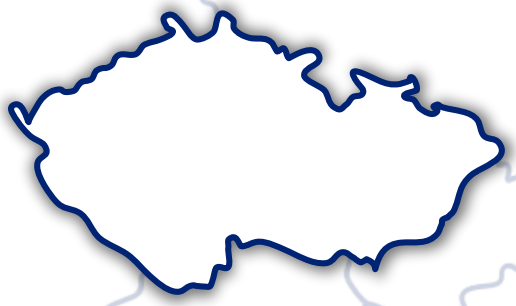
NÁRODNÍ STRATEGIE KYBERNETICKÉ BEZPEČNOSTI ČESKÉ REPUBLIKY



koordinovaný přístup **důvěra**

atribuce silná spojenectví

sebevědomá reakce

technologický rozvoj detekce hrozeb

bezpečnost strategická komunikace

OBSAH

ÚVODNÍ SLOVO

Kyberprostor a moderní technologie se staly nedílnou součástí našich životů. Postupující digitalizace české společnosti podporuje naši konkurenceschopnost, ekonomiku a zvyšuje náš blahobyt. Na druhou stranu přináší stále vyšší nároky na kybernetickou bezpečnost a v roce 2020 jsou na zabezpečeném kyberprostoru životně závislé zájmy České republiky. Žijeme v době nevyzpytatelného bezpečnostního prostředí a turbulentních společenských změn, které jsou umocněny technologickým rozvojem. Zaostávat za tímto rozvojem by bylo zejména v oblasti kybernetické bezpečnosti nebezpečné a neakceptovatelné.

Přístup České republiky ke kybernetické bezpečnosti byl od počátku založen na efektivním modelu spolupráce všech relevantních aktérů na národní i mezinárodní úrovni, v němž má každý subjekt jasně stanovené povinnosti i pravomoci. I díky tomu se kybernetická bezpečnost stala v posledních letech důležitým předmětem zahraniční politiky. Česká republika jako moderní evropská země proto bude pokračovat v tomto úsilí a dále se svými zahraničními partnery určovat trendy v zajišťování kybernetické bezpečnosti s cílem nalézt společnou cestu k udržení bezpečného digitálního prostředí.

Nové hrozby vyžadují inovativní řešení. Věřím proto, že Česká republika bude i nadále úspěšně plnit a realizovat své vize stanovené předchozí Národní strategií kybernetické bezpečnosti. Bude se snažit dosáhnout co nejvyššího stupně zabezpečení kyberprostoru a zajistit tak podmínky pro hladce fungující informační společnost. Stěžejní bude i nadále kybernetická ochrana, a to nejen kriticky důležitých prvků naší infrastruktury, ale i všech dalších systémů a sítí, aby mohli občané rozvíjet své aktivity a stát následovat své ekonomické a sociální zájmy. Tím nejdůležitějším pak zůstane posilování schopností a kapacit všech bezpečnostních složek státu, státních institucí a organizací, společností i jednotlivců čelit narůstajícím kybernetickým hrozbám. Právě odolnost je jedním ze základních pilířů a základních předpokladů účinného systému zajišťování kybernetické bezpečnosti v České republice.

Hlavními cílovými skupinami této strategie jsou bezpečnostní složky státu a další subjekty veřejné správy. Strategie však podporuje a informuje i ostatní části české společnosti, aby lépe porozuměly krokům státu při čelení kybernetickým hrozbám a rizikům. Slouží také společnosti jako zdroj informací k tomu, aby mohla kyberprostor a veškeré moderní technologie používat spolehlivě a bezpečně. Jsem přesvědčen, že nová Národní strategie kybernetické bezpečnosti posílí kybernetickou bezpečnostní politiku České republiky a její kvalitně vytvořený základ.

Ing. Karel Řehka

ředitel NÚKIB

Strategie plně respektuje logický rámec Metodiky přípravy veřejných strategií spolu s dalšími doporučeními. Strategie je strukturována do tří základních vizí: (i) sebevědomě v kyberprostoru, (ii) silná a spolehlivá spojenectví a (iii) odolná společnost 4.0, odpovídajících budoucímu strategickému směřování ČR s časovým přesahem do dalších let. V rámci těchto vizí jsou definovány základní principy naplňující myšlenky vizí. Ačkoliv se může zdát, že Strategie není časově ohraničená, její aktualizace bude podmíněna závaznou dobou pěti let a reakcí na závažné změny v kybernetickém bezpečnostním prostředí, přičemž specifické časové naplnění bude vycházet z konkrétních úkolů stanovených v Akčním plánu kybernetické bezpečnosti ČR na období let 2021-2025 (dále jen „Akční plán").

BEZPEČNOSTNÍ PROSTŘEDÍ: STRATEGICKÝ KONTEXT

Česká republika (dále jen „ČR“) se nachází ve stále složitějším bezpečnostním prostředí, které již několik let prochází zásadní proměnou. Velkou roli hraje kritická závislost státu a celé společnosti na moderních technologiích a kyberprostoru jako takovém.

Kybernetické hrozby dnes dosahují bezprecedentní úrovně, což významně souvisí s rozmachem digitalizace společnosti. Pokračuje trend, kdy se mnoho tradičních bezpečnostních hrozeb zcela nebo alespoň částečně přesouvá do kyberprostoru a dává vzniknout novým hrozbám, specifickým pro toto prostředí. Dochází rovněž k silnějšímu prolínání různých hrozeb a hybridizaci bezpečnostního prostředí, jehož dynamiku a rozsah umocňuje právě kyberprostor a moderní technologie. Všechny tyto hrozby mají jedno společné – jsou již natolik komplexní, že podrobují zkoušce důvěru veřejnosti ve stát a jeho instituce a v krajních případech mohou narušit stabilitu země, společnosti a demokratické uspořádání státu. Předpokladem pro přijímání a zavádění účinných opatření pro bezpečné fungování kyberprostoru je v první řadě schopnost státu a bezpečnostních složek porozumět dynamicky se rozvíjejícím hrozbám.

Zajišťování kybernetické bezpečnosti dnes výrazně přesahuje technologickou rovinu a vyžaduje ucelený přístup. Při jejím řešení je třeba vzít v úvahu i specifické politické, ekonomické, societální, kulturní či jiné aspekty a zájmy, které ovlivňují využívání naší závislosti na moderních technologiích a kyberprostoru. Diplomatická, právní, vzdělávací a další netechnická opatření jsou nezbytným nástrojem pro boj s kybernetickými hrozbami a budování odolné informační společnosti.

Lze identifikovat růst intenzity využívání kyberprostoru pro prosazování zahraničněpolitických zájmů států. ČR je dlouhodobě cílem kybernetické špionáže, jejímž záměrem jsou zejména státní instituce. Takto získávané informace útočníkovi poskytují výhodu při diplomatických jednáních, oslabují vyjednávací pozici ČR a ohrožují její strategické zájmy. Cílem státních aktérů přitom nejsou pouze orgány veřejné moci, ale rovněž se projevuje rostoucí zájem i o důležité soukromé subjekty, jako jsou malé a střední podniky s významným know-how, jakož i o akademickou sféru či výzkumné instituce. Zvýšené riziko průmyslové špionáže v podnicích, akademické a výzkumné sféře je úměrné rozvoji průmyslu v ČR a jeho dopady mohou výrazně oslabit naši konkurenceschopnost.

Státní a nestátní aktéři, mnohdy podporovaní nebo tolerovaní ze strany států, provádí cíleně škodlivé, ofenzivní kybernetické operace. Kyberprostor je relativně novou operační doménou a není překvapením, že dochází k navyšování armádních rozpočtů na kybernetické aktivity napříč státy NATO i zbytku světa. Lze tedy objektivně identifikovat vzrůstající význam vojenských operací v kyberprostoru a na určitých případech i trend intenzivního rozvoje schopností v této

Operační domény

Kyberprostor byl uznán jako operační doména vedle domény pozemní, námořní, vzdušné na summitu NATO ve Varšavě v roce 2016. Další doménou mezi stávajícími byl uznán vesmír v Londýně roku 2019.

doméně. Díky globálnímu technologickému pokroku, nárůstu aktivit nestátních aktérů a komercionalizaci kyberprostoru přitom nejsou sofistikované kybernetické a kinetické operace výsadou pouze nejvyspělejších států světa. I méně rozvinuté státy se mohou v této oblasti výrazně angažovat a dominovat zde. Automatizace, nové výpočetní modely, koncepty a pokročilé strojové učení s prvky umělé inteligence sice pozitivně stimulují nejen ekonomický rozvoj společnosti, avšak zároveň též podporují asymetrický boj a vylepšují ofenzivní možnosti a schopnosti útočníků, potažmo státních a nestátních aktérů v kyberprostoru.

Ústřední výzvou pro ČR je v této souvislosti soustředit se nejen na aktuální problémy kybernetické bezpečnosti, ale i na zisk schopnosti adaptace na nové, neustále se měnící bezpečnostní prostředí. K tomu musí ČR disponovat nezbytnými kapacitami a neustále hledat nové způsoby, jak čelit současným i budoucím hrozbám v kyberprostoru.

SYSTÉM ZAJIŠŤOVÁNÍ KYBERNETICKÉ BEZPEČNOSTI ČR

Struktura systému zajišťování kybernetické bezpečnosti v ČR je pojímána komplexně. Podílí se na něm značné množství subjektů, z nichž každý má vlastní roli a přispívá k zabezpečení kyberprostoru rozdílnými způsoby, které jsou dány působností a aktivitami těchto subjektů.

Za zajišťování národní bezpečnosti, a za řízení a funkčnost celého bezpečnostního systému ČR, je jakožto vrcholný orgán moci výkonné odpovědná vláda ČR.

Gestorem kybernetické bezpečnosti a ústředním správním orgánem pro oblast kybernetické bezpečnosti včetně ochrany utajovaných informací v oblasti informačních a komunikačních systémů a kryptografické ochrany je Národní úřad pro kybernetickou a informační bezpečnost (dále jen „NÚKIB"), jehož působnost je dána zákonem o kybernetické bezpečnosti (dále jen „ZKB") a zákonem o ochraně utajovaných informací a o bezpečnostní způsobilosti. Dále má na starosti problematiku neveřejné služby v rámci družicového systému Galileo. Mezi širokým spektrem aktivit představuje jeho ústřední činnost zajišťování kybernetické bezpečnosti ve smyslu ochrany kritické informační infrastruktury a dalších důležitých informačních a komunikačních systémů a sítí. Za tímto účelem byl zřízen vládní CERT (dále jen „GovCERT.CZ"), přičemž i další součásti NÚKIB poskytují povinným subjektům množství služeb. NÚKIB také zajišťuje mezinárodní spolupráci v oblasti kybernetické bezpečnosti. Dále je národním kontaktním bodem pro koordinaci výzkumu a vývoje a významnou měrou se podílí na vzdělávání a osvětě v této oblasti.

Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů je historicky první českou komplexní právní úpravou v oblasti kybernetické bezpečnosti. Vybraným veřejným a soukromým orgánům a osobám (povinné orgány a osoby) ukládá především povinnosti k zajištění bezpečnosti jejich kybernetické a informační infrastruktury, a rovněž upravuje působnost NÚKIB v oblasti koordinace a dozoru nad zajištěním kybernetické bezpečnosti ČR.

V úzké spolupráci s GovCERT.CZ působí rovněž národní CERT, jehož kompetence jsou vymezeny ZKB a veřejnoprávní smlouvou uzavřenou s NÚKIB. Národní CERT je pod názvem CSIRT.CZ od roku 2011 provozován sdružením CZ.NIC.

Zahraniční politiku, vztahy ČR s ostatními státy a mezinárodními organizacemi koordinuje Ministerstvo zahraničních věcí (dále jen „MZV"), v oblasti kybernetické bezpečnosti ve spolupráci s NÚKIB a dalšími orgány státní správy.

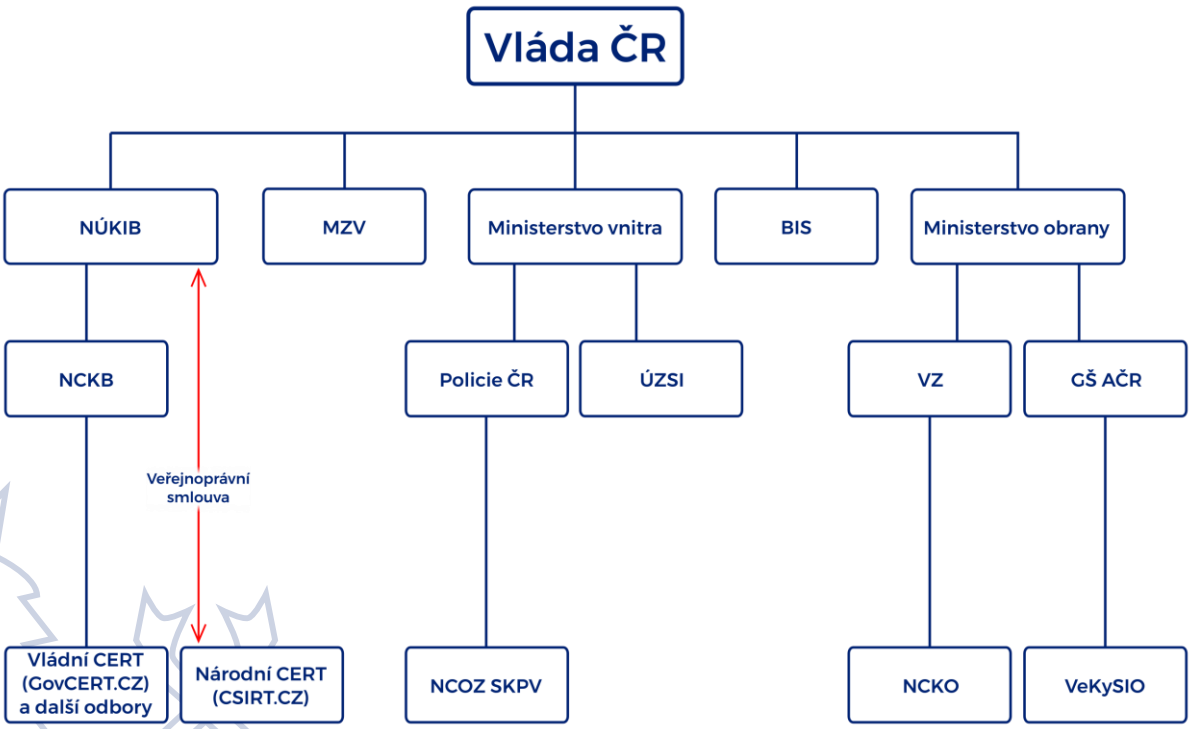
Na systému zajišťování kybernetické bezpečnosti se podílí i zpravodajské služby. V rámci svých kompetencí v oblasti kybernetické bezpečnosti působí Bezpečnostní informační služba (dále jen „BIS"), Vojenské zpravodajství (dále jen „VZ") a Úřad pro zahraniční styky a informace (dále jen „ÚZSI"), kteří zabezpečují, zpracovávají a analyzují informace důležité pro kybernetickou, potažmo národní bezpečnost ČR.

Policie ČR, konkrétně Národní centrála proti organizovanému zločinu Služby kriminální policie a vyšetřování (dále jen „NCOZ SKPV“), je národním kontaktním bodem pro kybernetickou kriminalitu a národním kontaktním místem pro hlášení závadného obsahu a závadových aktivit v síti Internet. Problematika potírání a prevence kybernetické kriminality náleží primárně orgánům činným v trestním řízení.

Stále důležitější složku systému zajišťování kybernetické bezpečnosti představuje schopnost vykonávat účinnou kybernetickou obranu státu proti nejzávažnějším kybernetickým hrozbám. V ČR představuje kybernetická obrana autonomní a specifickou oblast širšího konceptu kybernetické bezpečnosti, a zároveň oblast širšího konceptu zajištění obrany státu. Oproti kybernetické bezpečnosti se kybernetická obrana vyznačuje především odlišnou povahou působení v kyberprostoru, stejně jako odlišnou intenzitou útoků, na které reaguje. Za budování systému kybernetické obrany je v ČR odpovědné VZ.

Na kybernetické obraně se podílí i Armáda ČR, konkrétně Velitelství kybernetických sil a informačních operací (dále jen „VeKySIO“), které působí nezávisle, společně nebo v součinnosti s pozemními, vzdušnými a speciálními silami. Při ochraně kybernetického prostoru a vedení vojenských kybernetických operací úzce spolupracuje s VZ a jejich schopnosti se vzájemně doplňují.

Zajišťování kybernetické bezpečnosti v ČR



Systém zajišťování kybernetické bezpečnosti v ČR však netvoří pouze výše uvedené instituce disponující specifickým bezpečnostním mandátem a agendou. Problematika digitální ekonomiky nebo rozvoje telekomunikačního trhu je s kybernetickou bezpečností úzce spojena, proto je významná i role Ministerstva

průmyslu a obchodu, potažmo Českého telekomunikačního úřadu. Podobně důležité jsou i další subjekty, např. Ministerstvo vnitra se zaměřením na budování bezpečného e-Governmentu, nebo Ministerstvo školství, mládeže a tělovýchovy, jehož vliv na vzdělávací prostředí a vzdělávání nové generace občanů je neopominutelnou složkou pro řádné fungování systému zajišťování kybernetické bezpečnosti. Obdobně jsou do systému zapojeny i další instituce, které jsou klíčové ve svých oblastech.

Zásadní roli hrají i zástupci z řad povinných orgánů a osob podle ZKB. Právě tyto subjekty mají významný vliv na úroveň kybernetické bezpečnosti v ČR a efektivitu systému. Nesou odpovědnost za své vlastní zabezpečení, tedy naplňování a dodržování bezpečnostních zásad a opatření a udržování souladu s relevantní legislativou. Neméně podstatnou roli mají i další subjekty například z řad soukromého sektoru, akademie, asociací, sdružení a CSIRT týmů mimo veřejnou správu, které sice nespadají pod ZKB, ale jejich vliv a potřeba kvalitní spolupráce je pro fungování celého systému klíčová.

1. SEBEVĚDOMĚ V KYBERPROSTORU

ČR je již desetiletí relativně bezpečnou a ekonomicky prosperující zemí. Aby bylo toto tvrzení i nadále platné, je nutné se průběžně adaptovat na nejnovější hrozby, kterým je ČR vystavena. Základním předpokladem pro účinnou obranyschopnost ČR je v tomto směru ucelený systém detekce kybernetických hrozeb, závislý na schopnostech a kapacitách jednotlivých bezpečnostních složek, stejně jako na účinném fungování modelu národní spolupráce mezi bezpečnostními a dalšími složkami a koordinovaném, efektivním a včasném sdílení informací. Vzhledem k faktu, že v posledních letech také narůstá riziko ohrožení státu prostřednictvím kyberprostoru, musí ČR reagovat na celé spektrum nových výzev. Tyto výzvy přitom budou technického, právního i politického charakteru. I v kyberprostoru proto bude ČR vystupovat na vládní úrovni asertivně a rozhodně. Sebevědomým, zodpovědným přístupem ke kybernetické bezpečnosti na národní úrovni bude ČR posilovat svou prosperitu a navíc bude i nadále silným spojencem pro své partnery na mezinárodní úrovni.

1.1 Společný přístup ke kybernetické bezpečnosti

Zajišťování kybernetické bezpečnosti zahrnuje koordinaci množství státních i nestátních subjektů takovým způsobem, aby mohla ČR účinně čelit i těm nejzávažnějším a nejkomplikovanějším výzvám a hrozbám. Společný, integrovaný, celonárodní přístup k zabezpečování kyberprostoru a boji s kybernetickými hrozbami je zásadní. ČR proto bude usilovat o vylepšování stávajícího modelu identifikace a detekce kybernetických hrozeb, jejich následné analýzy a reakce. To přispěje k efektivitě využívání kapacit a schopností relevantních subjektů, zamezí duplicitě aktivit a přispěje k lepšímu využití lidských i finančních zdrojů v oblasti kybernetické bezpečnosti.

Současné složité bezpečnostní prostředí zvyšuje nároky na zahraniční a bezpečnostní politiku jednotlivých států, včetně schopností státu samostatně reagovat a odolávat kybernetickým hrozbám. Jednotný přístup a vnímání kybernetické bezpečnosti i obrany na všech úrovních politického rozhodování a řízení státu je proto zásadní. Představuje důležitý předpoklad pro účinné zvládání krizových situací civilního i vojenského charakteru v kyberprostoru, stejně jako významný předpoklad pro jejich prevenci. Nepřetržitá snaha o vylepšování modelu spolupráce a sdílení informací přispěje i k nalezení společného konsenzu nejen napříč jednotlivými státními institucemi, ale i domácím politickým spektrem v nejdůležitějších otázkách kybernetické bezpečnosti.

Důležitá je v tomto směru i civilně-vojenská spolupráce v zabezpečování kyberprostoru. Koncept celkové obrany státu dnes zahrnuje jak vojenskou podporu civilní společnosti, tak civilní podporu ozbrojených sil. Je potřeba pokračovat v úsilí vytvořit plně funkční model zajišťování kybernetické obrany ČR. Ten se musí opírat o relevantní právní úpravu i procedurální nastavení tak, aby jednotlivé složky měly jasně dané kompetence, které se navzájem doplňují. Vzájemná kooperace civilního a vojenského světa a nastavení funkčních pracovních procesů pak musí být

kontinuálně ověřováno jak každodenními aktivitami, tak i speciálními tréninky a cvičeními.

Zajišťovat kybernetickou bezpečnost ČR výlučně z pozice státu však není dostačující. Každá instituce, soukromá společnost či jednotlivec má svou úlohu a může pozitivně přispět do systému zajišťování kybernetické bezpečnosti. ČR proto musí nastavit a prosazovat takovou politiku kybernetické bezpečnosti, která bude konzistentně podporovat zapojení celé společnosti do procesu kybernetické bezpečnosti a posilovat její odolnost vůči kybernetickým hrozbám.

V neposlední řadě bude ČR i nadále pokračovat v aktualizaci svého vnitrostátního práva a vytváření srozumitelných, efektivních a racionálních právních předpisů v oblasti kybernetické bezpečnosti, aby byla schopna účinně reagovat na aktuální bezpečnostní situaci či trendy a poznatky z relevantních technických a společenskovědních oborů k problematice kybernetické bezpečnosti. Tento proces bude probíhat i na základě implementace unijního práva do národního právního řádu a rozvoje výkladu mezinárodně závazných právních norem, do kterého chce ČR i nadále aktivně přispívat.

1.2 Bezpečná infrastruktura

ČR se bude i nadále primárně zaměřovat na kontinuální navyšování odolnosti své strategické informační infrastruktury. Na základě vzájemné důvěry a spolupráce bude vytvářena kultura odolnosti u všech povinných subjektů dle ZKB. Právě tyto subjekty jsou totiž stěžejním pilířem kybernetické, potažmo národní bezpečnosti. Kybernetický útok na informační a komunikační systémy těchto orgánů a osob může mít oslabující a potenciálně devastující dopad pro bezpečnost státu, zabezpečení základních životních potřeb obyvatelstva nebo ekonomiku státu. Zároveň selhání jedné části infrastruktury může vést k selhání jejích dalších částí, a tím způsobit rozsáhlý kaskádový efekt. Proto představuje pro ČR jejich ochrana a zabezpečení nejvyšší prioritu. Je tedy nutné usilovat o kontinuální navyšování odolnosti infrastruktury.

Kvůli rozsáhlé automatizaci a digitalizaci průmyslu má v ČR zvláštní postavení kybernetická bezpečnost průmyslových řídicích a SCADA systémů, do které začíná pronikat i koncepce internetu věcí. Tyto specifické systémy jsou často součástí kritické infrastruktury státu. ČR si proto klade za cíl pokračovat v průběžné analýze a kontinuálním sledování jejich zabezpečení. V této souvislosti se bude ČR i nadále zasazovat o bezpečné budování telekomunikačních sítí nastupujících generací z pohledu kybernetické bezpečnosti, a stejně tak pokračovat v systematickém a pečlivém hodnocení rizik, nezbytných pro vytvoření a udržení odolné infrastruktury.

Internet věcí
Označení pro síť fyzických zařízení, jako jsou vozidla, domácí spotřebiče atd., která jsou vybavena elektronikou, softwarem, senzory, pohyblivými částmi a síťovou konektivitou, jež umožňuje těmto zařízením propojit se a vyměňovat si data.

Dalším trendem, který se nevyhýbá ani ČR, je postupný přechod na cloudová řešení, a to jak u systémů soukromé, tak i státní sféry. Tento přechod se dotkne

i povinných subjektů dle ZKB a s sebou, kromě nabídnutí nových možností a zvýšení funkčnosti, přinese i zvýšené nároky na řízení zabezpečení. ČR musí v tomto ohledu účinně reagovat, nastavovat bezpečnostní požadavky a efektivní opatření a dohlížet na jejich plnění.

Kybernetickou bezpečnost nelze považovat za čistě technickou záležitost. Spolehlivá, zabezpečená a odolná infrastruktura vyžaduje odpovídající strategii, vhodně nastavené politiky a procesy, komplexní právní rámec, aktivní spolupráci a adekvátní personální zajištění, včetně informovaného a připraveného managementu. Pro ČR je v tomto směru zásadní ucelený pohled na kybernetickou bezpečnost. Pouze pokud bude ČR vyhodnocovat kybernetické hrozby v širším kontextu, může jim efektivně čelit. Při zajišťování kybernetické bezpečnosti se tedy musí zohledňovat celá řada i netechnických aspektů. Systematické a pečlivé hodnocení rizik, které zahrnuje technické i netechnické aspekty kybernetické bezpečnosti, je nezbytné pro vytvoření a udržení skutečně odolné infrastruktury. Stěžejní otázkou je pak bezpečnost dodavatelského řetězce, tedy nutnost zajistit, že externí subjekty a osoby mající vliv na nejdůležitější infrastruktury státu nejsou z bezpečnostního hlediska rizikovými.

K dosažení vysoké úrovně kybernetické bezpečnosti jsou vyžadovány tomu odpovídající náklady, které musí být vynaloženy nejen s ohledem na národní bezpečnost státu, ale i v souvislosti s požadavky vyplývajícími z členství v mezinárodních organizacích. Nezbytnými podmínkami pro boj s kybernetickými hrozbami jsou dostatečné finanční zdroje na zabezpečení infrastruktury, technologický rozvoj, stejně jako připravení a kvalitní odborníci s odpovídajícím platovým ohodnocením a zajištěním systému jejich kontinuálního vzdělávání.

1.3 Účinná strategická komunikace

ČR bude zohledňovat význam strategické komunikace státu v kontextu kybernetické bezpečnosti, která nabyla v posledních letech výrazně na důležitosti. Aktivity státu v kybernetické bezpečnosti musí být kontinuálně komunikovány se všemi národními partnery, odbornou a širokou veřejnost nevyjímaje. Intenzivní strategická komunikace by měla být nastavena jak v rámci ČR, tak na mezinárodní úrovni.

> Strategická komunikace státu představuje synchronizaci aktivit, činů a komunikace jednotlivých státních subjektů takovým způsobem, aby byly předávány cílovému publiku koherentně veškeré potřebné informace pomocí jednotné pozice všech zapojených aktérů v dlouhodobém časovém horizontu s cílem zamezit zneužití případného informačního vakua k odlišným interpretacím.

Cílem útočníků v kyberprostoru v mnoha případech není pouze bezprostřední negativní účinek na důvěrnost, integritu nebo dostupnost informačních a komunikačních systémů či zařízení. Útočníci usilují o dosažení následného psychologického efektu a kybernetické útoky jsou využívány v rámci nejrůznějších vlivových informačních operací. Jejich prioritou je vyvolat nejistotu, strach či pocit ztráty bezpečí ve společnosti, popřípadě oslabit morálku obyvatelstva a důvěru občanů ve schopnosti státu, veřejných institucí a celkového demokratického uspořádání.

ČR proto musí plně porozumět informačnímu prostředí, jehož je součástí, a dynamice a komplexnosti kybernetických hrozeb, kterým čelí. Poté může nastavit koherentní dialog a komunikaci s veřejností. Všechny akce ze strany státu musí být koordinované napříč relevantními státními institucemi, přičemž důležité je zachování důvěryhodnosti občanů ve stát. Kromě komunikace běžných aktivit kybernetické bezpečnosti, potažmo naplňování politiky ČR v kybernetické bezpečnosti je důležitá i příprava, obratnost a schopnost reakce na nastalé krizové situace.

V neposlední řadě bude ČR posilovat principy digitální hygieny, kritické myšlení a mediální gramotnost ve společnosti. Tím ČR a její společnost dosáhne větší odolnosti proti škodlivým manipulacím v kyberprostoru i mimo něj.

1.4 Sebevědomá reakce

Politika kybernetické bezpečnosti představuje integrální součást bezpečnostní politiky ČR. Proto i zde ČR využívá proaktivní a rozhodný přístup založený na včasné detekci kybernetických hrozeb, jejich kvalitní analýze a bezodkladném přijímání adekvátních opatření. Přístup ČR i v kyberprostoru reflektuje primárně politiku aktivního předcházení konfliktům a preventivní diplomacii. V případě vypuknutí krize či konfliktu, pramenících z agresívních či jinak škodlivých aktivit v kyberprostoru, však bude připravena jednat neprodleně, důrazně a v případě potřeby využívat dostupných diplomatických, politických a v krajním případě i silových prostředků či jiných sankcí vůči agresorovi.

I v kyberprostoru je jedním z pilířů zajišťování bezpečnosti a obrany státu systém kolektivní obrany NATO, který počítá s využitím národních kapacit a schopnostmi aliančních partnerů včetně aktivního působení v kyberprostoru. K zajištění bezpečnosti přispívá i členství v EU a dalších mezinárodních organizacích či bilaterální spolupráce. Vzhledem k unikátní povaze kybernetických hrozeb, na které musí stát reagovat promptně a bez odkladu, je však v kybernetické bezpečnosti a obraně potřeba převzít odpovědnost za vlastní bezpečnost a zaměřit se na schopnost samostatné, agilnější reakce. Díky tomu bude ČR nejen schopnějším obráncem vůči škodlivým aktivitám agresorů, ale i spolehlivějším partnerem v mezinárodních vztazích.

ČR bude prostřednictvím kontinuální snahy o dosažení co nejvyššího stupně zabezpečení a viditelnou, sebevědomou reakcí na kybernetické hrozby posilovat svou celkovou odolnost v kyberprostoru i v rámci tzv. konceptu odstrašování. Ten bude přirozenou součástí systému zajišťování kybernetické bezpečnosti a obrany.

V tomto ohledu je velkou výzvou provádění atribuce. Určení zdroje a totožnosti protivníka je zásadním předpokladem jakékoliv účinné reakce. V kyberprostoru je však celá řada specifických překážek, které úspěšnou atribuci ztěžují. ČR si klade za cíl minimalizovat všechny výhody, jež kyberprostor poskytuje útočníkům. V tomto ohledu se ČR zaměří na posílení úsilí a kapacit systému národní spolupráce v oblasti

detekce, včasné reakce a nastavení národního systému atribuce kybernetických útoků a jiných škodlivých aktivit v kyberprostoru, který bude využívat co nejvíce zdrojů při provádění analýz, ale také bude obsahovat procesy pro efektivní a koordinované využití jejich výsledků. Pouze takto bude ČR moci působit sebevědomě v kyberprostoru a aktivně spolupracovat na atribuci se svými partnery jak bilaterálně, tak i v mezinárodních organizacích.

Atribuce
Proces přičitatelnosti škodlivých aktivit v kyberprostoru určitému zdroji k aktivitám konkrétního státu nebo aktivitám nezávislým na státních strukturách. Provádí se na technické, netechnické a všezdrojové úrovni. Na politické úrovni poté probíhá schválení atribuce a rozhodnutí o jejím využití.

1.5 Budoucí výzvy

V 21. století nelze reagovat na hrozby národní bezpečnosti pouze zpětně. ČR si tak klade za cíl zaujmout proaktivní přístup a snažit se novým hrozbám zavčasu porozumět, vytvářet odolnost a kapacity pro boj s nimi. V současné době zažíváme zásadní transformaci bezpečnostního prostoru umocněnou dynamickým rozvojem současných technologií. Umělá inteligence, kvantové počítače a další moderní koncepty vedou ke změně celého paradigmatu zajišťování kybernetické bezpečnosti. Stejně tak umocňují závislost státu a celé jeho společnosti na moderních technologiích a zároveň rozšiřují možnosti útočníků působit škodlivě v kyberprostoru proti státu, soukromým subjektům i běžným občanům. Lze přitom předpokládat jak proměnu schopností pachatelů v oblasti kybernetické kriminality, respektive sofistikovanější a technologicky náročnější způsoby páchání trestné činnosti a zvyšování jejich počtu, tak i důmyslnější způsoby státních a nestátních aktérů obecně provádět kybernetické útoky. V následujících letech může dojít i k bezprecedentní proměně povahy samotných konfliktů, nyní umocněných rozvojem přelomových technologií.

ČR proto musí vytvářet v rámci svých bezpečnostních institucí dostatečné kapacity pro identifikaci, analýzu a vyhodnocování nejen současných, ale i budoucích kybernetických a jiných hrozeb, které mohou ohrozit národní bezpečnost či ekonomickou a sociální prosperitu. Je také zapotřebí iniciovat rozlišování atributů pro běžnou kybernetickou kriminalitu a kybernetickou špionáž k optimalizaci podmínek pro plnění úkolů ze strany orgánů činných v trestním řízení a zpravodajských služeb.

ČR disponuje ojedinělým technickým a technologickým know-how v oblasti kybernetické bezpečnosti. Aby byla ČR vůči budoucím kybernetickým hrozbám co nejvíce resistentní, musí průběžně sledovat aktuální stav a být nadále aktivní na poli výzkumu a inovací v nových technologiích, kybernetické bezpečnosti jako takové a podporovat vznik výzkumných a vývojových center, stejně tak i český průmysl, v oblasti kybernetické bezpečnosti. Spolupráce s partnery z veřejné, akademické a soukromé sféry na výzkumu a vývoji v technologické a společenskovědní oblasti je tak zásadní. Musí být jasně určeny potřeby, problémy a priority v oblasti výzkumu a vývoje s cílem adekvátně reagovat na potřeby společnosti a uživatelské praxe. ČR a její relevantní státní instituce musí pro své partnery vybudovat takové zázemí, které bude posilovat vzájemnou informovanost a spolupráci mezi jednotlivými aktéry.

2. SILNÁ A SPOLEHLIVÁ SPOJENECTVÍ

Stěžejní vizi pro ČR, jakožto moderní evropskou zemi, představuje aktivní role při vytváření dialogu v mezinárodním prostředí, zejména v euroatlantickém prostoru. ČR bude vycházet z koherentních národních pozic a jasně definovaných strategických zájmů. Na tomto základě bude i nadále vytvářet a prohlubovat silná spojenectví se svými partnery v oblasti kybernetické bezpečnosti a obrany.

2.1 Efektivní mezinárodní spolupráce

Národní bezpečnost a prosperita ČR přímo závisí na stabilním, volně přístupném a bezpečném kyberprostoru. Jeho specifický otevřený charakter však umožňuje moderním hrozbám a rizikům snadno překročit hranice státu a působit globálně. Právě proto je mezinárodní bezpečnost jednou z nejdůležitějších dimenzí zajišťování kybernetické bezpečnosti. Pouze prostřednictvím aktivní mezinárodní spolupráce na bilaterálním a multilaterálním základě lze čelit výzvám kybernetické bezpečnosti.

Účinná mezinárodní spolupráce v kybernetické bezpečnosti vyžaduje propojení sféry civilní, vojenské a stejně tak sféry státní, soukromé a akademické na úrovni vnitrostátní. Synergie národních pozic je základním předpokladem pro úspěšné prosazování národních zájmů a bezpečnosti ČR v mezinárodním prostředí. Za společného národního přístupu bude ČR dále posilovat svou aktivní roli v mezinárodních organizacích, fórech a konferencích. Zaměří se zejména na prosazování zájmů ČR v rámci EU, NATO, OBSE, OSN a OECD. Speciální pozornost bude kladena i na problematiku přeshraniční spolupráce v rámci středoevropského prostoru. ČR zde bude působit jako země vedoucí dialog se státy regionu.

Důležitá je i společná reakce, koordinace a postup proti kybernetickým hrozbám s cílem nastavení odolného mezinárodního systému reakce. Za podstatnou součást tohoto systému ČR považuje schopnost koordinované atribuce a přijímání adekvátních opatření na základě sjednocených interpretací stávajících mezinárodněprávních závazků.

Podpora otevřeného, stabilního a bezpečného kyberprostoru bude zajištěna taktéž prostřednictvím mezinárodního úsilí o vytvoření hodnocení bezpečnosti digitálních procesů, produktů a služeb, které se staly běžnou součástí společnosti a které s sebou nesou vysoké riziko narušení bezpečnosti. ČR bude podporovat spolupráci mezi vládami, napříč sektory a občanskou společností při vytváření nových standardů kybernetické bezpečnosti umožňujících infrastrukturám a organizacím zdokonalovat svou obranyschopnost v kyberprostoru a posílit bezpečnost digitálních procesů, produktů a služeb v celém svém životním cyklu a dodavatelském řetězci. V neposlední řadě se ČR bude i nadále aktivně zapojovat do mezinárodní diskuse ohledně správy a řízení internetu (tzv. „internet governance“) a mezinárodních standardů v oblasti kybernetické bezpečnosti.

2.2 Prohlubování a tvorba aktivních spojenectví

Bilaterální spolupráce tvoří další zásadní komponentu mezinárodní spolupráce. ČR bude i nadále upevňovat stávající partnerství v kybernetické bezpečnosti a usilovat o účinná strategická spojenectví.

Tato spojenectví budou založena na sdílených hodnotách, společných zájmech a společném postoji ke kybernetickým hrozbám. Bilaterální spolupráce bude probíhat prostřednictvím rozličných kanálů a bude umocněna snahou o harmonizaci politik a přístupu ke kybernetické bezpečnosti v mezinárodních organizacích a platformách.

Odhalování nepřátelských aktivit se záměrem narušení svrchovanosti, územní celistvosti, principů demokracie a právního řádu ČR a jejích partnerů, vedoucích k cizím státním mocnostem, je jednou z výzev pro upevňování účinnosti bilaterální spolupráce a zapojení společných postupů v praxi.

ČR bude dále prohlubovat spolupráci s vybranými spojenci prostřednictvím navazování a udržování úzké spolupráce s relevantními zahraničními orgány a institucemi, sdílení strategických informací a aktivního zastupování ČR v relevantních mezinárodních organizacích a iniciativách.

2.3 Mezinárodní právní rámec

V souladu se svým euroatlantickým zakotvením zůstává ČR odhodlána chránit přístupnost, otevřenost, interoperabilitu, spolehlivost a bezpečnost kyberprostoru.

ČR v rámci svých zájmů a politik bude i nadále aktivně přispívat k tvorbě unijních právních norem a ustálení mezinárodních právních norem, zejména s ohledem na aktuální výzvy a potřeby vznikající jednáním státních i nestátních aktérů v kyberprostoru. V této souvislosti je nutné nové výzvy a právní problémy generované technologickým vývojem vykládat primárně pomocí dlouhodobě uznávaných pramenů vnitrostátního, mezinárodního i unijního práva a přizpůsobit jim ustálené postupy státních orgánů.

Zásadní výzvou bude pro ČR a státy euroatlantického prostoru tvorba jednotného přístupu k interpretaci a aplikaci mezinárodního práva veřejného v kyberprostoru, do které se ČR bude i nadále aktivně zapojovat stejně tak, jako do mezinárodní diskuse o nezávazných normách zodpovědného chování států, s cílem aktivně přispět ke stabilitě a odpovědnému chování států v kybernetickém prostoru. ČR bude zdůrazňovat použitelnost mezinárodního práva v oblasti ochrany lidských práv i v kyberprostoru.

ČR bude zodpovědně podporovat a pomáhat při spolupráci s partnerskými zeměmi při posílení kooperace mezi orgány činnými v trestním řízení a dalšími složkami zajišťujícími nadnárodní spolupráci v souvislosti s potíráním kybernetické kriminality a v oblasti vymáhání práva.

2.4 Schopnosti a expertíza

ČR potvrzuje svou ochotu a odpovědnost spolupracovat a aktivně pomáhat mezinárodním partnerům v otázkách posílení společné bezpečnosti a obranyschopnosti. Za tímto účelem budou vyvinuta konkrétní preventivní opatření zaměřená na předcházení škodlivé kybernetické aktivity státních i nestátních aktérů.

Své dosavadní schopnosti a expertízu bude ČR i nadále sdílet prostřednictvím cvičení kybernetické bezpečnosti, tréninků a dalších aktivit, které tak budou využity jako nástroj vhodný nejen k navyšování kybernetické bezpečnosti, ale také navazování a prohlubování vztahů s partnery. Vedle cvičení se pak ČR zaměří rovněž na sdílení legislativního a strategického rámce kybernetické bezpečnosti, a to zejména se státy, které své národní struktury teprve připravují.

ČR bude nadále klást důraz na podporu posílení kapacit kybernetické bezpečnosti v partnerských zemích pro boj s kybernetickými hrozbami. V neohraničeném teritoriu, jakým je kyberprostor, je nezbytné nahlížet na kybernetické hrozby jako na globální problém, kde v případě jeho nezabezpečení v cizím státě může být v konečném důsledku zasažena i ČR. Dále bude spolupracovat na expertíze v této oblasti taktéž ve snaze pomoci rozvojovým státům s navyšováním jejich odolnosti v oblasti kybernetické bezpečnosti.

ČR je připravena sdílet své schopnosti a expertízu s partnery a zejména pak s méně rozvinutými státy, které své kapacity v oblasti kybernetické bezpečnosti teprve zakládají. Posilováním schopností jednotlivých států zajišťovat kybernetickou bezpečnost na národní úrodni se tak zvýší odolnost a předejde se možnému zneužívání infrastruktury v těchto státech k páchání škodlivých činností v kyberprostoru dalšími útočníky.

3. ODOLNÁ SPOLEČNOST 4.0

V oblasti rozšíření a využívání moderních technologií patří ČR mezi špičku v Evropě. Česká společnost se díky tomu úspěšně proměňuje na společnost informační. Nastavený trend však s sebou přináší nejenom nárůst počtu koncových uživatelů v české společnosti, ale i hrozeb, kterým jsou tito uživatelé vystaveni. Jako problém s tím spojený lze identifikovat nedostatečnou digitální hygienu, nedostatečnou mediální gramotnost a kritické myšlení napříč celou společností. ČR se proto musí zaměřit na úspěšnou proměnu české společnosti na tzv. společnost 4.0. Stav, kdy je celá společnost schopna naplno využívat výhod moderních technologií a současně je schopna integrovat je do svého každodenního života tak, aby byla minimalizována kybernetická rizika. Kybernetická bezpečnost se proto musí stát nedílnou součástí běžného života občanů.

Digitální hygiena
Soubor zásad, postupů a návyků, které uživatelům umožňují bezpečný pohyb ve virtuálním prostředí. Jedná se tedy o proaktivní přístup uživatelů k přístupu ke své digitální stopě, zabezpečení, atd.

3.1 Zabezpečení digitální společnosti a veřejné správy

ČR již několik let usilovně digitalizuje veřejnou správu. Budování digitalizované infrastruktury veřejné správy musí probíhat s maximálním důrazem na zajištění kybernetické bezpečnosti již v počátcích samotné výstavby. Samotný chod celé infrastruktury a její správa však musí také dbát na vysokou míru zabezpečení proti kybernetickým hrozbám. V tomto směru je potřeba reflektovat aktuální bezpečnostní situaci, pravidelně provádět koordinovanou a kontinuální analýzu hrozeb a rizik a na jejím základě přijímat patřičná opatření.

Digitální infrastruktura bude dotvářena s cílem zajištění vzájemné kompatibility technologií užívaných v jednotlivých sektorech veřejné správy. V tomto ohledu bude ČR nadále podporovat využívání unifikovaných informačních kanálů umožňujících bezpečnou výměnu dat.

Další klíčovou vlastností digitální infrastruktury je robustnost. Stát musí garantovat plynulost fungování infrastruktury za všech okolností. Navzdory robustnosti je nutné rovněž přistoupit k vytvoření alternativních způsobů poskytování služeb v případech, kdy by došlo k narušení schopnosti státní správy poskytovat služby elektronicky.

3.2 Vzdělávání a osvěta

Kybernetické hrozby se s rozšiřováním moderních technologií a jejich zařazením do společnosti staly nedílnou součástí života všech obyvatel. ČR proto musí tuto situaci i nadále reflektovat a začleňovat problematiku kybernetické bezpečnosti do všech úrovní vzdělávacího systému, a to napříč obory. Je potřeba akcentovat především bezpečnostní rozměr jejich používání.

Prostřednictvím kvalitního a modernizovaného vzdělávání je nutné posilovat informační gramotnost, zodpovědnost a odolnost obyvatel, což povede i k celkovému posílení kybernetické bezpečnosti státu. V oblasti vzdělávání bude kladen důraz na

projekty, které cílí na osvojení návyků potřebných pro bezpečný pohyb na internetu a používání digitálních technologií již od úrovně mateřských škol.

Vedle vzdělávání dětí, žáků a studentů se bude stát soustředit i na vzdělávání dalších vybraných cílových skupin. Jednat se bude o pedagogické pracovníky či zaměstnance veřejné správy. Pedagogičtí pracovníci jsou stavebním prvkem vzdělávacího systému a jejich efektivní vzdělávání v kybernetické bezpečnosti je nezbytné pro rozvoj informační gramotnosti žáků a studentů i jich samotných jako občanů a výrazně napomůže úpravě vzdělávacího systému s ohledem na tuto problematiku. Vzdělávání zaměstnanců veřejné správy pak přispěje k větší odolnosti samotných subjektů veřejné správy proti kybernetickým hrozbám. Koncoví uživatelé bývají oblíbeným terčem útočníků v kyberprostoru. V tomto ohledu musí být ČR schopna poskytnout vhodné zázemí zejména pro specializované vzdělávání odborníků podílejících se na zajišťování sytému kybernetické bezpečnosti ve státě, stejně tak jako pro vzdělávání a osvětu dalších relevantních skupin.

Další významnou skupinou populace, která je vystavena negativním vlivům používání moderních technologií, jsou senioři. Na ně je zapotřebí edukativně působit zejména v oblastech schopností bezpečného používání digitálních technologií a rozeznávání dezinformací. Vedle seniorů budou pravidelně vzdělávány i další rizikové skupiny, které se vyskytují napříč všemi generacemi a vyžadují specifické zacílení.

Součástí vzdělávacích aktivit budou i nadále plošné i úzce zaměřené osvětové kampaně. Zodpovědné orgány státní správy budou za přispění zástupců soukromého sektoru, akademické sféry či neziskových organizací výrazným způsobem napomáhat k osvětě na poli kybernetické bezpečnosti. Osvětové akce pomáhají nejenom navyšovat informovanost o kybernetické bezpečnosti, ale i budovat důvěru prostřednictvím jejich otevřeného charakteru, který pomáhá přiblížit a popsat činnost státní správy a odpovědných subjektů soukromého sektoru či akademie.

Odolný systém zajištění kybernetické bezpečnosti

3.3 Rozšiřování expertní základny

ČR bude aktivně vytvářet a udržovat kvalifikovanou pracovní sílu v oblasti kybernetické bezpečnosti a rozvíjet tak svou základnu vzdělaných a motivovaných lidí jako jeden z nejcennějších zdrojů státu. Z toho důvodu musí ČR působit zejména na dvou základních úrovních.

První úrovní je identifikace současných talentů a motivace lidí ke studiu a práci v oblasti kybernetické bezpečnosti. Je proto zapotřebí systematicky investovat do moderních osvětových a vzdělávacích programů a koordinovat svou snahu s akademickou sférou. Zároveň musí orgány státní správy vynakládat prostředky na nábor stávajících talentů a také vytvoření patřičných pracovních podmínek. Státní správa musí být konkurenceschopná na vysoce konkurenčním trhu práce v oblasti kybernetické bezpečnosti. Musí vytvořit takové pracovní prostředí, které motivuje stávající talenty k rozhodnutí pracovat pro státní organizace, potažmo bezpečnostní složky státu.

Druhou úrovní je nastavení proaktivní práce s již vybranými jedinci. V této souvislosti musí státní správa usilovat o udržení svých pracovníků v oblasti kybernetické bezpečnosti. K tomuto účelu musí opět vytvořit patřičné pracovní podmínky. Nejedná se přitom pouze o odpovídající platové ohodnocení těchto zaměstnanců, ale i o vytvoření účinného motivačního systému interního vzdělávání, kariérního růstu a vhodnému nastavení konkurenceschopných podmínek.

Kromě těchto dvou základních úrovní je však zapotřebí nabídnout možnost podílet se na kybernetické bezpečnosti ČR i všem dalším renomovaným expertům, kteří pracují i vně státní správy. Využití jejich schopností bude v následujících letech vhodným způsobem institucionalizováno, a to zejména pro případy vážného ohrožení ČR, které by si vyžádalo větší množství lidských zdrojů, než je státu standardně k dispozici. Tento systém zapojení kybernetických expertů vně státní správy napomůže vytvořit časově dostupnou a kvalifikovanou skupinu dobrovolníků. ČR v této souvislosti nabídne uplatnění pro experty jak ze soukromého, neziskového, tak i akademického sektoru.

STRATEGICKÉ CÍLE

Vize		
Česká republika bude mít odolnou společnost a infrastrukturu, v kyberprostoru bude vystupovat sebevědomě a bude aktivně čelit celému spektru kybernetických hrozeb za pomocí spolehlivých spojenectví.		
Sebevědomě v kyberprostoru	**Silná a spolehlivá spojenectví**	**Odolná společnost 4.0**
Strategické cíle		
• Celonárodní přístup s důrazem na sdílení informací, koordinaci a spolupráci • Rozvoj schopností a kapacit státu v kybernetické bezpečnosti • Posílení zabezpečení a odolnosti infrastruktury • Rozvoj schopností predikce, detekce a agilní reakce na kybernetický útok • Účinná strategická komunikace • Prevence a potírání kybernetické kriminality	• Efektivní mezinárodní spolupráce • Tvorba spojenců • Prosazování zájmů ČR v zahraničí • Vytváření dialogu v mezinárodním prostředí • Podpora otevřeného a bezpečného chování v kyberprostoru • Export know-how	• Zajištění bezpečnosti digitalizace státní správy / eGovernmentu • Kvalitní systém vzdělávání • Osvětová činnost • Spolupráce státu, soukromé sféry a občanů • Vytváření expertní základny

IMPLEMENTACE

Národní strategie kybernetické bezpečnosti ČR je ve své podrobnější povaze převedena do konkrétních úkolů v rámci Akčního plánu. Oba dokumenty jsou tvořeny v koordinaci s relevantními subjekty zodpovědnými v podstatných oblastech kybernetické bezpečnosti pro plnění jednotlivých úkolů. Národní úřad pro kybernetickou a informační bezpečnost, jakožto gestor kybernetické bezpečnosti v ČR, bude průběžně sledovat, diskutovat, hodnotit a koordinovat plnění jednotlivých cílů. Hodnocení stavu kybernetické bezpečnosti bude prezentováno NÚKIB v rámci Zprávy o stavu kybernetické bezpečnosti v ČR za relevantní roky, jejíž přílohou bude hlášení o stavu naplňování Akčního plánu.

SEZNAM POUŽITÝCH ZKRATEK

BIS – Bezpečnostní informační služba

CERT – Cyber Emergency Response Team

ČR – Česká republika

EU – Evropská unie

GovCERT.CZ – vládní CERT

MZV – Ministerstvo zahraničních věcí

NATO – Severoatlantická aliance

NCKO – Národní centrum kybernetických operací

NCOZ SKPV – Národní centrála proti organizovanému zločinu Služby kriminální policie a vyšetřování

NÚKIB – Národní úřad pro kybernetickou a informační bezpečnost

OBSE – Organizace pro bezpečnost a spolupráci v Evropě

OECD - Organizace pro hospodářskou spolupráci a rozvoj

OSN – Organizace spojených národů

ÚZSI - Úřad pro zahraniční styky a informace

VeKySIO – Velitelství kybernetických sil a informačních operací

VZ – Vojenské zpravodajství