Národní plán výzkumu a vývoje v kybernetické a informační bezpečnosti do roku 2025

OBSAH

1. Úvod 1

2. Cíle a opatření rozvoje VaVaI v kybernetické a informační bezpečnosti 3

2.1 Opatření 1 — Rozvíjet proces sledování nových trendů v kybernetické a informační bezpečnosti a posilování spolupráce mezi veřejným, akademickým, neziskovým a soukromým sektorem 4

2.2 Opatření 2 — Prosazovat prioritní výzkumné oblasti a témata v kybernetické a informační bezpečnosti v rámci programů podpory VaVaI na národní a mezinárodní úrovni 6

2.3 Opatření 3 — Analyzovat potřebu a možnosti vzniku výzkumného programu výlučně pro oblast kybernetické a informační bezpečnosti 7

2.4 Opatření 4 — Zajistit zřízení Národního koordinačního centra výzkumu a vývoje v oblasti kybernetické bezpečnosti a plnění úkolů plynoucích z Nařízení Evropského parlamentu a Rady EU č. 2021/887, kterým se zřizuje Evropské průmyslové, technologické a výzkumné centrum kompetencí pro kybernetickou bezpečnost a síť národních koordinačních center 9

2.5 Opatření 5 — Navazovat mezinárodní spolupráci s důrazem na aktivní účast v rámci společně prováděného výzkumu a vývoje na úrovni EU a NATO 11

3. Prioritní výzkumné oblasti a témata VaVaI v kybernetické a informační bezpečnosti 13

3.1. Umělá inteligence a bezpečnost 13

3.2 Kryptografie a kvantové technologie 14

3.3 Bezpečný hardware, software a bezpečnost dodavatelského řetězce 16

3.4 Vzdělávání a rozvoj schopností 19

3.5 Bezpečnostní politika a krizové řízení 20

3.6 Ochrana osobních údajů a možnosti elektronického dokazování 21

4. Řízení rizik – omezení a předpoklady 22

Seznam zkratek 24

Plán plnění cílů 25

1. Úvod

Bezpečnostní prostředí, ve kterém se ČR aktuálně nachází, prochází zásadní změnou. Tato změna souvisí s prohlubující se závislostí společnosti na digitálních technologiích, což klade značné nároky na zajišťování kybernetické bezpečnosti státu. Nově nastupující technologie (EDTs), jakými jsou umělá inteligence (AI), kvantové technologie nebo autonomní systémy, tento trend v budoucnu významně urychlí[1]. Případné zneužití nově vznikajících technologií tak může způsobit značné škody nejen na kritické infrastruktuře státu, ale i na samotné odolnosti tzv. informační společnosti. Pokud si ČR chce udržet schopnost dlouhodobě čelit novým kyberbezpečnostním hrozbám, je v jejím strategickém zájmu podporovat výzkum, vývoj a inovace (dále jen „VaVaI“) v oblastech nově nastupujících technologií. Strategický význam VaVaI pro zajišťování kybernetické a informační bezpečnosti se mimo jiné odráží v:

- Národní strategii kybernetické bezpečnosti České republiky (dále jen „Národní strategie“)[2];
- Akčním plánu k Národní strategii kybernetické bezpečnosti České republiky na období let 2021–2025 (dále jen „Akční plán“)[3];
- Inovační strategii České republiky 2019–2030[4];
- Bezpečnostní strategii České republiky 2015[5];
- Auditu národní bezpečnosti 2016[6];
- Národní strategii umělé inteligence v České republice[7];
- Národní politice výzkumu, vývoje a inovací České republiky 2021+[8];

[1] Dostupné zde: Science & Technology Trends 2020–2040: Exploring the S&T Edge. 2020. Dostupné z: https://www.nato.int/nato_static_fl2014/assets/pdf/2020/4/pdf/190422-ST_Tech_Trends_Report_2020-2040.pdf.
[2] Dostupné zde: https://www.nukib.cz/cs/kyberneticka-bezpecnost/strategie-akcni-plan/.
[3] Dostupné zde: https://www.nukib.cz/cs/kyberneticka-bezpecnost/strategie-akcni-plan/.
[4] Dostupné zde: https://www.vyzkum.cz/FrontClanek.aspx?idsekce=866015.
[5] Dostupné zde: https://www.vlada.cz/assets/ppov/brs/dokumenty/bezpecnostni-strategie-2015.pdf.
[6] Dostupné zde: https://www.vlada.cz/assets/media-centrum/aktualne/Audit-narodni-bezpecnosti-20161201.pdf.
[7] Dostupné zde: https://www.vlada.cz/assets/evropske-zalezitosti/umela-inteligence/NAIS_kveten_2019.pdf.
[8] Dostupné zde: https://www.databaze-strategie.cz/cz/urad-vlady/strategie/narodni-politika-vyzkumu-vyvoje-a-inovaci-ceske-republiky-2021?typ=download.

- Meziresortní koncepci podpory bezpečnostního výzkumu ČR 2017–2023 s výhledem do roku 2030 (dále jen „MKBV2017+“)[9];
- Koncepci obranného aplikovaného výzkumu, vývoje a inovací na období 2016–2022[10];
- evropských programech veřejné podpory Digitální Evropa nebo Horizont Evropa[11].

Základní strategický rámec zajišťování kybernetické bezpečnosti v ČR je definován v Národní strategii a jejím Akčním plánu. Tvorba a aktualizace Národního plánu je na základě Akčního plánu[12)] v gesci Národního úřadu pro kybernetickou a informační bezpečnost (dále jen „NÚKIB“). Národní plán výzkumu a vývoje v kybernetické a informační bezpečnosti do roku 2025 (dále jen “Národní plán”) je úzce navázán na Národní strategii a reaguje na potřebu strategické koordinace výzkumných a vývojových aktivit na poli kybernetické a informační bezpečnosti. **Cílem Národního plánu je stanovit prioritní výzkumné oblasti v kybernetické a informační bezpečnosti a konkrétní opatření, které mají za cíl stimulovat výzkumné prostředí v ČR, posilovat spolupráci mezi akademickou, soukromou a veřejnou sférou ve výzkumu, vývoji a implementaci technologií v praxi, a rozvíjet zahraniční spolupráci.** Platnost Národního plánu je stanovena do roku 2025. Zhodnocení plnění opatření Národního plánu bude přílohou každoroční Zprávy o stavu kybernetické bezpečnosti ČR.

[9] Dostupné zde: https://www.mvcr.cz/vyzkum/clanek/koncepce-meziresortni-koncepce-podpory-bezpecnostniho-vyzkumu-cr.aspx.
[10] Dostupné zde: https://www.vyzkum.army.cz/sites/vyzkum.army.cz/files/dokumenty/zakladni-stranka/iii_koncepce.pdf.
[11] Dostupné zde: https://digital-strategy.ec.europa.eu/en/activities/work-programmes-digital. Dále zde: https://ec.europa.eu/info/research-and-innovation/funding/funding-opportunities/funding-programmes-and-open-calls/horizon-europe_en.
[12] Akční plán k Národní strategii kybernetické bezpečnosti ČR na období let 2021 až 2025, úkol č. 48: Pravidelně aktualizovat „Národní plán výzkumu a vývoje v kybernetické a informační bezpečnosti“, včetně prioritních výzkumných témat a konkrétních opatření pro naplňování cílů Národního plánu, zejména pak průběžně identifikovat prioritní výzkumná témata, která jsou klíčová pro zabezpečení kyberprostoru ČR a stanovit další cíle včetně konkrétních nástrojů, které přispějí k rozvoji výzkumného a inovačního prostředí v ČR a k prohloubení spolupráce mezi veřejným, soukromým a akademickým sektorem.

2. Cíle a opatření rozvoje VaVaI v kybernetické a informační bezpečnosti

NÚKIB pro potřeby Národního plánu provedl průzkum současného stavu veřejné podpory VaVaI v oblasti kybernetické a informační bezpečnosti. Hlavním zdrojem pro analýzu byl polostrukturovaný dotazník[13)], jehož cílem bylo identifikovat přednosti a nedostatky systému podpory VaVaI v zájmové oblasti. Za jeden z nejvýznamnějších problémů systému veřejné podpory VaVaI respondenti považují nedostatek výzkumných programů a výzev zaměřených výhradně na kybernetickou a informační bezpečnost. Někteří zástupci výzkumné komunity dále hodnotí národní systém podpory VaVaI jako poměrně nepřehledný. Z realizovaného průzkumu rovněž vyplývá, že značná část výzkumné komunity se zapojuje i do mezinárodních programů podpory VaVaI. To přináší především nové kontakty, zkušenosti a přístup k zahraničnímu know-how. Zapojování českých výzkumných týmů do mezinárodních konsorcií je však problematické jak z důvodů velké konkurence a s tím spojené relativně nízké šance na získání finanční podpory, ale především značné administrativní zátěže spojené s vypracováním a předložením projektové žádosti. Zvláště menší výzkumné organizace tento problém vnímají intenzivně a poukazují i na poměrně slabou metodickou podporu v rámci přípravné fáze projektové žádosti. Některé z těchto nedostatků prostředí VaVaI v ČR jsou proto reflektovány i v níže navržených opatřeních.

Národní plán stanovuje tři strategické cíle s ambicí **posílit kybernetickou a informační bezpečnost státu prostřednictvím výzkumných a vývojových aktivit.** Pozornost je primárně zaměřena na rozvoj klíčových výzkumných schopností státu, prioritizaci výzkumných oblastí s ohledem na jejich bezpečnostní přínos a posílení koordinace VaVaI, včetně podpory mezinárodní spolupráce. Přehled cílů:

[13] Respondenty polostrukturovaného dotazníku byli především zástupci Pracovní skupiny pro VaVaI v kybernetické bezpečnosti, Platformy pro výzkum a vývoj v kybernetické bezpečnosti a posléze i další vybraní zástupci veřejného i soukromého sektoru.

Tabulka: Přehled cílů

Cíl 1	**Identifikovat prioritní výzkumné oblasti v kybernetické a informační bezpečnosti a zajistit jejich stabilní podporu prostřednictvím národních a mezinárodních programů VaVaI.**
Cíl 2	**Rozvinout podpůrné, analytické a informační zázemí v oblasti VaVaI v kybernetické a informační bezpečnosti a vytvořit efektivní nástroje koordinace této oblasti.**
Cíl 3	**Nastavit efektivní zahraniční spolupráci a posílit roli ČR v evropském systému podpory VaVaI.**

2.1 Opatření 1 — Rozvíjet proces sledování nových trendů v kybernetické a informační bezpečnosti a posilování spolupráce mezi veřejným, akademickým, neziskovým a soukromým sektorem

Schopnost predikce nových technologických trendů může významně přispět k včasné reakci státu v nastavení systému podpory VaVaI a efektivního zacílení programů veřejné podpory. Pro fungování systému přenosu znalostí a zkušeností je klíčové zajistit úzkou spolupráci mezi akademickým, soukromým, veřejným a neziskovým sektorem. V českém prostředí doposud neexistovala platforma, která by umožňovala vzájemné sdílení zkušeností, potřeb a know-how v oblasti VaVaI mezi subjekty působící v kybernetické a informační bezpečnosti. Možnost vzájemného kontaktu přitom může vést k nalezení vazeb mezi výzkumnými schopnostmi akademické obce a potřebami koncových uživatelů, k zmapování nároků kladených pro uplatnění produktů na trhu nebo k vyhodnocení stavu národní a mezinárodní spolupráce v oblasti VaVaI. Platforma pro výzkum a vývoj v kybernetické a informační bezpečnosti (dále jen „Platforma“) byla ustanovena v roce 2021. Platforma má v tuto chvíli 22 členů a jejím cílem je propojit subjekty soukromé, veřejné a akademické sféry, které se zabývají výzkumem a vývojem v oblasti kybernetické a informační bezpečnosti, přičemž do budoucna je potřeba Platformu nadále rozvíjet.

Nástroje:

1. Spolupráce v rámci Platformy s cílem zintenzivnit vzájemnou komunikaci a výměnu informací.
2. Zpracování výhledové studie technologických trendů v kybernetické a informační bezpečnosti, která bude, mimo jiné, sloužit jako vodítko pro aktualizaci prioritních výzkumných oblastí a témat v kybernetické a informační bezpečnosti.
3. Analýza silných a slabých stránek národního výzkumu a vývoje v kybernetické a informační bezpečnosti s důrazem na identifikaci klíčových výzkumných schopností státu této oblasti.
4. Podpora zapojování koncových uživatelů do výzkumných projektů v oblasti kybernetické a informační bezpečnosti.
5. Podpora vzniku a rozvoje pracovišť zaměřených na oblasti klíčových technologií (KETs)[14] a nově nastupujících a přelomových technologií (EDTs) s důrazem na kooperaci výzkumných týmů napříč ČR s přesahem do zahraničí.

Indikátory:

- Efektivní využívání exitujících kapacit českého výzkumného prostoru a jejich další rozvoj.
- Propojování soukromého sektoru a akademických pracovišť s koncovými uživateli, včetně bezpečnostních složek.
- Zpracovaná výhledová studie technologických trendů v kybernetické a informační bezpečnosti.
- Počet zapojených koncových uživatelů v projektech kybernetické a informační bezpečnosti.
- Vznik nových a rozvoj stávajících pracovišť zaměřených na klíčové technologie (KETs) a nově nastupující a přelomové technologie (EDTs).

[14] Trendy v klíčových umožňujících technologiích: Analytická zpráva o technologických trendech a nově vznikajících technologiích. Technologické centrum AV ČR. Dostupné zde: https://www.tc.cz/cs/publikace/publikace/seznam-publikaci/trendy-v-klicovych-umoznujicich-technologiich.

2.2 Opatření 2 — Prosazovat prioritní výzkumné oblasti a témata v kybernetické a informační bezpečnosti v rámci programů podpory VaVaI na národní a mezinárodní úrovni

Dle Zprávy o stavu kybernetické bezpečnosti za rok 2020[15] stále roste počet kybernetických útoků proti českým institucím a obchodním společnostem ve všech sektorech. Do budoucna je nutné počítat se zvyšující se sofistikovaností nástrojů v rukách útočníků (např. spear-phishing s využitím deepfakes či pokročilé formy ransomware), což bude klást značné nároky na ochranu českého kyberprostoru. Aby ČR udržela krok s dynamickým rozvojem informačních a komunikačních technologií, je zapotřebí takové technologie identifikovat a směřovat veřejnou podporu do jejich výzkumu a vývoje. Omezené zdroje, které jsou na VaVaI k dispozici, je nutné směřovat do klíčových oblastí a maximalizovat jejich dopad na rozvoj excelentního výzkumu v kyberbezpečnosti. NÚKIB proto bude u poskytovatelů veřejné podpory a dalších institucí prosazovat prioritní výzkumné oblasti a témata s cílem zajistit jejich stabilní podporu a dostatečné financování. Poskytovatelé veřejné podpory podle zákona č. 130/2002 Sb., o podpoře výzkumu a vývoje z veřejných prostředků a o změně některých souvisejících zákonů (zákon o podpoře výzkumu a vývoje), ve znění pozdějších předpisů, následně zohlední prioritní výzkumná témata obsažená v Národním plánu při vyhlašování veřejných výzev programů podpory VaVaI[16]. V souladu s Národní politikou výzkumu, vývoje a inovací České republiky 2021+ budou prioritní výzkumné oblasti a témata rovněž prosazovány v pracovních programech implementujících rámcové programy EU pro výzkum a inovace Horizont Evropa a Digitální Evropa s cílem zintenzivnit integraci českého VaVaI do Evropského výzkumného prostoru.

Nástroje:

1. Vedení strategického dialogu s Úřadem vlády ČR, poskytovateli veřejné podpory a dalšími partnery v oblasti prioritizace tematického vymezení národních programů aplikovaného výzkumu a experimentálního vývoje.

[15] Zpráva o stavu kybernetické bezpečnosti za rok 2020. Dostupná zde: https://www.nukib.cz/cs/infoservis/dokumenty-a-publikace/zpravy-o-stavu-kb/.
[16] Úkol č. 49 Akčního plánu k Národní strategii.

2. Úzká spolupráce se zástupcem ČR v programovém výboru programu Horizont Evropa a členy odborných tematických skupin programového výboru.

Indikátory:

- Počet národních programů a výzev VaVaI akcentujících prioritní výzkumné oblasti kybernetické a informační bezpečnosti.
- Prioritní výzkumná témata v kybernetické a informační bezpečnosti budou součástí pracovních programů EU.

2.3 Opatření 3 — Analyzovat potřebu a možnosti vzniku výzkumného programu výlučně pro oblast kybernetické a informační bezpečnosti

Celosvětový nárůst investic do výzkumu a vývoje v kybernetické a informační bezpečnosti souvisí se vzrůstající potřebou čelit novým hrozbám v kyberprostoru. Na tento trend reagovala EU mimo jiné schválením programu Digitální Evropa, jehož významnou komponentou je kybernetická bezpečnost. V ČR v současné době neexistuje program veřejné podpory věnující se výlučně kybernetické a informační bezpečnosti. V rámci stávající veřejné podpory VaVaI je tato oblast pouze jednou ze zájmových tematických oblastí šířeji definovaných programů [např. Program Strategická podpora rozvoje bezpečnostního výzkumu ČR 2019-2025 (IMPAKT 1), Program na podporu průmyslového výzkumu a experimentálního vývoje TREND nebo Národní plán obnovy]. Ve sledovaném období proto NÚKIB učiní iniciační kroky směřující k případnému vzniku programu VaVaI, výlučně zaměřeného na oblast kybernetické a informační bezpečnosti. Vznik takového programu bude nutné posoudit s ohledem na zákonné limity pro nástroje realizace podpory VaVaI, procesní a finanční limity politiky VaVaI, absorpční kapacity českého výzkumného prostředí v oblasti kybernetické a informační bezpečnosti a dále s přihlédnutím k vnitřním kapacitám (personálním a finančním) potenciálního poskytovatele veřejné podpory. S ohledem na zákonnou povinnost NÚKIB zajišťovat výzkum a vývoj v kybernetické a informační bezpečnosti bude rovněž posouzena možnost zařazení NÚKIB mezi příjemce finančních prostředků z kapitoly státního rozpočtu na

podporu výzkumu a vývoje. Tento krok by, mimo jiné, umožnil realizaci strategických výzkumných a vývojových projektů v oblasti kybernetické a informační bezpečnosti.

Nástroje:

1. Zpracování analýzy možnosti zařazení NÚKIB mezi příjemce finančních prostředků z kapitoly státního rozpočtu na podporu výzkumu a vývoje.
2. Zpracování analýzy možnosti vzniku výzkumného programu zaměřeného výhradně na oblast kybernetické a informační bezpečnosti, navržení koncepce výzkumného programu, a případné zahájení prvních kroků vedoucí k jeho vzniku.

Indikátory:

- SWOT analýza možnosti zařazení NÚKIB mezi příjemce finančních prostředků z kapitoly státního rozpočtu na podporu výzkumu a vývoje.
- Metodika a časový harmonogram postupu pro vytvoření role příjemce finančních prostředků na podporu VaVaI a pro určení poskytovatele veřejných prostředků.
- Analytická zpráva posuzující dopady vzniku výzkumného programu výhradně pro oblast kybernetické a informační bezpečnosti. Důraz bude kladen na zhodnocení přínosu takového programu na zajišťování kybernetické bezpečnosti ČR, absorpčních kapacit českého výzkumného prostředí a také na posouzení vnitřních kapacit potenciálního poskytovatele finančních prostředků. Součástí zprávy bude i posouzení dopadů na legislativní rámec poskytování veřejné podpory a finančních dopadů na státní rozpočet.

2.4 Opatření 4 — Zajistit zřízení Národního koordinačního centra výzkumu a vývoje v oblasti kybernetické bezpečnosti a plnění úkolů plynoucích z Nařízení Evropského parlamentu a Rady EU č. 2021/887, kterým se zřizuje Evropské průmyslové, technologické a výzkumné centrum kompetencí pro kybernetickou bezpečnost a síť národních koordinačních center

V souladu s Nařízením Evropského parlamentu a Rady EU č. 2021/887, kterým se zřizuje Evropské průmyslové, technologické a výzkumné centrum kompetencí pro kybernetickou bezpečnost a síť národních koordinačních center (dále jen „Nařízení EU č. 2021/887“) je vytvářeno Evropské průmyslové, technologické a výzkumné centrum kompetencí pro kybernetickou bezpečnost (dále jen „Kompetenční centrum“) a na něj navazující Síť Národních koordinačních center. Usnesením vlády ČR ze dne 23. srpna 2021 č. 728 byl NÚKIB pověřen zajištěním zřízení Národního koordinačního centra výzkumu a vývoje v oblasti kybernetické bezpečnosti (dále jen „Centrum“) a koordinací jeho dalších činností. Centrum se stane integrální součástí NÚKIB, přičemž vybrané činnosti budou na základě Memoranda o spolupráci delegovány na partnerský subjekt. Mezi klíčové úkoly, které bude Centrum plnit, patří:

- vytvoření expertní komunity sestávající z dalších orgánů státní správy, akademických a výzkumných institucí a subjektů bezpečnostního a obranného průmyslu (dále jen „Komunita“), která bude následně napojena i na Kompetenční centrum;
- zprostředkování komunikace mezi Evropskou komisí, Kompetenčním centrem, Agenturou Evropské unie pro kybernetickou bezpečnosti, případně dalšími institucemi a subjekty na národní úrovni;
- předávání informací o prioritách a programech EU v oblasti kybernetické bezpečnosti na národní úroveň a o aktivitách a prioritách na národní úrovni v dané oblasti směrem k EU;
- poskytování podpory žadatelům o prostředky na výzkum a vývoj z relevantních programů EU (zejména Horizont Evropa a Digitální Evropa), případně při navazování kontaktů s partnerskými institucemi v dalších členských zemích EU;
- podporování a šíření výsledků činnosti Komunity a Kompetenčního centra na vnitrostátní, regionální nebo místní úrovni;

- šíření vzdělávacích programů v oblasti kybernetické bezpečnosti;
- poskytování finanční podpory třetím stranám, kterým Kompetenční centrum udělilo granty.

Fungování Centra rovněž přispěje k budování informačního zázemí pro partnery působící v kybernetické a informační bezpečnosti. V současné době existuje několik informačních zdrojů a nástrojů zprostředkovávajících informace o národních a mezinárodních výzkumných programech. Informace jsou však decentralizované a tematicky se nezaměřují výhradně na problematiku kybernetické bezpečnosti. Proto bude Centrum poskytovat informace o rámcových programech EU, aktuálních programových výzvách v oblasti kybernetické bezpečnosti a v roli zprostředkovatele podporovat zapojení obchodních společností, veřejné správy a výzkumných pracovišť do mezinárodních projektových konsorcií. Tyto činnosti budou prováděny v úzké spolupráci s již existujícími a zavedenými informačními centry (např. Národní informační centrum pro evropský výzkum, Česká styčná kancelář pro vzdělávání a výzkum v Bruselu apod.).

Nástroje:

1. NÚKIB zaštítí zřízení Centra a na něj navazující ustanovení Komunity na národní úrovni.
2. V součinnosti s Komunitou a dalšími národními partnery Centra stanoví NÚKIB národní prioritní osy spolupráce s Kompetenčním centrem v oblasti směřování evropského VaVaI v kybernetické bezpečnosti.
3. Budování informačního zázemí v rámci Centra, včetně vytvoření jednotného místa pro žádosti o zapojení do výzkumných projektů kybernetické bezpečnosti v programech Horizont Evropa a Digitální Evropa.
4. Navázání úzké spolupráce mezi Komunitou, Centrem a Evropskými centry pro digitální inovace (eDIHs), Národními centry kompetence a národními e-infrastrukturami.

Indikátory:

- Zřízení Centra.
- Nastavení formálního procesu pro vznik členství v Komunitě.
- Vznik národních prioritních os spolupráce s Kompetenčním centrem.

- Vytvoření jednotného informačního místa.
- Průběžná analýza kvality a intenzity spolupráce v rámci Komunity.

2.5 Opatření 5 — Navazovat mezinárodní spolupráci s důrazem na aktivní účast v rámci společně prováděného výzkumu a vývoje na úrovni EU a NATO

V současném globalizovaném světě je mezinárodní spolupráce jedním z klíčových předpokladů pro zajištění kybernetické bezpečnosti. Na poli VaVaI toto tvrzení platí dvojnásob, jelikož řadu kyberbezpečnostních výzev nebude možné řešit pouze na úrovni národních států. Například vznik a budování kvantově odolné sítě v EU či dynamický vývoj umělé inteligence (AI) klade značné nároky na výzkumné infrastruktury, rozpočty a expertízu. Pokud chce ČR uplatnit (a dále rozvíjet) silné stránky svého výzkumu a vývoje, je nezbytné prohlubovat spolupráci v rámci Evropského výzkumného prostoru s dalšími partnery mimo EU. Z dlouhodobého hlediska je pro ČR důležité navazovat a rozvíjet spolupráci s organizacemi a orgány Evropské Komise, které mají vliv na směřování VaVaI na úrovni EU či v rámci NATO. Jedná se především o Agenturu Evropské unie pro kybernetickou bezpečnosti, Generální ředitelství pro komunikační sítě, obsah a technologie, Generální ředitelství pro informatiku a Agenturu komunikačních a informačních systémů. V dalších uskupeních bude ČR vystupovat v roli pozorovatele, v případě zvýšeného zájmu o konkrétní problematiku v roli aktivního účastníka (např. v rámci Komunity evropského výzkumu a inovací pro bezpečnost – CERIS[17]). Jedním z klíčových nástrojů zahraniční spolupráce je zapojování českých výzkumných pracovišť a firem do strategických výzkumných iniciativ Evropské Komise a dalších mezinárodních projektových konsorcií. Podporována bude i účast koncových uživatelů v projektech strategického významu reflektující prioritní výzkumné oblasti Národního plánu, například s využitím portálu Evropské Komise Funding & Tender Opportunities. Z dosavadních zkušeností vyplývá, že ochota zapojit se do mezinárodních projektů souvisí mimo jiné s již existujícími vazbami mezi jednotlivými pracovišti. NÚKIB a další partneři proto budou podporovat

[17] Více o informací o komunitě zde: https://ec.europa.eu/home-affairs/secure-safe-resilient-societies/index_en.

vytváření sítě mezinárodních kontaktů a navazovat mezinárodní partnerství s využitím nástrojů vědecké diplomacie.

Nástroje:

1. Aktivní účast ČR ve strategických výzkumných iniciativách EU (např. European Quantum Communication Infrastructure - EuroQCI, European High-Performance Computing Joint Undertaking - EuroHPC či aktivity směřující ke zvyšování digitálních kompetencí).
2. Podpora zapojení českých subjektů do projektů financovaných z rámcových programů EU (Horizont Evropa, Digitální Evropa, Nástroj pro propojení Evropy).
3. Podpora zapojování českých odborníků do expertních skupin EU (Agentura Evropské unie pro kybernetickou bezpečnosti, Generální ředitelství pro komunikační sítě, obsah a technologie, Generální ředitelství pro informatiku), koordinace jejich činnosti a využívání výsledků těchto skupin.
4. Využití nástrojů podpory vědecké diplomacie k rozvoji kontaktů v zahraničí s podporou cyber attaché a vědeckých přidělenců.

Indikátory:

- Aktivní účast ČR ve strategických výzkumných iniciativách EU a výsledky této účasti.
- Zapojení VaVal subjektů do mezinárodních výzkumných projektů.
- Počet zapojených odborníků do expertní skupin EU a výsledky práce expertních skupin.
- Realizace zahraničních aktivit s využitím nástrojů vědecké diplomacie v prioritních výzkumných oblastech, včetně sledování praktických výstupů navázané spolupráce.

3. Prioritní výzkumné oblasti a témata VaVaI v kybernetické a informační bezpečnosti

Národní plán stanovuje šest prioritních výzkumných oblastí, jejichž dlouhodobá podpora může významně posílit bezpečnost českého kyberprostoru.

Tabulka: přehled prioritních výzkumných oblastí

Oblast 1	Umělá inteligence a bezpečnost
Oblast 2	Kryptografie a kvantové technologie
Oblast 3	Bezpečný hardware, software a bezpečnost dodavatelského řetězce
Oblast 4	Vzdělávání a rozvoj schopností
Oblast 5	Bezpečnostní politika a krizové řízení
Oblast 6	Ochrana osobních údajů a možnosti elektronického dokazování

3.1. Umělá inteligence a bezpečnost

V následujících třech letech můžeme očekávat zvyšující se uplatnění prvků umělé inteligence v oblastech průmyslu, dopravy či zdravotnictví. Pokročilé metody strojového učení mohou sloužit jako nástroj pro vyhledávání anomálií v rámci síťového provozu, odvozovat virové definice na bázi zkušeností či monitorovat, analyzovat nebo i řešit kybernetické bezpečností incidenty. Na druhé straně se umělá inteligence může stát zdrojem hrozeb. Útočníci ji mohou zneužít pro vytváření autonomního malwaru nebo botnetů, případně k zodolnění metod sociálního inženýrství (například při tvorbě *deepfakes*). V současnosti se také začínají objevovat zcela nové vektory útoků, které využívají zranitelnosti právě v algoritmech umělé inteligence a strojovém učení.

Hlavní témata v této oblasti:

- Vytváření modelů, technických standardů a testovacích platforem pro systémy umělé inteligence tak, aby bylo možno vyhodnocovat jejich bezpečnost.

- Výzkum a vývoj algoritmů umělé inteligence posilujících kybernetickou bezpečnost a odolnost strategických sítí a systémů státu, včetně zpracování velkých dat.
- Tvorba metodik a postupů zohledňujících vytváření bezpečného kódu umělé inteligence.
- Výzkum a analýza nových vektorů útoků, které jsou namířeny proti systémům umělé inteligence a strojového učení.
- Analýza etických a právních otázek spojených se zaváděním a rozvojem umělé inteligence a se zpracováním velkých objemů dat.

3.2 Kryptografie a kvantové technologie

V oblasti kryptografie je velmi důležité rozlišovat mezi kybernetickou a informační bezpečností. Ty se od sebe liší rozsahem způsobů využití kryptografie, možnostmi využití fyzické a režimové ochrany informačních systémů a kryptografických zařízení, a požadovanou mírou bezpečnostních garancí.

3.2.1 Kryptografie a kybernetická bezpečnost

Přestože je kryptografie schopna poskytnout velmi vysoké bezpečnostní garance, volba vhodných algoritmů a způsobů jejich použití (zejména jejich bezpečná implementace) je často obtížná a bývá zatížena chybami. Největšími zdroji bezpečnostních slabin v kryptografických systémech v oblasti kybernetické bezpečnosti jsou komplikovanost některých řešených problémů a různorodost reálných situací, a zároveň snaha o rychlý a finančně dostupný výsledek. Velmi častým zdrojem bezpečnostních problémů je i snaha o zpětnou kompatibilitu se zastaralými systémy a někdy i používání zastaralé kryptografie.

Z technologického hlediska je za největší zdroj kryptografických slabin považována nedostatečná ochrana implementací proti útokům tzv. fyzikálními postranními kanály. V této oblasti probíhá neustálý výzkum zahrnující hledání nových útoků i nových protiopatření. Proto jednou z nejdůležitějších výzev v kybernetické bezpečnosti je správné použití silné kryptografie, zejména u významných informačních systémů a kritické informační infrastruktury.

Hlavní témata v této oblasti:

- Bezpečnost kryptografických protokolů široce užívaných veřejností.
- Ochrana soukromí na internetu, v cloudech a při zpracovávání velkých dat.
- Vytváření metodik, postupů a doporučení ve vztahu ke kryptografickým nástrojům užívaných ze strany státní správy a veřejnosti.

3.2.2 Kryptografie a informační bezpečnost

V oblasti informační bezpečnosti jsou specifické výzvy kryptografického výzkumu a vývoje spojeny s vývojem a certifikací národních kryptografických prostředků pro ochranu utajovaných informací. Zejména jde o nutnost zajistit mimořádně vysoké bezpečnostní garance, přičemž je kladen důraz na snadnost použití kryptografických prostředků bez snížení bezpečnosti, kterou by měly zajišťovat především technologické a kryptografické ochranné mechanismy. To vyžaduje použití specifických kryptografických algoritmů a bezpečnostních mechanismů, rozsáhlé a hluboké analýzy kryptografické bezpečnosti a rozvíjení spolupráce v rámci NATO a EU. Nemalou výzvou je příprava zajištění interoperability v rámci NATO a převzetí a zavedení procedur manipulace s kryptografickým materiálem v rámci NATO a EU.

3.2.3 Kryptografie a kvantové technologie

V souvislosti s rozvojem kvantových technologií a kryptografické ochrany je nutné rozlišovat mezi tzv. post-kvantovou kryptografií na bázi kvantově odolných algoritmů s veřejnými klíči, a tzv. kvantovou kryptografií, která umožňuje ustanovení klíčů na bázi kvantových technologií (kvantová distribuce klíčů).

Kvantová kryptografie má v porovnání s tzv. post-kvantovou kryptografií zásadní potenciální výhodu. Jakmile bude mít dostatečné garance implementační bezpečnosti, bude teoreticky neprolomitelná bez ohledu na budoucí vývoj kryptoanalýzy. Proto probíhá v oblasti testování možností praktického nasazení kvantové kryptografie intenzivní výzkum a vývoj, do něhož se zapojuje i ČR.

Hlavní témata v této oblasti:

- Bezpečnost utajovaných kryptografických algoritmů, zejména schémat a protokolů pro řešení specifických potřeb vznikajících při vývoji národních kryptografických prostředků.
- Vývoj a využití softwarových nástrojů pro analýzu kryptografické bezpečnosti.
- Vývoj a implementace kvantově odolné kryptografie do národních kryptografických prostředků využívajících veřejné klíče.
- Výzkum a vývoj metod hodnocení hrozeb a rizik, tvorba krizových scénářů a metodik v oblasti kryptografické ochrany.
- Výzkum a vývoj dalších bezpečnostních nástrojů v oblastech kvantových počítačů, kvantových sítí a kvantových senzorů.

Další témata z oblastí kompromitujícího vyzařování, ochrany utajovaných informací a služby PRS systému Galileo:

- Vývoj nových metod zajišťujících adekvátní ochranu utajovaných informací stupně utajení Důvěrné a vyšší před jejich možným únikem kompromitujícím vyzařováním.
- Vývoj metod eliminace bezpečnostních rizik fotonických komunikačních sítí.
- Výzkum a vývoj technologií zaručující bezpečný příjem signálu veřejně regulované služby satelitního systému Galileo a vládní satelitní komunikace (GOVSATCOM).

3.3 Bezpečný hardware, software a bezpečnost dodavatelského řetězce

Aktivity, které směřují k adekvátnímu zabezpečení ICT produktů a služeb, jsou stále nedostatečné. Dochází k rozvoji a nasazování celé řady nových technologií, jako jsou 5G sítě nebo Internet věcí, které mohou v budoucnu přinést řadu dalších bezpečnostních výzev. Existující problémy v zabezpečení systémů a současný rozmach využití metod strojového učení povede ke vzniku nových forem malware a jejich modularitě. Zásadní roli v oblasti zajišťování bezpečnosti IT technologií a služeb tak do budoucna budou mít EU certifikace

kybernetické bezpečnosti, jejichž smyslem je zvýšit důvěru v produkty, služby a procesy v oblasti informačních a komunikačních technologií[18].

3.3.1 Sítě 5G

V krátkodobém horizontu můžeme očekávat především rozšíření hybridních *non-standalone* 5G sítí[19] a počátky aktivního budování *standalone* 5G sítí s unikátní decentralizovanou a virtualizovanou architekturou. Z tohoto základu budou odvozeny první významné aplikace 5G v průmyslu a Internetu věcí. S tím je spojena hrozba zneužití 5G technologií například pro průmyslovou špionáž. Vzhledem k velmi omezenému počtu společností schopných dodávat pokročilé 5G komponenty, je zde hlavním rizikem zneužití pozice dodavatele, ať už ekonomicky, nebo ke kybernetickým útokům.

Hlavní témata v této oblasti:

- Vývoj a výzkum postupů a nástrojů pro zabezpečení 5G technologií, především pro zajištění bezpečného dodavatelského řetězce.
- Vývoj nástrojů pro zaručení stability připojení v rámci 5G sítí.

3.3.2 Internet věcí

Rozvoj Internetu věcí rozšíří možnosti monitoringu a optimalizace ve všech odvětvích lidské činnosti. Jedná se například o chytré domácnosti, města, zdravotnictví nebo dopravu a průmysl. Zabezpečení zařízení Internetu věcí je často až na posledním místě, a tak se mohou jednoduše stávat cílem nebo prostředkem útoků.

Hlavní témata v této oblasti:

- Vytvoření nástrojů pro zajištění odolnosti zařízení Internetu věcí.
- Vývoj metod a nástrojů integrování lidského aspektu a rozhodování v rámci zajišťování bezpečnosti Internetu věcí.

[18] Nařízení Evropského parlamentu a Rady (EU) 2019/881 („Akt o kybernetické bezpečnosti“). Více o EU certifikacích kybernetické bezpečnosti dostupné zde: https://www.nukib.cz/cs/kyberneticka-bezpecnost/vyzkum/eu-certifikace-kyberneticke-bezpecnosti/.

[19] Jedná se o 5G antény využívajících 4G architekturu a infrastrukturu.

3.3.3 Cloud computing

Nedostatek odborníků na informační technologie a snaha o snižování nákladů vede čím dál větší počet organizací k využívání služeb cloud computingu pro správu dat. Využívání těchto služeb výrazně přispívá k větší efektivitě a úspoře nákladů na zpracování a uchovávání dat a jejich obsluhu. Z pohledu jednotlivých organizací se jedná o krok k větší efektivitě a úsporám. Nicméně využívání cloudových služeb také znamená, že se citlivá data organizací nacházejí v prostředí, jehož údržbu a monitoring nemají plně pod kontrolou, a které je dostupné z internetu. Cloudová infrastruktura navíc v mnoha případech bývá nevhodně nakonfigurována. Obchodní tajemství a další citlivá data umístěná v cloudových úložištích představují lákavý cíl jak pro cizí státní aktéry, tak pro kyberkriminální skupiny.

Hlavní témata v této oblasti:

- Vývoj nových nástrojů pro zabezpečení cloudových infrastruktur a služeb, včetně zajištění bezpečného dodavatelského řetězce.
- Vývoj metodik a postupů pro procesní zabezpečení cloudových služeb.

3.3.4 Ostatní technologie a přístupy

Další technologie, například *blockchain,* představují nástroj s velkým potenciálem pro autentizaci a případně i pro celkové nahrazení současných metod autentizace. Důležitou oblastí VaVaI jsou rovněž ochrana před DDoS útoky, bezpečnost průmyslových sítí a SCADA/ICS systémů, nebo potřeba vývoje nástrojů detekčních technik a threat intelligence v souvislosti s nástupem nových typů malware. Významným budoucím trendem je větší propracovanost phishingových útoků, u kterých můžeme očekávat, že v dohledné době budou využívat i nástroje umělé inteligence. V krátkodobém horizontu lze navíc očekávat, že ruku v ruce s digitalizací poroste i pravděpodobnost kybernetických útoků a phishing a spear-phishing bude nadále velmi využívaným prostředkem těchto útoků.

Hlavní témata v této oblasti:

- Vývoj a analýza síťové komunikace a unikátních detekčních technik v síťovém provozu s využitím pokročilého managementu bezpečnostních informací a threat intelligence.
- Vývoj nástrojů pro automatickou detekci a ochranu proti phishingu, spear-phishingu a deepfakes.
- Vývoj nástrojů a nových metod forenzní analýzy.
- Vývoj nových metod ochrany před DDoS útoky.
- Analýza a výzkum možností zabezpečení průmyslových sítí a systémů SCADA/ICS v souvislosti s rozvojem Internetu věcí a využívání cloudových služeb.
- Analýza možností uplatnění distribuované decentralizované databáze (*blockchain*) v kybernetické bezpečnosti.

3.4 Vzdělávání a rozvoj schopností

Vzdělávání a osvěta jednotlivých občanů, tak i celé společnosti, hrají nezastupitelnou roli ve zvyšování úrovně kybernetické bezpečnosti. Potřeba zvyšování povědomí o kybernetické a informační bezpečnosti ještě stále není vnímána jako běžná součást osobní bezpečnosti občanů[20]. Druhou hlavní výzvou v této oblasti je současný problém nedostatku odborníků na kybernetickou bezpečnost. Ten je významným determinujícím faktorem pro zajištění kybernetické bezpečnosti (nejen) ČR a jeho řešení si vyžádá komplexní úsilí ve všech oblastech[21]. Je třeba podporovat růst počtu škol (střední školy, vyšší odborné školy a vysoké školy) zaměřených na kybernetickou bezpečnost a rozvoj jejich studijních oborů a programů. Vedle vzdělávání a vychovávání nových odborníků je třeba věnovat prostor i udržení a rozvíjení stávajících zaměstnanců-odborníků kybernetické bezpečnosti.

[20] Tento nedostatek v oblasti úrovně a zvyšování kompetencí občanů ČR v kybernetické bezpečnosti byl na strategické úrovni identifikován a adresován tím, že byla přijata opatření ve Strategii vzdělávací politiky České republiky do roku 2030+, která směřují ke zvýšení úrovně digitálních dovedností absolventů škol.

[21] Zpráva o stavu kybernetické bezpečnosti České republiky za rok 2020.
Dostupné z: https://www.nukib.cz/download/publikace/zpravy_o_stavu/Zprava_o_stavu_KB_2020.pdf.

Hlavní témata v této oblasti:

- Vývoj nových a aktualizace stávajících vzdělávacích rámců a programů, které budou reflektovat potřebu začlenění a zvýšení kvality témat kybernetické bezpečnosti do všech úrovní vzdělávací soustavy ČR.
- Motivace studentů pro studium oborů spojených s kybernetickou bezpečnostní a motivace stávajících zaměstnanců pro setrvání v oboru kybernetické a informační bezpečnosti.
- Vytvoření systému klasifikací profesí v kybernetické a informační bezpečnosti a bezpečnostní správy informačních a komunikačních systémů včetně náplně činností, které dané profese vykonávají.

3.5 Bezpečnostní politika a krizové řízení

Kybernetická bezpečnost není pouze technickou záležitostí. Na národní i mezinárodní úrovni vzniká řada bezpečnostních strategií, které reflektují kybernetickou bezpečnost. Na mezinárodní úrovni se navíc tato oblast dostává do popředí bezpečnostních zájmů EU a NATO. Vedle toho nadále roste potřeba právní regulace kybernetické a informační bezpečnosti, včetně potřeby vzniku krizových scénářů pro různé organizace. Všechny organizace by měly mít zpracovány krizové plány pro zvládání případných kybernetických incidentů. S tím úzce souvisí i téma kybernetických bezpečnostních cvičení, které slouží ke kontrole schopností a znalostí krizových manažerů těchto organizací.

Hlavní témata v této oblasti:

- Analýza možností inovací a optimalizace národního a mezinárodního systému zajišťování kybernetické bezpečnosti.
- Tvorba krizových scénářů, metodik a typových postupů pro zvládání kybernetických incidentů.
- Výzkum možností implementace cvičení, zaměřených na kybernetickou bezpečnost, do plánu cvičení orgánů krizového řízení.

- Vytváření metodik a postupů pro hodnocení technických i netechnických hrozeb a rizik.
- Vývoj technických nástrojů pro simulaci kybernetických bezpečnostních cvičení.

3.6 Ochrana osobních údajů a možnosti elektronického dokazování

Ochrana osobních údajů a soukromí jednotlivce představuje provázanou oblast založenou na hodnotách, jakými jsou možnost izolace dat jednotlivce nebo jeho schopnost kontrolovat dostupnost dat o své osobě. V kontextu kybernetické bezpečnosti je třeba zdůraznit, že absolutní většina osobních údajů je v současné době uložena na digitálních zařízeních. Kybernetické incidenty tak často mohou mít za cíl právě zisk citlivých osobních údajů o osobách nebo mohou tyto údaje využívat k útokům proti těmto osobám. Správně nastavené nástroje pro zabezpečení osobních údajů v organizaci tak mohou výrazně snížit riziko krádeže identity. Osobní údaje a digitální stopa mohou být zároveň využívány i proti útočníkům, a to především jako prostředek elektronického dokazování.

Hlavní témata v této oblasti:

- Vytváření nových nástrojů pro ochranu osobních údajů v kontextu jejich možné ztráty nebo zneužití v kyberprostoru.
- Vytváření metodik a postupů pro správné nastavení vnitřní politiky organizace pro ochranu osobních údajů.
- Vytváření a rozvoj nástrojů pro využívání digitální stopy jako prostředků pro elektronické dokazování, mj. v souvislosti s budoucím Nařízením EU o přeshraničním přístupu k elektronickým důkazům.

4. Řízení rizik – omezení a předpoklady

Potenciální rizika ohrožující naplňování stanovených cílů Národního plánu jsou: nedostatečný důraz na podporu VaVaI v kybernetické a informační bezpečnosti na národní úrovni a v rámci jednotlivých organizací; slabá spolupráce napříč veřejným, akademických a soukromým sektorem; omezené personální kapacity a v neposlední řadě i pokles finančních prostředků na realizaci politiky VaVaI, která je a bude významným hybatelem v předmětné oblasti.

Riziko spojené s nedostatečným akcentem na podporu VaVaI v kybernetické a informační bezpečnosti představuje významnou překážku pro realizaci některých opatření tohoto Národního plánu. V rámci národní podpory VaVaI by se v takovém případě nepodařilo prosadit prioritní výzkumné oblasti v rámci programů podpory VaVaI na národní a mezinárodní úrovni (opatření 2) a s vysokou pravděpodobností by v budoucnu nedošlo k podpoře vzniku výzkumného programu výlučně pro oblast kybernetické a informační bezpečnosti. Avšak s ohledem na současný vývoj bezpečnostních hrozeb ve světě a platné strategické materiály v ČR a zahraničí lze předpokládat, že význam kybernetické a informační bezpečnosti v oblasti VaVaI bude růst, nikoliv klesat či stagnovat.

Prevencí rizika spojeného s nedostatečnou součinností mezi veřejným, akademických a soukromým sektorem je především důraz na její koordinaci a vytváření prostředí pro její vznik. Součástí opatření 1, 3 a 5 je řada nástrojů, které si kladou za cíl vytvořit podmínky pro vznik vzájemně prospěšné spolupráce.

Nedostatečné personální kapacity pro zajištění podpory a koordinace VaVaI v kybernetické a informační bezpečnosti mohou mít negativní dopad na počet realizovaných aktivit, termíny jejich plnění a v neposlední řadě i na jejich kvalitu. Z tohoto důvodu je vypracován plán plnění cílů, včetně gestorství a termínů. Počet opatření rovněž odpovídá možnostem a kapacitám zainteresovaných stran, přičemž řada opatření je přímo v gesci NÚKIB. V této souvislosti se NÚKIB opírá o předpoklad rozvoje vlastních kapacit dle vládou schválené Koncepce rozvoje NÚKIB[22]. Reakcí na výskyt tohoto rizika je omezení činnosti na plnění klíčových úkolů.

[22] Dokument je dostupný zde:
https://www.nukib.cz/download/publikace/strategie_akcni_plany/Koncepce_rozvoje_NUKIB.pdf.

V takovém případě NÚKIB, ve spolupráci s dalšími partnery, provede revizi jednotlivých opatření, přičemž nejvyšší prioritou bude realizace závazků vycházejících z právních předpisů ČR a EU.

Riziko nedostatku finančních prostředků na realizaci politiky VaVaI je významné a může souviset s nepříznivým vývojem ekonomické situace ČR v důsledku pandemie COVID-19. V takovém případě hrozí snížení objemu finančních prostředků na realizaci stávajících programů podpory VaVaI či omezení zahraničních aktivit. Rovněž by bylo velice obtížné zahájit diskusi o vzniku výzkumného programu výlučně pro oblast kybernetické a informační bezpečnosti a s ním spojené jednání o případném navýšení finančních zdrojů na veřejnou podporu VaVaI. Přetrvávající výskyt pandemie COVID-19 a s ní spojená opatření mohou rovněž omezit realizaci osobních setkání a nástrojů zahraniční spolupráce, například výzkumné diplomacie.

Dalším dílčím rizikem je periodicita vyhlašování programů veřejné podpory a příslušných výzev. Schválení programů podpory VaVaI závisí na politické vůli, a proto nelze s jistotou určit, zda bude program v daném období schválen, a jaké finanční prostředky na něj budou alokovány. NÚKIB má v tomto směru omezené možnosti, jak těmto rizikům předcházet. Jedním ze způsobů je aktivní účast NÚKIB při vytváření priorit pro VaVaI v ČR, či úzká spolupráce s jednotlivými poskytovateli veřejné podpory. V neposlední řadě je třeba vhodně nastavit a podporovat spolupráci s dalšími zainteresovanými stranami a tuto spolupráci dále prohlubovat. Úspěšná realizace řady opatření je odvislá od společného postupu.

Seznam zkratek

AV ČR – Akademie věd ČR
CEF – Nástroj pro propojení Evropy
CERIS – Komunita evropského výzkumu a inovací pro bezpečnost
ČR – Česká republika
DG CONNECT – Generální ředitelství pro komunikační sítě, obsah a technologie
DG DIGIT – Generální ředitelství pro informatiku
eDIHs – Evropská centra pro digitální inovace
ENISA – Agentura Evropské unie pro kybernetickou bezpečnost
EU – Evropská unie
IoT – Internet věcí
MD – Ministerstvo dopravy
MO – Ministerstvo obrany
MPO – Ministerstvo průmyslu a obchodu
MŠMT – Ministerstvo školství, mládeže a tělovýchovy
MV – Ministerstvo vnitra
MZV – Ministerstvo zahraničních věcí
NATO – Severoatlantická aliance
NCI Agency – Agentura komunikačních a informačních systémů
PČR – Policie ČR
RVVI – Rada pro výzkum, vývoj a inovace
TA ČR – Technologická agentura ČR
TC AV ČR – Technologické centrum Akademie věd ČR
ÚV – Úřad vlády ČR
VaVaI – Výzkum, vývoj a inovace

Plán plnění cílů

OPATŘENÍ	NÁSTROJ	INDIKÁTOR	GESCE	SPOLUPRACUJE	TERMÍN SPLNĚNÍ
1	Spolupráce v rámci Platformy s cílem zintenzivnit vzájemnou komunikaci a výměnu informací.	Propojování soukromého sektoru a akademických pracovišť s koncovými uživateli, včetně bezpečnostních složek.	NÚKIB	MV, MŠMT, MO, MPO, MZV, RVVI, ÚV, zpravodajské služby, AV ČR, PČR, TA ČR, TC AV ČR, neziskový, akademický a soukromý sektor	průběžně
1	Zpracování výhledové studie technologických trendů v kybernetické a informační bezpečnosti, která bude, mimo jiné, sloužit jako vodítko pro aktualizaci prioritních výzkumných oblastí a témat v kybernetické a informační bezpečnosti.	Zpracování výhledové studie technologických trendů v kybernetické a informační bezpečnosti.	NÚKIB	MPO, TC AV ČR	2023
1	Analýza silných a slabých stránek národního výzkumu a vývoje v kybernetické a informační bezpečnosti s důrazem na identifikaci klíčových výzkumných schopností státu této oblasti.	Analytická zpráva.	NÚKIB	MŠMT, MPO	2023
1	Podpora zapojování konečných uživatelů do výzkumných projektů v oblasti kybernetické a informační bezpečnosti.	Počet zapojených konečných uživatelů v projektech kybernetické a informační bezpečnosti.	NÚKIB	MV, uživatelé výsledků	průběžně
1	Podpora vzniku a rozvoje pracovišť zaměřených na oblasti klíčových technologií (KETs) a nově nastupujících a přelomových technologií (EDTs) s důrazem na kooperaci výzkumných týmů napříč ČR s přesahem do zahraničí.	Vznik nových a rozvoj stávajících pracovišť zaměřených na klíčové technologie (KETs) a nově nastupující a přelomové technologie (EDTs).	MŠMT, MPO	NÚKIB, akademický sektor	průběžně

2	Vedení strategického dialogu s ÚV, poskytovateli veřejné podpory a dalšími partnery v oblasti prioritizace tematického vymezení národních programů aplikované výzkumu a experimentálního vývoje.	Počet národních programů a výzev VaVaI akcentujících prioritní výzkumné oblasti kybernetické a informační bezpečnosti.	NÚKIB	ÚV, RVVI, MŠMT, MV, MPO, TA ČR, TC AV ČR	průběžně
2	Úzká spolupráce se zástupcem ČR v programovém výboru programu Horizont Evropa a členů odborných tematických skupin programového výboru.	Prioritní výzkumná témata v kybernetické a informační bezpečnosti součástí pracovních programů EU.	NÚKIB	MŠMT, MV	průběžně
3	Zpracování analýzy možnosti zařazení NÚKIB mezi příjemce finančních prostředků z kapitoly státního rozpočtu na podporu výzkumu a vývoje.	SWOT analýza možnosti zařazení NÚKIB mezi příjemce finančních prostředků z kapitoly státního rozpočtu na podporu výzkumu a vývoje. Metodika a časový harmonogram postupu pro vytvoření role příjemce finančních prostředků na podporu výzkumu a vývoje a pro určení poskytovatele veřejných prostředků.	NÚKIB	MŠMT, RVVI, ÚV, TC AV ČR, TA ČR	2023
3	Zpracování analýzy možnosti vzniku výzkumného programu zaměřeného výhradně na oblast kybernetické a informační bezpečnosti, navržení koncepce výzkumného programu a případné zahájení prvních kroků vedoucí ke vzniku programu VaVaI výhradně pro kybernetickou a informační bezpečnost.	Analytická zpráva posuzující dopady vzniku výzkumného programu pro oblast KIB. Důraz bude kladen na zhodnocení přínosu takového programu na zajišťování kybernetické bezpečnosti ČR, absorpčních kapacit českého výzkumného prostředí a také na posouzení vnitřních kapacit potenciálního poskytovatele finančních prostředků. Součástí zprávy bude i posouzení dopadů na legislativní rámec poskytování veřejné podpory a finanční dopady na státní rozpočet	NÚKIB	MŠMT, ÚV, RVVI, TC AV ČR, MV	2024
4	NÚKIB zaštítí zřízení Centra a na něj navazující ustanovení Komunity na národní úrovni.	Zřízení Centra. Nastavení formálního procesu pro vznik členství v Komunitě.	NÚKIB	MZV, MPO	2022

4	V součinnosti s Komunitou a dalšími národními partnery Centra stanoví NÚKIB národní prioritní osy spolupráce s Kompetenčním centrem v oblasti směřování evropského VaVaI v kybernetické bezpečnosti.	Vznik národních prioritních os spolupráce s Kompetenčním centrem.	NÚKIB	MV, MŠMT, MO, MPO, MZV, MD, ÚV, neziskový, akademický a soukromý sektor	2023
4	Budování informačního zázemí v rámci Centra, včetně vytvoření jednotného místa pro žádosti o zapojení do výzkumných projektů kybernetické bezpečnosti v programech Horizont Evropa a Digitální Evropa.	Vytvoření jednotného informačního místa.	NÚKIB	MV, MPO, TC AV ČR, TA ČR, ÚV	průběžně
4	Navázání úzké spolupráce mezi Komunitou, Centrem a Evropskými centry pro digitální inovace (eDIHs), Národními centry kompetence a národními e-infrastrukturami.	Průběžná analýza kvality a intenzity spolupráce v rámci Komunity.	NÚKIB	MV, MŠMT, MO, MPO, MZV, MD, ÚV, neziskový, akademický a soukromý sektor a další externí partneři	průběžně
5	Aktivní účast ČR ve strategických výzkumných iniciativách EU (např. European Quantum Communication Infrastructure - EuroQCI, European High-Performance Computing Joint Undertaking - EuroHPC či aktivity směřující ke zvyšování digitálních kompetencí).	Aktivní účast ČR ve strategických výzkumných iniciativách EU a výsledky této účasti.	ÚV, MPO, MŠMT	NÚKIB, MV, MŠMT, MO, MZV, MD, neziskový, akademický a soukromý sektor a další externí partneři	průběžně
5	Podpora zapojení českých subjektů do projektů financovaných z rámcových programů EU (Horizont Evropa, Digitální Evropa, Nástroj pro propojení Evropy).	Zapojení VaV subjektů do mezinárodních výzkumných projektů.	MV	NÚKIB, MPO, TC AV ČR	průběžně
5	Podpora zapojování českých odborníků do expertních skupin EU (Agentura Evropské unie pro kybernetickou bezpečnosti, Generální ředitelství pro komunikační sítě, obsah a technologie, Generální ředitelství pro informatiku), koordinace jejich činnosti a využívání výsledků těchto skupin.	Počet zapojených odborníků do expertní skupin EU a výsledky práce expertních skupin.	ÚV, MZV, NÚKIB	MV, MŠMT, MPO, MD	průběžně

5	Využití nástrojů podpory vědecké diplomacie k rozvoji kontaktů v zahraničí s podporou cyber attaché a vědeckých přidělenců.	Realizace zahraničních aktivit s využitím nástrojů vědecké diplomacie v prioritních výzkumných oblastech, včetně sledování praktických výstupů navázané spolupráce	MZV	NÚKIB, MV	průběžně