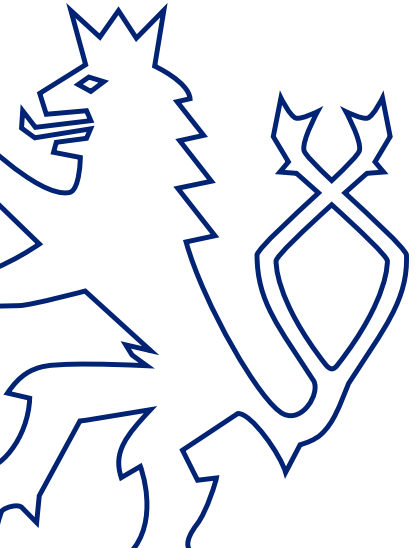
AKČNÍ PLÁN K NÁRODNÍ STRATEGII KYBERNETICKÉ BEZPEČNOSTI ČESKÉ REPUBLIKY NA OBDOBÍ LET 2021 AŽ 2025



ÚVODNÍ SLOVO

K úspěšnému naplnění a dosažení hlavních cílů *Národní strategie kybernetické bezpečnosti České republiky* je zapotřebí dle stanoveného časového rámce realizovat či úspěšně naplňovat úkoly uvedené zde v *Akčním plánu k Národní strategii kybernetické bezpečnosti pro období let 2021 až 2025*.

U stanovených úkolů je potřebná aktivní součinnost a spolupráce orgánů a osob povinných ve smyslu zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů, a dalších subjektů veřejné správy ČR v koordinaci a dle potřeb uvedeného odpovědného subjektu.

Odpovědné subjekty jsou za plnění úkolů odpovědni dle zákonem vymezených působností a kompetencí.
Role a působnost jednotlivých institucí dle zákona tak nejsou tímto Akčním plánem dotčeny.

V tomto dokumentu jsou používány zkratky, jejichž vysvětlení je uvedeno na konci v sekci *Seznam použitých zkratek*.

OBSAH

A. SEBEVĚDOMĚ V KYBERPROSTORU

	Kód	Úkol	Odpovědný subjekt	Časový rámec
SPOLEČNÝ PŘÍSTUP KE KYBERNETICKÉ BEZPEČNOSTI	1.	Vytvořit a na národní úrovni provozovat zabezpečenou platformu pro komunikaci a sdílení informací o kybernetických hrozbách a zranitelnostech, zejména s ohledem na řešení rozsáhlejších národních a mezinárodních kybernetických bezpečnostních incidentů.	NÚKIB	Od Q2 2021 průběžně
	2.	Rozvíjet efektivní a koordinovanou spolupráci mezi NÚKIB, PČR a zpravodajskými službami v oblasti kybernetické bezpečnosti, včetně spolupráce s orgány a osobami povinnými dle ZKB, zejména při řešení kybernetických bezpečnostních incidentů a nastavit jasné procesy pro tuto spolupráci.	NÚKIB PČR zpravodajské služby	Průběžně
	3.	Vytvořit návrh umožňující jednotný postup pro hlášení kybernetických bezpečnostních incidentů relevantním orgánům státní správy, které takové hlášení vyžadují.	NÚKIB ve spolupráci s relevantními aktéry	Q4 2022
	4.	Sbližovat přístup ke kybernetické bezpečnosti a ochraně utajovaných informací v informačních a komunikačních systémech v souladu s „*Koncepcí rozvoje Národního úřadu pro kybernetickou a informační bezpečnost*“. Navrhnout případné změny přístupu na základě analýzy současného stavu a potřeb.	NÚKIB ve spolupráci s: MO MV MZV NBÚ ÚV ČR zpravodajské služby	Od Q1 2024 průběžně
	5.	Na základě uzavřených memorand s kontrolními a regulatorními orgány státu prohlubovat spolupráci, a zefektivňovat kontrolní i regulatorní činnost těchto orgánů.	ČNB ČTÚ NÚKIB SÚJB ÚCL ÚOOÚ	Průběžně
	6.	Vytvořit návrh posuzování rizikového profilu dodavatelů a uplatňování omezování vysoce rizikových dodavatelů na národní úrovni pro bezpečné zavádění a realizaci telekomunikačních sítí nastupujících generací.	NÚKIB ve spolupráci s: ČTÚ MPO MZV zpravodajské služby	Q2 2022

	7.	Vytvořit návrh posuzování rizikového profilu dodavatelů na národní úrovni a uplatňování omezování vysoce rizikových dodavatelů do systémů regulovaných ZKB.	NÚKIB ve spolupráci s: MPO MV MZV zpravodajské služby	Q1 2024
	8.	Navázat a prohlubovat spolupráci se zastřešujícími organizacemi z jednotlivých odvětví PZS (svazy či jiné platformy) a spolupracovat s nimi na rozvoji kybernetické bezpečnosti.	NÚKIB	Průběžně
	9.	Vhodně propojovat činnosti vedoucí k navyšování kybernetické bezpečnosti s aktivitami navyšujícími rovněž odolnost ČR proti hybridním hrozbám.	AČR MO MV MZV NÚKIB zpravodajské služby	Průběžně
	10.	Zpracovat návrh národní politiky koordinovaného zveřejňování zranitelností.	NÚKIB	Q4 2021
	11.	Rozšiřovat a upevňovat spolupráci se soukromým sektorem; navyšovat povědomí o činnostech NÚKIB a možnostech vzájemné spolupráce.	NÚKIB	Průběžně
STRATEGICKÁ KOMUNIKACE	12.	Provádět komunikační kampaně na podporu národních cílů v oblasti kybernetické bezpečnosti.	NÚKIB ve spolupráci s relevantními aktéry v závislosti na řešené problematice	Průběžně
	13.	Vytvořit metodiku pro strategickou komunikaci relevantních subjektů na národní úrovni pro případ reakce na kybernetické incidenty, útoky a jiné hrozby.	NÚKIB ve spolupráci s: MO MV MZV NSZ PČR VSZ zpravodajské služby	Q2 2022

BEZPEČNÁ INFRASTRUKTURA	14.	Podporovat a poskytovat metodickou podporu při nasazování detekčních systémů pro monitorování provozu sítí a kybernetických bezpečnostních událostí v rámci státní správy.	NÚKIB	Průběžně
	15.	Vyhledávat zranitelnosti u povinných orgánů a osob podle ZKB i subjektů mimo působnost ZKB.	NÚKIB	Průběžně
	16.	Za předem dohodnutých podmínek i nadále provádět penetrační testování s cílem odhalit chyby a zranitelnosti v informačních systémech a sítích povinných orgánů a osob dle ZKB.	NÚKIB	Průběžně
	17.	Vypracovat metodický dokument k řízení bezpečnosti dodavatelů a poskytnout ho orgánům a osobám povinným dle ZKB.	NÚKIB ve spolupráci s: MF MPO MV	Q4 2022
	18.	Připravit návrh aktualizace standardů šifrování pro orgány a osoby povinné dle ZKB zohledňující nástup kvantových počítačů a s tím související hrozbu prolomení současných metod šifrování.	NÚKIB	Q1 2024
	19.	Skrze tvorbu metodických materiálů, realizaci cvičení, sdílením informací o hrozbách, poskytnutím e-learningových kurzů a dalšími relevantními způsoby navyšovat kybernetickou bezpečnost zdravotnického sektoru.	NÚKIB ve spolupráci s: MZdr	Průběžně
	20.	Vytvářet, organizovat a realizovat technická, netechnická i kombinovaná cvičení kybernetické bezpečnosti pro orgány a osoby povinné dle ZKB, další relevantní partnery a organizovat rozsáhlá sektorová cvičení se scénáři vytvořenými na míru jednotlivým odvětvím.	NÚKIB	Průběžně
	21.	Vytvořit návrh jednotné sítě státní správy a souvisejících navazujících, relevantních projektů, s cílem navýšit kybernetickou bezpečnost státních institucí s pomocí plošně aplikovaných standardů zabezpečení.	MF MV NÚKIB VZ ve spolupráci s: BIS	Q2 2022
ROZVOJ SCHOPNOSTÍ	22.	Naplňovat „*Koncepci rozvoje Národního úřadu pro kybernetickou a informační bezpečnost*“ a rozvíjet schopnosti a kapacity NÚKIB například v oblastech kontroly, nových technologií nebo sektorových specializací.	NÚKIB	Průběžně dle schváleného dokumentu

	23.	Pokračovat v posilování systému kybernetické obrany prostřednictvím budování schopností NCKO jako součásti VZ se zaměřením na logistické, personální a finanční zabezpečení, ale i další aspekty důležité pro jeho efektivní fungování.	VZ	Průběžně
	24.	Aktualizovat národní systém detekce kybernetických útoků, který bude využívat všechny dostupné národní zdroje.	MV NÚKIB zpravodajské služby	Q4 2022
	25.	Posilovat personální a další kapacity potřebné k tvorbě, přípravě a organizaci technických, netechnických a dalších relevantních cvičení kybernetické bezpečnosti s cílem zajištění obrany ČR.	AČR MO VZ	Průběžně
	26.	Ve spolupráci s organizátory začleňovat prvky kybernetické bezpečnosti do existujících relevantních národních či sektorových cvičení.	NÚKIB	Průběžně
	27.	Vytvářet a aktivně se podílet na komunikačních a procedurálních cvičeních zaměřených na efektivitu spolupráce mezi aktéry a rychlou výměnu informací v oblasti kybernetické bezpečnosti, kriminality a obrany.	NÚKIB ve spolupráci s: AČR MO MZV PČR zpravodajské služby	Průběžně
	28.	Zapojovat národní partnery do řešení scénářů mezinárodních cvičení kybernetické bezpečnosti a tím přispívat k posilování spolupráce, nastavování a koordinaci postupů během řešení reálných kybernetických hrozeb.	AČR MO NÚKIB	Průběžně
	29.	Vytvořit platformu zapojující dobrovolníky z řad kybernetických expertů a institucionalizovat jejich využití při zajišťování kybernetické bezpečnosti.	NÚKIB	Q3 2023
	30.	Zapojovat soukromý sektor při zajišťování kybernetické obrany a aktivně s ním v tomto spolupracovat.	VZ ve spolupráci s: BIS MO NÚKIB ÚZSI	Od Q1 2022 průběžně

SEBEVĚDOMÁ REAKCE	31.	Vytvořit, implementovat a v relevantních případech aktivovat efektivní národní rámec plnohodnotné atribuce závažných kybernetických útoků.	MZV NÚKIB PČR ÚV ČR zpravodajské služby	Od 2021 průběžně
	32.	Konsolidovat rámec možných reakcí na kybernetické útoky a bezprostřední hrozby a nastavit systém pro jejich koordinované využití.	AČR MO MZV NÚKIB PČR zpravodajské služby ve spolupráci s: MV	Q4 2022
	33.	Konsolidovat přístupy k odstrašování kybernetických útoků s cílem následně koncepčně využívat všech dostupných možností pro co nejefektivnější odstrašení původců útoků.	MO MZV NÚKIB VZ ve spolupráci s: BIS ÚZSI	Q4 2023
	34.	Vypracovat koncepci rozvoje schopností rychlé reakce určené k řešení rozsáhlých bezpečnostních incidentů.	NÚKIB PČR zpravodajské služby	Q4 2024
PREVENCE A POTÍRÁNÍ KRIMINALITY	35.	Rozvíjet a posilovat schopnosti Policie ČR v oblasti kybernetické kriminality v souladu s „*Koncepcí rozvoje Policie ČR do roku 2027*“ a „*Strategií boje s kybernetickou kriminalitou*“.	PČR	Průběžně dle schválených koncepčních dokumentů
	36.	Koordinovat s co největší mírou synergie aktivity NÚKIB a Policie ČR v oblasti preventivních programů, a to zejména skrze výměnu informací.	MV NÚKIB PČR	Průběžně

	37.	Provést analýzu mezinárodně-právních závazků v oblasti kybernetické kriminality a kybernetické bezpečnosti a tyto závazky reflektovat při spolupráci mezi aktéry kybernetické bezpečnosti, kybernetické kriminality a implementovat je do relevantních metodik.	NÚKIB ve spolupráci s: MSp MV MZV NSZ PČR zpravodajské služby	Q2 2022
NÁRODNÍ PRÁVNÍ ÚPRAVA	38.	Na základě analýz a s ohledem na technologický a společenský vývoj aktualizovat a vytvářet srozumitelné, efektivní a proporcionální zákonné a podzákonné předpisy v oblasti kybernetické bezpečnosti, zejména pokud jde o nastavení úrovně zabezpečení ukládané orgánům a osobám povinným dle ZKB.	NÚKIB	Průběžně
	39.	Na základě průběžně prováděných analýz dopadů regulace dle ZKB vydefinovat systémy, které jsou důležité pro chod státu a jeho bezpečnost a dosud nespadají pod zákonnou regulaci. V případě existence takových systémů navrhnout příslušné změny legislativy.	NÚKIB	Od Q4 2024
	40.	Provést právní revizi stavu kybernetického nebezpečí v kontextu dalších krizových stavů a připravit návrhy pro případné legislativní změny.	NÚKIB ve spolupráci s: MO MV MZV ÚV ČR zpravodajské služby	Q2 2023
	41.	Provést analýzu právních možností rychlého operativního nákupu technických nebo programových prostředků k nasazení protiopatření v období krizových stavů, k provádění opatření podle § 11 ZKB nebo za stavu kybernetického nebezpečí, a v případě potřeby navrhnout legislativní úpravu.	MV NÚKIB ve spolupráci s: MMR	Q4 2021
	42.	Analyzovat a případně zpracovat návrh legislativy upravující odbornou způsobilost osob vykonávající některou z rolí podle VKB.	NÚKIB	Q4 2025

	43.	Provést analýzu současného stavu kompetencí a spolupráce s cílem navrhnout změny příslušných právních norem tak, aby byly v souladu s nejlepší praxí v oblasti kybernetické kriminality, kybernetické bezpečnosti a kybernetické obrany.	NÚKIB PČR VZ ve spolupráci s: BIS MSp MV NSZ ÚZSI	Q1 2023
ÚPRAVY A AKTUALIZACE REGULATORNÍHO RÁMCE	44.	Porovnat vybrané v současnosti užívané metody analýzy rizik s cílem ověřit, zda jsou v souladu s požadavky VKB a zda jsou současně efektivně použitelné pro různé organizace. Výstup tohoto projektu bude v obecné rovině nabídnut orgánům a osobám povinným dle ZKB i široké veřejnosti.	NÚKIB ve spolupráci s: MV	Q2 2022
	45.	Aktualizovat a vytvářet soubor doporučených standardů a osvědčených postupů, které mohou být nápomocné ke zvládání kybernetických bezpečnostních rizik i subjektům mimo regulaci ZKB.	NÚKIB	Průběžně
	46.	Plnit úkoly vyplývající z „*Aktu o kybernetické bezpečnosti*“ v oblasti EU certifikací kybernetické bezpečnosti informačních a komunikačních technologií.	NÚKIB ve spolupráci s: ČIA	Průběžně
	47.	Vytvořit regulatorní rámec bezpečnosti cloud computingu.	NÚKIB	Q3 2022
VĚDA A VÝZKUM	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.	NÚKIB ve spolupráci s: MMR MO MPO MŠMT MV MZV PČR zpravodajské služby	Průběžně každé dva roky

	49.	Zohledňovat při vyhlašování veřejných soutěží a výzev národních a mezinárodních programů podpory výzkumu, vývoje a inovací prioritní výzkumná témata obsažená v „*Národním plánu výzkumu a vývoje v kybernetické a informační bezpečnosti*“.	MMR MO MPO MŠMT MV MZV TA ČR ÚV ČR	Průběžně
	50.	Iniciovat a podílet se na realizaci výzkumných projektů s partnery z veřejné, soukromé a akademické sféry na národní, evropské i globální úrovni.	NÚKIB ve spolupráci s: MO MV MZV PČR TA ČR TC AV ČR zpravodajské služby	Průběžně
	51.	Podporovat vznik a fungování Evropského centra excelence v oblasti AI na území ČR a jeho zaměření na kybernetickou bezpečnost jako jednu z prioritních oblastí.	ÚV ČR ve spolupráci s: MD MPO MŠMT MZV NÚKIB	Průběžně

B. SILNÁ A SPOLEHLIVÁ SPOJENECTVÍ

	Kód	Úkol	Odpovědný subjekt	Časový rámec
EFEKTIVNÍ MEZINÁRODNÍ SPOLUPRÁCE	52.	Vytvořit a pravidelně svolávat meziresortní platformu pro koordinaci činností ústředních orgánů státní správy v oblasti kybernetického prostoru s dopadem na zahraniční vztahy, včetně aktivit ČR v mezinárodních organizacích a integračních seskupeních.	MZV ve spolupráci s: ČTÚ MO MPO MSp MV NÚKIB ÚV ČR	Od Q3 2021 průběžně
	53.	Meziresortně spolupracovat při zahraničních aktivitách týkajících se oblasti kybernetické bezpečnosti a obrany.	ČTÚ MO MPO MSp MV MZV NÚKIB ÚV ČR	Průběžně
	54.	Aktivně spolupracovat v rámci EU s Evropskou komisí a dalšími unijními institucemi a agenturami s cílem zajistit větší koherenci v kybernetických tématech.	MZV NÚKIB ve spolupráci s: MO MPO MV	Průběžně
	55.	Posilovat aktivní roli a prosazovat zájmy ČR v oblasti kybernetické bezpečnosti v rámci EU, a za tímto účelem spolupracovat se zahraničními partnery, ostatními členskými státy a orgány EU na vytváření funkční a účelné evropské regulace a na tvorbě a implementaci právních předpisů a neprávních dokumentů EU.	MZV NÚKIB ve spolupráci s: ČTÚ MPO MV	Průběžně
	56.	Spolupracovat s NATO a spojenci na implementaci politiky kybernetické obrany a bezpečnosti NATO a reagovat na aktuální výzvy. Prohlubovat spolupráci zejména s ohledem na reakci na kybernetické bezpečnostní incidenty a výměnu technických i netechnických informací o hrozbách a zranitelnostech.	MZV NÚKIB VZ ve spolupráci s: AČR MO PČR	Průběžně

	57.	Aktivně se zapojovat do sdílení informací o kybernetických bezpečnostních incidentech, výměny informací o škodlivých kódech mezi státy na úrovni mezinárodních organizací, jejichž je ČR členem, agentury ENISA a dalších platforem typu, TF-CSIRT či FIRST.	NÚKIB	Průběžně
	58.	Podporovat tvorbu a konsolidaci mezinárodních komunikačních a informačních kanálů mezi CERT/CSIRT pracovišti, mezinárodními organizacemi a akademickými centry.	NÚKIB	Průběžně
	59.	Posilovat aktivní roli a prosazovat zájmy ČR v kybernetických tématech v rámci OBSE, a to zejména při vytváření a následné implementaci opatření pro zvyšování důvěry mezi státy v kyberprostoru.	MZV NÚKIB	Průběžně
	60.	Posilovat aktivní roli ČR v rámci OECD v oblasti kybernetické a digitální bezpečnosti; zejména se podílet na tvorbě strategických dokumentů a doporučení.	MPO MZV NÚKIB ÚV ČR	Průběžně
	61.	Aktivně spolupracovat s národními organizacemi kybernetické bezpečnosti ve středoevropském regionu (i za využití stávající platformy CECSP), východoevropském regionu a oblasti západního Balkánu.	NÚKIB	Průběžně
	62.	Aktualizovat a upravit proces mezinárodní spolupráce v určování PZS/KII, zejména při určování přeshraničních závislostí, v souladu s chystanou změnou směrnice NIS.	NÚKIB	Od Q3 2023, dle přijetí revize směrnice NIS
PROHLUBOVÁNÍ A TVORBA AKTIVNÍCH SPOJENECTVÍ	63.	Navazovat a prohlubovat bilaterální spolupráci s partnerskými institucemi vybraných států v oblasti kybernetické bezpečnosti a obrany, zejména s klíčovými partnery ČR v této oblasti jako jsou členské státy EU, USA, Izrael, Jižní Korea, Austrálie aj.	MZV NÚKIB ve spolupráci s: AČR MO zpravodajské služby	Průběžně
	64.	Vysílat do zahraničí v odůvodněných případech kyberatašé a národní experty, a to za účelem prohlubování strategicky významné spolupráce s klíčovými partnery ČR nebo ve strukturách EU a NATO.	NÚKIB ve spolupráci s: MO MZV	Průběžně
	65.	Aktivně participovat v koordinačních a reaktivních mezinárodních iniciativách v oblasti kybernetické bezpečnosti (zejména ve strukturách EU a NATO) a prosazovat pozici ČR v koalicích se státy stejného hodnotového nastavení.	MZV NÚKIB	Průběžně

	66.	Aktivně spolupracovat s partnerskými a spojeneckými státy při koordinované atribuci a reakci na závažné kybernetické útoky a incidenty.	MO MZV NÚKIB PČR zpravodajské služby	Průběžně
	67.	Účastnit se a aktivně participovat na organizaci, přípravě a provádění mezinárodních cvičení a prostřednictvím společných kybernetických cvičení aktivně posilovat síť významných partnerů v oblasti kybernetické bezpečnosti.	AČR MO MZV NÚKIB	Průběžně
MEZINÁRODNÍ PRÁVO, SPRÁVA INTERNETU A LIDSKÁ PRÁVA ONLINE	68.	Vytvořit ucelenou národní pozici ČR k interpretaci stávajícího mezinárodního práva v oblasti kybernetické bezpečnosti a obrany.	MZV ve spolupráci s: MO MSp NSZ NÚKIB zpravodajské služby	Q4 2021
	69.	Vytvořit přehled implementace nezávazných norem odpovědného chování států v kyberprostoru a aktivně se podílet na prosazování jejich dodržování, bránit jejich rozmělňování a oslabování mj. v oblasti dodržování lidských práv.	MZV ve spolupráci s: NÚKIB	Q4 2021 a dále průběžně
	70.	Prostřednictvím aktivní kybernetické diplomacie prosazovat stávající mezinárodní právo a nezávazné normy zodpovědného chování států v kyberprostoru.	MZV ve spolupráci s: MSp NÚKIB	Průběžně
	71.	Aktivně spoluutvářet mezinárodní diskusi na půdě OSN ke zvyšování bezpečnosti a stability kyberprostoru, a to zejména v rámci prvního a třetího výboru Valného shromáždění v New Yorku a v rámci jednání organizovaných UNODC ve Vídni; zaměřit se na interpretaci mezinárodního práva a nezávazných norem zodpovědného chování států v kyberprostoru, opatření pro zvyšování důvěry a spolupráce na rozvoji kapacit v digitální oblasti.	MZV ve spolupráci s: MSp NÚKIB	Průběžně
	72.	Zapojit se do mezinárodní diskuse ohledně správy a řízení internetu (tzv. "internet governance"), vč. Internet Governance Forum a prosazovat účast soukromého i akademického sektoru.	MPO MZV NÚKIB	Průběžně
	73.	Monitorovat přípravu a podílet se na zavádění a v rámci kapacit i na tvorbě harmonizovaných norem EU a technických i netechnických standardů v rámci mezinárodních standardizačních organizací (např. Mezinárodní telekomunikační unie) s přesahem do kybernetické bezpečnosti a správy internetu.	ČTÚ MPO MZV NÚKIB	Průběžně

SDÍLENÍ SCHOPNOSTÍ A EXPERTIZY	74.	Vytvářet a organizovat cvičení v oblasti kybernetické bezpečnosti pro zahraniční partnery ČR v koordinaci a synergii s dalšími mezinárodními aktivitami ČR.	NÚKIB ve spolupráci s: MZV	Průběžně
	75.	Sdílet zkušenosti dobré praxe z rozličných oblastí kybernetické bezpečnosti s ostatními zahraničními partnery, zeměmi, mezinárodními organizacemi a nevládními organizacemi.	NÚKIB ve spolupráci s: MZV	Průběžně
	76.	Organizovat mezinárodní konference, školení, kurzy, semináře či vzdělávací projekty v oblasti kybernetické bezpečnosti.	NÚKIB ve spolupráci s: MO MV MZV zpravodajské služby	Průběžně
	77.	Aktivně přispívat národní expertizou a prostředky k činnosti NATO CCD COE a podílet se na výzkumných a výcvikových aktivitách centra.	MO NÚKIB	Průběžně
	78.	Posilovat kapacity třetích zemí v oblasti kybernetické bezpečnosti s využitím nástrojů zahraniční rozvojové spolupráce a ekonomické diplomacie v souladu se „*Strategií zahraniční rozvojové spolupráce*“ a „*Koncepcí zahraniční politiky ČR*“, a to skrze realizaci jak bilaterálních, tak multilaterálních projektů, například v rámci platforem Global Forum on Cyber Expertise (GFCE), Rozvojový program OSN (UNDP), Mezinárodní telekomunikační unie (ITU), Konference OSN o obchodu a rozvoji (UNCTAD) nebo Freedom Online Coalition (FOC).	MZV ve spolupráci s: ČRA MPO MSp MV NÚKIB	Průběžně

C. ODOLNÁ SPOLEČNOST 4.0

	Kód	Úkol	Odpovědný subjekt	Časový rámec
ZABEZPEČENÍ DIGITÁLNÍ VEŘEJNÉ SPRÁVY	79.	Dle přístupu „security by design“ navrhnout proces zabezpečení systémů e-Governmentu, a to již od počátku vytváření a realizace jednotlivých prvků.	MV NÚKIB Vládní zmocněnec pro IT a digitalizaci	Q4 2021
	80.	Již od počátku realizace jednotlivých systémů e-Governmentu zajistit dodržování navržených procesů určených k zajištění jejich kybernetické bezpečnosti.	MV NÚKIB Vládní zmocněnec pro IT a digitalizaci	Od Q1 2022 průběžně
	81.	Vytvořit metodiku bezpečného kódu pro státní správu s cílem podpořit vývoj bezpečného software.	MV ve spolupráci s: NÚKIB	Q4 2021
	82.	Zajistit rozvoj dohledového centra e-Governmentu s cílem vytvořit jednotné Vládní dohledové centrum, poskytující jednotný monitoring a dohled pro systémy e-Governmentu a další relevantní systémy.	MV ve spolupráci s: MO MZV NÚKIB ÚV ČR zpravodajské služby	Q4 2023
	83.	Vypracovat koncepci ochrany neutajovaných informací citlivé povahy.	NÚKIB ve spolupráci s: MO MV MZV NBÚ zpravodajské služby	Q4 2023
	84.	Vytvořit a nastavit rámec pro zajištění důvěrnosti informací v e-mailové komunikaci pomocí šifrování, a to napříč státní správou.	NÚKIB	Q3 2022
	85.	Efektivně nastavit výzvy IROP 2021–2027 pro oblast eGovernmentu a kybernetické bezpečnosti k zajištění kybernetické bezpečnosti vybraných informačních systémů ČR.	MMR ve spolupráci s: MV NÚKIB	Průběžně

	86.	Sdílet zkušenosti, know-how, metodické materiály a příklady dobré praxe z oblasti řízení ICT projektů kybernetické bezpečnosti napříč veřejnou správou, s důrazem na projekty spolufinancované EU a budoucí výzvu IROP II.	NÚKIB ve spolupráci s: MMR	Průběžně
	87.	Maximálně využít v programovém období EU 2021+ prostředky EU pro projekty zvyšující odolnost KII/VIS/PZS vůči kybernetickým hrozbám.	NÚKIB	Průběžně
	88.	Podílet se na bezpečném rozvoji Smart Cities v ČR v souladu s „*Koncepcí SMART Cities – odolnost prostřednictvím SMART řešení pro obce, města a regiony*“, a to například metodickým vedením, konzultacemi.	NÚKIB ve spolupráci s: MMR	Průběžně
KVALITNÍ SYSTÉM VZDĚLÁVÁNÍ	89.	Vypracovat národní plán vzdělávání v oblasti kybernetické bezpečnosti.	NÚKIB ve spolupráci s: MO MPSV MSp MŠMT MV MZdr MZV PČR ÚV ČR	Q4 2022
	90.	Aktivně nabízet e-learningový kurz kybernetické bezpečnosti všem úředníkům a zařadit jej mezi povinné vstupní vzdělávání. Nabízet e-learningový kurz i dalším zájemcům veřejného i soukromého sektoru.	NÚKIB ve spolupráci s: MV ÚV ČR	Průběžně
	91.	Pokračovat v modernizaci rámcových vzdělávacích programů na základní a středoškolské úrovni s cílem podporovat témata kybernetické bezpečnosti a digitálních kompetencí.	MŠMT ve spolupráci s: NÚKIB	Q4 2023
	92.	Spolupracovat s vysokými školami, vyššími odbornými školami a středními školami (včetně podpory konceptu Juniorních center excelence) na tvorbě a zavádění nových studijních programů, oborů, učebních plánů a inovativních prvků výuky v oblasti kybernetické bezpečnosti.	NÚKIB ve spolupráci s: MŠMT	Průběžně

	93.	Pomocí moderních výukových metod a technologií zvyšovat úroveň vzdělanosti učitelů i žáků v oblasti kybernetické bezpečnosti.	MŠMT ve spolupráci s: MV NÚKIB	Průběžně
	94.	Připravit podpůrný materiál k zajištění a zabezpečení distanční formy vzdělávání na úrovni základního a středního školství.	MŠMT ve spolupráci s: NÚKIB	Q3 2021
OSVĚTOVÁ A VZDĚLÁVACÍ ČINNOST	95.	Přímo se podílet na výuce oborů, programů a předmětů kybernetické bezpečnosti a příbuzných témat zejména na vysokých, ale i na vybraných vyšších odborných a středních školách.	NÚKIB	Průběžně
	96.	Poskytovat vedení a konzultace závěrečných prací studentům vysokých a vyšších odborných škol v tématech kybernetické a informační bezpečnosti.	NÚKIB	Průběžně
	97.	Rozvíjet a udržovat e-learningovou platformu pro vzdělávání s důrazem na cílové skupiny úředníků veřejné správy, pedagogických pracovníků, IT administrátorů, manažerů kybernetické bezpečnosti a dalších profesionálů zastávajících role podle ZKB, a dále zranitelné skupiny populace: děti, mládež a seniory.	NÚKIB ve spolupráci s: MPSV MSp MŠMT MV ÚV ČR	Průběžně
	98.	Využívat stávajícího systému vzdělávání a prevence včetně platforem v oblasti kybernetické bezpečnosti (například poradní skupina Digikoalice, Safer Internet Board apod.) ke vzdělávání, prevenci a osvětě v oblasti kybernetické bezpečnosti.	NÚKIB ve spolupráci s: MSp MŠMT MV PČR	Průběžně
	99.	Analyzovat současný stav trhu práce s cílem identifikovat základní požadavky na experty v oblasti kybernetické bezpečnosti a reflektovat je v rámci příslušných politik státu.	MPSV ve spolupráci s: MPO NÚKIB	Q2 2022
	100.	Vzdělávat odbornou i širokou veřejnost v oblasti kybernetické bezpečnosti formou školení, konferencí, workshopů a dalších aktivit.	NÚKIB	Průběžně

ODBORNÉ VZDĚLÁVÁNÍ A POSILOVÁNÍ EXPERTNÍ ZÁKLADNY	101.	S ohledem na dostupné kapacity školit nové a stávající zaměstnance veřejné správy v oblasti kybernetické bezpečnosti včetně orgánů a osob povinných dle ZKB.	NÚKIB	Průběžně
	102.	Vytvářet a připravovat osvětové a vzdělávací materiály, e-learningové kurzy a další vzdělávací aktivity pro nové i stávající příslušníky ozbrojených sil a bezpečnostních sborů.	NÚKIB ve spolupráci s: AČR Celní správa GIBS GŘ HZS MV PČR Vězeňská služba zpravodajské služby	Průběžně
	103.	Realizovat expertní vzdělávací aktivity pro soudce a státní zástupce v oblasti kybernetické kriminality.	PČR ve spolupráci s: Justiční akademie	Průběžně
	104.	Integrovat kybernetická cvičení do vzdělávání specialistů a školení expertních příslušníků bezpečnostních sborů.	NÚKIB ve spolupráci s: Celní správa GIBS GŘ HZS MV PČR Vězeňská služba	Průběžně
	105.	Navyšovat a zkvalitňovat vzdělávání poskytované orgánům a osobám povinným dle ZKB týkající se povinností vyplývajících z bezpečnostních opatření dle VKB.	NÚKIB	Průběžně

SEZNAM ZKRATEK

AČR – Armáda České republiky
AI – umělá inteligence
BIS – Bezpečnostní informační služba
CCD COE – NATO Cooperative Cyber Defence Centre of Excellence
CECSP – Central European Cyber Security Platform
CERT – Computer Emergency Response Team
CSIRT – Computer Security Incident Response Team
ČIA – Český institut pro akreditace
ČNB – Česká národní banka
ČR – Česká republika
ČRA – Česká rozvojová agentura
ČTÚ – Český telekomunikační úřad
ENISA – Evropská agentura pro bezpečnost sítí a informací
EU – Evropská unie
FIRST – Forum of Incident Response and Security Teams
FOC – Freedom Online Coalition
GFCE – Global Forum on Cyber Expertise
GIBS – Generální inspekce bezpečnostních sborů
GŘ HZS – Generální ředitelství Hasičského záchranného sboru
ICT – informační a komunikační technologie
IT – informační technologie
ITU – Mezinárodní telekomunikační unie
IROP – Integrovaný regionální operační program
KII – kritická informační infrastruktura
MD – Ministerstvo dopravy

MF – Ministerstvo financí

MMR – Ministerstvo pro místní rozvoj

MO – Ministerstvo obrany

MPO – Ministerstvo průmyslu a obchodu

MPSV – Ministerstvo práce a sociálních věcí

MSp – Ministerstvo spravedlnosti

MŠMT – Ministerstvo školství, mládeže a tělovýchovy

MV – Ministerstvo vnitra

MZdr – Ministerstvo zdravotnictví

MZV – Ministerstvo zahraničních věcí

NATO – Severoatlantická aliance

NBÚ – Národní bezpečnostní úřad

NCKO – Národní centrum kybernetických operací

NIS – Network and Information Systems

NÚKIB – Národní úřad pro kybernetickou a informační bezpečnost

NSZ – Nejvyšší státní zastupitelství

OBSE – Organizace pro bezpečnost a spolupráci v Evropě

OECD – Organizace pro hospodářskou spolupráci a rozvoj

OSN – Organizace spojených národů

PČR – Policie České republiky

PZS – provozovatel základní služby

SÚJB – Státní úřad pro jadernou bezpečnost

TA ČR – Technologická agentura České republiky

TC AV ČR – Technologické centrum Akademie věd České republiky

TF-CSIRT - The Task Force on Computer Security Incident Response Teams

UNCTAD – Konference OSN o obchodu a rozvoji

UNDP – Rozvojový program OSN
UNODC – Úřad Organizace spojených národů pro drogy a kriminalitu
USA – Spojené státy americké
ÚCL – Úřad pro civilní letectví
ÚOOÚ – Úřad pro ochranu osobních údajů
ÚV ČR – Úřad vlády České republiky
ÚZSI – Úřad pro zahraniční styky a informace
VIS – významný informační systém
VKB – vyhláška č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat
VSZ – Vrchní státní zastupitelství
VZ – Vojenské zpravodajství
ZKB – zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů