacích na míru). Řadu těchto problémů mohou efektivně spravované programy podpory bezpečnostního výzkumu výrazně omezit, protože sbližují uživatele a technologické talenty i expertní komunity z „nedostatkových" oborů.

V Evropské unii již bezmála dvě dekády existuje dedikovaná podpora bezpečnostního výzkumu, podobně jako v řadě členských zemí (v tuto chvíli cca 9, s nevlivnější skupinou 5 velkých členských zemí a s účastí Velké Británie). Společnou charakteristikou těchto programů je snaha o komplementaritu mezi domácí podporou a evropskými tématy. K tomu se hlásí i tento návrh a formulované dílčí zájmové oblasti podprogramů respektují významné okruhy zájmu, zahrnuté do cestovních map pro evropskou podporu.[3] Tím se otevírá možnost českým subjektům se na tyto soutěže lépe připravit a zvýšit vlastní relevanci pro případné partnery. Z dobré praxe podpory v EU vychází také nově navrhované členění programových projektů na specificky vymezené typy.

Je třeba také vyzdvihnout fakt, že se programy bezpečnostního výzkumu v ČR dlouhodobě vyhnuly nebo se vymanili z často kritizovaných problémů, které sdílelo financování evropské a také v řadě členských států. Šlo zejm. o to, že programy bezpečnostního výzkumu implementovaly různé agentury pro podporu vědy, bez větší vazby na, nebo s omezenou ingerencí ze strany odborné a uživatelské komunity, pramenící z výrazně menší míry důvěry zejm. konečných uživatelů. Snahu omezení těchto problémů reprezentuje přesun této agendy z DG Commerce na DG Home v roce 2016 a obdobné posuny v některých členských státech. V USA je celá agenda, kterou u nás nazýváme souhrnně jako bezpečnostní výzkum, rozdělena mezi 2 poskytovatele: Department of Justice a Department of Homeland Security. To je dáno historicky, ale koncepčně odpovídá tento přístup českému nastavení.

Modelově tak ukotvení bezpečnostního výzkumu na MV odpovídá uznané dobré praxi v EU i v USA, sdílené např. ve Švédsku či Itálii. Návrh tohoto programu se snaží z toho zakotvení těžit a akcentuje vstupy, které úzké sepětí podpory bezpečnostního výzkumu s regulací bezpečnostní politiky i s praxí jejího prosazování nabízí.

1.3 KONTEXT SITUACE V POSKYTOVÁNÍ VEŘEJNÉ PODPORY NA BV V ČR

Ani v ČR neexistují programy podpory bezpečnostního výzkumu ve vakuu a mají řadu zajímavých a pro formulaci tohoto programu důležitých kontextů. **Tím nejdůležitějším je potřeba vyváženě komunikovat a propojovat zájmová témata bezpečnostního systému a dalších aktérů, jejichž zájmy nemusí být a priori bezpečnostní, ale mohou mít zásadní dopad na některé bezpečnostní problémy**. I proto program přichází s otevřeností a dedikovaným podprogramem, který směřuje do zájmového spektra za hranicemi bezpečnostního systému.

[3] V PP1 jde zejména o zahrnutí většiny priorit EMPACT - cyklus prioritizace, který používá pro vlastní zacílení činnosti EU/Europol, nebo z již provedených prioritizací vývojových témat pro oblast prevence rizik katastrof

Druhým dlouhodobým kontextem provozu těchto programů je zakotvení expertizy a schopností přínosný výzkum a vývoj realizovat. Jádro komunity BV tvoří veřejné vysoké školy a veřejné výzkumné instituce (v USA jde o malé a střední podniky, v EU o velké zbrojařské koncerny, v jednotlivých členských státech potom nezřídka specializované státní výzkumné organizace). Tato situace plyne z charakteristik místního trhu (viz výše), ale zároveň také z dlouhodobě minimálních investic do přetížených specializovaných bezpečnostních výzkumných organizací, kontrastující s významnými investicemi do veřejného výzkumného sektoru. Role státních VO je tedy silně omezena jejich kapacitou. Programy bezpečnostního výzkumu se tomu musí přizpůsobit, protože nejsou k nápravě tohoto stavu určeny a ani na ní neaspirují. Schopnosti akademické sféry navíc vynikají v některých tématech, kde tzv. resortní VO nepůsobí.[4] **Mainstreaming bezpečnostních témat mezi těmito silnými hráči výzkumné sféry je proto dalším klíčovým úkolem těchto podpor**. Bez nich nelze předpokládat, že by se bezpečnostní systém dokázal s některými trendy vyrovnat.

Poměrně unikátní charakteristikou podpory v ČR je fakt, že **MV je největším donorem na oblast chemické, biologické, radiační a jaderné ochrany (a obrany). Stejná situace panuje také v kyberbezpečnosti (a obraně)**, ve forenzních vědách, a v bezpečnostních/obranných robotických aplikacích. Je to dáno speciálními charakteristikami těchto témat ve vztahu k jejich zpracování v civilní bezpečnosti a v obranném sektoru. Jde o vzájemné styčné plochy a také témata, kde je nejvyšší příbuznost mezi oběma agendami. Na druhou stranu je nutné dodat, že vzájemné propojení těchto agend není zdaleka tak úzké a příbuznost tak velká, jak se lze na první pohled domnívat. Tato témata také reprezentují nadresortní povahu bezpečnostního výzkumu (i když nejsou jediná), ať už v relaci k MO, tak k NUKIB nebo MZd/MZe/MŽP nebo SUJB. Programy MV doposud dokázaly s touto charakteristickou výzvou pracovat efektivně **a vytvořit skutečně funkční systém meziresortní spolupráce**. Tento program s tímto modelem dále pracuje a nadresortní charakter zachovává, stejně jako prvky kolaborativního rozhodování.

Lze očekávat, že se vzájemná komplementarita zejm. s MO v některých oblastech ještě prohloubí, v souvislosti s nově akcentovaným zájmem MO o podporu nastupujících technologií. Existuje celá řada oblastí, kde lze podpořit v zásadě aplikačně agnostické technologie s potenciálem pro dvojí užití. Tuto podporu při absenci veřejných soutěží v resortu obrany může do značné míry saturovat právě a mnohdy také jedině bezpečnostní výzkum a v některých případech se tomu tak již děje. Programy navrhovaného typu tak v těchto tématech hrají obtížně zastupitelnou roli.

2 IDENTIFIKACE PŘÍLEŽITOSTÍ A ZÁJMOVÝCH TÉMAT

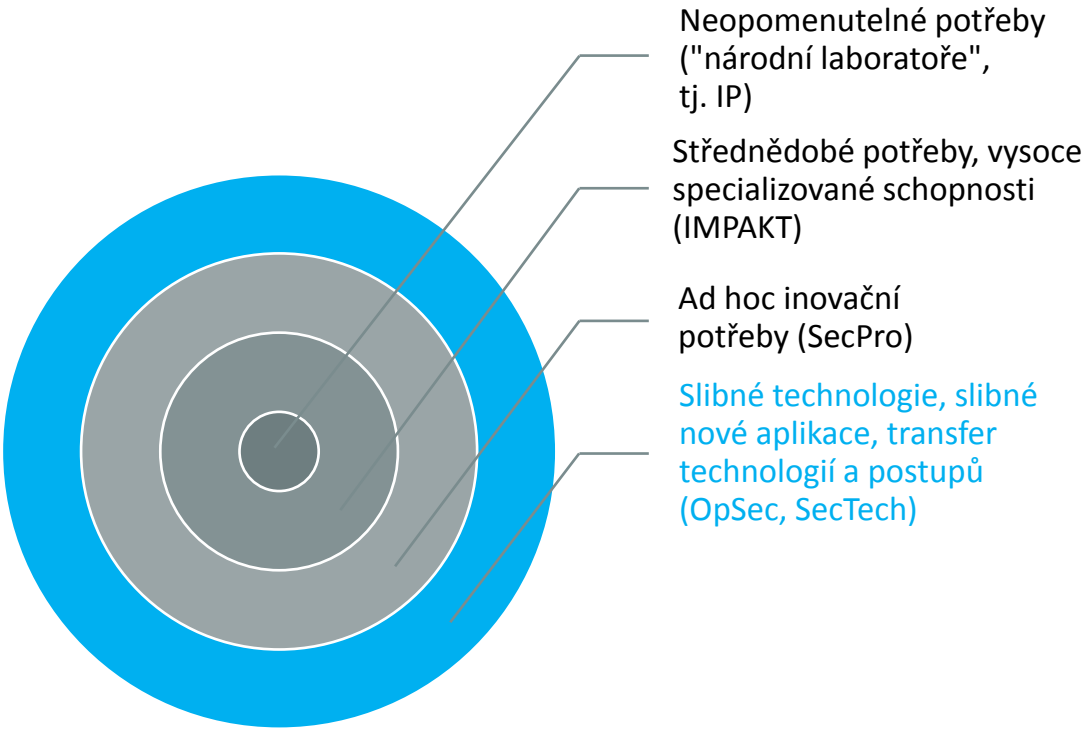
2.1 ROLE V PORTFOLIU BV PODLE MKBV2017+

Program OpSec je jedním z tahounů portfolia podpory bezpečnostního výzkumu. Jde o třetí generaci základního typu podpory, který vycházel z počátečních tezí o potřebách a možnostech přínosu z takto zacílené podpory. Program je velmi otevřený, dokonce nejotevřenější ze všech existujících programových nástrojů. To ovlivňuje řadu jeho nastavení a interakcí s ostatními programy. Podle MKBV2017+ má program OpSec postihovat jednak podpůrné schopnosti v oblasti zajišťování bezpečnosti (zde zejm. reprezentované PP3) anebo témata významným budoucím přínosem (reprezentovaná PP1 a PP2 a jejich propojením s prioritami dokumentů bezpečnostní politiky se střednědobou platností).

[4] zjednodušující termín zahrnuje primárně příjemce institucionální podpory MV, do jisté míry zde lze také hovořit o VO v působnosti resortu obrany.

Program cílí na slibné budoucí technologie nebo potenciálně slibné aplikace, formulované uchazeči v rámci veřejných soutěží. Tím se liší od programu SecPro, který je tažen uživatelskou poptávkou a je realizován skrze veřejné zakázky na služby ve výzkumu, vývoji a inovacích. Další odlišnost reprezentuje zaměření programu SecPro na nejvyšší stupně technologické vyspělosti (viz níže). OpSec, naproti tomu, umožňuje a předpokládá poměrně rozsáhlou podporu aplikovaného výzkumu, tedy projektů, které usilují o ověření slibných technologických konceptů, nebo posouvání zásadních technologií, namísto zcela precizní aplikace a jejího dotažení k tržní použitelnosti.

Program IMPAKT se od OpSec také podstatnou měrou liší. Přestože je realizován formou veřejné soutěže a projekty jsou nakonec formulovány také uchazeči, důraz na úzké propojení s uživatelem je výrazně větší, zároveň se podporují projekty vysoce specifické a tomu odpovídá i způsob zadávání. IMPAKT ale především cílí na rozvoj strategických technologických oblastí a doplňuje tak OpSec o další, stabilnější nástroj pro uchazeče a témata, u kterých lze očekávat dlouhodobý zásadní význam pro schopnosti bezpečnostních sborů. Jde tedy o program podstatným způsobem méně otevřený, s výraznějším zaměřením na dopady na řešitelskou organizaci. I proto je omezen na výzkumné organizace, které tvoří jádro schopností bezpečnostního výzkumu (ze kterých potom v důsledku a s využitím jiných programů, těží průmyslová sféra).

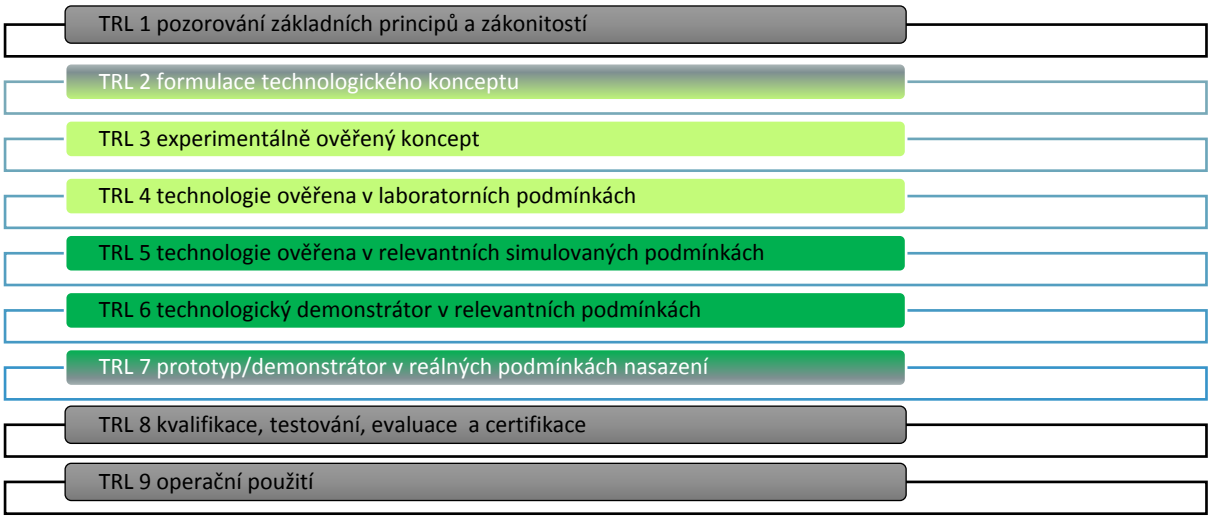


Obrázek 1: Schématické znázornění portfolia BV podle významu

Organizace příjemců institucionální podpory se na programu OpSec podílí především jako projektový partneři, kteří korigují obsah a zacílení projektů ve specializovaných zájmových oblastech. Účelovou podporu poskytovatel dlouhodobě nepovažuje za hlavní zdroj prostředků pro tyto organizace a tomu přizpůsobuje i parametry programu. Tím se ovšem nijak nesnižuje jejich celkový význam právě z hlediska směřování projektů a specifického přínosu k jejich realizaci, kde je role těchto subjektů nezastupitelná. Faktem zůstává, že v minulých generacích programu byla tato podpora jedním z objemově nejvýznamnějších zdrojů pro tyto organizace. To je ovšem dáno prostými fakty – do jisté míry shodou v zaměření, která logicky plyne z podstaty činnosti těchto organizací, a především neadekvátně nízkým zajištěním jejich činnosti z jiných zdrojů (zejm. IP). Je tak logické, že svou

absorpční kapacitu úspěšně saturují z nejvhodnějšího dostupného nástroje. I v této generaci programu OpSec hodlá poskytovatel sledovat a korigovat tento efekt a dále motivovat příjemce IP k roli „center přitažlivosti“ v tématech vlastní expertizy, která stimulují, korigují a staví na schopnostech civilní veřejné výzkumné sféry a spolupráci s podniky.

Jak bylo uvedeno výše, s ohledem na nutnost řídit některá specifická finanční rizika pro poskytovatele a zároveň otevřít zázemí podpory bezpečnostního výzkumu co nejširšímu a nejperspektivnějšímu spektru partnerů, člení se podpora v programu na 3 typy. Každý z nich reprezentuje charakteristické projekty, které známe z minulých generací programu a zároveň pohled na typická rizika jejich podpory. Základem pro členění technologických projektů je stupnice technologické vyspělosti (viz obr. níže). Světlou barvou je označen prostor korelující s financováním aplikovaného výzkumu, tmavě potom odpovídající podpoře experimentálního vývoje.



Obrázek 2: Stupnice technologické vyspělosti (Technology Readiness Level, TRL)

Minulé zkušenosti ukazují, že “převládající typ činnosti” je jedním z nejčastějších předmětů gamingu[5] ze strany uchazečů. Zároveň jde z hlediska definic výsledků o činnosti, a tedy výsledky velmi odlišné. Zatímco u aplikovaného výzkumu lze stále očekávat dominantní publikační aktivitu (i když nutně v jiných typech časopisů), u experimentálního vývoje lze naopak očekávat většinu tzv. “aplikovaných” výsledků podle Metodiky hodnocení. Škála TRL je proto pro vyhodnocení charakteru projektu a nastavení očekávání od jeho výsledků daleko nejvhodnější a nejreprezentativnější nástroj. I proto se navrhuje uvedené členění. Omezení gamingu potom může přinést částečné zefektivnění podpory.

V tomto smyslu je návrh komplementární s programem SecTech, který se omezuje pouze na TRL 5 a výše, ve snaze jednak stimulovat větší snahu o posouvání nadějných projektů směrem k uplatnitelnosti na trhu (je omezen na komerčně uplatnitelné akce), ale také k vytvoření prostoru pro pokračující projekty, vzešlé právě z různých podpor aplikovaného výzkumu (zde nebo v programu IMPAKT). Zároveň SecTech umožňuje i vývojové a předkomerční testování a vyhodnocování, čímž dále doplňuje i tento návrh. Programy na sebe v jistém smyslu navazují a tvoří společně blok otevřených podpor, jejichž přínosy jsou nejen praktické, ale také usilují o podporu bezpečnostního průmyslu a jeho vztahů s akademickou sférou.

[5] Účelového výkladu nebo přizpůsobování se definicím, které ovlivňují finanční alokaci

Na rozdíl od programů ostatních nejsou SecTech a OpSec taženy uživatelskou poptávkou, ale naopak usilují o otevření prostoru pro slibné nové technologie, které mohou mít značnou uživatelskou hodnotu. I proto OpSec otevírá prostor pro investice do technologií s výrazně delším horizontem potenciální uplatnitelnosti. To umožní MV posouvat technologie klíčové pro budoucí uživatelské potřeby a stimulovat tak výzkumné zázemí pro budoucí bezpečnostní průmysl (mnohdy s řadou pozitivních externalit). Uživatelé se tak do projektů zapojují především v rámci hodnocení[6] a v rovině spolupráce s řešiteli v průběhu projektu. Na druhou stranu zájmové oblasti a témata jsou pouze obecněji definována na základě systematického vhledu do bezpečnostní politiky.

Pro zjednodušení uvádíme schematický pohled na portfolio programů BV perspektivou uchazeče:

- **IMPAKT je pro ty, bez jejichž dlouhodobého zapojení do BV nebo služeb se v budoucnu ve snaze o získání relevantních bezpečnostních inovací neobejdeme**
- **SecPro je pro ty, kteří jsou schopni uvést do praxe nápady a řešení potřeb, které definuje uživatel**
- **OpSec je pro ty, kteří mají nápady, o kterých se domnívají, že mohou bezpečnostní inovace přinést a chtějí je ověřit nebo posunout dál.**
- **SecTech je pro ty, kteří již disponují technologiemi, které lze pro bezpečnostní inovace uplatnit, je však nutné je modifikovat nebo dopracovat, aby mohly na trh či došly využití v bezpečnostním sektoru.**
- **OpSec a SecTech/SecPro zároveň tvoří vzájemně navazující příležitosti, které lze konsekutivně využívat k rozvoji stejné technologie.**

2.2 STUDIE ABSORPČNÍ KAPACITY[7]

2.2.1 Účastníci

Poskytovatel realizoval studii absorpční kapacity formou vzdáleného dotazníkového šetření, do kterého se aktivně zapojilo celkem 50 respondentů.[8] Prakticky ve všech případech respondenti indikují předchozí zkušenosti s programy bezpečnostního výzkumu (pravděpodobně byla studie takto také zacílena). Ve 3 případech individuální respondenti indikují absenci takové zkušenosti, nicméně v jejich organizacích lze předchozí kontakty i čerpání podpory doložit. Výzkumné organizace reprezentovalo 33 odpovědí, zatímco podniky 17. To relativně odpovídá poměru zapojení do předchozích generací soutěžních programů MV.

Malé podniky byly zastoupeny 6ti respondenty, přičemž 1 se kvalifikuje jako startup přímo zaměřený na bezpečnostní aplikace. Jde o zjevný deficit studie, protože při zběžném pohledu na akcelerační programy v ČR lze identifikovat celou řadu subjektů tohoto typu se značnou relevancí pro zapojení do tohoto nebo podobných programů. Středních podniků bylo zastoupeno 7. Zde je situace opačná, prakticky ve všech případech jde o hráče již etablované, u kterých minimálně část portfolia reprezentují aplikace v zájmovém okruhu tohoto programu. Stejně lze hodnotit 4 zapojené velké podniky.

[6] Osvědčený model byl testován v minulé generaci programu

[7] Provedena poskytovatelem, data zpřístupněna zpracovateli těchto podkladových materiálů.

[8] 4 odpovědi nejsou z hlediska studie nijak relevantní, neboť jde o prázdné záznamy bez uvedení jakýchkoliv údajů.

50 respondentů dokonce reprezentuje pouze menší část všech příjemců podpory z předchozích 2 generací programu. V každém z nich bylo podpořeno více než 100 unikátních příjemců, **napříč programovými generacemi potom přes 150 unikátních příjemců.**

Už jenom na základě spektra účastníků lze studii považovat pouze za indikativní. Nereflektuje totiž podstatnou skupinu potenciálních uchazečů – organizací bez předchozího kontaktu s těmito programy. Druhým problémem je absence pohledu nejslibnější části podnikového segmentu – malých podniků a startupů, které pracují na relevantních technologiích (které jsou ale stále aplikačně agnostické).

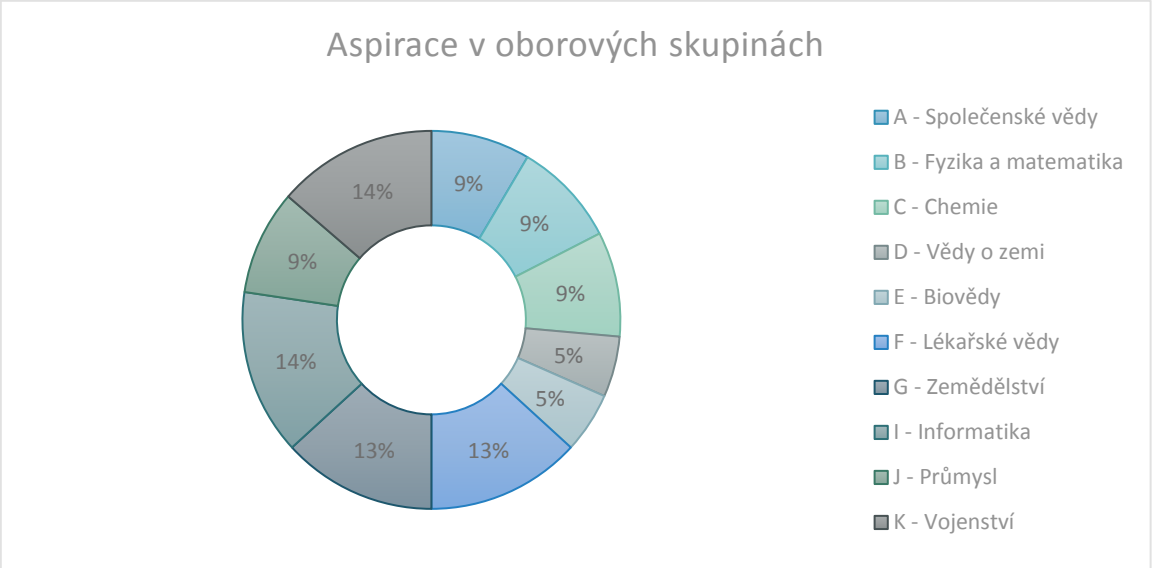
Vedle absence nových potenciálních žadatelů je vhodné upozornit také na to, že pouze 8 respondentů dříve podporu neobdrželo, přestože o programech podpory věděli. Lze se tak domnívat, že studie indikuje výrazně nižší zájem než jaký lze ve skutečnosti předpokládat při zahrnutí již v zásadě informovaných žadatelů. Segment neinformovaných žadatelů nadále opomíjíme.

2.2.2 Finance

V rámci studie indikovali účastníci řádový rozsah finančních požadavků na projekt a vlastní absorpční kapacitu v podobě očekávaného počtu přihlašovaných projektů. **Z těchto údajů lze odhadnout objem předpokládaných přihlášek ve výše popsaném omezeném vzorku poptávky na 3 240 mil. CZK.**

2.2.3 Obory

Výsledky studie ukazují na **pokračující mezioborovou relevanci** programu tohoto typu. Podobně jako v obou předchozích generacích, i zde účastníci studie indikují aspirace napříč všemi oborovými skupinami podle číselníku IS VaVaI. Graf níže tyto shrnuje po oborových skupinách.

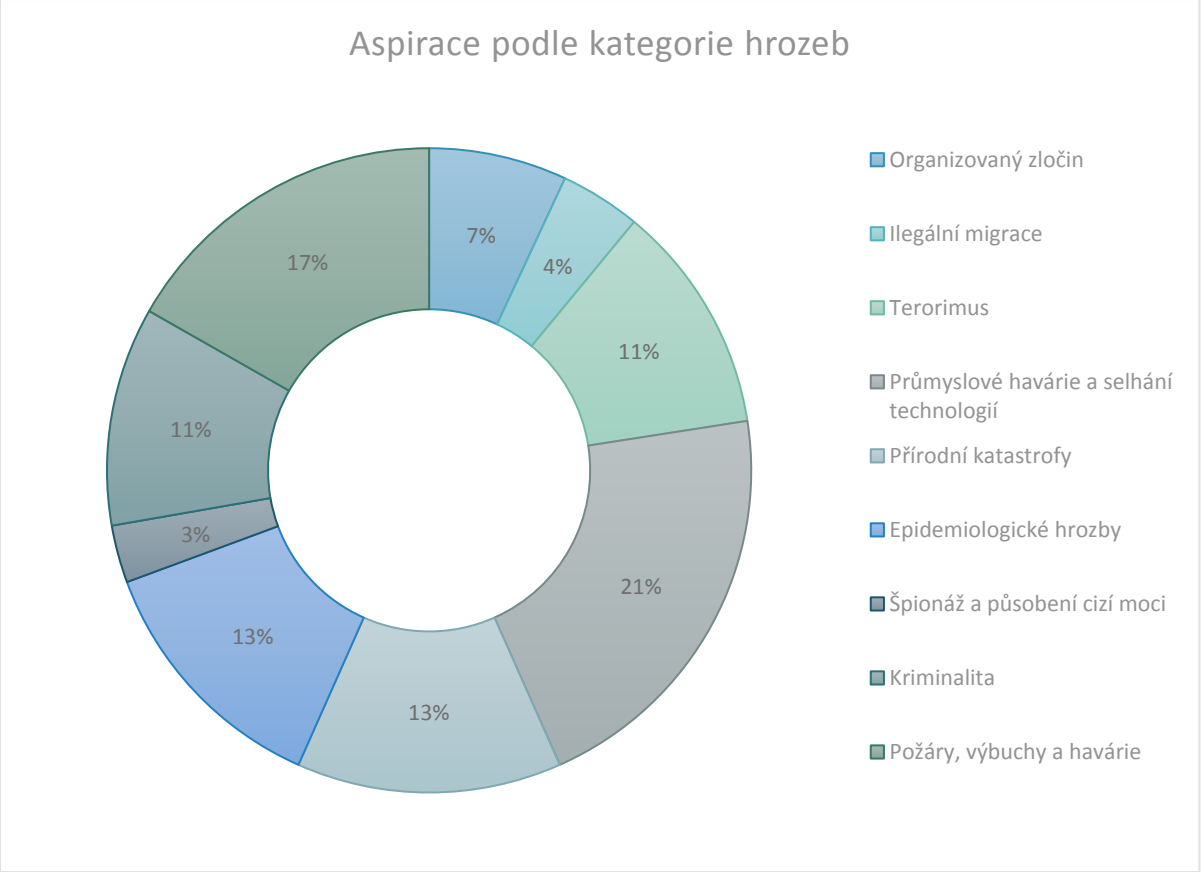


Zcela multioborový charakter je jednou z odlišností tohoto programu od dalších nástrojů v portfoliu BV, které mají, byť jen částečně, snahu oborové rozložení návrhů, a tedy i podpory korigovat. Nazíráno studií absorpční kapacity je vhodné pokračovat v modelu úplného oborového otevření, aby zůstala zachována stimulační role programu z hlediska kreativity podávaných návrhů. To ovšem také představuje výzvu v podobě nutnosti řídit efektivně zacílení projektů (v dřívějších generacích programu bylo patrné spekulativní podávání irelevantních návrhů).

2.2.4 Priority

Z hlediska odpovědi na bezpečnostní hrozby lze odpovědi v průzkumu klasifikovat jako značně diverzifikované. **Z pohledu prioritních skupin MKBV2017+ je rozložení takřka rovnoměrné** (po cca 5% korekci u prio Management bezpečnostních informací, která se při pohledu na parametry odpovědí nezdá zcela pochopenou).

Z pohledu domněle řešených bezpečnostních hrozeb již situace není zcela jednoznačná. Obecně převládají ambice odpovědět na hrozby přírodního původu nebo z oblasti selhání technologií (typicky kyberbezpečnost infrastruktury). Výrazně menší odezvu potom mají dynamické a do značné míry palčivější výzvy v oblasti vymáhání práva. V průzkumu tak lze pozorovat významný nesoulad mezi poptávkou po inovačních (technologických) řešeních, která v oblasti vymáhání práva výrazně dominuje, s nabídkou, v podobě aspirací uchazečů. To jednak dokládá specifické vlastnosti trhu bezpečnostních technologií a jistou bezradnost na obou stranách rovnice, dále ale také reflektuje zaměření předchozích generací programu.



Integrovanou „mapu“ intenzity zájmu o prioritní témata ukazuje Příloha 2 (s omezenou vypovídací hodnotou). Je z ní patrno mimo jiné to, že v celém souboru nedominují ani tak témata krizové připravenosti, jako témata podpůrná, vyžadující výrazně menší rozsah interakce s bezpečnostním systémem a s koncovými uživateli. Tento schematický pohled je ale pro jakoukoliv smysluplnou reflexi v nastavení programu nutné doplnit kvalitativním pohledem na zamýšlená témata, protože se

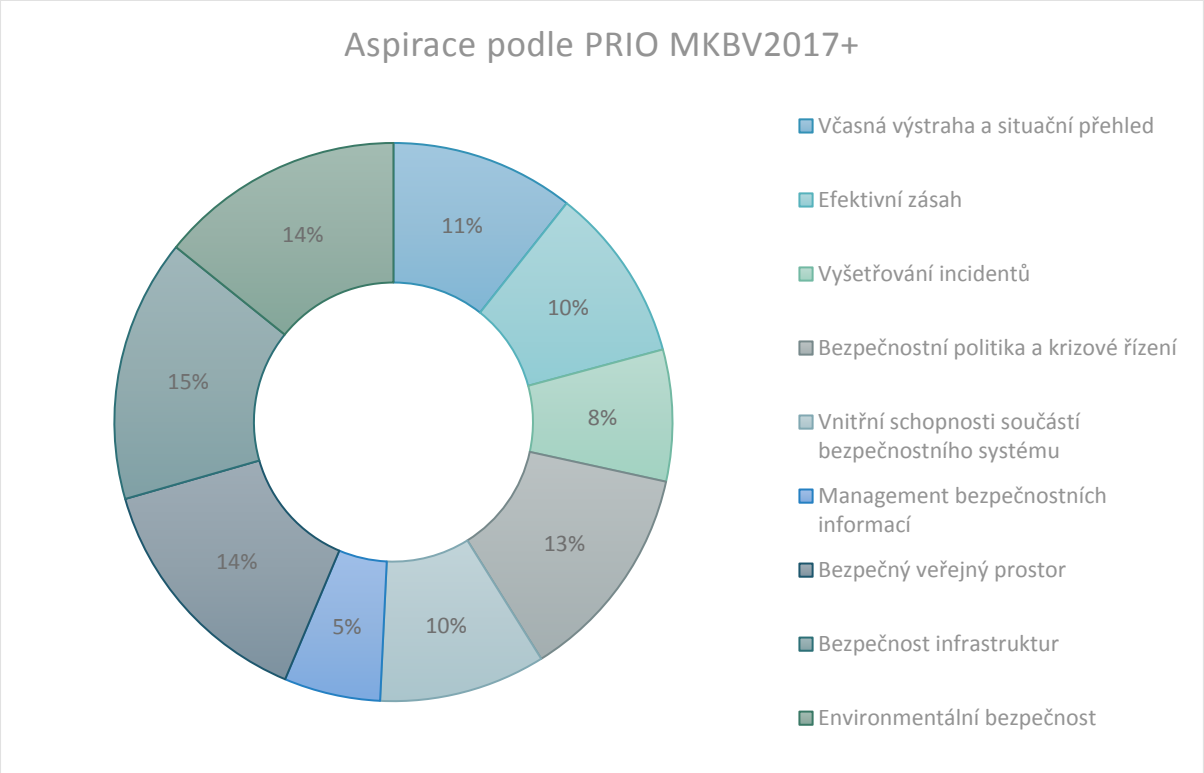
nezřídka stává, že zejm. pohled na přínos k řešení jednotlivých bezpečnostních hrozeb je ovlivněn flagrantním rozdílem mezi reálnými potřebami a chápáním uchazečů.[9]

Při tomto pohledu je potom zjevné, že v celém souboru existují pohledem uchazečů v zásadě 3 významné zájmové oblasti.

1, periferní a průřezová témata, která MKBV2017+ řadí do priority C (odolná společnost), která nejsou přímo spojena nebo nejsou zcela vázána na činnost bezpečnostních a záchranných sborů, přestože s touto činností mohou souviset nebo v těchto tématech může docházet k interakcím

2, incidenty s vysokým počtem obětí a katastrofy právě z hlediska činnosti bezpečnostních a záchranných sborů (při bližším pohledu lze v této kategorii zaznamenat i referenční hrozbu terorismu, kde se respondenti soustředí na odpověď na bombové nebo CBRN útoky, zatímco z hlediska bezpečnostní politiky jde především o problém zpravodajského charakteru).

3, vymáhání práva, které je při pohledu na přílohu 2 distinktivně méně zastoupenou problematikou, při pohledu na referenční hrozby ovšem zastoupenou zhruba rovnoměrně.



2.3 ZKUŠENOSTI Z PŘEDCHOZÍCH GENERACÍ PROGRAMU

Nad rámec studie absorpční kapacity zahrnujeme do úvahy o finančním nastavení programu také následující zkušenosti z předchozích generací programu:

[9] Typicky u terorismu – zatímco základním nástrojem boje proti terorismu je zpravodajská činnost a de facto tak potřeby odpovídají boji proti organizovanému zločinu, uchazeči typicky navrhují např. ochranné prostředky pro hasiče, zjevně tendujíc k „řešení terorismu“ jako řešení následků útoku (mnohdy jen některého typu)

- Zkušenosti naznačují, že u nespecifických otevřených soutěží existuje hladina relevantní poptávky, odpovídající cca 1 mld. financovatelných projektů, při zachování hranice úspěšnosti kolem cca 30% přihlášek
- Problém je zcela nepravidelné vyhlašování, které „poptávku“ po podpoře deformuje v neprospěch poskytovatele a zároveň otevírá prostor pro duplicity, protože se někteří uchazeči rozhodnout zkoušet přihlásit v nevhodných programech (a někteří poskytovatelé nepovažují za vhodné dodržovat limity vlastních kompetencí).
- Vezmeme-li v potaz zpětně dopočtené údaje za předchozí programy, odpovídala reálná prezentovaná poptávka za dobu realizace v případě VG 9,8 mld. CZK a v případě VI 13,8 mld. CZK[10];
- Pokud by poskytovatel aspiroval na udržení 35% úspěšnosti, znamenalo by to vydat v programu VG cca 2,9 mld. CZK (odtud navýšení pro program VI)
- Pokud by poskytovatel aspiroval na udržení 30% úspěšnosti v programu VI, znamenalo by to vydat cca 4,1 mld. CZK (odtud drobné navýšení pro OpSec)

Program VG[11]	přihlášeno	vybráno	finance	úspěšnost
VS1	202	68	1 023 960 000	34%
VS2	267	34	484 618 000	13%
VS3	273	32	355 915 000	12%
Total	742	134	1 864 493 000	19%

Program VI[12]	přihlášeno	vybráno	finance	úspěšnost
VS1	340	49	948 589 000	14%
VS2	306	61	903 793 000	20%
VS3	145	63	789 282 000	43%
VS4 (covid)[13]	69	27	245 241 840	39%
Total	860	200	2 886 905 840	29%

2.4 TRIANGULACE PROGRAMOVÝCH PARAMETRŮ

Studii lze pro některé její vlastnosti považovat spíše za indikativní, proto jsou parametry programu triangulovány z širšího informačního základu. Zejména u finančního výhledu je nutné považovat studii pouze za vedlejší zdroj informací. Zkušenosti z předchozích generací programu se ukazují být konzistentnější.

Protože program zachovává rozsáhlou otevřenost i mimo absolutní jádro priorit MKBV2017+, není důvod předpokládat, že bude poptávka výrazně nižší než u minulých generací programu. Navíc se lze domnívat, že dlouhodobé investice a celkový růst kvality výsledků a prohlubující se zaměření na aplikovaný výzkum u velké části výzkumné sféry povede spíše k navýšení poptávky v horizontu

[10] Dopočteno na základě výsledků jednotlivých veřejných soutěží
[11] Údaje viz IS VaVaI, přístup 6.5.2021
[12] Údaje viz IS VaVaI, přístup 6.5.2021
[13] Nešlo o soutěž obecného charakteru pro všechna programová témata, ale úzce vymezenou reakci na Covid a související deficity v připravenosti na epidemiologické krize

realizace programu. Lze tedy očekávat hranici celkové poptávky v horizontu cca 10 mld. CZK, a to při zohlednění úvahy, že spuštění dalších dvou programů BV v mezidobí (byť s minimálním financováním) povede ke korekci poptávky směrem dolů. Při žádoucí úspěšnosti cca 30 – 35% projektů docházíme k uvedenému návrhu rozpočtu. Ten také reflektuje požadavky MKBV2017+ a relaci k ostatním nástrojům podpory bezpečnostního výzkumu.

Zároveň se požadavky drží v realistických limitech možností státního rozpočtu. Je třeba upozornit, že bezpečnostní výzkum je dlouhodobě disproporčním terčem nesystémových a nesystematických opatření ať už v rámci snah o šetření ve vědním rozpočtu, nebo k saturaci jiných potřeb dalších politik. Dlouhodobě je tak celý systém rozkolísaný, nestabilní, a především v reálných termínech, při započtení vývoje vědního rozpočtu, ale i inflace, podpora spíše klesá. Prezentovaný požadavek usiluje o korekci tohoto nepříznivého trendu, aniž by přinášel nepřijatelnou zátěž pro státní rozpočet.

Rozložení financí do podprogramů reflektuje studii absorpční kapacity s korekcí cca 5% u priority management bezpečnostních informací, která, jak bylo uvedeno, nebyla nejspíš zcela správně pochopena. Specifikace podprogramů do jisté míry reflektuje studii, ale zejm. dlouhodobé zkušenosti s rozsahem a spektrem témat bezpečnostního výzkumu napříč programy a s inovačními potřebami jednotlivých segmentů bezpečnostní politiky.

Návrh zachovává multioborovost, jako jednu z klíčových charakteristik. Návrh nijak neomezuje oborové zaměření projektů. Lze očekávat, že k posunu v trendech mezi podporovanými projekty dojde, zejm. ve vztahu k informatickým oborům, které mají dlouhodobě rostoucí zastoupení. To je ale výsledkem trendů v bezpečnostním prostředí, nikoliv vychýlením nastavení podpor. Program v tomto směru navazuje na předchozí generace, u kterých byla oborová otevřenost považována za pozitivum.

I tematicky si program zachovává značnou otevřenost. V minulých generacích programu byla míra otevřenosti větší – pokrývaly takřka celé relevantní tematické pole. To se ukázalo jako mírně problematické, protože řada témat nebyla řešena vůbec, což navozovalo nepřesný dojem, že je program špatně nastaven. V současnosti je situace odlišná a program vychází z priorit bezpečnostní politiky, upravených pro zachování jisté míry otevřenosti a reflexe všech relevantních zájmových oblastí. Program ovšem není a ani nemá být otevřeným pro zcela jakékoliv téma v relevantním prostoru. To by neodpovídalo MKBV2017+, která roli jednotlivých programů ve vztahu k uživatelským schopnostem přesněji vymezuje.

Dlouhodobým tahounem kvalitních návrhů jsou výzkumné organizace (dokonce napříč programy). I proto se očekává, že i v tomto programu, přes částečné zaměření na podporu bezpečnostního průmyslu, bude tento trend pokračovat a výzkumné organizace budou skupině příjemců dominovat. To vede k relativně skromnému nastavení očekávané spoluúčasti příjemců podpory. Tu ale do jisté míry zvyšují specifické požadavky na typy projektů (spoluúčast se zvyšuje proti předchozím generacím na základě rizikovosti jednotlivých typů). Dalším faktorem je potom rostoucí zastoupení malých a středních podniků a relativně malé zastoupení podniků velkých, které obecně míru spoluúčasti příjemců snižuje. Není to však na překážku, protože rizikovost podpory s tímto faktorem neroste. Naopak, poskytovatel ve smyslu Národní politiky VaVaI považuje tento trend za pozitivní.

Poskytovatel se snaží aktivně řídit rizika, odhalená v minulých generacích programu, a to převzetím evropského modelu diverzifikace programových typů nejen formou zadání, ale také formou finančních parametrů. Tento přístup umožňuje i efektivnější hodnocení, protože napojení žádostí na škálu TRL interpretovanou cestou nastavení typu projektu přinese přehlednější popis aspirací

řešitele. Zároveň, doufejme, tento přístup přinese také rozumnější a užší spektrum záměrů v oblasti využití výsledků. Tam v minulých programech dominovalo přímé předávání výsledků konečným uživatelům s mnohdy problematickými výsledky. Uvedený postup by také měl omezit problém gamingu s typem činnosti, který pro některá konsorcia determinuje intenzitu a tím mnohdy i objem podpory, a související problém minimálního zapojování průmyslových partnerů do některých projektů.

3 INTERVENČNÍ LOGIKA

3.1 CÍLE PROGRAMU

Hlavní cíl: Hlavním cílem programu je systematicky podněcovat a rozvíjet zájem výzkumné a inovační sféry o zapojení do řešení bezpečnostních výzev pro moderní společnost a tvořit tak základnu pro tvorbu a rozvoj konkurenceschopných bezpečnostních inovací.

Dílčí cíle programu konceptualizují očekávané přínosy na úrovni jednotlivých projektů, resp. konceptualizují „bezpečnostní přínosy" programu. Každý z projektů by měl důvěryhodně dokumentovat, jak jeho výsledky přispějí k naplnění některé z těchto přínosových kategorií.

1. zefektivnění plánování, koordinace a regulace (tj. zefektivnění přípravy na krizové situace/incidenty na úrovni referenčního objektu);
2. zvýšení bezpečnosti zasahujících/vyšetřujících;
3. zvýšení efektivity činnosti zasahujících/vyšetřujících;
4. zvýšení dostupnosti služeb bezpečnostního systému (tj. rozsahu nebo kvality služeb/schopností);
5. zefektivnění včasného varování (zejména prodloužení doby na reakci, zvýšení spolehlivosti varování);
6. snížení ohrožení (tj. omezení pravděpodobnosti vzniku negativních dopadů krizové situace/incidentu na referenční objekt);
7. a zmírnění následků (tj. omezení intenzity a rozsahu dopadů krizové situace/incidentu/jevu[14] na referenční objekt).

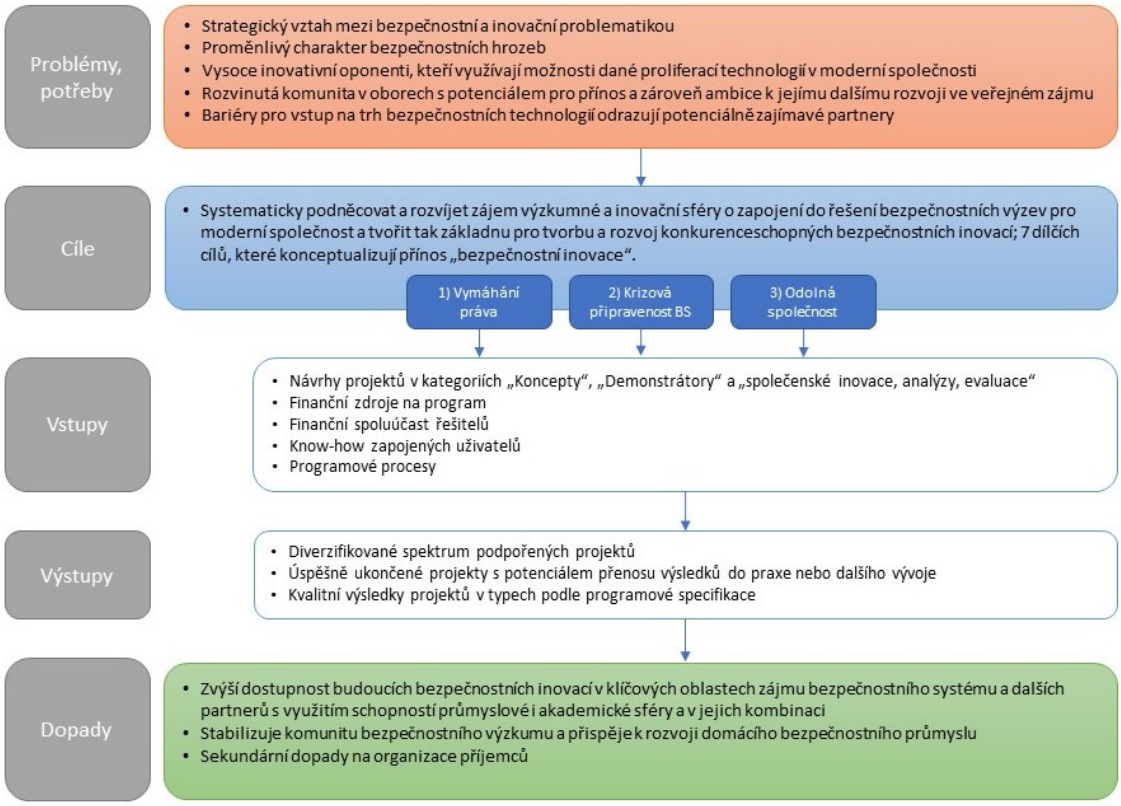
Protože jsou v ČR programy tradičně organizovány administrativně, nikoliv tematicky, je zásadně problematické být při určování cílů a přínosů precizní. Protnutí tak rozdílných témat, jaké pokrývá tento program znemožňuje užití ustálených terminologií a vyžaduje značné generalizace. Proto se zde prezentuje vlastní konceptualizace „bezpečnostního přínosu". Ta vychází z jednoduché úvahy – bezpečnostní přínos znamená zlepšení služby při zachování nákladů nebo snížení nákladů při zachování kvality služby. Výše uvedené kategorie reprezentují kvalitativní změnu u „služby".

3.2 ČLENĚNÍ NA PODPROGRAMY

Program se člení na podprogramy na základě 3 vstupů. Prvním je průzkum absorpční kapacity (výše), druhým jsou dosavadní zkušenosti poskytovatele s nabídkou i poptávkou v bezpečnostním výzkumu (viz hodnocení předchozích programů) a třetím potom charakteristické tematické okruhy bezpečnostní politiky i praxe.

[14] Vzhledem k rozsahu témat a také s ohledem na odlišnosti v terminologii budou tyto termíny v textu užívány volněji, bez jinak obvyklé vazby na konkrétní kontexty uživatelských organizací nebo legislativu.

- Podprogram 1 reprezentuje zájmovou oblast kriminální policie a zpravodajských služeb, která vyniká svými vlastními charakteristikami a postupy, včetně rozsáhlé forenzní praxe a která je zároveň nejpostiženější inovacemi u protivníků.
- Podprogram 2 reprezentuje především schopnost odpovědět na závažné bezpečnostní incidenty, potenciálně incidenty s velkým množstvím obětí. Jde opět o velmi specifickou, ale zároveň komplexní oblast, kde posilování schopností zároveň snižuje rizika při událostech/zásazích menšího rozsahu.
- Podprogram 3 je potom charakteristický zaměřením na témata, která jsou na průsečíku zájmů bezpečnostního systému a odpovědností či činností dalších aktérů a která mají významné přesahy mimo bezpečnostní systém.



Obrázek 3: Schéma intervenční logiky programu OpSec

3.2.1 Dopady

Jako všechny programy bezpečnostního výzkumu, i tento usiluje o rozvoj bezpečnostních inovací a paralelní pozitivní dopady na komunitu bezpečnostního výzkumu a její členské subjekty. Protože se program orientuje na nižší TRL, nelze explicitně deklarovat, že dopady projektů budou odpovídat přínosu do praxe zavedených inovací, protože to nelze predikovat.

Obdobně, nelze specifikovat např. jakých konkrétnějších oblastech budou dopady realizovány. To by odporovalo logice otevřené soutěže, ve které se vyberou nejzajímavější a nejperspektivnější projekty. Horším projektům se prostor kvůli naplnění programové kvóty jakéhokoliv typu nedává.

Bezpečnostní přínos na úrovni jednotlivých projektů je konceptualizován již v kapitole „cíle programu“ tak, aby celý text odpovídal dikci zákona, který předpokládá, že ve veřejné soutěži cíle projektů navrhují příjemci tak, aby dosáhli cílů programu. Pokud tedy chceme motivovat příjemce

k nastavování SMART cílů projektů, je nutné dílčí cíle programu vymezovat jako kvalitativní změnu. Není ale nezbytné takové vymezení opakovat v rámci dopadů programu.

4 SPECIFIKACE PODPROGRAMŮ

Členění na podprogramy je vedené metodologickým požadavkem na současné pokrytí maximálního relevantního spektra případů, ale zároveň jejich smysluplného rozdělení na jednoznačně charakteristické podmnožiny. Východiska a shrnutí pro jednotlivé podprogramy zmiňuje předchozí kapitola. Všechny podprogramy maximálně vychází ze souvisejících platných dokumentů bezpečnostní politiky, kdekoliv došlo k jejich aktualizaci a kdekoliv byly tyto aktualizace autorovi zpřístupněny.

Stejně jako MKBV2017+ vychází i formulace podprogramu ze snahy oddělovat od sebe nesrovnatelné skupiny schopností bezpečnostního systému a sdružovat ty příbuzné tak, aby docházelo k maximálně relevantní soutěži. Některá témata potom mohou zasahovat do více podprogramů tam, kde se dotýkají zcela distinktivních schopností.[15] V ojedinělých případech jsou do vymezení podprogramu zahrnuta témata související s celkovým zaměřením, ale zároveň shrnující silné stránky výzkumné sféry.[16]

Mírné odchylky, které návrh jednotlivých podprogramů zahrnuje,[17] vychází z koncepce rozhodovacích procesů pro tento program. Ta velí nejen sdružovat příbuzná témata, ale v uživatelských panelech také koncentrovat typické odbornosti. Některá témata se proto uvádí v podprogramech, které lépe reflektují odbornosti nutné k jejich posouzení a zasazení do kontextu, aniž by docházelo k přílišné konkurenci vzájemně zcela nesouvisejících témat.

Speciální postavení má problematika CBRN incidentů. Související témata byla zařazena do PP2 na explicitní žádost poskytovatele, přestože je lze vnímat za významně specifická, a tedy potenciálně zakládající samostatný podprogram.

4.1 VYMÁHÁNÍ PRÁVA

Proti období formulace MKBV2017+ došlo k zásadnímu posunu ve formulaci Koncepce rozvoje Policie, jejíž novela byla schválena v roce 2020. Proti dřívějším generacím programu a v návaznosti na zkušeností získané při správě celého portfolia napříč program BV je nově formulován samostatný podprogram pro velmi specifickou množinu témat, spojených s činností kriminální policie, Celní správy a, do jisté míry také zpravodajských služeb, zejm. u nejzávažnějších a nejnebezpečnějších forem kriminality.

Referenční hrozby podle Koncepce rozvoje PČR jsou následující:

- Boj proti terorismu a extremismu
- Boj proti obchodu s drogami
- Potírání kybernetické kriminality

[15] Např. terorismus (vyšetřování a preemptivní činnost závisí na schopnostech kriminálního zpravodajství, podobně jako boj proti organizovanému zločinu, zatímco řešení typických incidentů – držení rukojmí, aktivní střelec nebo NVS spadá zahrnuje schopnosti zcela jiné). Podobný příklad je kyberbezpečnost – do PP1 patří témata spojená s vyšetřováním kyberkriminality, zatímco do PP3 patří témata spojená s ochranou KI.
[16] Např. tam, kde se zájmová oblast protíná s projekty, podpořenými v PP1 IMPAKT
[17] např. vyšetřování požárů, resp. technologie pro zásahové jednotky)

- Boj proti korupci a hospodářské kriminalitě
- Potírání nelegální migrace

Pro ty stanoví koncepce řadu cílů a opatření, na které níže přímo navazuje formulace očekávaných přínosů tohoto podprogramu, kdekoliv je to relevantní. Dílčí cíle podprogramu potom operacionalizují tyto přínosy.

Ozvěny koncepce rozvoje PČR lze hledat také v dalších podprogramech, kde jde zejména o témata, která jsou sdílená s dalšími složkami IZS nebo kde se činnost PČR významně protíná s činností dalších aktérů (např. doprava).

4.1.1 Očekávané přínosy podprogramu 1

Podprogram přinese cílené zaměření pozornosti žadatelů na priority MKBV2017+ „Efektivní zásah“ a „Adaptabilní bezpečnostní systém“ v oblasti boje proti organizovanému zločinu a dalším závažným formám kriminality, s důrazem na priority Koncepce rozvoje Policie ČR a dalších souvisejících dokumentů. Tyto hrozby i schopnosti, nasazované v rámci boje proti nim se od další činnosti bezpečnostních sborů výrazně liší, jsou charakteristické neustále se adaptujícím oponentem a vysokou mírou inovace na jeho straně. Zároveň reprezentují značnou část inovační poptávky policie (a dalších bezpečnostních sborů).

V rámci bezpečnostní politiky vynikají následující zájmové oblasti, reprezentující jádro poptávky konečných uživatelů výsledků, a tedy i žádoucí oblasti přínosu projektů:

- Forenzní zkoumání, které je dlouhodobě páteří vyšetřování prakticky všech druhů kriminality (cíl A)
- Adaptace na trendy závažné kriminality a zneužívání moderních technologií k jejímu páchání (cíle B – D)
- Analytika, práce s informacemi a efektivní vytěžování maximálního spektra informačních zdrojů (cíl E)
- Znalostní a technologická základna pro inovace ve vyšetřování prioritizovaných typů závažné trestné činnosti (cíle F – I)

4.1.2 Cíle a zaměření podprogramu 1

(A) Moderní nástroje forenzního zkoumání napříč obory
(B) Technologie a znalosti pro adaptaci na zneužívání moderních technologií k páchání trestné činnosti a pro online vyšetřování
(C) Technologie a znalosti pro odhalování a prokazování speciálních typů organizované trestné činnosti, zejm. environmentální kriminality, padělání a ilegálního obchodu s uměním nebo předměty kulturního dědictví či s dalšími kvazikomoditami
(D) Technologie pro prvosledové hlídky, zásahové a speciální jednotky
(E) Strategická, taktická a kriminální analýza a metody práce s informacemi, včetně nástrojů jejich získávání a zpracování ze širokého spektra zdrojů
(F) Technologie a znalosti k odhalování a prokazování kybernetické kriminality
(G) Technologie a znalosti k odhalování a prokazování obchodu s drogami
(H) Technologie a znalosti k odhalování a prokazování korupce a hospodářské kriminality
(I) Technologie a znalosti k odhalování a prokazování nelegální migrace a obchodu s lidmi

4.1.3 Finanční alokace na podprogram 1

Finanční alokace na podprogram 1 činí 30% celkových nákladů programu v každém roce.

Finanční alokace na podprogram reflektuje zastoupení relevantních témat ve studii absorpční kapacity a odhad, založený na výskytu souvisejících témat v předchozích generacích programu.[18]

4.2 PODPROGRAM 2: KRIZOVÁ PŘIPRAVENOST BEZPEČNOSTNÍCH A ZÁCHRANNÝCH SBORŮ

4.2.1 Očekávané přínosy podprogramu 2

Podprogram přinese cílené zaměření pozornosti žadatelů na priority MKBV2017+ „Efektivní zásah" a „Adaptabilní bezpečnostní systém" v oblasti krizové připravenosti bezpečnostních a záchranných sborů s důrazem na priority rozvojových dokumentů v oblasti krizového řízení a ochrany obyvatelstva.

V rámci bezpečnostní politiky vynikají následující zájmové oblasti, reprezentující jádro poptávky konečných uživatelů výsledků, a tedy i žádoucí oblasti přínosu projektů:

- Zvládání přírodních katastrof, průmyslových havárií a dalších incidentů s potenciálně vysokým počtem obětí (cíle A – C)
- Problematika efektivního nasazování a ochrany sil a prostředků bezpečnostního systému (cíle D-F)
- Služební příprava a výcvik napříč schopnostmi bezpečnostních a záchranných sborů (cíle G – H)

4.2.2 Cíle a zaměření podprogramu 2

(A) Technologie a znalosti pro zvládání incidentů s přítomností CBRN látek a/nebo výbušnin
(B) Technologie a znalosti pro zvládání katastrof, průmyslových havárií a incidentů s vysokým počtem obětí
(C) Technologie a znalosti pro vyšetřování požárů a průmyslových havárií
(D) Technologie a znalosti pro sledování a snižování zdravotní zátěže a zdravotních rizik u příslušníků bezpečnostního systému, jak během zásahu, tak dlouhodobě
(E) Technologie a znalosti pro zajištění efektivní dostupnosti služeb bezpečnostního systému a pro operační řízení
(F) Technologie a znalosti pro zvýšení ekonomické efektivity při zajišťování služeb bezpečnostního systému
(G) Výcvikové metody a technologie
(H) Technologie a znalosti pro rozvoj práce se služebními zvířaty

4.2.3 Finanční alokace na podprogram 2

Finanční alokace na podprogram 2 činí 30% celkových nákladů programu v každém roce.

Finanční alokace na podprogram reflektuje zastoupení relevantních témat ve studii absorpční kapacity a odhad, založený na výskytu souvisejících témat v předchozích generacích programu.

4.3 PODPROGRAM 3: ODOLNÁ SPOLEČNOST

Jak již název napovídá, tento podprogram sdružuje témata, které mají zásadní společenské přesahy a kde se, slovy MKBV2017+, setkávají a překrývají odpovědnosti bezpečnostního systému a dalších veřejných, privátních i společenských aktérů a skupin. Podprogram navazuje na část priorit BV, u

[18] Viz např. Moravec, L. (2014) 'Research Market Gap in Law Enforcement Technology: Lessons from Czech Security Research Funding Programmes.' Central European Journal of Public Policy, Vol. 8, No. 2, pp. 28-49.

kterých poskytovatel předpokládá také možnost zapojení dalších poskytovatelů. K tomu skutečně dochází[19] a formulace podprogramu je malým příspěvkem k vyjasňování vzájemných poměrů mezi relevantními programy. Přestože je nutné zařazení jednotlivých projektů vyhodnocovat ad hoc, byl tento podprogram formulován tak, aby byly překryvy s jinými programovými nástroji co nejmenší. A to i vzdor bizarním aspiracím některých z nich, např. v rovině proklamací o relevanci pro boj proti terorismu.

Témata jsou záměrně volena obecněji, než v předchozích případech a jejich vazby na související koncepční dokumenty jsou také volnější. Je to dáno snahou o rozšíření prostoru pro vstupy žadatelů (podle studie absorpční kapacity lze v tomto podprogramu čekat největší koncentraci respondentů), ale také tím, že související koncepce nelze vždy jednoznačně nebo snadno transformovat na témata BV. Přesto, podprogram je formulován tak, aby postihl nejširší možné relevantní spektrum témat a témat speciálního zájmu, která v souvislosti s těmito koncepcemi rezonují.

4.3.1 Očekávané přínosy podprogramu 3

Podprogram přinese cílené zaměření pozornosti žadatelů na prioritu MKBV2017+ „Resilientní komunity“. Záměrně jde o podprogram charakteristický velkou diverzitou témat, stále ale vychází nebo zahrnují priority strategických a koncepčních dokumentů bezpečnostní politiky. Specificky jsou zahrnuta témata, kde dochází ke značnému překryvu mezi činností bezpečnostního systému, resp. jeho jednotlivých složek s aktivitami dalších aktérů (samosprávy, neziskový sektor, další úřady, občané přímo..). Mezi nejvýznamnější vstupy lze zařadit Koncepci prevence kriminality a odpovídající pasáže Koncepce rozvoje PČR, dále Koncepci environmentální bezpečnosti. I plnění těchto zadání lze vnímat za přínos podprogramu 3.

Rozsah témat odpovídá členění priority „Resilientní komunity“:

- Bezpečná infrastruktura (cíle A-D)
- Bezpečný veřejný prostor (cíle E-I)
- Environmentální bezpečnost (cíle J-L)

4.3.2 Cíle a zaměření podprogramu 3

(A) Kyberbezpečnost kritické infrastruktury a klíčových služeb
(B) Fyzická ochrana KI
(C) Bezpečnost a vymáhání práva v dopravě
(D) Bezpečnost a autenticita v dodavatelských řetězcích a ekonomických vztazích
(E) Bezpečnostní aplikace pro chytrá města a regiony
(F) Ochrana měkkých cílů
(G) Právo, etika a soukromí ve vztahu k moderním technologiím ve veřejném prostoru
(H) Prevence kriminality a protispolečenských jevů, zejm. ve vztahu ke zvláště ohroženým skupinám (ženy, děti, senioři), a to jak ve veřejném prostoru, tak v kyberprostoru
(I) Veřejný informační prostor a prevence jeho zneužívání k subverzivním a/nebo kriminálním aktivitám

[19] Např. v kyberbezpečnosti se MV zaměřuje na kritickou infrastrukturu a kyberkriminalitu, zatímco v programech např. TAČR lze hledat témata z okruhu ochrany spotřebitelů a běžných uživatelů; obdobně u environmentální bezpečnosti se MV zaměřuje na problematiku ekologických havárií, jejich prevence, případně predikce klimatických extrémů, které přímo souvisí s potenciálně nebezpečnými situacemi, zatímco MŽP tato témata vnímá a postihuje ve významně širších kontextech; konečně v oblasti ochrany veřejného prostoru (fyzického i virtuálního) nacházíme řadu aktérů a MV se soustředí opět pouze na témata nejúžeji spojená s vlastní působností nebo s oblastmi zájmu koncepčních dokumentů s přesahy do bezpečnostní politiky.

(J) Snižování negativních dopadů činnosti bezpečnostních a záchranných sborů na životní prostředí
(K) Prevence rizik ekologických katastrof
(L) Naturogenní hrozby, jejich dynamika, vyhodnocování a predikce, včetně vztahu ke klimatické změně

4.3.3 Finanční alokace na podprogram 3

Finanční alokace na podprogram 3 činí 40% celkových nákladů na program.

Finanční alokace na podprogram reflektuje zastoupení relevantních témat ve studii absorpční kapacity a odhad, založený na výskytu souvisejících témat v předchozích generacích programu.

5 TYPOLOGIE PROJEKTŮ[20]

Za účelem usnadnění hodnocení, ale také výpočtu relativní podpory pro projekt zavádí program projektovou typologii. Jde o model obvyklý v zahraničí (Rámcové programy EU, SBIR/STTR), který umožňuje zvýšit metodologickou spolehlivost hodnocení, omezit gaming ze strany uchazečů a zároveň řídit rizika vkladů ze strany poskytovatele. Zároveň nejde o praxi zcela neznámou v ČR, přestože se obvykle realizuje podle jiného klíče. Např MZd realizuje v rámci jedné soutěže min 2 různé typy projektů – standardní a juniorní. V tomto případě nejde o nic jiného než jiný klíč k členění soutěže.

Technicky by mělo být možné členění a následné dodržení omezujících parametrů snadno implementovat do ISTA. Z hlediska takového systému se musí jednat o banální operaci v podobě nastavení číselníku a podmínek odvislých od zařazení.

5.1 PROOF-OF-CONCEPT (KONCEPTY)

Tyto projekty se pohybují na nižších stupních technologické vyspělosti. Jsou charakteristické tím, že jejich ukončení nepřináší výsledky plně testovatelné nebo aplikovatelné v uživatelském prostředí, ale jasnou představu o možnostech, limitech dané technologie a požadavcích na následující vývoj. Za projekty tohoto typu považujeme takové, které postupují od formulovaného technologického konceptu, přes jeho experimentální ověření až po laboratorní ověření navazující technologie. U projektů tohoto typu lze pokročit až do TRL 4, tedy k laboratorní validaci. **Financování projektů tohoto typu je odvozeno od limitů pro aplikovaný výzkum.**

5.2 TECHNOLOGICKÝ VÝVOJ (DEMONSTRÁTORY)

Tento typ projektu pracuje s již ověřenými nebo akceptovanými technologickými koncepty, které dále rozvíjí směrem k aplikacím. Typickým koncovým stavem takového projektu je TRL 6, tedy demonstrátor v relevantním prostředí, odpovídajícím budoucímu nasazení. V tomto programu lze aspirovat až na TRL 7, tedy demonstrátor ve skutečném prostředí nasazení. Program ovšem a priori nefinancuje testování a evaluace ze strany uživatelů ani certifikační procesy. K tomu jsou určeny programy SecPro a SecTech. **Financování těchto projektů je odvozeno z limitů pro experimentální vývoj. Maximální podpora na projekt (bez ohledu na typ uchazeče) v tomto instrumentu tvoří 80%**

[20] Pokud poskytovatel realizuje unifikované soutěže, je nutné tuto typologii zanést do přihlášek a nastavit automatické vymáhání limitů.

způsobilých nákladů s výjimkou projektů, jejichž jediným řešitelem jsou organizační jednotky organizačních složek státu.

5.3 METODY, POSTUPY, EVALUACE, SPOLEČENSKÉ INOVACE

Z důvodu nekompatibility Metodiky hodnocení výsledků výzkumných organizací se obecně akceptovaným přístupem k hodnocení pokroku v technologických projektech a pro některé typy výsledků, zejm. N a H stanoví pravidla, odpovídající TRL 9, je pro tyto zavedena zvláštní kategorie projektů. Takovou strukturu ale nelze vykládat jako rezignaci na postupné zavádění TRL do procesu rozhodování o projektech. V těchto případech je nutné trvat na plnění charakteristických znaků jednotlivých stupňů, tedy zejm. ověřování na empiricky relevantních vzorcích a situacích (TRL6), včetně reálných případových studií (TRL7). Proces certifikace a souvisejících úprav lze považovat za TRL 8. Teprve potom lze metodické materiály nebo evaluativní studie považovat za úplné. **Maximální výše podpora bez ohledu na složení konsorcia je 90% způsobilých nákladů s výjimkou projektů, jejichž jediným řešitelem jsou organizační jednotky organizačních složek státu.**

6 REFLEXE INTERNACIONALIZAČNÍCH CÍLŮ MKBV2017+

6.1 PROGRAM JAKO ZÁLOHA PRO UNIKÁTNÍ MEZINÁRODNÍ SPOLUPRÁCE

Program je zdrojem pro projekty v mezinárodní spolupráci VO tam, kde lze převzít zahraniční hodnocení a zároveň kde takovou podporu nezajišťuje ve své působnosti jiný poskytovatel (zejm. MŠMT). Lze tedy přímo přidělit účelovou podporu tam, kde lze akceptovat mezinárodní hodnocení [21]

Ve smyslu § 7 odst. 4 totiž lze „Účelovou podporu poskytne poskytovatel po provedení veřejné soutěže ve výzkumu, vývoji a inovacích podle tohoto zákona nebo na základě zadání veřejné zakázky podle zákona o zadávání veřejných zakázek, s výjimkou případů podle odstavců 5 a 6 **a těch projektů, kde výběr projektů proběhl na mezinárodní úrovni.**"

Tuto roli lze alternativně svěřit programu IMPAKT, kde to má zdánlivě větší logiku. Je však třeba připomenout, že program IMPAKT disponuje relativně omezenými zdroji, zatímco v OpSec lze očekávat dostatečnou dostupnost finančních prostředků, čistě na základě rozdílu v celkových alokacích.

6.2 PROGRAM JAKO PODPŮRNÝ NÁSTROJ INTERNACIONALIZACE BEZPEČNOSTNÍHO VÝZKUMU

Program by mělo být možné využít jako podpůrný nástroj internacionalizace CZ bezpečnostního výzkumu, především, ale nikoliv pouze, ve vztahu k Horizontu Evropa. Takovou roli obdobné programy plní i u dalších evropských partnerů a dává proto smysl tento účel vtělit i do OpSec. Tuto roli programu lze vtělit především do ZD a následně do hodnotícího procesu, a to jednou nebo kombinací následujících možností:

- Bodová bonifikace v hodnocení za efektivní mezinárodní spolupráci, prokázanou skrze detailní *Letter of Intent* a zároveň zapracovanou do ostatních aspektů návrhu – bonifikace nepřekročí 10% celkového bodového hodnocení

[21] Např. příležitost pro MV/MO zapojit ČR do Coalition Warfare Programu s USA, zde uplatňovat Dual Use technologie – CBRN a kyberbezpečnostní, v některých případech i jiné; obdobně lze rozběhnout lead agency debaty s dalšími internacionalizačními partnery (zejm. NL a IL v kyberbezpečnosti a SWE v oblasti prevence rizik katastrof).

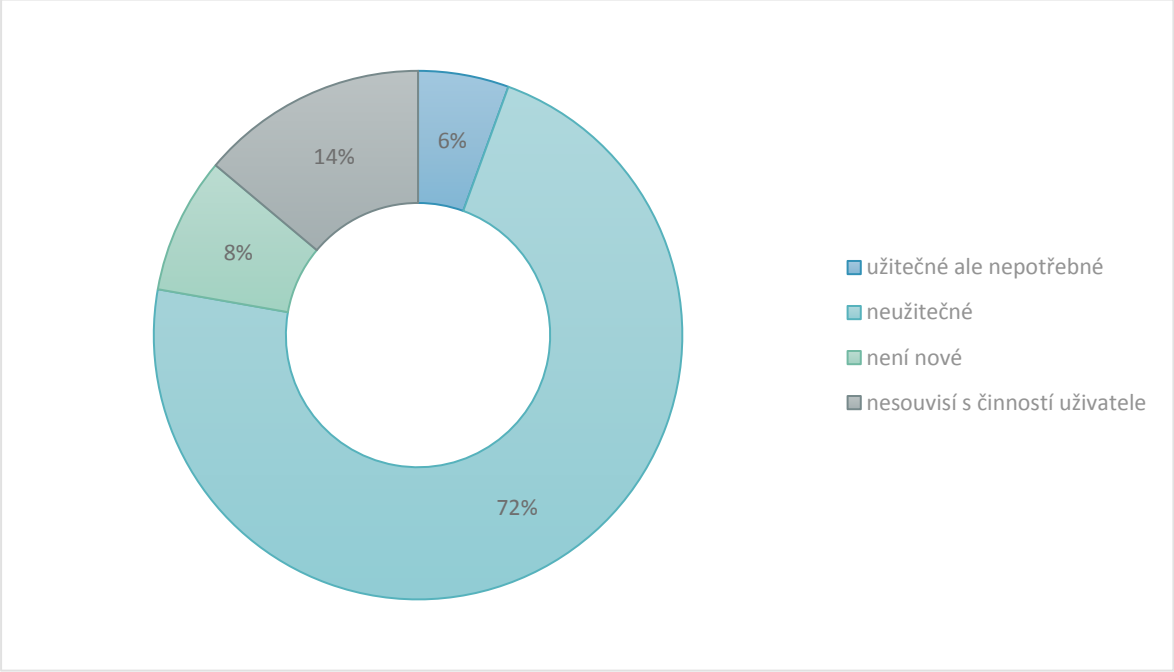
- Bodová bonifikace za přímou vazbu projektu na předpokládané budoucí výzvy v Horizon EU, ve výzvách pro bezpečnou společnost (odkaz na konkrétní výzvu v pracovním programu) – bonifikace nepřekročí 10% celkového bodového hodnocení

V případě efektivní mezinárodní spolupráce na tématu relevantním pro budoucí výzvu v HE se doporučuje zpřístupnit až 15% bonifikaci.

7 ZAPOJENÍ UŽIVATELŮ

Zkušenosti zejména Evropské komise s implementací evropských rámcových programů, ale i MV s obdobnými aktivitami na poli národního bezpečnostního výzkumu potvrzují, že role uživatele ve výběru projektů je naprosto klíčovým parametrem. Výše uvedená specifika trhu bezpečnostních technologií, stejně jako specifické podmínky nasazování technologických řešení v těchto sborech mají pro výběr projektových návrhů zásadní relevanci. Dlouhodobě jsou v portfoliu MV úspěšnější projekty, které aktivně akcentují také zapojení uživatelů do jejich řešení.

Z těchto důvodu MV dlouhodobě pracuje s oběma tématy. Celý systém je několikastupňový. Programové poradní orgány jsou uživatelsky obsazovány, protože jsou centrem debaty o potenciálních aplikačních dopadech projektů. Vedle toho bylo v programu VI úspěšně testováno uživatelské hodnocení, jako součást oponentního procesu. Samostatnou kapitolou je tlak na to, aby byli uživatelé do projektů aktivně zapojování v některé ze standardních forem.



Graf 1: Kategorizace výtek k předloženým projektům, které uživatel – Policie ČR – nepodpořil ve veřejných soutěžích[22]

I projekty, které lze považovat za vědecky nebo technologicky kvalitní totiž zdaleka nemusí splňovat náročné požadavky nasazení v bezpečnostních sborech. Ty navíc nemusí být řešitelům intuitivně zcela jasné. Jak dokumentuje Graf 2, řada projektů, výtkám k projektům z hlediska funkčnost, resp. přínosnosti pro uživatele dominuje právě neužitečnost. Proto je nutné, aby podíl uživatelského

[22] 36 z 89 referenčních projektů z VG3VS, v ostatních veřejných soutěžích v předchozích generacích programu jsou trendy srovnatelné

vstupu do hodnocení v principu rostl s mírou otevřenosti soutěže, což by mělo eliminovat nebo minimalizovat tato rizika. V tomto programu se proto navrhuje institucionalizace ověřeného modelu uživatelského hodnocení na úrovni odborných kolegií pro jednotlivé podprogramy.

Zapojení uživatelů do programových projektů je nutné také regulovat v zadávací dokumentaci. Tabulka 1 shrnuje základní možné modality tohoto zapojení, a to bez přímé vazby na programová kritéria. Je ale nezbytné poznamenat, že tato indikativní tabulka nezohledňuje veškeré požadavky na dosažení jednotlivých stupňů TRL. Zejména u konzultací je nutné mít na paměti, že kde TRL úroveň předpokládá testování za skutečných podmínek nasazení, je nutné toto testování skutečně provést. V případech, kdy jeho provedení striktně nezávisí na přístupu k uživatelské infrastruktuře mohou konzultace stačit. Zapojení uživatele touto formou ale nijak nezbavuje řešitele povinností spojených s dosahováním jednotlivých stupňů TRL.

Tabulka 1: Modality zapojení uživatele a některé jejich charakteristiky

Typ zapojení	Mechanismus zapojení	Doporučení	TRL
Aktivní výzkumný/vývojový podíl uživatelské organizace	Reprezentant uživatelské sféry je přímo zapojen do projektového konsorcia a provádí aktivity výzkumného/vývojového charakteru	U uživatelů – bezpečnostních a záchranných sborů nebo ústředních správních úřadů - je tato forma spolupráce možná pouze cestou jimi zřizovaných VO; v případě orientace na privátní subjekty je možno zapojovat podle obecných pravidel zadávací dokumentace a platných právních předpisů	TRL 3-8
Uživatel se podílí pouze cestou testování a evaluace nebo pilotního nasazení	Uživatelská organizace může, ale nemusí, být součástí projektového konsorcia, a vykonává činnosti umožňující dodatečný vývoj výsledku podle testů za skutečných, či částečně skutečných, podmínek nasazení, nebo vyhodnocení takových testů; uživatel dodává know-how o operačním kontextu, zajišťuje přístup k infrastruktuře nebo ke specializovaným schopnostem, přičemž se přímo podílí na testování.	Pokud je zamýšleno přímé zapojení do konsorcia, platí omezení podle varianty "aktivní výzkumný podíl"; pro zapojení uživatelů mimo konsorcium platí, že taková spolupráce musí být smluvně podložena, a to v míře detailu dostatečné k řešení plánovaných aktivit tohoto typu, včetně komunikačního mechanismu, pravidel přístupu k infrastruktuře/do areálů, kontaktních osob a očekávaného rozsahu pracovního vytížení, pravidel nakládání s know-how uživatele a omezení v této oblasti (mlčenlivost, ochrana utajovaných informací, obchodní tajemství, zvláštní skutečnosti) apod., přístupu k výsledkům určeným k testování a k výstupům z testů. Přístup k testovacím verzím a před-finálním výsledkům je třeba ošetřit tak, aby nedocházelo ke kolizi s ustanoveními § 16, odst. 4 zákona č. 130/2002 Sb. o podpoře výzkumu, vývoje a inovací z veřejných prostředků.	TRL 6-8
Uživatel poskytuje infrastrukturu, databáze a datové zdroje a/nebo artefakty	Uživatelská organizace nemusí být součástí projektového konsorcia, ale je součástí formalizovaného mechanismu výměny dat, artefaktů nebo zajištění přístupu k testovací infrastruktuře. Uživatel se přímo nepodílí na testování.	Tato modalita spolupráce je smluvně zajištěna před zahájením projektu a před jeho financováním. Předmětem smluvního zajištění není pouze závazek k předávání nutných dat, nýbrž také pravidla dalšího nakládání s nimi a jejich ochrany v případě, že si jejich operační kontext takovou ochranu žádá. Zároveň je však třeba postupovat ve smyslu schválených strategií k otevřenému přístupu k	TRL 4-7

		vědeckým informacím a také závazku vlády otevírat vládní data pro rozvoj některých disciplín výzkumu umělé inteligence.	
Uživatel se podílí cestou pravidelných věcných konzultací	Uživatel/é jsou součástí formalizovaného mechanismu předávání informací a konzultací, jehož účelem je získávat vstupy k jednotlivým fázím projektu a ke specifickým vlastnostem výsledků. Uživatel dodává know-how o operačním kontextu, přístup k infrastruktuře nebo specializované schopnosti, přičemž se na testování přímo nepodílí. Uživatel v tomto případě není součástí konsorcia, uvedený mechanismus je však stálý a je užíván se opakovaně.	Spolupráce tohoto typu by měla by písemně (ne nutně smluvně) podložena, včetně popisu konzultačního mechanismu a očekávání obou stran od takové spolupráce. V principu se doporučuje realizovat předávání know-how o operačním kontextu nebo dalších specifických informací pouze v případě, že jsou uživateli, který taková data poskytuje, zpřístupněny před-finální nebo testovací verze výsledků. Obdobné doporučení lze vznést tam, kde je požadován přístup k infrastruktuře uživatele nebo zpřístupnění jiných schopností uživatele za účelem testování nebo do vývoje výsledků projektu. Přístup k testovacím verzím a před-finálním výsledkům je třeba ošetřit tak, aby nedocházelo ke kolizi s ustanoveními § 16, odst. 4 zákona č. 130/2002 Sb. o podpoře výzkumu, vývoje a inovací z veřejných prostředků.	TRL 4-8
Uživatel je zapojen na úrovni směrování projektu	Uživatelská komunita je zmapována. Konzultační mechanismus nemá stálou nebo pravidelnou povahu, reprezentanti uživatelské sféry jsou kontaktováni ad hoc za účelem obecnější debaty o směřování projektu nebo zacílení jeho výsledků, předmětem těchto debat obecně nejsou operační specifika anebo operační kontext pro účely testování. Výstupy směřují spíše k lepšímu zacílení výsledků nežli k podpoře rozvoje jejich konkrétních vlastností.	Spolupráce tohoto typu je veskrze neformální. V tomto modu však nelze předpokládat přístup k infrastruktuře nebo schopnostem uživatele, nebo extenzivní předávání know-how. Konzultace se orientují spíše na obecné podmínky uplatnitelnosti výsledků nebo vymezování silných a slabých stránek nabízených řešení, nebo na komentáře k problémům, které projekt postihují s ohledem na expertizu uživatelů.	TRL 3-6

Uživatel není přímo zapojen	U projektů, kde jejich charakter zapojení uživatele nevyžaduje, se přesto doporučuje pravidelně zvažovat jeho zapojení některou z méně strukturovaných forem, zejména za účelem omezení implementačních rizik (plynoucích z neznalosti operačního kontextu, nebo speciálních regulatorních nebo jiných nároků) a zvýšení uplatnitelnosti výsledků.	Zapojení uživatelů v průběhu projektu cestou připojení ke konsorciu není možné. V méně strukturovaných formách spolupráce platí doporučení uvedená výše, podle intenzity zapojení uživatele.	N/A

8 NASTAVENÍ PROCESŮ VÝBĚRU A HODNOCENÍ PROJEKTŮ

8.1 ORGÁNY PROGRAMU

8.1.1 Rada

Rada programu má 9 členů z toho:

- 1 předseda reprezentuje OBVPV, Radu řídí a odpovídá za zajištění jejího chodu;
- 8 členů by mělo mít emeritní status a reprezentoval „skupinu moudrých“ ve vztahu k bezpečnostnímu výzkumu a jeho tématům;

Doporučuje se následující seznam nominujících a/nebo členů:

- RVVI – zpravodaj pro BV (nehlasuje)
- BRS – reprezentant/ka pracovní skupiny pro BV, resp. VCNP (nehlasuje)
- Reprezentant/ka komunity CBRN[23]
- NPP pro SKPV (příp. reprezentant problematiky kriminální služby s akceptovaným veřejným kreditem)[24]
- NGŘ pro civilní nouzovou připravenost a KŘ (příp. reprezentant komunity krizového řízení s akceptovaným veřejným kreditem)
- Bývalý nebo současný představitel/ka zpravodajské komunity (pokud lze najít někoho s čistým veřejným profilem)[25]
- Představitel/ka neziskového sektoru (nejlépe s orientací na prevenci kriminality nebo práci s oběťmi)
- Představitel/ka komunity kyberbezpečnosti nebo NUKIB[26]

[23] Alternativně Ing. Dana Drábová, SUJB
[24] Doporučení: Ing. Jiří Bouček, bývalý ředitel UZČ
[25] Doporučení: brig. gen. Václav Žid, VZ
[26] Doporučení: NŘ NUKIB Ing. Jaroslav Šmíd

8.1.2 Uživatelské kolegium pro PP1

- PČR – až 1x za každý UCP, 2x centrální analytika
- CS – až 1x CTL, 1x odbor pátrání
- VS – až 2x napříč funkčními celky
- OBP MV – 2x

8.1.3 Uživatelské kolegium pro PP2

- HZS – 4x (min 2 zástupci krajských HZS, 1x prapor humanitárních operací, 1x CBRN)
- MZd – 1x
- SUJB – 2x
- PČR – 4x (1x OO, 1x ZJ/prvosledové hlídky/Urna, 1x kynologie/hipologie, 1x KŘP)
- MO – 1x
- Asociace záchranných služeb – 1x

8.1.4 Uživatelské kolegium pro PP3

Toto kolegium by se pro účely posuzování projektů mělo dále dělit na 3 pracovní skupiny podle dominujících témat ve výzvě nebo mezi přihláškami. Města a kraje by se měla buď vyjadřovat ke všemu, nebo vstupovat rovným zastoupením do všech 3 skupin.

- Partnerská města a kraje (celkem 3 nebo 6) – primárně Plzeň,[27] Praha, Brno/Jihomoravský kraj, Ostrava/Moravskoslezský kraj (přičemž se doporučuje u nominací akcentovat jedince schopné rozhodovat o spolupráci s takovými projekty v rámci realizace nebo implementace, spíše než lokální organizace na podporu inovačních firem a nelze nominovat město z již zastoupeného kraje a naopak)
- MŽP – 1x
- ČIŽP – 1x
- MZe – 1x
- Ochrana KI – 1x NUKIB, 1x NAKIT, 1x HZS (KI), 1x PČR, 1x dopravní PČR
- OPK MV – 1x
- PČR prevence – 1x
- MSp – 1x
- OBP MV – 1x
- Neziskový sektor – 1x práce s oběťmi domácího nebo sexuálního násilí nebo PK

8.2 SBĚR TÉMAT

V souladu s účelem programu i s jeho legislativním zakotvením navrhují témata jednotlivých projektů jejich řešitelé. Podstatou návrhů by měla být snaha naplnit cíle podprogramů, do kterých se budou jednotlivé návrhy přihlašovat. **Formulaci cílů jednotlivých výzev je tak nezbytně nutné věnovat značnou pozornost.**

Program tedy předpokládá, že tematická zaměření výzev budou formulována na základě spolupráce se širokým spektrem partnerů. V podprogramech 1 a 2 zejména s uživatelskou sférou, v podprogramu 3 zejm. s aktéry relevantními pro jeho témata (NUKIB, provozovatelé KI, města a územně samosprávné celky a další subjekty). Součástí přípravy výzev by měly být technologické dny

[27] Důrazně se doporučuje zvážit zapojení Správy informačních technologií města Plzně, jde o vedlejší složku IZS, která zároveň podporuje podnikatelskou a inovační činnost ve městě, cestou vlastních projektů podle potřeb města. V ČR jde v zásadě o unikátní model.

a workshopy mezi uživatelskou a inovační sférou, aby došlo k navázání dostatečných kontaktů před samotnou přípravou výzvy.

8.3 VARIANTY SOUTĚŽÍ A WORKFLOW

Program předpokládá především realizaci jednostupňových veřejných soutěží. V takovém případě by postup hodnocení měl odpovídat Variantě 4, podle přílohy 1 tohoto dokumentu.

Na základě minulých zkušeností byla zvažována také možnost realizace dvoustupňových veřejných soutěží. Po překonání prvotní bariéry, spočívající v dříve nevyužívaném postupu lze tuto variantu doporučit jako standardní a jednostupňovou soutěž používat pouze ad hoc k účelům, hodným zvláštního zřetele.

Bezpečnostní výzkum obecně, i s přihlédnutím ke dřívějším zkušenostem spadají otevřené výzvy v těchto tématech pod podmínku zákona č. 130/2002 Sb. v platném znění, resp. jeho § 22, odst. 1, který uvádí: **„Dvoustupňovou veřejnou soutěž ve výzkumu, vývoji a inovacích může poskytovatel podle tohoto zákona vyhlásit tehdy, je-li nezbytné nebo účelné od sebe oddělit posouzení účelnosti navrhovaného řešení a jeho porovnání s vyhlášenými cíli a podmínkami programu (první stupeň) a hodnocení odborné úrovně a proveditelnosti návrhu projektu (druhý stupeň), nebo v případě, je-li nezbytné postupně vyjasnit způsob plnění vyhlášených cílů a podmínek programu."**

Autor této studie má za to, že bezpečnostní výzkum je prototypickým příkladem naplnění první podmínky. Z hlediska žadatelů jde také o postup výhodný. Ve dvoustupňové soutěži by měl být v prvním kroku kladen důraz na obsahovou – uživatelsky relevantní – část projektu, formulaci jeho cílů a jejich souladu s cíli programu. Pro ostatní parametry projektů lze poptávat pouze obecný odhad. To by uchazečům, odmítnutým zejm. pro nesoulad s podstatou programu nebo z obdobných důvodů, mělo ušetřit značný objem práce na přípravě projektů, které obecně nemají šanci uspět. Poskytovateli by postup umožnil především relativně rychlou selekci nezpůsobilých návrhů a zároveň možnost srovnat postavení uživatele ve vztahu k hodnocení projektů. Postup by to byl transparentnější, protože by se eliminovaly z rozhodování uživatelsky nevhodné návrhy, které nezřídka mohou získat vysoká oponentní hodnocení.

Zásadní problém pro aplikaci postupu dvoustupňovou soutěží je její zákonné ukotvení. Přestože se ve výše citovaném ustanovení předpokládá, že první stupeň vyhodnotí účelnost a soulad návrhu s cíli programu (což je logické), přenáší se do tohoto stupně povinnosti dvojího externího hodnocení, které pro tyto účely není v kontextu bezpečnostního výzkumu vhodné. Naopak, druhý stupeň, kde by takové hodnocení smysl dávalo, tento postup nepředepisuje. Nejefektivnější způsob implementace programu, tedy dvoustupňová soutěž s uživatelským panelem ve stupni prvním a oponentním hodnocením ve stupni druhém je tak přinejmenším na hraně zákona (a očekávání příjemců).

Programový návrh proto otevírá možnost dvoustupňovou soutěž uspořádat, ale v současném kontextu zpracovatel studie tento postup nepředpokládá. Vzhledem k době trvání programu ale lze uvažovat o možné zákonné změně a následném přechodu na tento typ soutěží (nejen v tomto programu). Alternativně lze uvažovat o vyjasnění požadavků na tyto soutěže s RVVI a realizaci uživatelského hodnocení na základě 2 posudků v prvním kole a doplnění dalšího odborného pohledu na celý projekt v kole druhém. Při implementaci dvoustupňové soutěže je totiž zásadní motivací snaha ušetřit navrhovatelům práci s přípravou celých projektů tam, kde je návrh irelevantní z hlediska programových nebo uživatelských požadavků.

8.4 STRATEGIE KOMUNIKACE

Na základě platné Koncepce ochrany obyvatelstva, která vyzívá k zásadnímu přehodnocení a prohloubení iniciativy k propagaci bezpečnostního výzkumu a v návaznosti na související opatření MKBV2017+ se doporučuje zvážit zavedení přikládání povinné komunikační strategie projektu k jeho návrhu. Zároveň by ZD měla reflektovat minimální požadavky na takovou strategii:

- na popularizaci výsledků a informace o projektu by mělo být možné alokovat až nižší jednotky procent celkového rozpočtu s tím, že podíl by měl klesat s rostoucími náklady na projekt
- minimální standard pro označování výstupů, výsledků a majetku pořízeného z projektu
- reportingový mechanismus, odpovídající současnému dotazníku pro sledování implementace v redukované formě jako součást roční zprávy
- návody a sjednocující postupy pro komunikaci o projektech a výsledcích na sociálních sítích
- minimální požadavky na intenzitu popularizační aktivity (tj. přinejmenším web nebo samostatná stránka na webu příjemce, popularizace v médiích a mezi odbornou veřejností)

8.5 FORMÁLNÍ HODNOCENÍ

Realizace v souladu se zákonem.

8.6 HODNOCENÍ ZPŮSOBILOSTI PRO FINANCOVÁNÍ Z PROGRAMU:

1) Navrhovaná aktivita naplňuje definičních znaků výzkumné či vývojové činnosti podle *Frascati Manuálu*.[28]
2) Nejde o základní výzkum? – základní výzkum se v tomto programu nepřipouští
3) Jde o bezpečnostní výzkum/vývoj? – má úzký vztah k jednoznačně definovaným prioritám bezpečnostní politiky dále k jejich specifickému vymezení v programu?
4) Není duplicitní s projekty již podporovanými u jiných poskytovatelů nebo v některém z jiných programů bezpečnostního výzkumu?
5) Jde o projekt? – programy, tj. skupiny projektů, návrhy s vágně vymezenými výsledky nebo s několika obsahovými liniemi, byť i příbuznými, které lze bez ohrožení přínosu z realizace odděleně považovat za samostatně realizovatelné, nejsou způsobilé
6) Projekt nemá charakter rešeršních nebo srovnávacích studií, bez ohledu na případný mezinárodní referenční rámec, a nemá charakter běžné analytické podpory činnosti předkladatele nebo uživatele;
7) Projekt splňuje veškeré nároky na etiku výzkumu a práce s lidskými/zvířecími subjekty – předkladatel dodal stanovisko relevantní etické komise, pokud se v projektu vyskytují činnosti, které jej předpokládají

8.7 POSTUP HODNOCENÍ PŘIJATÝCH NÁVRHŮ

V rámci soutěže se uchazeč hlásí k jednomu z dílčích cílů programu, do skupiny projektů, odpovídající členění na podprogramy a zároveň ke třídy schopností, odpovídající členění priorit MKBV2017+.

1. Rada programu:

[28] OECD (2015), *Frascati Manual 2015: Guidelines for Collecting and Reporting Data on Research and Experimental Development, The Measurement of Scientific, Technological and Innovation Activities*, OECD Publishing, Paris.

1.1. Hodnotí BK související se způsobilostí pro program podle kap. 8.4.
1.2. Prověřuje přiřazení způsobilých projektů do jednotlivých skupin a toto zařazení případně mění

2. Oponentní hodnocení způsobilých projektů, oponenti se přidělují na základě oborové shody, nikoliv „přihlášení“ oponenta k tematické oblasti
   2.1. V případě, že rozdíl v hodnocení oponentů překročí hranici, automaticky se poptává třetí posudek
3. Uživatelské hodnocení v uživatelských panelech, které zřizuje Rada a které reprezentují maximum zainteresovaných stran; hodnocení reprezentuje konsensus nebo výsledek hlasování v panelu, nikoliv individuální hodnocení zpravodaje panelu. Zároveň by panely měly sledovat standardní distribuci hodnocení.[29]
   3.1. Potenciál pro deklarovaný přínos
   3.2. Implementační potenciál
4. Rada sjednotí hodnocení oponentů a uživatelů podle následujícího klíče:
   4.1. Oponentní hodnocení je průměrem všech realizovaných posudků
   4.2. Celkové hodnocení projektu je součtem oponentního hodnocení a uživatelského hodnocení

Výsledky hodnocení

OBVPV předkládá Radě ke schválení mechanicky provedené výsledky ve 3 samostatných protokolech, které shrnují výsledky hodnocení podle bodů 5.1 a 5.2, kap 3.2.2. Rada vyhodnotí a koriguje případná sporná nebo jinak vadná hodnocení (identifikuje poskytovatel a panely, Rada sama rozpory nevznáší). Rada může projekty z podpory pouze vyřadit, nemůže ale další projekty předřadit nebo posunout do financovaného pásma.[30]

Rada schvaluje 3 seznamy projektů, doporučených k podpoře v rámci limitů každého z výše uvedených podprogramů.

V rámci vyhodnocování celé soutěže může Rada doporučit úpravu limitů pro financování mezi jednotlivými podprogramy, a to do maximální výše 20% alokovaných limitů, při udržení celkového limitu financování soutěže. Pro účely zachování transparentnosti by tyto změny měly reflektovat především výkyvy v rozsahu a charakteru poptávky v jednotlivých programech. Účelové úpravy, přesouvající rozpočet ve prospěch konkrétních projektů by měly být omezeny nižším procentem.

8.8 SMLUVNÍ ŘÍZENÍ

V souladu se zákonem č. 130/2002 Sb., není proto nutné stanovit nový proces. Žádoucí je pouze revize smlouvy ve smyslu:

- rozšíření a prohloubení pravidel publicity, včetně webové prezentace projektů, s důrazem na roli MV v podpoře; v současnosti si řada příjemců nejspíše ani neuvědomuje jakoukoliv povinnost tohoto typu – je třeba ji precizně regulovat a vymáhat. Inspirací budiž smlouvy k projektům z operačních programů MŠMT.
  - minimální povinností by mělo být viditelné označování (A) majetku, (B) výsledků projektu, přičemž „viditelnost“ lze stanovit z hlediska umístění i velikosti označení

[29] Lze zvážit několik modelů sběru hodnotících výroků, za nejvhodnější lze považovat 2 hodnocení v rámci panelu, průměr a navazující diskusi s korekcí (model obdobný Radám programu) nebo model sběru názorů od všech členů panelu a jejich součet nebo průměr

[30] Mechanismus řešení sporů je třeba dopracovat, realisticky jich ale bude minimum, pokud se dobře nastaví automat na poptávání dalších posudků o velkých rozdílů.

- minimálním standardem by měla být dedikace programu a logo MV v barevné nebo černobílé variantě podle příručky vizuální identity MV

8.9 ADMINISTRACE A KONTROLA

V souladu s platnou legislativou.

8.10 ZÁVĚREČNÉ HODNOCENÍ PROJEKTŮ

Relevance[31]

- Potenciál pro přínos výsledků podle hodnocení ve veřejné soutěži (přenáší se)
- Soulad zaměření projektu s cíli programu (přenáší se)
- Soulad projektu se znalostními doménami strategických dokumentů, které program podporuje, zejm. RIS3 a Inovační strategie (přenáší se)

Funkčnost

- Hodnocení vlastního zapojení ze strany uživatele
- Výsledky kontrol a auditu
- Přínosy pro příjemce

Efektivita projektu

- Počet výsledků
  - Byl splněn minimální nutný počet?
- Minimální intenzita produkce
  - byla splněna? Binární
- Hodnocení kvality výsledků projektu
  - tj. v kalibraci podle stupnice hodnocení kvality výsledků podle platné Metodiky hodnocení výsledků výzkumných organizací a v intencích materiálu známého jako M17+ (A, B, C, D s nestejně velkými intervaly mezi jednotlivými stupni)
  - hodnotí se každý výsledek projektu zvlášť, a to **s využitím škály podle M17+** tak, aby byla zajištěna alespoň částečná přenositelnost tohoto hodnocení mezi programy a do hodnocení výsledků příjemců IP.
  - **hodnocení kvality výsledků aplikační povahy probíhá především z pohledu kritéria společenské relevance podle M17+. To v praxi znamená, že nedílnou součástí uzavření projektu musí být pro tyto výsledky implementační plán, jehož parametry a realističnost je nutné zahrnout do hodnocení.**
  - U projektů typu proof-of-concept se předpokládá navazující vývoj, zatímco u demonstrátorů snaha o jejich tržní/uživatelské uplatnění (tj. dokončení vývoje transfer nebo přímá implementace).
  - **Při kalibraci hodnocení a sledování výsledků je nutné se zabývat také argumentací výzkumné komunity ve vztahu k chápání aplikovaného výzkumu**[32]

[31] Jako hodnocení relevance vnímáme uživatelské hodnocení při vstupu do soutěže a hodnocení BK Radou; hodnotit relevanci ex-post nedává smysl; pouze v případě, že by se projekt radikálně odchýlil od svojí podstaty, to by ale měla odhalit průběžná kontrola nebo komunikace během projektu

- Ke zvážení je varianta prohloubení závěrečného hodnocení (kvůli kredibilitě a výše zmíněné přenositelnosti) a jeho realizace s využitím stejných oponentů, kteří projekt hodnotili ve VS, doplnit o celkové hodnocení zpravodajem a v některých programech také o hodnocení uživatelské. Celkově by měl poskytovatel usilovat o konvergenci procesu i metodiky hodnocení mezi programy.

8.11 HODNOCENÍ DOPADŮ PROJEKTU (JAKO SOUČÁST HODNOCENÍ DOPADŮ PROGRAMU)

Z hlediska dopadů programu je podstatná komplexita vazeb mezi schopnostmi bezpečnostního systému a jednotlivými bezpečnostními hrozbami. Jednoduše řečeno, snížením rizika u jedné hrozby, lze nepřímo snižovat riziko i hrozeb jiných, pokud mezi nimi existuje silná potenciální kauzální vazba. Nad to lze řadu rizik snížit posílením obecněji uplatnitelných schopností bezpečnostního systému.

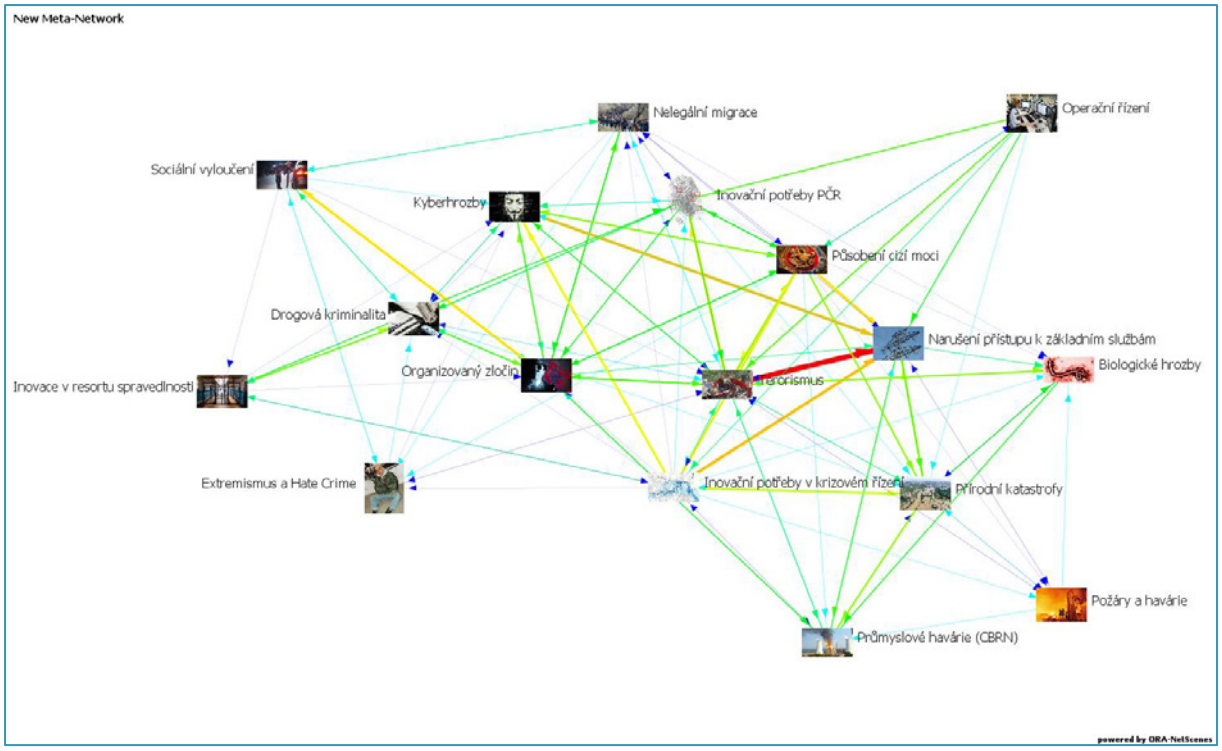
Z hlediska sledování programu a jeho vlivu na bezpečnost je proto zdaleka nejpodstatnější, **zda jsou projekty zaměřeny na skutečné potřeby bezpečnostního systému, zda mají výsledky kvalitních parametrů a tyto jsou implementovány do praxe**. Poslední z uvedených faktorů je předmětem sledování implementace projektů v post-projektovém období. Na něj navazuje hodnocení dopadů.

Pro ilustraci přinášíme mapu relačních vztahů inovačních priorit a hrozeb, zpracovanou na základě 22 relevantních dokumentů bezpečnostní politiky v období přípravy MKBV2017+. Ta dokumentuje, že i v rovině teoretické jsou vazby mezi inovací např. v policejním vybavení a jednotlivých bezpečnostních hrozeb natolik komplexní, že je prakticky nelze do hodnocení realisticky zahrnout.[33]

V souvislosti s členěním na podprogramy lze vnímat, že jádro programu OpSec tvoří podpory pro budoucí inovace v oblasti vymáhání práva, resp. v zájmové oblasti kriminální služby (zde inovační potřeby PČR) v PP1, dále v oblasti operačního a krizového řízení v PP2 a, konečně, v PP3 otázky související především s prevencí antisociálních jevů a s dostupností služeb kritické infrastruktury (v tomto diagramu dominantně spadá pod inovační potřeby v krizovém řízení a kyberhrozby). Program tedy pokrývá plné spektrum definovaných zájmových oblastí bezpečnostní politiky s relevantním členěním s ohledem na nutné standardy implementace programu.

[32] https://vedavyzkum.cz/blogy-a-komentare/michael-sebek/aplikacnimu-vysledku-muzeme-odpustit-mnohe-ale-ne-to-ze-neni-aplikovan

[33] Jinak řečeno, nelze hodnotit dopad projektů v oblasti kyberbezpečnosti měnícím se počtem kybernetických útoků; takové hodnocení by nesplnilo metodologické kritérium konstrukční platnosti, ekvivalentní vulgarizace lze najít v celé debatě o hodnocení „dopadů“ podpory aplikovaného výzkumu a vývoje



Obrázek 4: relační vztahy inovačních priorit a bezpečnostních hrozeb podle dokumentů CZ bezpečnostní politiky

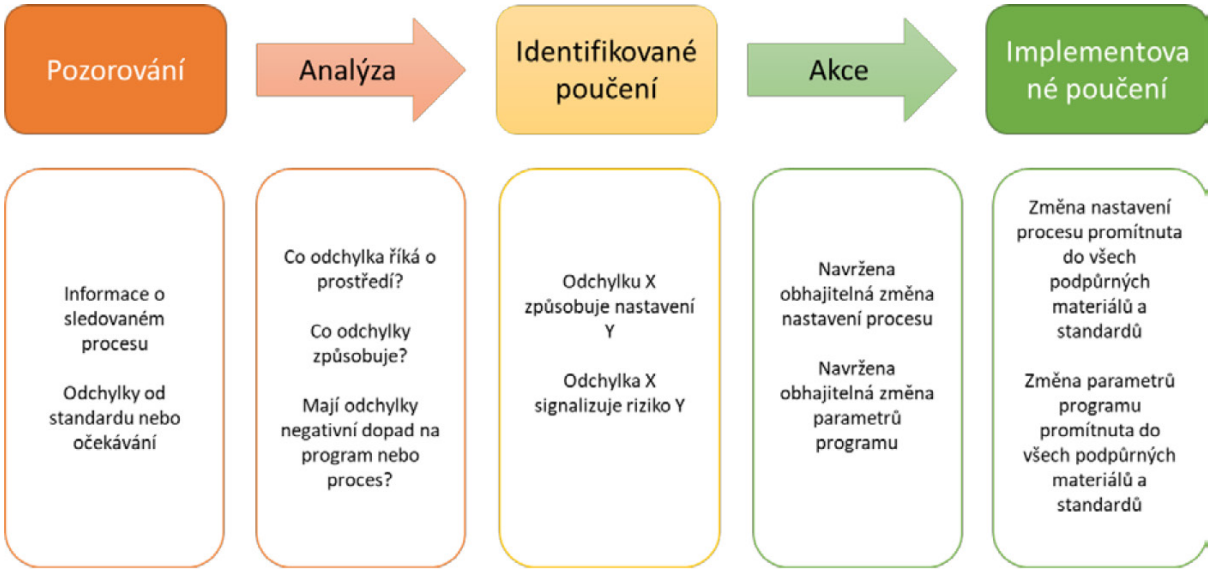
I proto se **předpokládá realizace především případových studií k posouzení „dopadů“ výsledků na praxi konečných uživatelů**. Tyto případové studie by měly verifikovat „přínos“ výsledku, který vyhodnotí konečný uživatel vždy při závěrečném hodnocení projektu. Jak je z tabulky v návrhu programu patrno, návrh hodnocení se nesnaží příliš vzdalovat od podstaty programu a praktických limitů, jakkoliv formulované intervenční logiky v oblasti bezpečnosti.

9 DALŠÍ PROGRAMOVÉ PROCESY

9.1 UČENÍ ZE ZKUŠENOSTÍ

Učení ze zkušeností je pro poskytovatele takřka nejnutnějším procesem, který jediný umožňuje kontinuální zefektivňování služeb. V principu platí, že čím složitější program, tím častější a detailnější by učení ze zkušeností mělo být. Každopádně by se ale nemělo odchylovat od níže prezentovaného konceptu. Jednoduše řečeno, zjistit odchylku od požadovaných parametrů zdaleka nestačí. I další návazná aktivita by měla snést základní analytické standardy a její závěry by měly být obhajitelné v kontextu dostupné nejlepší praxe.

Nejvhodnějšími momenty pro provedení srovnávacích pozorování jsou místa v programovém harmonogramu, kde dochází k přechodům mezi procesy, resp. se u vymezených skupin projektů přechází z procesu do procesu. V kontextu programu jde tedy zejména o období po skončení výběru potřeb nebo po ukončení zadávání větších skupin projektů. V rámci tohoto programu se potom naskýtají možnosti k zevrubnému pohledu na vlastní procesy také v momentech interim hodnocení a/nebo ukončení skupin projektů.



Obrázek 5: Konceptuální schéma procesu učení ze zkušeností

Je třeba mít na paměti, že realizace procesu učení ze zkušeností, by měla být formalizovaná, i když může jít o tak základní aktivitu, jakou je sledování nejčastěji kladených dotazů, vyhodnocení srozumitelnosti ZD, následného rozhodnutí, zda ZD upravit a/nebo publikovat standardizované vysvětlení. I toto by však mělo být systematicky zdokumentováno.

Zájmové oblasti pro učení ze zkušeností je možné a nutné stanovit pro každý proces samostatně a tomu přizpůsobit zdroje dat pro pozorování i přístupy k analýze. Výjimkou je sledování indikátoru „délka zadávacího procesu“, který vyžaduje text programu. Tento indikátor se dá dále dělit na jednotlivé fáze zadávání a umožňuje tak odhalit problematická místa celého procesu a po zevrubnějším pohledu také důvody, které k problémům vedou.

9.2 Hodnocení programu

Součástí textu programu.

Samostatný indikátor „Počet realizovaných výzkumných projektů v oblasti environmentální bezpečnosti“ podle KEB2021+ je vtělen do hodnocení programu, protože jej požaduje platná Koncepce environmentální bezpečnosti ve své části, úkolující BV.

10 Doplňkové aktivity k realizaci programu

10.1 Stanovení finančních limitů

S ohledem na zkušenosti z minulých generací programu se doporučuje harmonizovat normativy pro výpočet osobních nákladů, resp. pro odměňování s relevantním zdrojem, např. s limity, které MŠMT uplatňuje v programových projektech z OP. Ad hoc posuzování nákladů v místě a čase obvyklých se neukazuje jako zcela efektivní cesta k vyhodnocování projektů, protože lze obtížně nastavit spolehlivost hodnocení mezi posuzovateli.

10.2 Projektové řízení

Je nezbytné avizovat a propagovat možnost najímání projektových manažerů, resp. administrativních sil z projektových prostředků a možná tento krok zahrnout do hodnocení. Je totiž zjevné, že

opakované výtky na adresu administrativní náročnosti projektů plynou z toho, že tyto úkoly na sebe přebírá řešitelský tým a role manažera projektu pravidelně splývá s rolí hlavního řešitele.

10.3 MANUÁLY

Vzhledem k tomu, že se tento program vrací ke konceptu uživatelského hodnocení, je podstatné dopracovat instrukční materiály pro oponenty obou typů s důrazem na kalibraci hodnocení. Cílem by mělo být prezentovat kvalitativně vymezenou škálu odpovídající standardní statistické distribuci (tedy NEodpovídající škále pro školní známkování). Trvajícím problémem hodnocení totiž zůstává nadhodnocování průměrných projektů. To do značné míry kopíruje právě přístup „školních známek", kde je nejvyšší hodnocení přiřazováno „bezchybnému", nikoliv zcela výjimečnému výkonu.

10.4 SBĚR DAT Z PROJEKTOVÝCH NÁVRHŮ, SOUTĚŽÍ A ZE ZÁVĚREČNÉHO HODNOCENÍ:

V rámci formulářů a dalších nástrojů sběru dat je nutné v celém rozsahu životního cyklu projektu sbírat relevantní data pro hodnocení programu i projektů. Dotazníková šetření, uplatňovaná na sledování nakládání s výsledky nebo prezentace projektu by měly být realizovány i v průběhu řešení. Nejpozději na konci řešení projektu je třeba získat data k sekundárním dopadům podpory na řešitele, protože jde o klíčový zdroj informací k formulaci dalších programů.

Samostatnou kapitolu potom tvoří získávání dat o zákaznické spokojenosti – tedy pohledu řešitelů na práci poskytovatele a jeho zaměstnanců. I zde je značný prostor pro učení ze zkušeností a rozvoj programových procesů.

10.5 VYHODNOCOVÁNÍ SOUTĚŽÍ:

Oborové portfolio – pro hodnocení soutěží i pro popis programu se doporučuje používat číselník oborů FORD; mimo jiné eliminuje absurdní přiřazování oborů AQ, KA a forenzních projektů do společenských věd. Na diskrepance v přiřazování těchto oborů a jejich přímou souvislost s programy bezpečnostního výzkumu poskytovatel několikrát zcela bezvýsledně upozorňoval správce IS VaVaI v průběhu několika let (!!), lze se proto domnívat, že k pozitivnímu posunu nedojde. Pro účely hodnocení programu a mapování portfolia schopností napříč výzkumným sektorem se číselník FORD tedy jeví vhodnější.

11 ANALÝZA VAZBY NA PLATNÉ DOKUMENTY POLITIKY VAVAI

11.1 NÁRODNÍ POLITIKA VÝZKUMU, VÝVOJE A INOVACÍ

MV při přípravě programových nástrojů bezpečnostního výzkumu vychází z předpokladu, dle kterého jsou koncepce poskytovatelů nástroji plnění Národní politiky výzkumu, vývoje a inovací 2021+ (dále jen „NP VaVaI"), ale zároveň reprezentují odpovědnost poskytovatelů v jejich vlastních specializovaných oblastech působnosti. Programy, které koncepce definují, na NP VaVaI implicitně navazují. V případě Programu je to zejména návaznost na opatření NP VaVaI č. 22: **Rozvoj obranného**
a bezpečnostního výzkumu s možností využití v civilních aplikacích a opatření č. 27: **Redefinice Národních priorit orientovaného výzkumu, experimentálního vývoje a inovací s cílem zvýšení odolnosti české společnosti – podpora specifických výzkumných programů relevantních pro oblasti**

definovaných hrozeb s celospolečenským dopadem. Zajišťování obrany a bezpečnosti patří mezi hlavní úlohy každého státu, které významně ovlivňuje jak rozvoj aplikovaného výzkumu, tak společenské změny. Podstata branně-bezpečnostní problematiky a značná exkluzivita státu (jako jejího garanta) vyžadují specifický přístup k tvorbě expertních vstupů dotčených politik.

Ze zkušeností předních českých výzkumných organizací, zaměřených na průmyslovou (smluvní) výzkumnou spolupráci také plyne, že řadu situací usnadňuje podpora právě tohoto typu spolupráce. Program proto podporuje realizaci kolaborativních projektů. Lze jej proto považovat také za nástroj plnění opatření NP VaVaI č. 20: **Podpora dlouhodobé spolupráce ve VaVaI mezi výzkumnými organizacemi a podniky a uplatnění společných výsledků aplikovaného výzkumu v praxi.**

V rámci portfolia bezpečnostního výzkumu je Program zaměřen na řadu dalších opatření NP. Komplexní programové portfolio bezpečnostního výzkumu totiž zahrnuje nástroje pro rozvoj lidských zdrojů, udržování partnerství se zahraničními partnery, ale i úzkou spolupráci s těmi místními (program IMPAKT) a méně i více specializovanou účelovou podporu, podél celé škály technologické vyspělosti, od aplikovaného výzkumu po velmi pokročilý vývoj (programy SOUTĚŽ, SecPro a SECTECH – viz výše).

Program se také podílí na realizaci opatření NP č. 21: **Realizace Národní RIS3 strategie** a opatření č. 25: **Komplexní podpora rozvoje a využití umělé inteligence**. Opatření 28: Podpora spolupráce výzkumné a aplikační sféry a uplatnění jejich výsledků v environmentální oblasti naplňuje program v rozsahu, jaký požaduje MŽP v koncepci environmentální bezpečnosti a zároveň u témat, která reprezentují bezpečnostní a environmentální rozhraní (environmentální kriminalita a dopady činnosti bezpečnostních sborů na životní prostředí).

Konkrétněji, poskytovatel předpokládá, že realizace programu přispěje k naplnění následujících cílů NP VaVaI:

- Cíl 1 Nastavit strategicky řízený a efektivně financovaný systém výzkumu, vývoje a inovací ČR:
    - 1.11 Motivovat poskytovatele institucionální a účelové podpory VaVaI k orientaci části výzkumných kapacit na specifickou podporu monitorování, analýz a návrhů řešení aktuálních výzev a hrozeb s celospolečenským dopadem (focus area).
- Cíl 4 Podpořit rozšíření spolupráce mezi výzkumnou a aplikační sférou v oblasti výzkumu, vývoje a inovací:
    - 4.1 Při přípravě a implementaci programů podporovat rozvoj spolupráce mezi výzkumnou a aplikační sférou ve všech relevantních výzkumných oborech.
    - 4.4 Vytvořit nástroje pro podporu dlouhodobé strategické spolupráce mezi výzkumnou a aplikační sférou.
    - 4.5 Nadále podporovat dlouhodobou spolupráci ve VaVaI mezi výzkumnými organizacemi a podniky a uplatňování společných výsledků aplikovaného výzkumu v praxi.
- Cíl 5 Dosáhnout rozvoje výzkumu, vývoje a inovací v podnicích a ve veřejném sektoru:
    - 5.1 Podpořit podniky v rozvoji výzkumných, vývojových a inovačních aktivit v ČR vedoucích k produkci s vyšší přidanou hodnotou.
    - 5.7 Sledovat a metodicky spolupracovat na zavádění výsledků VaVaI do veřejného sektoru, podporovat zapojení veřejného sektoru do vytváření poptávky po výzkumu a vývoji a do spolupráce při realizaci projektů výzkumu.

11.2 INOVAČNÍ STRATEGIE[34]

Inovační strategie je svým charakterem i logikou dokumentem výrazně obecnějším a hierarchicky vzato výše postaveným, než aby přímo ovlivňoval charakteristiky konkrétních programů podpory. Pro jeho efektivní fungování je nutné vytvářet průnik s posláním poskytovatelů a účelem jejich jednotlivých podpor. Přesto lze i Program vztáhnout ke dvěma cílům tohoto dokumentu, resp. jej vnímat jako součást souboru opatření k plnění této strategie. Jde o:

- cíl „posílit účelovou podporu institucí, jejichž výsledky se uplatňují v praxi a účelovou podporu aplikovaného společenskovědního výzkumu“ cestou „zapojování firem do projektů výzkumu s výzkumnými organizacemi při soukromém kofinancování“ (kap. Financování a hodnocení výzkumu a vývoje). Tomu odpovídá zaměření programu na spolupráci akademické a podnikové sféry i důraz na uživatelsky podmíněné vlastnosti výsledků, které jsou v segmentu bezpečnostních technologií pro uplatnění v praxi klíčové. Kofinancování je dáno limity veřejné podpory podle evropské legislativy.

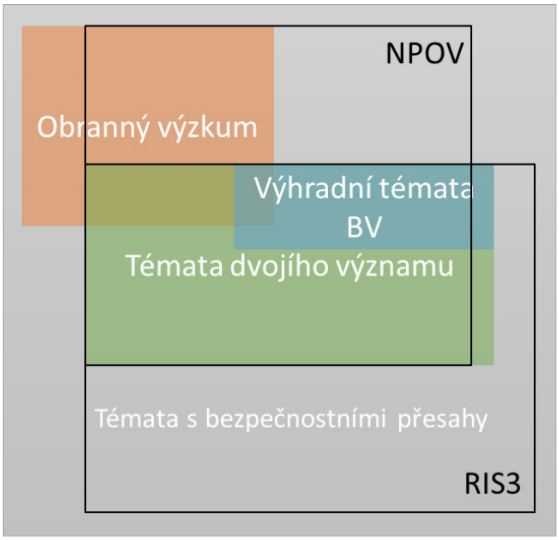
- cíl „podporovat zavádění výsledků aplikovaného výzkumu v oblasti transformativních technologií do praxe“ cestou „podpory ve výzvách národních programů VaVaI pro technologická řešení a inovace v oblasti automatizace, robotizace a umělé inteligence“ (kap. Digitální stát, výroba a služby). Tato tři témata jsou velmi podstatnou součástí předvídatelných inovací v oblastech vymáhání práva nebo krizového řízení, což jsou primární funkce státu.

11.3 VAZBA NA NPOV A RIS3

Při hodnocení vazeb programu na NPOV a RIS3 je nutné mít na paměti kontext vzniku všech dotčených dokumentů. V první řadě jde o NPOV, jejichž vznik, podmíněný dobovou situací, nebral nijak v potaz inovační potřeby bezpečnostního systému. Složení pracovní skupiny nebylo s ohledem na úkoly bezpečnostního systému v žádném případě reprezentativní a dostupné „priority“ to jen prokazují.

Klíčovým dokumentem, který také vykazuje nejdetailnější vazbu na bezpečnostní politiku a její potřeby, díky dříve nevídané hloubce obsahové analýzy této politiky, je MKBV2017+. Ta člení obsah bezpečnostního výzkumu na 3 kategorie – nejširší „témata s bezpečnostními přesahy“ kde je žádoucím společenským přínosem dlouhodobá stabilita, spolehlivost a udržitelnost společenských, ekonomických a environmentálních systémů, přes témata dvojího významu, kde je žádoucím společenským přínosem snižování rizik a zvyšování odolnosti, až po výhradní témata BV, která cílí na posilování schopností bezpečnostního systému. Z podstaty věci jde vždy o podmnožiny, tj. posilování schopností bezpečnostního systému přispívá snižování rizik a zvyšování odolnosti společnosti, což zvyšuje stabilitu, spolehlivost a udržitelnost širších společenských systémů.

[34] Usnesení vlády č. 104/2019



Obrázek 6: schematické znázornění obsahového rozsahu témat bezpečnostního výzkumu v různých dokumentech[35]

Posledním dokumentem v pořadí, který nabízí určitou formu systematizace zájmového pole bezpečnostního výzkumu je kap. „Společenské výzvy" RIS3 strategie **po aktualizaci v roce 2018**. Ta plně transponuje závěry MKBV2017+ a proto reflektuje pohled na rozsah a obsah bezpečnostního výzkumu daný závěry pracovní skupiny k MKBV2017+ a v důsledku také všech strategických dokumentů z oblasti bezpečnostní politiky, které MKBV2017+ shrnuje. Protože jde o dokument s velmi rozsáhlou platností a uplatněním v celé řadě politik, nejen té striktně bezpečnostní, byla v rámci tvorby podkladů využita ta nejširší možná konceptualizace bezpečnosti, která zahrnuje i témata mimo poskytovatelskou roli MV. Je také vhodné připomenout, že v tomto dokumentu nejsou zahrnuty dřívější ani novější obsahová vymezení obranného výzkumu. Vzdor populární představě totiž bezpečnostní a obranná politika nejsou v natolik zásadním překryvu, zejména pak ne, pokud jde o výzkumnou podporu inovačních potřeb.

Propojením všech konceptů z celé této palety dokumentů vzniká Obr. 4. Vzhledem k tomu, že se Program zaměřuje na širší spektrum priorit MKBV2017+, zahrnující i některá témata s bezpečnostními přesahy, **je možné deklarovat, jeho plnou shodu s RIS3 a významnou shodu s NPOV**. **Konečný rozsah shody s NPOV nelze stanovit dříve, než bude známa množina podpořených projektů a jejich zaměření.**

Program přímo nepracuje s konceptem znalostních domén z RIS3 strategie. K posílení jejich podpory je určen program SECTECH. Z hlediska konformity s RIS3 lze tedy program označit za nástroj jejího plnění v aplikační doméně „Bezpečnostní výzkum". Přínos v jednotlivých znalostních doménách lze potom opět hodnotit až na základě výsledků veřejných soutěží a charakteru podpořených projektů.

11.4 Eliminace překryvů s ostatními poskytovateli

Z programů ostatních poskytovatelů podpory lze očekávat potenciální překryvy zejm. u TAČR, mj. pro jeho implementační roli u programů MD a MŽP, dále u MO a MPO. Řešení rizika překryvů je v každém případě nutné nahlížet jinak, protože ne všechny dotčené programy jsou formulované skrze stejný přístup a se stejnou hloubkou věcného vymezení. Tato kapitola shrnuje některá opatření pro eliminaci těchto rizik.

[35] Velikost jednotlivých obrazců nutně nevypovídá o rozsahu

11.4.1 TAČR

U programů TAČR, které nejsou připravovány jako implementace priorit jiných resortů je nejzásadnějším opatřením pro zabránění duplicitám vzájemná koordinace a spolupráce na vyhodnocení sporných případů. Situaci komplikuje nestejný přístup k vymezování programů – klíčem k unikátnímu programu není vždy věcná stránka, ale např. typ podporovaného subjektu nebo vědní oborové zaměření. Samostatným případem jsou potom programy Center kompetence, kde k překryvu v limitním rozsahu dochází, a to z toho důvodu, že MV obdobným programem nedisponuje. Ani u CK však nedochází k narušení kompetenčního rozložení podle priorit MKBV2017+.[36] Stejná situace potom panuje u programu DELTA, kde opět neexistuje ekvivalent MV a některá témata jsou zařazena po vzájemné dohodě.

11.4.2 Doprava 2020+

Program Doprava 2020+, realizovaný TAČR ve prospěch MD se ostatní praxi spolupráce s agenturou vymyká. Potenciál překryvu představuje především následující pasáž:

> 2) Bezpečná a odolná doprava a dopravní infrastruktura Specifický cíl se zaměří na vývoj nových metod a standardů pro dopravní infrastrukturu a dopravní prostředky, které povedou k trvalému snižování nehodovosti a souvisejícím škodám na životech, zdraví i majetku. Výzkum se dále zaměří na zajištění odolnosti a spolehlivosti (resilience) dopravních prostředků, infrastruktury, informačních a komunikačních systémů a jejich služeb a také jejich bezpečnosti nejen ve významu „safety“ (zejména snížení nehodovosti), ale také odolnosti dopravní infrastruktury ve smyslu odolnosti vůči přírodním vlivům v důsledku očekávaných změn klimatu nebo ve smyslu odolnosti vůči terorismu včetně kaskádových efektů selhání prvků dopravní infrastruktury a jejich potenciálních dopadů na ostatní sektory. Výzkum se bude také věnovat progresivním systémům řízení provozní bezpečnosti, které využívají pokročilé formy analýzy a řízení rizik. V rámci výzkumu budou využívány moderní simulační a vizualizační nástroje, včetně systémů virtuální reality. Dále bude důraz kladen také na zajištění bezpečnosti informačních systémů v oblasti dopravní infrastruktury, jejíž zajištění je v současné době stále více aktuální. V rámci výzkumu bude zohledněna spolupráce s bezpečnostními složkami a související výměna informací.

Při formulaci programu zjevně nebyla věnována dostatečná pozornost vzájemnému vymezení obou programů a za rizikovou lze považovat především poslední část, týkající se činnosti bezpečnostního systému na dopravní infrastruktuře, která se může překrývat i s jádrem priorit BV. Na druhou stranu zmínky o terorismu lze v kontextu etablované praxe v řešení této hrozby považovat za zcela bezrizikové.

Protože navrhovaný program OpSec navazuje na širokou paletu strategických dokumentů bezpečnostní politiky i aktualizovanou Koncepci rozvoje PČR, nepovažoval autor za vhodné téma bezpečnosti dopravní infrastruktury zcela vyřadit (přestože výše uvedený text prakticky nedává prostor pro věcné oddělení). Téma je tak zahrnuto ve třetím podprogramu obecnou formou, ale s důrazem na vymáhání práva, které by mezi podpořenými projekty mělo dominovat. Naopak, otázka vylepšování stavebních materiálů apod. by z tohoto programu podporována být neměla, protože se očividně vztahuje k Doprava2020+.

Pro řešení překryvů zde bude klíčový proces identifikace duplicit.

[36] Centra, u kterých dochází k překryvu se orientují na různé formy bezpečnosti infrastruktur, což je téma, u kterého MKBV2017+ uznává možnost vstupu jiných poskytovatelů.

11.4.3 Ministerstvo životního prostředí

Podobně, jako v případě programu Doprava 2020+ je i zde situace přehledná. Program MŽP, který na několika místech odkazuje na problematiky environmentální bezpečnosti (kde MV překryvy akceptuje a považuje za přirozené) a environmentální kriminality (kde by MV trvalo na výhradní roli, kdyby zde roli vymahatele práva nehrála také Česká inspekce životního prostředí), je implementován v TAČR.

I zde tedy bude klíčový proces identifikace a vyhodnocení duplicit. Protože je spektrum aktérů v těchto tématech relativně malé, bude celá věc snazší.

11.4.4 Ministerstvo obrany

U Ministerstva obrany lze očekávat komplementaritu, spíše než překryvy. Je to dáno specializovanou povahou obou problematik, kde přirozené překryvy existují, zejm. v oblastech CBRN a kyberbezpečnosti, případně některých telekomunikačních a senzorových technologií. Nejde však o překryv natolik zásadní, aby hrozilo neefektivní financování. Programy MO striktně reagují na potřeby armády a jsou realizovány pouze cestou veřejných zakázek na služby ve výzkumu a vývoji. Už to samo o sobě dává dostatečný prostor pro případnou koordinaci.

Na druhou stranu je MV největším donorem účelové podpory pro výzkumné organizace v resortu, a to právě proto, že široce podporuje uvedené dvě hlavní problematiky společného zájmu. Další koordinace obou ministerstev je tedy žádoucí. I proto se v tomto programu, jako tradičně, předpokládá zapojení zástupce MO do poradního orgánu, aby vznikl další kanál pro výměnu informací o rizikových projektech.

11.4.5 Ministerstvo průmyslu a obchodu

MPO je ve zcela specifické pozici. Dlouhodobě spravuje finančně významný a pouze omezeným způsobem vyhraněný program, který ale překryvy s programy MV nevykazuje, pokud ano, pak v jednotkách projektů za celá programová období.[37] Na druhou stranu existuje řada programových aktivit MPO, které nejsou striktně spojené s rozpočtem na výzkum a vývoj, ve kterých je riziko větší, zejm. v poslední době v rámci tzv. reakce na epidemii Covid-19.

Vedle toho lze jistou míru pozitivního překryvu hledat u aktivit podřízených agentur. V nedávné době byla ohlášena řada akceleračních programů, z nichž jeden se orientuje na reakce na krize a ústy reprezentantů CzechInvestu má ambice inkubovat bezpečnostní technologie.

Z toho plyne minimální riziko z dlouhodobě minimální koordinace ve věci výzkumných a vývojových programů, přestože to teoreticky prostor pro duplicity je. Ukazuje se, že ty, které se zde vyskytují spíše plynou z minimální informovanosti o programech BV a tradiční relaci uchazečů s MPO, než ze snahy systém překonat. Je také nutné dodat, že dosavadní přístup MPO ke koordinaci nebo k věcnému vymezení vlastních programů vůči ostatním poskytovatelům byl spíše antagonistický.

U akcelerátoru a dalších aktivit, které přímo nespadají do výzkumného a vývojového financování je třeba spíše hledat a využívat synergie, zejm. i programu SecTech, částečně i zde, v programu OpSec. To je ale věc koordinace budoucí, bez vlivu na programové parametry.

[37] TC AV (2016) *Souhrnná výzkumná zpráva o stavu prostřední bezpečnostního výzkumu v ČR*

12 ANALÝZA VAZBY NA PLATNÉ DOKUMENTY BEZPEČNOSTNÍ POLITIKY

Strategické dokumenty bezpečnostní politiky tvoří složitý relační (nikoliv hierarchický) systém. V rámci přípravy MKBV2017+ byla provedena analýza těchto relačních vztahů z 22 platných a relevantních dokumentů, které vznáší požadavky na bezpečnostní výzkum a/nebo definují inovační směry a priority. Z těchto dokumentů byla vytvořena mapa relačních vztahů 93 bezpečnostních hrozeb, kterým je věnována pozornost, a 94 inovačních potřeb.[38] Nestejná úroveň (míra detailu) nejen mezi dokumenty, ale i uvnitř sledovaných dokumentů, prakticky znesnadňuje rozumný výběr a přímé zahrnutí.[39]

Výsledkem procesu obsahové analýzy je proto formulace prioritizovaného věcného vymezení bezpečnostního výzkumu, které prezentuje MKBV2017+, a ve kterém jsou sjednoceny charakteristické požadavky napříč celým spektrem výše studovaných dokumentů.[40] V Programu se předpokládá financování projektů v plném spektru zájmových oblastí ze všech 3 prioritních cílů podpory bezpečnostního výzkumu:[41]

Efektivní zásah (cíl v prioritě řešení bezpečnostních incidentů)

Zasahující personál budoucnosti je schopen 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.

V rámci tohoto prioritního cíle jsou rozvíjeny následující zájmové oblasti:

- Včasná výstraha a situační přehled
- Efektivní intervence
- Vyšetřování incidentů

Adaptabilní bezpečnostní systém (cíl v prioritě rozvoj bezpečnostního systému)

Základem uvažování o bezpečnosti jsou prediktivní analýza, soustavná analýza rizik, modelování, simulace a evaluace. Bezpečnostní systém budoucnosti z nich těží a promítá jejich závěry do regulace i plánování na všech rozhodovacích úrovních. Jednotlivé bezpečnostní složky a součásti bezpečnostního systému se vnitřně vyvíjí a optimalizují vlastní plány, postupy, řídící 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.

V rámci tohoto prioritního cíle jsou rozvíjeny následující zájmové oblasti:

[38] Alespoň vzdáleně relevantních pro bezpečnostní výzkum, potřeby typu zvýšení rozpočtu nebo navýšení počtů personálu nebyly zahrnuty.

[39] Bezpečnostního výzkumu se na této úrovni navíc dotýkají i další dokumenty, jako např. strategie Průmysl 4.0, kterou materiál také zohledňuje.

[40] Na věcném vymezení bezpečnostního výzkumu, včetně jeho prioritních cílů panuje široký konsensus napříč zainteresovanými stranami, neboť se valná většina součástí bezpečnostního systému podílela na práci komise, která MKBV2017+ formulovala.

[41] Prioritní cíl 2 „Adaptabilní bezpečnostní systém“ nezahrnuje priority vhodné k realizaci v tomto program.

- Bezpečnostní politika a krizové řízení
- Vnitřní schopnosti součástí bezpečnostního systému
- Management bezpečnostních informací

Resilientní komunity (cíl v prioritě snižování rizik a zvyšování odolnosti)

Kultura bezpečnosti proniká i do uvažování o službách, prostředí a společnosti. Prostor, společenství i jeho klíčové podpůrné systémy se proaktivně zapojují do opatření ke snižování rizik katastrof nebo protispolečenských jevů, přičemž si zachovávají značnou míru tolerance rizika. Rozvíjí se předpoklady pro zachování kontinuity služeb a přístupu k nim a respektu k základním společenským hodnotám a potřebám zranitelných skupin obyvatelstva v průběhu krizové situace nebo pod tlakem protispolečenských jevů. Infrastruktury a jejich kritické prvky i části veřejného prostoru jsou navrhovány a stavěny tak, aby odolávaly přírodním katastrofám, haváriím i projevům protispolečenského chování a umožňovaly flexibilní, kontrolované využití v době krizové situace a rychlou obnovu. Proaktivní bezpečnostní kontrola, jako prvek zvyšování odolnosti, je přizpůsobena dynamice pohybu osob a zboží, i standardům lidských práv a zachování důstojnosti jedince. Komunity zasažené závažným bezpečnostním incidentem jsou schopny se s nimi rychle a úspěšně vypořádat, včetně minimalizace okamžitých i dlouhodobých a chronických následků.

V rámci tohoto prioritního cíle jsou rozvíjeny následující zájmové oblasti:

- Bezpečný veřejný prostor
- Bezpečnost infrastruktur
- Environmentální bezpečnost

Program svým zacílením plně koresponduje s aktuální Národní RIS3 strategií, ve které je bezpečnostní výzkum jako nadresortní a multioborový nově obsahově akcentován v doménách výzkumné a inovační specializace a zároveň naplňuje také konkrétní společenskou výzvu „Zvýšená bezpečnostní rizika a proměnlivost bezpečnostních hrozeb“, která spadá do gesce Ministerstva vnitra a má též vazbu na resortní programy podpory bezpečnostního výzkumu. Základním principem jednotlivých misí v této výzvě je cestou systematického využívání i budování výzkumných kapacit získávat a efektivně rozvíjet inovativní znalosti, metody a technologie, které umožňují bezpečnostnímu systému ČR a jeho zainteresovaným partnerům čelit současným i budoucím rizikům, která plynou z uvedených měnících se realit bezpečnostního prostředí. Mise v této společenské výzvě primárně cílí na prioritní cíle MKBV2017+, a to na Efektivní zásah a Adaptabilní bezpečnostní systém.

Národní priority orientovaného výzkumu jsou v tomto směru selektivní podmnožinou obou dokumentů, přičemž dominantní překryv lze shledat s MKBV2017+.

Podporovaná témata budou dále specifikována v návazných dokumentech, zejména v zadávacích dokumentacích k jednotlivým veřejným soutěžím. Specifikace umožňuje reagovat na silné stránky českého výzkumného prostředí a přiblížit program dalším strategickým iniciativám, které bezpečnostní výzkum a priori nezmiňují (např. Strategie AI).

Naproti tomu, některé dokumenty, klíčové pro přípravu MKBV2017+ byly v minulém období pozměněny. Níže proto komentujeme změny nejvýznamnější.

12.1 KONCEPCE ROZVOJE POLICIE ČR

Současný dokument je v mnohém znatelně přehlednější než jeho předchůdce. Lze na něm proto stavět jak vymezení podprogramu 1 (přímý důsledek zohlednění tohoto dokumentu v programu), tak

přenést některá témata do podprogramů ostatních. Autor při tom vychází z vymezení nejvýznamnějších hrozeb, se kterými koncepce pracuje a z dílčích cílů a témat, která dokument identifikuje v reakci na tyto hrozby.

Nová koncepce se místy přibližuje žádoucímu chápání rozvoje bezpečnostního sboru jako rozvoje – schopností – naplňovat očekávání, což je přístup shodný s MKBV2017+. I proto operacionalizujeme jednotlivá témata obdobným, způsobem a v jednotlivých podprogramech očekáváme jak referenci vůči tématům výzev, tak zároveň vůči schopnostem, které se s nimi pojí. V rámci snahy o efektivní získání nejvhodnějších témat jsou reflektovány také některé nově vzniklé vnitřní koncepční dokumenty policie, které identifikují témata či zájmové oblasti, ne vždy v inovačním kontextu, která ale lze v rámci snahy o inovace propojit se silnými stránkami českého výzkumného a vývojového prostředí.

Referenční hrozby

Koncepce rozvoje PČR

- Boj proti terorismu a extremismu
- Boj proti obchodu s drogami
- Potírání kybernetické kriminality
- Boj proti korupci a hospodářské kriminalitě
- Potírání nelegální migrace

Dílčí témata podle koncepce a dalších relevantních dokumentů

- Adaptace na změny charakteru kriminality (včetně zahrnutí nově vydané **Koncepce boje proti environmentální kriminalitě**)
- Policejní analytika (včetně reflexe nově vydané **Koncepce policejní analytiky**)
- Efektivní nástroje pro podporu trestního řízení
- Moderní nástroje forenzního zkoumání

12.2 KONCEPCE ENVIRONMENTÁLNÍ BEZPEČNOSTI

U novelizované Koncepce environmentální bezpečnosti je situace svým způsobem jednodušší. Koncepce ve svém textu přímo uvádí úkoly, spojené s problematikou bezpečnostního výzkumu. Konkrétně jde o:

- 3.3 Podporovat realizaci výzkumu transformujících se hrozeb a jejich kombinací a přenos výsledků do praxe
- 3.3.2. Začlenit oblast environmentální bezpečnosti a snižování rizika katastrof do navazujících programů bezpečnostního výzkumu

Jde však o formulace velmi obecné, které umožňují řadu různých interpretací a zároveň se do značné míry překrývají s existujícím programem MŽP, realizovaným na TAČR. Poskytovatel se problematiky environmentální bezpečnosti nezříká a opět konceptualizuje uvedená témata do několika dílčích cílů podprogramu, který je k tomu určen. V návaznosti na požadavek této koncepce se také zavádí do hodnocení programu indikátor „počet projektů zaměřených na environmentální bezpečnost“ bez prahové hodnoty, za účelem monitoringu této zájmové oblasti.[42]

[42] Prahovou hodnotu jednak koncepce nepožaduje, dále ji nelze v otevřené soutěži vymáhat a tedy zajistit plnění

13 ANALÝZA RIZIK

Uvedena v textu programu

13.1 POTENCIÁLNÍ NEGATIVNÍ DOPADY PROGRAMU

Autor studie si není vědom hodnověrné debaty o negativních dopadech financování bezpečnostního výzkumu z veřejných prostředků v žádné ze zemí, které toto financování nabízí.

Nejbližší této charakteristice je debata v americkém akademickém prostředí z přelomu minulé dekády, vztahující se ke konkurenci při náboru lidských sil, kterou generuje soutěž mezi privátním a vládním obranným výzkumem. Její podstatu lze shrnout tak, že lze dokumentovat, že při rychlém nárůstu financování může tato soutěž vytlačit cenu práce a tím de facto výrazně zneefektivnit celý systém financování. Je ale třeba dodat, že celá studie vychází z partikulárního prostředí US obranného (nikoliv bezpečnostního) výzkumu, který zároveň táhnou vládní finance a privátní realizátoři, při zachování silného vládního výzkumného sektoru.

V tom směru nejde o situaci, která by byla, byť jen vzdáleně, srovnatelná s kteroukoliv podporou bezpečnostního výzkumu, v USA nebo v Evropě, tím méně v ČR. Strukturální podmínky jsou natolik odlišné, že se k této debatě nelze odvolávat.

14 DOPORUČENÍ EX-ANTE HODNOTITELŮ

Ing. Michal Pazour, Ph.D. – Technologické centrum Akademie věd ČR, s.r.o. (nebo jiný zástupce oddělení strategických studií TC AV)

- oddělení je ve vědní politice jediným expertním pracovištěm v ČR, zároveň zde existuje elementární povědomí o specifických požadavcích na bezpečnostní výzkum i o způsobu, jakým se má ex-ante hodnocení realizovat

Mgr. Martin Duda – Centrum podpory inovací VŠB-TUO, člen předsednictva Technologické agentury ČR[43]

Zároveň se doporučuje pro ex-ante hodnotitele vypracovat strukturovaný požadavek, odpovídající návrhu nového postupu schvalování programů a zvážit jejich finanční ohodnocení obdobné odměnám za hodnocení nejkomplikovanějších projektů ve veřejné soutěži.

[43] Je nutné zdůraznit mlčenlivost ve vztahu k ostatním členům předsednictva a vedení kanceláře TAČR minimálně do otevření meziresortního připomínkového řízení, resp. projednávání programu v RVVI.

PŘÍLOHA 1: VARIANTY ČLENĚNÍ PROGRAMU

Nejzásadnějším problémem pro dopracování návrhu programu SOUTĚŽ 3 je v tuto chvíli nedokončený koncept struktury programu. Tento dokument přináší základní varianty pro rozhodování o celém nastavení programu. Členění programu ovlivňuje efektivitu různých možných postupů hodnocení a ty potom ovlivňují portfolio projektů, které ze soutěží vzejde. Varianty tedy toto východisko zohledňují a propojují členění a hodnocení. Skutečné rozhodnutí, které je nezbytné učinit, se potom reálně vztahuje spíše k očekáváním, která poskytovatel od programu, resp. od podpořených projektů má.

Dokument vychází z MKBV2017+ v tom smyslu, že předpokládá realizaci projektů napříč spektrem priorit bezpečnostního výzkumu, jak je tato koncepce definuje. To však nezbytně neznamená, že se toto členění musí propsat do formulace programu. Nelze zapomínat na to, že MKBV2017+ stanoví celé zájmové pole BV a jeho členění. To v praxi znamená, že všechny podpořené projekty musí do tohoto členění zapadat, nikoliv, že jej programy musí (slepě) kopírovat. Členění podle MKBV2017+ lze použít jak k obraznému vertikálnímu členění, tak k pomyslně horizontálnímu – vymezení podprogramů.

Všechny uvedené varianty jsou z hlediska administrativní náročnosti velmi podobné. Předpokládají realizaci soutěží, které vždy zahrnou všechny podprogramy. Členění má především administrativní význam, který zpřesňuje a koriguje hodnocení a zároveň ovlivňuje objem prostředků, který lze na jednotlivá témata vydat.

Jednotlivé varianty se také liší hodnotícími postupy. Ty jsou konstruovány tak, aby přesně dopovídaly konceptu dané varianty a zároveň omezovaly metodologické nešvary, které předchozí generace programu vykazovaly. Zejména jde o malou diverzitu názorů na jednotlivá témata v Radě.[44] Dále jde o porovnávání neporovnatelného v tom smyslu, že soutěže a hodnotící systém míchají zcela odlišné typy projektů i naprosto odlišná zacílení do jednoho celku. Jakákoliv srovnání pak logicky pokulhávají z pohledu kredibility.

VARIANTA 1 – BEZ PODPROGRAMŮ

Tato varianta vychází ze zcela otevřeného konceptu programu. Představa o fungování nástroje je zde taková, že sama otevřenost a „kolektivní kvalita“ hodnocení zajistí financování těch nejlepších projektů s potenciálem pro nejvyšší dopady. Zároveň, tato varianta předpokládá, že poskytovatel nemá strukturované priority (tj. že nepreferuje některé dílčí cíle nad jinými) a nemá potřebu korigovat rozsah podpory, která bude/může být vydána na témata z hlediska MKBV2017+ periferní.

Jak členit?

V této variantě nedochází ke členění na podprogramy.

Jak hodnotit?

Kdo hodnotí:

- Rada programu, kterou tvoří nominanti uživatelských organizací a oborových spolků
- Oponenti, kteří se přidělují ad hoc podle oborové (a výlučně oborové) shody z databáze oponentů TAČR (z celé její šíře, bez zohlednění individuálního „přihlášení“ k BV)

[44] Obecná diverzita je naopak vysoká, Rady programů jsou dosud velmi reprezentativní; nenabízí ale možnost srovnání názorů v jednotlivých dílčích tématech, která jsou obvykle zastoupena jedním až dvěma odborníky.

Postup a cíle hodnocení

A, hodnocení BK a způsobilosti pro program Radou

B, hodnocení výzkumné relevance a projektového nastavení oponenty

C, hodnocení uživatelských parametrů navrhovaných výsledků (v rozsahu cca 35 – 40% bodů, lze zvážit hodnocení efektivity návrhu, tj. uživatelských parametrů za vložené prostředky – viz MKBV2017+) zpravodajem Rady

Nejde o koncept zcela nový, navazuje na zkušební postupy realizované v programu VI v první a druhé veřejné soutěži. Je vhodné připomenout, že výsledky těchto soutěží byly přijaty lépe, než zásahy Rady do jednotlivých hodnocení nebo model korekcí zpravodajem.

Postup hodnocení by tedy měl být následující:

1. V rámci soutěže se uchazeč hlásí k dílčím cílům, to ale nemá na proces hodnocení vliv
2. Rada programu:
   2.1. Hodnotí BK související se způsobilostí pro program
3. Oponentní hodnocení způsobilých projektů
   3.1. V případě, že rozdíl v hodnocení oponentů překročí hranici, automaticky se poptává třetí posudek
4. Uživatelské hodnocení zpravodajem Rady, ta by měla sledovat standardní distribuci hodnocení (tj. každý zpravodaj by měl mít možnost vysoce hodnotit pouze určité procento projektů, podobně u hodnocení nízkých, tomu by měla odpovídat kalibrace hodnocení a související body).
5. Rada sjednotí hodnocení oponentů a uživatelů podle následujícího klíče:
   5.1. Oponentní hodnocení je průměrem všech realizovaných posudků
   5.2. Celkové hodnocení projektu je součtem oponentního hodnocení a uživatelského hodnocení

Výsledky hodnocení

Výsledkem hodnocení je jeden seznam projektů doporučených k podpoře na základě bodového zisku. Další úkony se neprovádí.

Výhody

- Minimální požadavky na organizaci práce při hodnocení
- Není nutné vyhodnocovat předchozí poptávku pro nastavení limitů podprogramů

Nevýhody

- Jde prakticky o pokračování stávající praxe dohadování se nad seznamem vzájemně neporovnatelných návrhů
- Pokračuje problém se závěrečným i dopadovým hodnocením, který plyne z naprosto nepředvídatelného portfolia projektů
- Zachovává prostor pro dominantní jednotlivce v radě prosazovat své preference (ne vždy nevyhnutelně preference nominující organizace)
- Komplikuje uživatelské hodnocení, zejm. v oblastech mimo přímou působnost bezpečnostního systému
- Neumožňuje řídit alokaci na téma a může se tak snadno stát (a nasvědčuje tomu i průzkum absorpční kapacity), že převládnou témata periferní zájmu bezpečnostního systému, u kterých se ještě obtížněji vyhodnocuje implementace a dopad.

VARIANTA 2 – PODPROGRAMY PODLE TEMATICKÝCH OKRUHŮ

Tato varianta vychází z představy, že otevřenost soutěžního nástroje představuje zároveň jeho největší slabinu, a proto je třeba program důkladně korigovat. Stanoví proto nástroje předběžné kvalifikace zájmových oblastí, ve kterých lze vymezit cíle natolik specifické a uživatelskou odbornost natolik jednoznačnou, aby bylo možné tyto korekce realizovat na základě širokého konsensu (především uživatelů). Zároveň varianta předpokládá, že snahou poskytovatele sice je reflektovat poptávku, ale při tom udržet koncentraci financování v oblastech s nejvyšším dopadem na primární cílový prostor, tedy na schopnosti bezpečnostního systému.

Jak členit?

V této variantě by měl být program členěn podle tematických os na:

- PP1: Kybernetická a informační bezpečnost;
- PP2: Boj proti závažné trestné činnosti;
- PP3: CBRN ochrana;
- PP4: Prevence rizik katastrof a incidentů s vysokým počtem obětí;

Detailní témata v podprogramech lez definovat na základě různých dokumentů bezpečnostní politiky, ale není to zcela nutné. Vertikální členění projektů napříč podprogramy by mělo odpovídat prioritám koncepce. K těm by se uchazeči měli hlásit, ale nejsou pro management programu určující.

Jak hodnotit?

Kdo hodnotí:

- Rada programu, kterou tvoří vždy 2 zástupci každého ze 4 uživatelských panelů (v případě, že management MV preferuje nominace, je vhodné nominace poptat právě a jedině do Rady programu).
- Uživatelské panely, které tvoří nestejný počet reprezentantů uživatelských organizací, které jsou pro téma daného podprogramu relevantní; panel je hodnotící odborné těleso, nespravuje program, skládá je proto OBVPV na co nejširším základě; zástupce do Rady zvolí panely ze svého středu na inauguračním jednání, členem panelu je vždy reprezentant OBVPV (typicky předseda Rady programu)
- Oponenti, kteří se přidělují ad hoc podle oborové (a výlučně oborové) shody z databáze oponentů TAČR (z celé její šíře, bez zohlednění individuálního „přihlášení“ k BV)

Postup a cíle hodnocení

Tato varianta zahrnuje několikastupňové hodnocení. Snahou navrženého systému hodnocení je zajistit, aby specifické otázky související s projektem hodnotil vždy ten nejpovolanější orgán. Proto se navrhuje hodnocení rozdělit na:

A, hodnocení BK a způsobilosti pro program

B, hodnocení výzkumné relevance a projektového nastavení

C, hodnocení uživatelských parametrů navrhovaných výsledků (v rozsahu cca 35–40% bodů, lze zvážit hodnocení efektivity návrhu, tj. uživatelských parametrů za vložené prostředky – viz MKBV2017+)

Nejde o koncept zcela nový, navazuje na zkušební postupy realizované v programu VI v první a druhé veřejné soutěži. Je vhodné připomenout, že výsledky těchto soutěží byly přijaty lépe, než zásahy Rady do jednotlivých hodnocení nebo model korekcí zpravodajem.

Postup hodnocení by tedy měl být následující:

1. V rámci soutěže se uchazeč hlásí do skupiny projektů, odpovídající členění na podprogramy
2. Rada programu:
   2.1. Hodnotí BK související se způsobilostí pro program
   2.2. Prověřuje přiřazení způsobilých projektů do jednotlivých skupin
3. Oponentní hodnocení způsobilých projektů
   3.1. V případě, že rozdíl v hodnocení oponentů překročí hranici, automaticky se poptává třetí posudek
4. Uživatelské hodnocení v uživatelských panelech, které zřizuje Rada a které reprezentují maximum zainteresovaných stran; hodnocení reprezentuje konsensus nebo výsledek hlasování v panelu, nikoliv individuální hodnocení zpravodaje panelu. Zároveň by panely měly sledovat standardní distribuci hodnocení.
5. Rada sjednotí hodnocení oponentů a uživatelů podle následujícího klíče:
   5.1. Oponentní hodnocení je průměrem všech realizovaných posudků
   5.2. Celkové hodnocení projektu je součtem oponentního hodnocení a uživatelského hodnocení

Výsledky hodnocení

OBVPV předkládá Radě ke schválení mechanicky provedené výsledky ve 4 samostatných protokolech, které shrnují výsledky hodnocení podle bodů 5.1 a 5.2, kap 3.2.2. Rada vyhodnotí a koriguje případná sporná nebo jinak vadná hodnocení (identifikuje poskytovatel a panely, Rada sama rozpory nevznáší). Rada může projekty z podpory pouze vyřadit, nemůže ale další projekty předřadit nebo posunout do financovaného pásma.[45]

Rada schvaluje 4 seznamy projektů, doporučených k podpoře v rámci limitů každého z výše uvedených podprogramů.

V rámci vyhodnocování celé soutěže může Rada doporučit úpravu limitů pro financování mezi jednotlivými podprogramy, a to do maximální výše 20% alokovaných limitů, při udržení celkového limitu financování soutěže. Pro účely zachování transparentnosti by tyto změny měly reflektovat především výkyvy v rozsahu a charakteru poptávky v jednotlivých programech. Účelové úpravy, přesouvající rozpočet ve prospěch konkrétních projektů by měly být omezeny nižším procentem.

Výhody

- Předznamenává programové členění pro období po roce 2023[46]
- Umožňuje soutěžení jen mezi relevantními tématy, tím také relevantní hodnocení a srovnání.
- umožňuje kontrolu nad finančními alokacemi do jednotlivých témat (nedojde tak k odčerpání vetší části prostředků do periferních témat)
- Metodologicky vzato jde o variantu nejspolehlivější – spolehlivost mezi soudci je v panelovém přístupu výrazně vyšší, což může korigovat i vadná oponentní hodnocení, kde lze spolehlivosti mezi soudci dosáhnout jen velmi obtížně

[45] Mechanismus řešení sporů je třeba dopracovat, realisticky jich ale bude minimum, pokud se dobře nastaví automat na poptávání dalších posudků o velkých rozdílů.

[46] předjímám změnu konceptu programů po roce 2023, opuštění modelu vymezení programu metodou výběru (soutěž – zakázka) a dalšími technickými parametry a zavedení modelu věcného vymezení programů (kyberbezpečnost – boj s organizovaným zločinem atd.), s rozvrstvením každého programu podle typologie projektů. Jde o praxi odpovídající rámcovým programům EU, která se odklání od současné byrokratické formy programování.

- Významně snižuje vliv jednotlivce – člena Rady a diverzifikuje hodnocení.
- Zahrnuje uchazeči dobře přijaté a transparentnější uživatelské hodnocení, které výrazně napravuje nedostatky oponentních řízení (ze zkušenosti z VI).

Nevýhody

- Vyžaduje předběžnou alokaci na podprogramy na základě rozsáhlého vzorku dat, průzkum absorpční kapacity je v tomto směru nedostatečný, protože nemá reprezentativní vzorek
- Umožňuje jen méně flexibilní úpravy mezi alokacemi na základě skutečné poptávky (v rozsahu do 20% financí podle pravidel pro podprogramy)
- složité skládání panelů, protože u podprogramů stále nejde o jasně vyhraněné oblasti zájmu

VARIANTA 3 – PODPROGRAMY PODLE PRIORIT BV

Tato varianta vychází z představy, že otevřenost soutěžního nástroje představuje zároveň jeho jistou slabinu, a proto je třeba program korigovat, zejm. ve vztahu k prioritám MKBV2017+. Stanoví proto nástroje předběžné kvalifikace zájmových oblastí, ve kterých lze vymezit cíle dostatečně specifické, aby bylo možné tyto korekce realizovat na základě vzájemné interakce v širokých, přesto lépe vymezených uživatelských skupinách. Zároveň varianta předpokládá, že snahou poskytovatele sice je reflektovat poptávku, ale také udržet koncentraci financování v tématech s vyšší prioritou z hlediska MKBV2017+ (a v relaci k programům ostatním).

Jak členit?

V této variantě by měl být program členěn podle prioritních os MKBV2017+, a to na:

- PP1: Efektivní zásah
- PP2: Adaptabilní bezpečnostní systém
- PP3: Bezpečná společnost

Uchazeči by se dále měli hlásit do jednotlivých podskupin v jednotlivých tématech tak, jak je vymezuje MKBV2017+.

Detailní témata v jednotlivých kategoriích lze definovat na základě různých dokumentů bezpečnostní politiky, ale není to zcela nutné. Protože ale přetrvává směšování různých typů i témat projektů v jednotlivých podprogramech, vyžaduje tato varianta aktivní přístup poskytovatele při vymezování veřejných soutěží a jejich zužování tak, aby si hodnocení zachovalo alespoň základní míru spolehlivosti.

Jak hodnotit?

Kdo hodnotí:

- Rada programu, kterou tvoří vždy 2 zástupci každého ze 4 uživatelských panelů (v případě, že management MV preferuje nominace, je vhodné nominace poptat právě a jedině do Rady programu).
- Uživatelské panely, které tvoří nestejný počet reprezentantů uživatelských organizací, které jsou pro téma daného podprogramu relevantní; panel je hodnotící odborné těleso, nespravuje program, skládá je proto OBVPV na co nejširším základě; zástupce do Rady zvolí panely ze svého středu na inauguračním jednání, členem panelu je vždy reprezentant OBVPV (typicky předseda Rady programu)
- Oponenti, kteří se přidělují ad hoc podle oborové (a výlučně oborové) shody z databáze oponentů TAČR (z celé její šíře, bez zohlednění individuálního „přihlášení“ k BV)

Postup a cíle hodnocení

Tato varianta zahrnuje několikastupňové hodnocení. Snahou navrženého systému hodnocení je zajistit, aby specifické otázky související s projektem hodnotil vždy ten nejpovolanější orgán. Proto se navrhuje hodnocení rozdělit na:

A, hodnocení BK a způsobilosti pro program

B, hodnocení výzkumné relevance a projektového nastavení

C, hodnocení uživatelských parametrů navrhovaných výsledků (v rozsahu cca 35 – 40% bodů, lze zvážit hodnocení efektivity návrhu, tj. uživatelských parametrů za vložené prostředky – viz MKBV2017+)

Nejde o koncept zcela nový, navazuje na zkušební postupy realizované v programu VI v první a druhé veřejné soutěži. Je vhodné připomenout, že výsledky těchto soutěží byly přijaty lépe, než zásahy Rady do jednotlivých hodnocení nebo model korekcí zpravodajem.

Postup hodnocení by tedy měl být následující:

1. V rámci soutěže se uchazeč hlásí do skupiny projektů, odpovídající členění na podprogramy
2. Rada programu:
   2.1. Hodnotí BK související se způsobilostí pro program
   2.2. Prověřuje přiřazení způsobilých projektů do jednotlivých skupin
   2.3. vyhodnotí poptávku a stanoví limity pro financování v jednotlivých podprogramech, respektující limity pro výzvu jako celek
3. Oponentní hodnocení způsobilých projektů
   3.1. V případě, že rozdíl v hodnocení oponentů překročí hranici, automaticky se poptává třetí posudek
4. Uživatelské hodnocení v uživatelských panelech, které zřizuje Rada a které reprezentují maximum zainteresovaných stran; hodnocení reprezentuje konsensus nebo výsledek hlasování v panelu, nikoliv individuální hodnocení zpravodaje panelu. Zároveň by panely měly sledovat standardní distribuci hodnocení.
5. Rada sjednotí hodnocení oponentů a uživatelů podle následujícího klíče:
   5.1. Oponentní hodnocení je průměrem všech realizovaných posudků
   5.2. Celkové hodnocení projektu je součtem oponentního hodnocení a uživatelského hodnocení

Výsledky hodnocení

OBVPV předkládá Radě ke schválení mechanicky provedené výsledky ve 4 samostatných protokolech, které shrnují výsledky hodnocení podle bodů 5.1 a 5.2, kap 3.2.2. Rada vyhodnotí a koriguje případná sporná nebo jinak vadná hodnocení (identifikuje poskytovatel a panely, Rada sama rozpory nevznáší). Rada může projekty z podpory pouze vyřadit, nemůže ale další projekty předřadit nebo posunout do financovaného pásma.[47]

Rada schvaluje 3 seznamy projektů, doporučených k podpoře v rámci limitů každého z výše uvedených podprogramů.

[47] Mechanismus řešení sporů je třeba dopracovat, realisticky jich ale bude minimum, pokud se dobře nastaví automat na poptávání dalších posudků o velkých rozdílů.

Výhody

- umožňuje kontrolu nad finančními alokacemi do jednotlivých témat (nedojde tak k odčerpání vetší části prostředků do periferních oblastí)
- model uživatelských panelů v tomto případě snižuje riziko ze jmenovacích procesů v uživatelských organizacích (ale méně, než u varianty 2)
- zahrnuje uchazeči dobře přijaté a transparentnější uživatelské hodnocení, které výrazně napravuje nedostatky oponentních řízení (ze zkušenosti z VI).
- alokace lze přímo navázat na průzkum absorpční kapacity

Nevýhody

- neřeší problém slabé spolehlivosti hodnocení, který plyne z porovnávání vzájemně zcela nesouvisejících nebo slabě souvisejících projektů
- Umožňuje jen méně flexibilní úpravy mezi alokacemi na základě skutečné poptávky (v rozsahu do 20% financí podle pravidel pro podprogramy)
- pokud bude alokace přímo vázána na provedený dotazník k absorpční kapacitě, bude největší program MV pravděpodobně zaměřen zejména na periferní témata BV

VARIANTA 4 – MODIFIKOVANÁ V2[48]

Na základě diskuse s OBVPV se navrhuje varianta 4, hybridní model, vycházející z variant 2 a 3. Hlavním důvodem k tomuto návrhu je logistika provozu programu v počátečním období implementace. Při současném a očekávaném rozsahu personálního a technického zajištění není je nutné logickou ambici programu otevřít prostor pro ambiciózní rozvoj po roce 2023 částečně omezit. Zároveň ale varianta reaguje na nutné požadavky revize výběrových procesů a zachovává panely uživatelů, jako fundamentální koncept v hodnocení návrhů.

Efektivní zvládnutí implementace této varianty bude ale vyžadovat tematizaci výzev a obecně hlubší přípravné procesy, protože se do jisté míry sníží tematické restrikce vtělené původně o V2.

Jak členit?

V této variantě pracujeme s konceptem 3 podprogramů, odvozených z variant 2 a 3, s úzkou vazbou na MKBV2017+:

PP1: Vymáhání práva

PP2: Zvládání krizí a incidentů s vysokým počtem obětí

PP3: Bezpečná společnost

V této variantě se doporučuje realizovat dvojí přihlášení projektu – vždy k podprogramu a k cíli programu. Pro PP1 a PP2 lze zpřístupnit přihlašování k prioritám „Efektivní zásah“ a „Adaptabilní bezpečnostní systém“, zatímco v PP3 je nutno se omezit na odpovídající periferie témat MKBV2017+ (s referenčními objekty životní prostředí, veřejný prostor a infrastruktura). U témat, která do jisté míry prochází napříč podprogramy (zvláště kyberbezpečnost) je třeba vytvořit prostor přímo v textu programu a následně jednotlivých výzev.

Identifikaci příslušnosti projektu k prioritě MKBV2017+ lze ale zajistit vlastním kódováním poskytovatele pro potřeby hodnocení této koncepce. Z hlediska provozu programu se jeví jednodušší

[48] Dopracováno na základě konzultace 20/4/2021

identifikovat tematické okruhy podle studie absorpční kapacity a integrovat je s posunem ve strategiích bezpečnostní politiky (tam, kde k posunu došlo).

Nejvhodnějším způsobem zahrnutí kyberbezpečnostních témat je jejich rozlišení podle referenčního objektu. Pokud jde o kybernetickou kriminalitu, její šetření apod. spadá projekt do PP1; pokud jde o ochranu sítí a předcházení „útokům" na infrastruktury institucí, pak spadá do PP3. Tento model je nutné rigidně vymáhat, aby se omezily problémy s nevhodnou alokací projektů posuzovatelům.

Jak hodnotit?

Kdo hodnotí:

- Rada programu, kterou tvoří vždy 2 zástupci každého ze 4 uživatelských panelů (v případě, že management MV preferuje nominace, je vhodné nominace poptat právě a jedině do Rady programu).
- Uživatelské panely, které tvoří nestejný počet reprezentantů uživatelských organizací, které jsou pro téma daného podprogramu relevantní; panel je hodnotící odborné těleso, nespravuje program, skládá je proto OBVPV na co nejširším základě; zástupce do Rady zvolí panely ze svého středu na inauguračním jednání, členem panelu je vždy reprezentant OBVPV (typicky předseda Rady programu)
- Oponenti, kteří se přidělují ad hoc podle oborové (a výlučně oborové) shody z databáze oponentů TAČR (z celé její šíře, bez zohlednění individuálního „přihlášení" k BV)

Postup a cíle hodnocení

Tato varianta zahrnuje několikastupňové hodnocení. Snahou navrženého systému hodnocení je zajistit, aby specifické otázky související s projektem hodnotil vždy ten nejpovolanější orgán. Proto se navrhuje hodnocení rozdělit na:

A, hodnocení BK a způsobilosti pro program, zařazení do podprogramu

B, hodnocení výzkumné relevance a projektového nastavení

C, hodnocení uživatelských parametrů navrhovaných výsledků (v rozsahu cca 35 – 40% bodů, lze zvážit hodnocení efektivity návrhu, tj. uživatelských parametrů za vložené prostředky – viz MKBV2017+)

Nejde o koncept zcela nový, navazuje na zkušební postupy realizované v programu VI v první a druhé veřejné soutěži. Je vhodné připomenout, že výsledky těchto soutěží byly přijaty lépe, než zásahy Rady do jednotlivých hodnocení nebo model korekcí zpravodajem.

Postup hodnocení by tedy měl být následující:

5. V rámci soutěže se uchazeč hlásí do skupiny projektů, odpovídající členění na podprogramy a zároveň ke třídy schopností, odpovídající členění priorit MKBV2017+
6. Rada programu:
   6.1. Hodnotí BK související se způsobilostí pro program
   6.2. Prověřuje přiřazení způsobilých projektů do jednotlivých skupin a toto zařazení případně mění
7. Oponentní hodnocení způsobilých projektů
   7.1. V případě, že rozdíl v hodnocení oponentů překročí hranici, automaticky se poptává třetí posudek
8. Uživatelské hodnocení v uživatelských panelech, které zřizuje Rada a které reprezentují maximum zainteresovaných stran; hodnocení reprezentuje konsensus nebo výsledek hlasování

v panelu, nikoliv individuální hodnocení zpravodaje panelu. Zároveň by panely měly sledovat standardní distribuci hodnocení.

9. Rada sjednotí hodnocení oponentů a uživatelů podle následujícího klíče:
   9.1. Oponentní hodnocení je průměrem všech realizovaných posudků
   9.2. Celkové hodnocení projektu je součtem oponentního hodnocení a uživatelského hodnocení

Výsledky hodnocení

OBVPV předkládá Radě ke schválení mechanicky provedené výsledky ve 3 samostatných protokolech, které shrnují výsledky hodnocení podle bodů 5.1 a 5.2, kap 3.2.2. Rada vyhodnotí a koriguje případná sporná nebo jinak vadná hodnocení (identifikuje poskytovatel a panely, Rada sama rozpory nevznáší). Rada může projekty z podpory pouze vyřadit, nemůže ale další projekty předřadit nebo posunout do financovaného pásma.[49]

Rada schvaluje 3 seznamy projektů, doporučených k podpoře v rámci limitů každého z výše uvedených podprogramů.

V rámci vyhodnocování celé soutěže může Rada doporučit úpravu limitů pro financování mezi jednotlivými podprogramy, a to do maximální výše 20% alokovaných limitů, při udržení celkového limitu financování soutěže. Pro účely zachování transparentnosti by tyto změny měly reflektovat především výkyvy v rozsahu a charakteru poptávky v jednotlivých programech. Účelové úpravy, přesouvající rozpočet ve prospěch konkrétních projektů by měly být omezeny nižším procentem.

Výhody

- Méně pracné než V2
- Netrpí některými neduhy V3 (zejm. oddělením problematik vymáhání práva a zásahů v krizi vytváří prostor pro efektivní vytvoření panelů pro obě oblasti)
- Má užší vazbu na MKBV2017+ než V2
- Stále umožňuje kontrolu nad finančními alokacemi na periferní témata
- model uživatelských panelů v tomto případě snižuje riziko ze jmenovacích procesů v uživatelských organizacích (ale méně, než u varianty 2)
- zahrnuje uchazeči dobře přijaté a transparentnější uživatelské hodnocení, které výrazně napravuje nedostatky oponentních řízení (ze zkušenosti z VI).

Nevýhody

- Snižuje se přehlednost hlavních tematických os BV, které kopírují V2 (tematickou osou je míněno empiricky prokazatelně opakovaně vysoce zastoupené téma v návrzích i v podpořených projektech, které lze považovat za dostatečně ohraničené)
- Vyžaduje precizní formulaci témat podprogramů a rozpracování specializace výzev. Relativní otevřenost programu je třeba nahradit sevřeností výzev
- Umožňuje jen méně flexibilní úpravy mezi alokacemi na základě skutečné poptávky (v rozsahu do 20% financí podle pravidel pro podprogramy)

DOPORUČENÍ

V ČR a na MV dlouhodobě etablovaný model vymezování programů pomocí mechanismu výběru projektů je zásadně problematický. Neumožňuje srovnávání srovnatelného a zároveň neumožňuje funkční nastavení cílů (cílů jako změny stavu). Namísto toho se za cíle vydává tematické rozvrstvení,

[49] Mechanismus řešení sporů je třeba dopracovat, realisticky jich ale bude minimum, pokud se dobře nastaví automat na poptávání dalších posudků o velkých rozdílů.

či omezení obsahu. To má zásadní dopady na spolehlivost hodnotících procesů a tou cestou také na efektivitu vynakládání veřejných prostředků.

Protože současná situace v rámci politiky výzkumu a vývoje neumožňuje tuto běžnou, jakkoliv špatnou, praxi zvrátit a přiblížit se tak efektivnějším zahraničním modelům věcného vymezení programu a jeho naplňování pomocí různých nástrojů (EU, USA), je nutné učinit alespoň některé kroky k prevenci zmírnění negativních dopadů této praxe na navrhovaný program. **To v zásadě vylučuje variantu 1.**

Varianty 2, 3 se liší především tematickým členěním. V kontextu zkušeností s činností Rad programu, zejm. v programech uvedených do praxe v návaznosti na MKBV2017+ se jeví jako nejefektivnější zvolit takové tematické členění, které umožní sestavení maximálně koherentních uživatelských panelů, kde názorová pluralita bude plynout z odlišných pohledů na sdílenou zkušenost s praxí. Ve zkratce: kde nebude nutné konfrontovat pohledy krizového řízení a např. kriminalistickou expertizu. **To splňuje varianta 2**, přestože je z hlediska MKBV2017+ méně intuitivní.

Varianta 3 by také přinesla zafixování v současnosti nastavovaného programového schématu daleko za budoucí koncepci 2023+, která by se právě otázkou opuštění modelu vymezování programu metodou výběru projektů měla zabývat především.

Dlouhodobé negativní trendy v personálním zajištění agendy BV jednoznačně favorizují varianty jednodušší (čti s nižším počtem podprogramů a procesů). Dalším zásadním faktorem je momentální zatížení OBVPV v čase při implementaci programů, zejm. post-projektovými aktivitami. Vedle toho je třeba vzít v úvahu také širší portfolio programů BV, kde již dochází k výrazné podpoře některých témat. **Proto byla vypracována hybridní varianta (V4), která zahrnuje procesní inovace z V2 a V3, zachovává podstatnou a zřetelnou vazbu na MKBV2017+ a zároveň reflektuje tematické osy, které lze v rámci poptávky po podpoře BV dlouhodobě sledovat.**

PŘÍLOHA 2: INTENZITA ZÁJMU O TÉMATA PODLE STUDIE ABSORPČNÍ KAPACITY

		Prio A			Prio B			Prio C			
	Hrozby / schopnosti	Včasná výstraha a situační přehled	Efektivní zásah	Vyšetřování incidentů	Bezpečnostní politika a krizové řízení	Vnitřní schopnosti součástí bezpečnostního systému	Management bezpečnostních informací	Bezpečný veřejný prostor	Bezpečnost infrastruktur	Environmentální bezpečnost	
LEA + ZS	Organizovaný zločin	6	5	7	5	6	6	10	8	3	56
	Ilegální migrace	2	2	3	4	3	4	6	5	3	32
	Terorimus	10	10	5	10	9	5	16	13	10	88
	Špionáž a působení cizí moci	3	2	5	2	3	2	3	5	0	25
	Kriminalita	6	6	10	11	7	6	15	10	4	75
KŘ + HZS	Průmyslové havárie a selhání technologií	15	14	6	16	14	5	16	21	21	128
	Přírodní katastrofy	8	10	3	12	8	4	10	15	15	85
	Epidemiologické hrozby	11	12	5	13	8	5	8	11	15	88
	Požáry, výbuchy a havárie	10	13	5	17	11	5	13	17	19	110
		71	74	49	90	69	42	97	105	90	

PŘÍLOHA 3 – MAPA PRIORIT PROGRAMU VE VZTAHU K MKBV2017+

	posílení schopnosti řešit bezpečnostní incidenty Efektivní zásah			rozvoj bezpečnostního systému Adaptabilní bezpečnostní systém			snižování rizik a zvyšování odolnosti ve společnosti Resilientní komunity		
	Včasná výstraha a situační přehled	efektivní intervence	vyšetřování incidentů	Vnitřní schopnosti bezpečnostního systému	Management bezpečnostních informací	bezpečnostní [50] politika a krizové řízení	Environmentální bezpečnost	bezpečnost infrastruktur	bezpečný veřejný prostor
Organizovaný zločin	1H, G, A, B, C, I; 3A	1H, G, A, B, C, I; 2A, G, H, 3A	1H, G, A, B, C, I, 2G, 3A	2D, E, F, G, H, 3J	1H, G, A, B, C, E, I	1E	1C	3A, D	3H, 3I
Ilegální migrace	1I, A,	1I, A, 2G, H	1I, A, 2G	2D, E, F, G, H, 3J	1I, A, E	1E			
Terorismus	1I, A, B, C,	1I, A, C, D; 2A, B, G, H, 3F	1I, A, B, C, 2G, H	2D, E, F, G, H, 3J	1I, A, B, C, E	1E	3K	3A, B	3F, 3H, 3I
Kriminalita	1H, G, A, B, C,	1H, G, A, B, C, D, 2G, H	1H, G, A, B, C, 2G, H	2D, E, F, G, H, 3J	1H, G, A, B, C, E, 3E	1E	1C, 3K	3A, B, C, D	3E, 3F, 3H, 3I
Průmyslové havárie a selhání technologií	2E, 3G	2A, B, G, H 3A	2C, G, H, 3A	2D, E, F, G, H, 3G, 3J	2E, 3E, 3G		2C, A, B, 3K	3A, B, C, D	3E, 3G, 3H, 3I

[50] Priority v oblasti bezpečnostní politiky a krizového řízení poskytovatel zcela vědomě upozadil ve prospěch jejich disproporční podpory v programu SECPRO, který je podle zkušeností ze dvou generací dřívějších programů pro tyto cíle výhodnější a vhodnější; odpovídá tomu i vyřazení výsledků typu H z akceptovatelných hlavních výsledků tohoto programu

Požáry, výbuchy, havárie	2E	2A, B, G, H 3F	2C, G, H	2D, E, F, G, H, 3J	2E, 3E		2C, A, B, 3K	3A, B, C, D	3E
Přírodní katastrofy	2E, 3L	2A, B, G, H		2D, E, F, G, H, 3J	2E, 3E		2B, 3K, 3L	3B	3E
Epidemiologické hrozby	2E, 3L	2A, B, G		2D, E, F, G, H, 3J	2E, 3E		2B, 3K, 3L		3E
Špionáž a působení cizí moci	1H, G, A, B, C, I; 2G	1H, G, A, B, C, I; 2A, G, 3A	1H, G, A, B, C, I, 2G, 3A	2D, E, F, G	1H, G, A, B, C, E, I			3A, 3D	3I

Elektronický podpis - 6.10.2021
Certifikát autora podpisu :
Jméno : JUDr. Jiří Nováček
Vydal : PostSignum Qualified CA 4
Platnost do : 8.7.2022 10:40:25-000 +02:00