

Národní strategie kybernetické bezpečnosti

A large graphic of a Christmas tree composed of binary code (0s and 1s) on a blue background with a white diagonal stripe. The tree is formed by rows of varying lengths of 0s and 1s, creating a triangular shape. The background is a solid blue color, and a white diagonal stripe runs from the bottom left towards the top right, passing behind the tree. The overall style is modern and digital.

2026

NÚKIB



Národní úřad
pro kybernetickou
a informační
bezpečnost

Obsah

4 Úvodní slovo ředitele NÚKIB

6 Seznam použitých zkratk

8 Shrnutí strategie

14 Vnější faktory: Bezpečnostní prostředí

22 Vnitřní faktory: Systém zajišťování kybernetické bezpečnosti v Česku

28 Vize a strategické cíle

30 Strategická oblast: Bezpečná strategická infrastruktura

34 Strategická oblast: Celospolečenská připravenost a rozvoj

37 Strategická oblast: Mezinárodní spolupráce a prosazování zájmů

41 Implementace

41 Zdroje dat

Úvodní slovo ředitele NÚKIB

Vážené dámy, vážení pánové,

Národní strategie kybernetické bezpečnosti, kterou právě čtete, stojí na pevných základech více než patnáctileté tradice strategického budování bezpečného kyberprostoru Česka na národní i mezinárodní úrovni. V současnosti jsme svědky zásadních změn v mezinárodním bezpečnostním prostředí, kdy nejen kybernetické hrozby nabývají nových podob a jejich původci nových ambicí.

Současná doba je protkána neustálým tlakem na digitalizaci všech oblastí života, což nás staví před výzvu, jak zajistit stabilitu, ochranu a udržitelný rozvoj informačních technologií i společnosti samotné.

Mnohé z těchto technologií jsou dnes nezbytnou součástí fungování státu, hospodářství i každodenní komunikace nás, občanů. Zároveň sledujeme rostoucí závislost na těchto technologiích, spojenou s vyšším rizikem jejich zneužití ke kybernetickým útokům. Rozsah i intenzita kybernetických útoků v posledních letech prudce rostou a rozhodně svůj potenciál ještě nevyčerpaly. Je proto třeba více než kdy dříve klást důraz na posilování obranných kapacit, využívání moderních bezpečnostních technologií a na prohlubování spolupráce mezi veřejným, soukromým a akademickým sektorem.

Tato strategie navazuje na klíčové národní a nadnárodní strategické dokumenty, které vymezují základní bezpečnostní směřování Česka a potvrzují jeho pevné ukotvení v Evropské unii (EU) a Severoatlantické alianci (NATO). Jedná se například o Bezpečnostní strategii České republiky a Obrannou strategii České republiky, obě z roku 2023, Strategii kybernetické bezpečnosti EU pro digitální dekádu z roku 2020 a Strategickou koncepci NATO z roku 2022. Významnou roli při tvorbě tohoto dokumentu hrály též zkušenosti z přípravy a plnění předchozích národních strategií kybernetické bezpečnosti, které nám poskytly cenné poznatky o fungování systému zajišťování kybernetické bezpečnosti v Česku. Kromě nezbytné analýzy současného bezpečnostního prostředí a vytyčení cílů na následující roky je součástí této strategie rovněž realistický pohled na současné vnitřní kapacity Česka a identifikace oblastí, které je třeba dále zlepšovat. Věnovat se přitom musíme kromě technické roviny také stále více společenským tématům, jako jsou efektivní naplňování právního rámce nebo rozvoj mezinárodní spolupráce.



Ing. Lukáš Kintr

Ředitel Národního úřadu
pro kybernetickou
a informační bezpečnost

Jsem přesvědčen, že úspěšné naplnění strategické vize v tak široké oblasti, jako je kybernetická bezpečnost, spočívá především v interdisciplinárním přístupu a synergii mezi všemi zúčastněnými subjekty. Společně musíme vytvářet prostředí, kde se bezpečnost stává nedílnou součástí každého rozhodnutí – ať už se jedná o zavádění nových technologií, přijímání legislativy, vzdělávání odborníků, nebo sdílení informací v osobním životě. Investice do kybernetické bezpečnosti a zejména do těch, kteří ji pro nás zajišťují, jsou přitom nejen nutností, ale i konkurenční výhodou, která podporuje ekonomický růst naší země.

Česko má dobré předpoklady pro to, aby úspěšně čelilo novým hrozbám, a věřím, že tato strategie poslouží jako dlouhodobý základ nejen pro posílení naší obranyschopnosti a bezpečnosti v digitálním i fyzickém prostředí, ale i pro podporu prosperity a soudržnosti Česka.

Národní úřad
pro kybernetickou
a informační bezpečnost



Tato Národní strategie kybernetické bezpečnosti (NSKB) byla připravena Národním úřadem pro kybernetickou a informační bezpečnost (NÚKIB) a v srpnu 2025 byla s platností od roku 2026 schválena vládou České republiky, čímž nahradila předchozí strategii z roku 2021.

Seznam použitých zkratek

5G	5th Generation Mobile Network (5. generace mobilních sítí)
6G	6th Generation Mobile Network (6. generace mobilních sítí)
AČR	Armáda České republiky
APT	Advanced Persistent Threat
BIS	Bezpečnostní informační služba
CERT	Computer Emergency Response Team (tým rychlé reakce na kybernetické incidenty)
ČLR	Čínská lidová republika
ČTÚ	Český telekomunikační úřad
EDT	Emerging and Disruptive Technologies (nové a přelomové technologie)
ENISA	Evropská agentura pro kybernetickou bezpečnost
EU	Evropská unie
GDPR	Obecné nařízení o ochraně osobních údajů
IKT	Informační a komunikační technologie
InKyS	Informační a kybernetické síly
IoT	Internet of Things (Internet věcí)
IP4	Indo-Pacific Four (neformální označení pro Austrálii, Nový Zéland, Japonsko a Korejskou republiku jakožto indopacifické partnery NATO)
ITU	International Telecommunication Union (Mezinárodní telekomunikační unie)
MO	Ministerstvo obrany
MPO	Ministerstvo průmyslu a obchodu
MŠMT	Ministerstvo školství, mládeže a tělovýchovy
MV	Ministerstvo vnitra
MZV	Ministerstvo zahraničních věcí
NATO	North Atlantic Treaty Organization (Severoatlantická aliance)
NBÚ	Národní bezpečnostní úřad
NCKO	Národní centrum kybernetických operací

NSKB	Národní strategie kybernetické bezpečnosti
NÚKIB	Národní úřad pro kybernetickou a informační bezpečnost
OBSE	Organizace pro bezpečnost a spolupráci v Evropě
OECD	Organisation for Economic Cooperation and Development (Organizace pro hospodářskou spolupráci a rozvoj)
OSN	Organizace spojených národů
PČR	Policie České republiky
PPP	Public Private Partnership (Partnerství veřejného a soukromého sektoru)
RF	Ruská federace
ÚZSI	Úřad pro zahraniční styky a informace
VZ	Vojenské zpravodajství

Shrnutí strategie

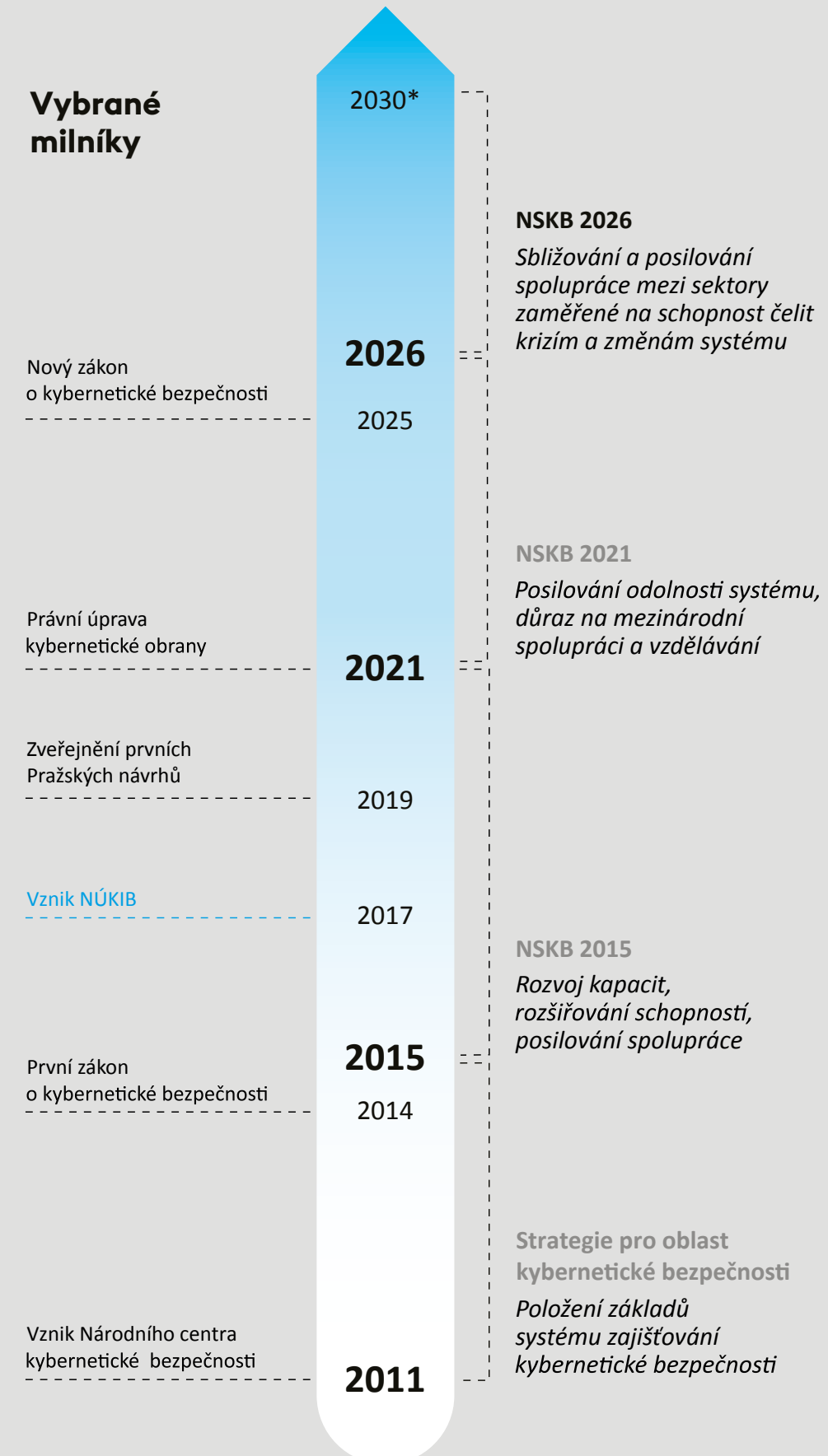
NSKB je vrcholným národním strategickým dokumentem pro kybernetickou bezpečnost a nedílnou součástí strategického rámce Česka. Vytváří jednotný a koordinovaný rámec zaměřený na:

- **bezpečnost a odolnost informačních a komunikačních systémů,**
- **kybernetickou obranu,**
- **kybernetickou diplomacii,**
- **boj s kybernetickou kriminalitou a posilování odolnosti společnosti vůči hrozbám v kyberprostoru.**

NSKB je rozdělena na analytickou a strategickou část. Analytická část popisuje současné bezpečnostní prostředí a stav zajišťování kybernetické bezpečnosti Česka. Je založena na SWOT analýze, která popisuje faktory vnější (hrozby a příležitosti prostředí) a vnitřní (silné a slabé stránky systému zajišťování kybernetické bezpečnosti Česka).

Navazující strategická část na základě těchto poznatků formuluje vizi a stanovuje strategické cíle k jejímu naplnění. NSKB vychází z Metodiky přípravy veřejných strategií Ministerstva pro místní rozvoj.

Vývoj strategického směřování Česka v kyberprostoru



*Zákonnou povinností je aktualizovat NSKB alespoň jedenkrát za 5 let, může se tak ale stát i dříve.

Analýza současného stavu

VNĚJŠÍ FAKTORY

Bezpečnostní prostředí

Hrozby

Mezinárodní bezpečnostní prostředí se zhoršuje a snižuje se jeho stabilita, což se projevuje i v kyberprostoru.

Množství útočníků a jejich schopnosti se zvyšují. Česku škodí hlavně státy podporované skupiny a kyberkriminalita.

Pokračuje globální rozvoj a profesionalizace kyberkriminality, která se objemem celkových škod aktuálně vyrovná nejsilnějším ekonomikám světa.

Zvyšující se závislost na konvenčních i nových technologiích a jejich dodavateli vede k nárůstu zranitelnosti.

Osobní a jiné citlivé údaje jsou nekontrolovaně šířeny a jejich zpracování probíhá ve státech s různou úrovní bezpečnosti.

Příležitosti

Prohlubování národní a mezinárodní spolupráce při zajišťování kybernetické bezpečnosti a obrany může kompenzovat nedostatek zdrojů a kapacit.

Intenzivnější spolupráce soukromého, akademického a veřejného sektoru posiluje schopnost zvládat krize v kyberprostoru.

Nové technologie mohou zvýšit efektivitu boje s kybernetickými hrozbami.

Investice do kybernetické bezpečnosti mohou kromě navýšení ochrany znamenat také konkurenční výhodu na trhu a mohou být jedním ze stimulů ekonomického růstu.

Zdroje pro financování kybernetické bezpečnosti lze kromě vlastních prostředků soukromých a veřejných organizací čerpat i z projektů a dotačních programů EU.

VNITŘNÍ FAKTORY

Systém zajišťování kybernetické bezpečnosti v Česku

Slabé stránky

Personální kapacity a financování kybernetické bezpečnosti nejsou dostatečné ve veřejném ani soukromém sektoru.

Existují významné rozdíly v úrovni bezpečnostní kultury a zabezpečení napříč regulovanými subjekty i celou společností.

Dotační podmínky a regulace, zejména ty z EU, jsou nepřehledné a neustále narůstají.

U bezpečnostních složek státu převažuje reaktivní přístup, některé procesy nejsou dostatečně nastaveny nebo jsou komplikované.

Silné stránky

Česko má vybudovaný vyspělý systém zajišťování kybernetické bezpečnosti.

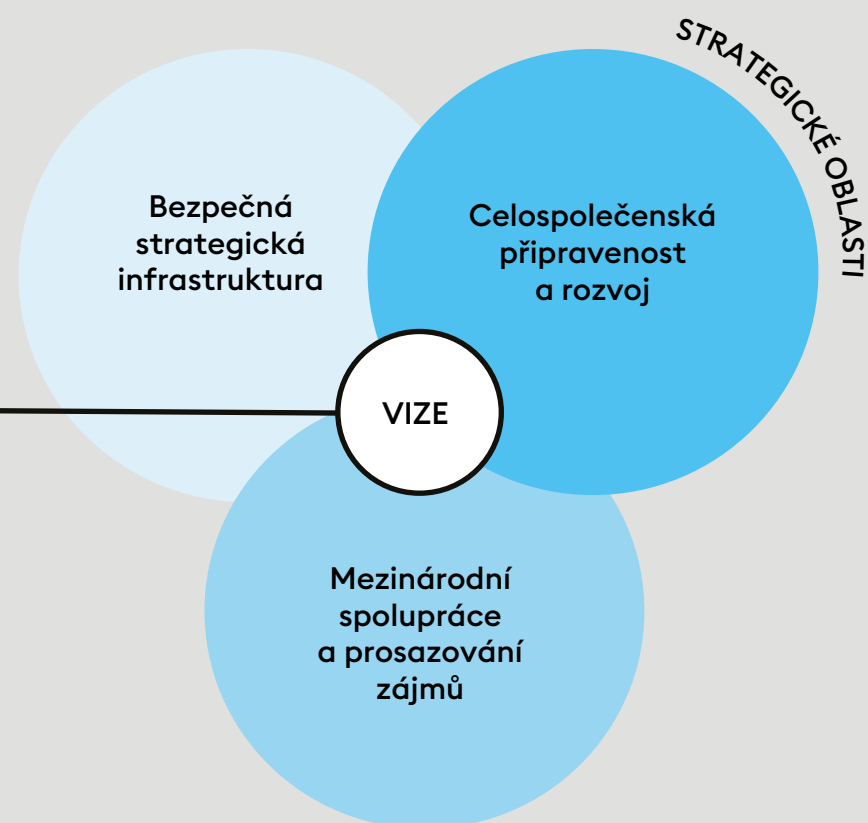
České instituce a experti mají vysokou úroveň expertízy a dobrou pověst v mezinárodním prostředí.

Napříč soukromým, akademickým a veřejným sektorem existuje dobře fungující bezpečnostní komunita.

Český soukromý a akademický sektor má vysoký inovační potenciál.

Vize a strategické cíle

Česko bude bezpečným a digitálně vyspělým státem s odolnou informační infrastrukturou, vzdělanou, kriticky myslící a inovativní společností a silnými mezinárodními i domácími partnerstvími, s jejichž pomocí zajistí efektivní ochranu a prosazování svých zájmů v kyberprostoru.



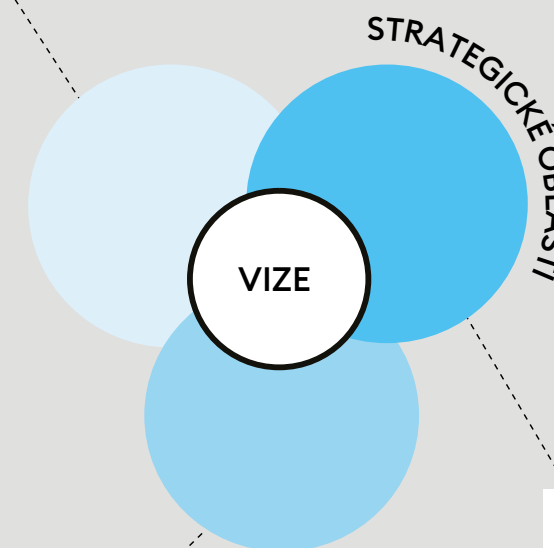
„Efektivně řízená a odolná infrastruktura bez rizikových závislostí proaktivně chrání organizace i jednotlivce před hrozbami v kyberprostoru.“

„Sebevědomé zahraniční vystupování Česka a budování důvěryhodných partnerství zajišťujících jeho silnou pozici v mezinárodním prostředí a vedoucí pozici v regionu.“

„Vzdělaná společnost s dostatkem expertů, vzájemná spolupráce a podpora inovací jako předpoklad dlouhodobě udržitelné bezpečnosti.“

STRATEGICKÉ CÍLE

- Ochrana a odolnost strategické infrastruktury před předvídanými i nepředvídanými hrozbami
- Proaktivní přístup, efektivní detekce a účinná reakce na kybernetické útoky a krize, včetně kybernetické obrany a boje s kybernetickou kriminalitou
- Regulace vyvažující národní bezpečnost a individuální práva jednotlivců
- Posílení financování a efektivnější nakládání se zdroji ve veřejném sektoru
- Sjednocování veřejné IT architektury a posílení data governance s důrazem na bezpečnost
- Prosazování bezpečných a odolných dodávek nejen do strategické infrastruktury



STRATEGICKÉ CÍLE

- Posilování počtů a motivace odborníků za účelem dlouhodobé udržitelnosti vysoké úrovně kybernetické bezpečnosti Česka
- Rozvoj celospolečenských digitálních kompetencí a bezpečnostní kultury
- Intenzivní spolupráce ke koordinaci a překonání rozdílů mezi sektory
- Rozvoj znalostí a schopností odborníků v kybernetické bezpečnosti
- Podpora výzkumu a inovací v oblasti kybernetické bezpečnosti
- Podpora vzniku bezpečných technologických alternativ

STRATEGICKÉ CÍLE

- Navazování nových a posilování stávajících strategicky významných partnerství
- Aktivní prosazování zájmů, cílů a priorit Česka při utváření mezinárodních pravidel i práva EU
- Asertivní vystupování proti nepřátelskému působení škodlivých aktérů v kyberprostoru, včetně atribuce útoků, diplomatické reakce a uplatňování sankcí
- Podpora otevřené strategické autonomie
- Ochrana globálního, otevřeného, bezpečného a svobodného kyberprostoru
- Posilování mezinárodního sdílení informací a rozvojové spolupráce

Vnější faktory: Bezpečnostní prostředí



Mezinárodní bezpečnostní situace se zhoršuje, dochází k otřesům dosavadní bezpečnostní architektury. Jsme svědky globálního mocenského soupeření a proměny mezinárodního řádu, kdy u některých států dochází k přenastavení jejich mezinárodních zájmů a způsobu jejich prosazování. Hrozí eskalace stávajících ozbrojených konfliktů a nelze vyloučit vypuknutí nových. Kyberprostor se stal standardním bojištěm současných mezinárodních konfliktů.

Dynamický technologický vývoj přináší nové příležitosti, ale i hrozby, zatímco s těmi původními se svět dosud nevypořádal. Závislost států a společnosti na informačních a komunikačních technologiích (IKT) dále narůstá a s tím roste i význam zranitelností těchto technologií a jejich zneužití škodlivými aktéry. Možnosti útočníků se rozšiřují a setrvale roste množství kybernetických útoků i jejich potenciálních cílů. Kybernetická bezpečnost tak dále nabývá na významu jako jeden ze základních předpokladů fungování ekonomiky státu a ochrany práv jednotlivců.

Utváří se nová geopolitika kyberprostoru

Mezinárodní bezpečnostní situace se v posledních letech prudce mění. Svobodný a otevřený Internet, založený na vícestranném modelu správy, je dlouhodobě pod útokem některých států, které se snaží tento model omezit a fragmentovat a Internet kontrolovat. Kybernetické operace probíhající nejen v souvislosti s válkou na Ukrajině nebo v rámci izraelsko-palestinského konfliktu potvrzují, že kyberprostor se stal standardním kolbištěm současných konfliktů a dochází k tzv. weaponizaci kyberprostoru. Je využíván pro vojenské účely, hybridní působení, přípravu potenciálního operačního prostředí pro možné zapojení v případě ozbrojených konfliktů. Tento trend bude nepochybně dále pokračovat a dotýká se i Česka. I za situace být zatím jen hrozícího ozbrojeného konfliktu, který by zahrnoval spojenecké státy NATO, lze očekávat intenzivní kybernetické útoky vedené na vojenskou i civilní infrastrukturu. To platí i pro případy, kdy by Česko sloužilo pouze jako tranzitní a hostující země pro spojenecké jednotky a techniku.

Přístup k datům, technologiím, výrobním kapacitám a surovinovým nebo jiným zdrojům je a dále bude klíčový. Stále více se zde přitom projevuje posilování vlivu nadnárodních korporací na úkor národních států. **Výzvou pro Česko, EU i NATO je dosahovat otevřené strategické autonomie, tedy rovnováhy mezi soběstačností a ekonomickou otevřeností vnějšímu světu, kterou komplikuje zejména nedostatek vlastních bezpečných a konkurenceschopných technologických alternativ, jenž prohlubuje závislost na technologiích zahraničních rivalů.**

PŘÍLEŽITOST

Většina států včetně Česka nemá dostatečné příležitosti a kapacity na to, aby si veškeré potřebné zdroje a technologie zajistila sama. Řešením této situace je pro státy s omezenými zdroji intenzivní spolupráce se spolehlivými partnery, a to na nadnárodní i mezinárodní úrovni. Klíčová je v tomto ohledu spolupráce zejména v rámci NATO a EU, dále také v OBSE, OECD, ITU, Radě Evropy a Organizaci spojených národů (OSN). Na národní úrovni pak napříč jednotlivými složkami státu, průmyslem a občanskou společností.

Ověřeným modelem pro posilování a prohlubování spolupráce jsou například účelově vymezená partnerství veřejného a soukromého sektoru (tzv. Public Private Partnership) nebo prohlubování spolupráce s národními i zahraničními partnery na projektech výzkumu a vývoje.

Podpora vývoje a výroby bezpečnostních řešení v rámci Česka, EU a NATO má potenciál nejen posílit kybernetickou odolnost všech zapojených států, ale i přispět k jejich ekonomickému růstu a prosperitě. Společná koordinace a sjednocování regulací a veřejných politik pak také přispívá k jednotnému a celkově vyššímu bezpečnostnímu standardu a může snížit transakční náklady přeshraničního obchodního styku.

Aktéři hrozeb

Hlavními aktéry ohrožujícími kybernetickou bezpečnost Česka i širšího demokratického světa jsou státy, které vedou sofistikované kybernetické operace s politickými cíli. Tyto aktivity slouží především k prosazování strategických zájmů, oslabování protivníků a získávání zpravodajsky cenných informací.

Ruská federace (RF): Dlouhodobá a bezprostřední hrozba pro bezpečnost Česka

RF je největší přímou a dlouhodobou hrozbu nejen pro kybernetickou bezpečnost Evropy. Ve své strategii kombinuje kybernetické útoky s hybridním působením s cílem oslabit obranyschopnost států, podkopat důvěru v demokratické instituce a destabilizovat společnost i ekonomiku.

RF se v kyberprostoru vůči Česku a jeho spojencům chová agresivně a jeho aktivity zahrnují kyberšpionáž, sabotáž a vlivové operace. Zaměřuje se primárně na strategické instituce státu, ale také na soukromé podniky a jednotlivce, kteří vystupují proti ruským zájmům nebo podporují Ukrajinu. Útok vedený ze strany RF proti českým institucím skrze zranitelnosti aplikace Microsoft Outlook byl také prvním případem veřejné atribuce kybernetického útoku ze strany Česka. Došlo k ní v květnu 2024.

Agresivní politika RF, válka na Ukrajině a hrozba konfliktu RF se spojeneckým státem NATO zůstanou pro Česko zásadním zdrojem hrozeb i do budoucna. Lze přitom očekávat, že po případném uzavření míru na Ukrajině relokuje RF uvolněné kapacity na další škodlivé působení v kyberprostoru a na přípravu na další ozbrojený konflikt.

Další státní aktéři

Pro Česko jsou v kyberprostoru zdrojem hrozeb také:

Korejská lidově demokratická republika, která páchá finanční kyberkriminalitu za účelem financování jaderného programu, obchází sankce a provádí kyberšpionáž zaměřenou na strategicky důležité technologie, včetně zbrojního výzkumu a satelitních systémů.

Íránská islámská republika, která se obecně zaměřuje na kybernetické útoky proti západním státům, Izraeli a arabským zemím v Perském zálivu, přičemž v Česku bylo škodlivé působení Íránu detekováno ve vztahu ke kritické infrastruktuře v oblasti vodoхозяйství.

S ohledem na velmi dynamický vývoj mezinárodního bezpečnostního prostředí nelze v následujících letech vyloučit, že se mezi původce hrozeb pro Česko v kyberprostoru zařadí i další státy.

Čínská lidová republika (ČLR): Sofistikovaný aktér s globálními ambicemi

ČLR představuje komplexní systémovou výzvu pro demokratické státy. Usiluje o přetvoření mezinárodního řádu ve svůj prospěch, k čemuž využívá kombinaci kybernetických operací, socioekonomického tlaku a hybridního působení. Její kybernetické operace jsou primárně zaměřené na špionáž a získání přístupu do kritických systémů s cílem je ve vhodnou chvíli ovládnout nebo zneužít (tzv. prepositioning). Cílem jsou státní instituce, akademický sektor, elektronické komunikace a odvětví s vysokou strategickou hodnotou. Kyberšpionážní útok ČLR na české Ministerstvo zahraničních věcí (MZV) byl druhým případem veřejné atribuce ze strany Česka, provedené v květnu 2025.

Hrozbou ze strany ČLR je pro Česko také vysoké zastoupení čínských technologií ve strategické infrastruktuře. To s ohledem na čínské právní prostředí a bezpodmínečnou povinnost čínských společností spolupracovat s tamějším režimem zvyšuje hrozbu špionáže, sabotáže a technologické závislosti. Lze očekávat, že expanzivní politika ČLR, včetně rostoucího napětí v oblasti Indo-Pacifiku a zejména Tchaj-wanu, bude i v následujících letech zdrojem hrozeb pro ekonomickou a technologickou bezpečnost Česka.

Uvedené státy v kyberprostoru zpravidla operují prostřednictvím vysoce sofistikovaných tzv. APT skupin (z anglického Advanced Persistent Threats), jejichž členové jsou napojeni na zpravodajské služby nebo armády uvedených států. Tyto skupiny nicméně nemusí být vždy přímo pod státní kontrolou a mohou sledovat i vlastní kyberkriminální nebo hacktivistické cíle. APT skupiny provádějí dlouhodobé sofistikované cílené operace a usilují o dlouhodobou skrytou přítomnost v napadených systémech. Pro Česko představují největší hrozbu APT skupiny napojené na RF a ČLR.

Významným škodlivým aktérem jsou pro Česko také **kyberkriminální skupiny**, jejichž hlavní motivací je generování ekonomického prospěchu. Ty se v některých případech z neformálních kriminálních gangů proměnily v legitimní obchodní společnosti, které nástroje škodlivého působení komerčně vyvíjejí a prodávají (tzv. **kyberkriminalita jako služba**) anebo své kriminální nebo jiné škodlivé aktivity kryjí legitimní činnostmi.

Vysoce sofistikované nástroje k páčání této trestné činnosti, včetně technologií umělé inteligence, které byly dříve dostupné jen pro ekonomicky silné státní aktéry nebo jimi podporované subjekty, jsou nyní levnější a snadno dostupné i pro méně schopné útočníky. Lze očekávat, že do budoucna bude tento trend pokračovat a nadále poroste počet kybernetických útoků i útočníků, stejně jako škody, které kyberkriminalita způsobuje.

Boj orgánů činných v trestním řízení s kyberkriminalitou a její prevenci přitom navzdory klesající anonymitě online prostředí ztěžuje zvýšené využívání anonymizačních prostředků a služeb. Probíhající diskuse o možnosti jejich plošného narušování orgány činnými v trestním řízení však naráží na obavy ze vzniku nových zranitelností a zneužitelnosti ze strany škodlivých aktérů, které by mohly mít za důsledek ohrožení obsahu veškeré elektronické komunikace.

V roce 2023 globální škody způsobené kyberkriminalitou dosáhly 191 bilionů korun českých, což by objemem finančních prostředků odpovídalo třetí největší ekonomice světa. Doroku 2030 se očekává nárůst globálních škod způsobených kyberkriminalitou až na 690 bilionů korun českých, tedy na téměř trojnásobek oproti roku 2023. Očekává se, že výnosy z kyberkriminality v roce 2025 globálně překonají výnosy z ilegálního obchodu s drogami¹.

České banky u svých klientů evidovaly jen v roce 2023 téměř 70 tisíc obětí kriminality páchané v kyberprostoru, které celkově utrpěly škodu ve výši 1,35 miliardy korun českých. Oproti roku 2022 se tak počet bankami zaznamenaných skutků v Česku ztrojnásobil, část obětí přitom útok zřejmě vůbec neohlásila².

Z hlediska dopadů svého působení jsou pro Česko prozatím méně závažnými, ale obecně relevantními aktéry hrozeb i **hacktivistické skupiny**, které využívají kyberprostor k politickému, sociálnímu nebo jinému aktivismu a v některých případech mají též návaznost na státní aktéry.

Řada uvedených státních i nestátních aktérů spolu na krátkodobé nebo dlouhodobé bázi spolupracuje nebo koordinuje svou činnost, což hrozby s nimi spojené dále násobí.

Technologický rozvoj urychluje změnu prostředí

Vlivem technologického rozvoje, pokračující digitalizace a geopolitického napětí jsou kybernetické útoky sofistikovanější a dostupnější než kdy dříve a útočníci toho aktivně využívají. **Podle analýzy společnosti Check Point Software Technologies vzrostl v Česku ve třetím čtvrtletí roku 2024 průměrný počet kybernetických útoků na jednu společnost meziročně o 69 %³.**

Nové a přelomové technologie, z anglického Emerging and Disruptive Technologies (EDT), zásadně mění způsob, jakým funguje digitální i fyzický svět. Umělá inteligence, kvantová výpočetní technika, internet věcí, autonomní dopravní nebo vojenské systémy, cloudové technologie nebo některé technologie nových generací sítí elektronických komunikací (např. 5G a 6G) zrychlují tempo, jakým se proměňuje společnost, ekonomika i fungování státu a bezpečnost. EDT přinášejí nové možnosti efektivity a výkonnosti, ale také zvyšují energetickou náročnost, snižují transparentnost fungování IT systémů a otevírají prostor pro vznik nových kybernetických hrozeb a zranitelností.

PŘÍLEŽITOST

Spolu s novými hrozbami narůstá i potřeba hledat nová bezpečnostní řešení. EDT, obzvláště **umělá inteligence a postkvantová kryptografie, otevírají dveře k efektivnějším a pokročilejším možnostem posílení kybernetické bezpečnosti a obrany nejen proti novým, ale i proti stávajícím hrozbám.** Tak jako v jiných oblastech lidské činnosti mohou i při zavádění a provozu nástrojů kybernetické bezpečnosti nové technologie přinést rovněž výraznou úsporu celkových nákladů na zabezpečení.

Kromě vzniku nových technologií hrají významnou roli pro bezpečnost Česka a jeho spojenců také nové způsoby využití těch stávajících. Příkladem mohou být satelitní služby, které kromě navigace stále častěji slouží i k přenosu dat a šifrovacích klíčů, čímž snižují závislost na pozemní infrastruktuře, ale zároveň přinášejí více cest pro narušení bezpečnosti přenášených informací.

Narůstá komplexita a množství dat v kyberprostoru

Pokračuje trend zvyšujícího se množství a složitosti IKT a systémů, které je využívají, a jejich zvyšující se vzájemné propojenosti. Stávají se stále náročnějšími na správu, zabezpečení a efektivní monitoring hrozeb. **Důsledky kybernetických útoků nebo neúmyslných technických chyb tak mohou být pro společnost horší než kdy dříve.** I drobné narušení bezpečnosti jednoho systému může způsobit rozsáhlé ochromení dodávky pitné vody, provozu vlaků, poskytování zdravotní péče nebo výroby a distribuce pohonných hmot. Nízká prioritizace kybernetické bezpečnosti v organizaci nebo investice do nedůvěryhodných a nedostatečně zabezpečených technologií tak mohou způsobit rozsáhlé ekonomické ztráty a zneužití citlivých dat nebo i přímé ohrožení zdraví a života osob.

PŘÍLEŽITOST

Zájem jednotlivců i organizací o kybernetickou bezpečnost se zvyšuje a s tím také ekonomické příležitosti v této oblasti. Přestože investice do zajištění kybernetické bezpečnosti představují pro soukromé i veřejné rozpočty finanční zátěž, tyto investice se dlouhodobě vyplácí. **Výdaje na bezpečnostní opatření jsou pro organizace téměř bezvýhradně násobně levnější než náklady na řešení škod spojených s úspěšným kybernetickým útokem.** Například podle zprávy⁴ Evropské agentury pro kybernetickou bezpečnost (ENISA) zaznamenaly organizace, které investovaly do moderních bezpečnostních nástrojů zahrnujících umělou inteligenci a automatizaci, v průměru snížení nákladů na únik dat o 38,4 milionu korun českých a zkrácení doby potřebné k identifikaci a řešení kybernetického incidentu o 108 dní.

Na celostátní a celospolečenské úrovni jsou pak vhodně zvolené investice do kybernetické bezpečnosti strategickým vkladem do know-how, technologického rozvoje a ekonomické konkurenční výhody Česka.

Příležitost pro rozvoj a posílení kybernetické bezpečnosti představuje také **efektivní čerpání dostupných vnějších finančních zdrojů, například z dotačních programů EU.**

Globální dodavatelské řetězce jsou zranitelné a mohou být ochromeny nebo kompromitovány. Závislost na zahraničních dodavatelských technologiích zvyšuje riziko strategické závislosti Česka na cizích státech a omezuje jeho schopnost řešení krizových situací. Na jednotlivých dodavatelských jsou přitom z důvodu jejich tržní dominance nebo nedostatku vhodných alternativ často závislá celá odvětví. Zejména ve veřejném sektoru pak změnu dodavatele komplikují i nevýhodná smluvní ujednání, která mohou vést až k praktické vázanosti fungování organizace na stávajícího dodavatele – stavu označovaném jako tzv. vendor lock-in.

Jednotlivci a organizace o sobě v kyberprostoru sdílí velké množství dat včetně osobních a jiných citlivých údajů. Tato data, která jsou sdílena jak úmyslně a vědomě, tak neúmyslně nebo zcela nevědomě, **se následně stávají aktivem společností, jejichž služby je zpracovávají a dále prodávají a soukromé i veřejné subjekty z nich mohou vyvodit nebývalý rozsah informací.** Na tomto trendu se obzvláště podepisuje šíře využívání mobilních a IoT zařízení nebo digitalizace veřejných služeb a evidencí. Data jsou také nezřídka ukládána mimo EU nebo země s obdobnými standardy ochrany, což výrazně zvyšuje riziko jejich krádeže nebo zneužití. Nárůst využívání digitálních identit a digitalizace finančních transakcí v kombinaci s pokročilými metodami sociálního inženýrství také usnadňuje páchaní **finančních podvodů.**

ENISA⁴ zaznamenala v EU za druhou polovinu roku 2023 a první polovinu roku 2024 přes 11 000 kybernetických incidentů, přičemž mnoho z nich se událo v rámci veřejné infrastruktury a soukromých společností. Průměrné náklady byly vyčísleny na více než 97 milionů korun českých.

Níže jsou uvedeny vybrané příklady útoků a zranitelností s významným dopadem na veřejnou infrastrukturu:

Při napadení **Irské zdravotní služby (2021)**, které vedlo k nucenému vypnutí všech jejích informačních systémů, musela řada nemocnic odložit plánované zákroky a vyšetření. Požadované výkupné činilo v přepočtu **440 milionů korun českých**, ale vláda tuto platbu odmítla provést. Celkové škody měly dosáhnout až **15 miliard korun českých** a plné obnovení systémů trvalo přes tři měsíce.

Útok ruskojazyčného kyberkriminálního gangu na informační systémy **Kostariky (2022)** na několik týdnů paralyzoval fungování 27 státních institucí a ohrozil finanční systém země. Hackeři požadovali výkupné v přepočtu ve výši **470 milionů korun českých**, které vláda odmítla zaplatit, přičemž celkové škody jen pro soukromý sektor měly představovat téměř **3 miliardy korun českých** v průběhu 48 hodin.

Ransomwarový útok na subdodavatele britské zdravotní služby **NHS Advanced (2023)** způsobil výpadky u více než 200 nemocnic a klinik. Přestože výše zaplaceného výkupného nebyla zveřejněna, škody se odhadují v přepočtu na **stovky milionů až miliardy korun českých.**

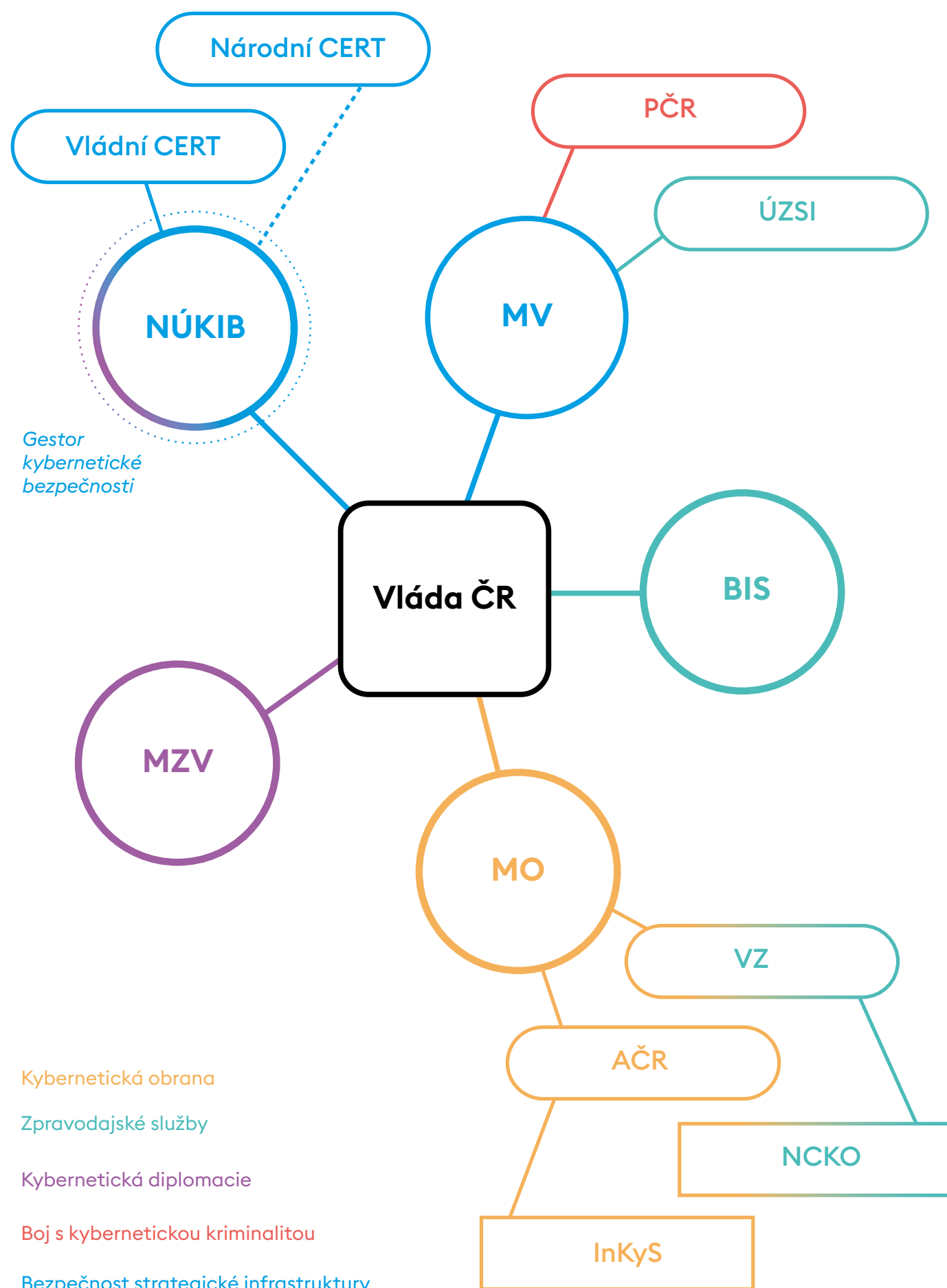
Chyba v aktualizaci bezpečnostního nástroje společnosti **CrowdStrike (2024)** způsobila globální výpadek systému Windows u přibližně **8,5 milionu instalací, včetně finančních systémů a systémů veřejné správy, letecké dopravy a záchranných složek.** Přestože nešlo o úmyslný útok, ale o nezáměrnou zranitelnost v dodavatelském řetězci, odhaduje se, že náklady plynoucí z omezení služeb přesáhly **220 miliard korun českých.**

Vnitřní faktory: Systém zajišťování kybernetické bezpečnosti v Česku



Česko má vyspělý systém zajišťování kybernetické bezpečnosti se silnou pozicí NÚKIB a dalších státních institucí, jehož součástí je i soukromý, akademický a neziskový sektor. Kybernetická bezpečnost se stala pro Česko důležitou součástí národní bezpečnosti. Přes veškeré pokroky a další budování odolnosti a reakčnosti vůči stále sofistikovanějším hrozbám komplikují zejména nedostatek financí, odborníků a alternativních technologických řešení i nerovnoměrná úroveň zabezpečení subjektů regulace.

Role klíčových institucí v systému zajišťování kybernetické bezpečnosti v Česku



Zajišťování kybernetické bezpečnosti se v Česku za patnáct let probíhajícího strategického plánování posunulo od technické disciplíny, omezené na jednotlivé organizace, k celospolečenskému a multidisciplinárnímu tématu a klíčové součásti národní bezpečnosti. Na položených základech se dále budují kapacity kybernetické obrany, čelí kybernetické kriminalitě a rozvíjí kybernetická diplomacie.

Na systému zajišťování bezpečného kyberprostoru Česka se kromě NÚKIB coby ústředního správního úřadu pro kybernetickou bezpečnost podílí i gestoři jednotlivých klíčových oblastí (viz schéma výše). V duchu celostátního přístupu je do systému zapojena řada dalších státních orgánů, které v rámci své působnosti zásadním způsobem přispívají k bezpečnému kyberprostoru, jako například Ministerstvo průmyslu a obchodu, Český telekomunikační úřad nebo Ministerstvo školství, mládeže a tělovýchovy. Zvláštní postavení pak mají vládní a národní CERT, které koordinují vnitrostátní monitoring, detekci a reakci na kybernetické bezpečnostní incidenty. NÚKIB a další státní instituce se v těchto oblastech postupně staly respektovanými a důvěryhodnými autoritami v domácím i mezinárodním prostředí.

Kromě regulační, dozorové a koordinační role státu se na zajišťování kybernetické bezpečnosti Česka podílejí i nestátní subjekty, veřejný a soukromý sektor tak společně tvoří strategickou infrastrukturu Česka. Úroveň její celkové bezpečnosti vychází z úrovně zabezpečení jednotlivých regulovaných subjektů a z jejich schopnosti vzájemné spolupráce a sdílení informací.

Regulované subjekty

Regulované subjekty jsou v kontextu NSKB veřejnoprávní nebo soukromoprávní organizace a jednotlivci, kterým plynou práva a povinnosti z právních předpisů upravujících některou z oblastí kybernetické bezpečnosti. Příkladem takových právních předpisů jsou zákon o kybernetické bezpečnosti, zákon o elektronických komunikacích nebo obecné nařízení o ochraně osobních údajů (GDPR).

Strategická infrastruktura

Strategickou infrastrukturou jsou zařízení, prostředky a jiné prvky systémů strategicky významných pro zajištění fungování státu a společnosti. V oblasti kybernetické bezpečnosti spadají do strategické infrastruktury zejména informační a komunikační systémy státu a dalších regulovaných subjektů.

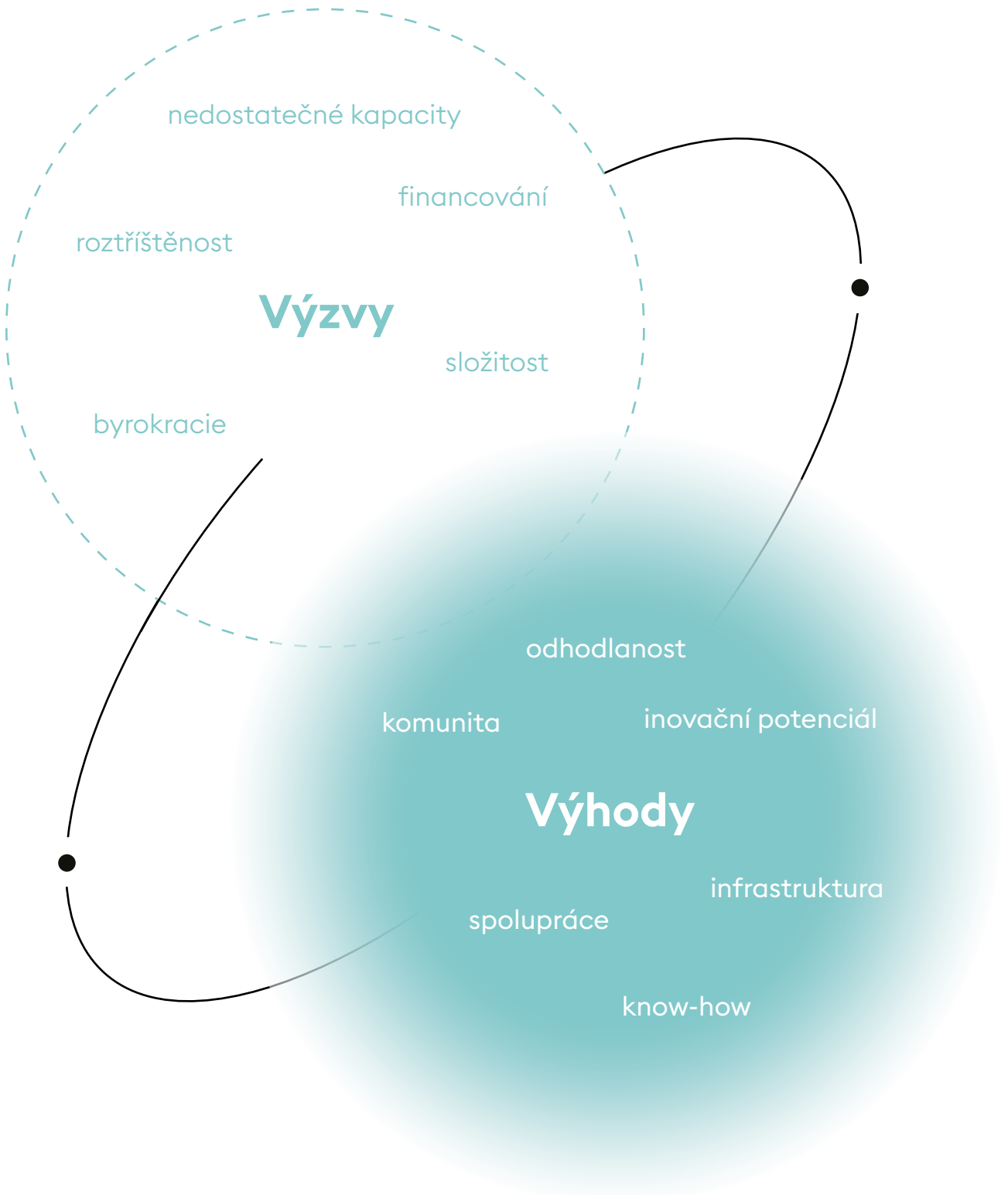
V oblasti ochrany strategické infrastruktury v kyberprostoru a výkonu státní správy v této oblasti patří Česko dlouhodobě mezi světové průkopníky. V roce 2014 přijalo jako jeden z prvních států na světě ucelený zákon o kybernetické bezpečnosti, vycházející ze soudobé právní nauky a z odvětvových standardů. Česko je aktivní v přípravě a implementaci legislativy a politik EU a NATO a navrhuje vlastní bezpečnostní mechanismy, jako je například prověřování bezpečnosti dodavatelských řetězců strategické infrastruktury. Mnohé státy v Evropě i zbytku světa začínaly budovat své kapacity a právní rámce v kybernetické bezpečnosti až výrazně později a zkušenosti zdejších odborníků v technických i netechnických oborech jsou dlouhodobě vysoce poptávaným a ceněným vývozním artiklem české diplomacie.

Česko má také dobře fungující komunitu kyberbezpečnostních expertů různých specializací napříč státními i nestátními institucemi, která se těší důvěře u soukromých a akademických subjektů a spolu s nimi je zdrojem inovací a nositelem unikátního know-how. **Vysoká kvalifikace českých expertů a jejich inovační potenciál se projevují i ve skutečnosti, že některé z celosvětově nejrozšířenějších komerčních bezpečnostních nástrojů v IKT vyvíjí české společnosti nebo mají tuzemský původ.** V oblasti výzkumu a vývoje v kybernetické bezpečnosti se zvyrazňuje role NÚKIB jakožto národního koordinátora, který podporuje účast českého průmyslu a akademiků na přeshraničních projektech a zprostředkovává jim grantové financování.

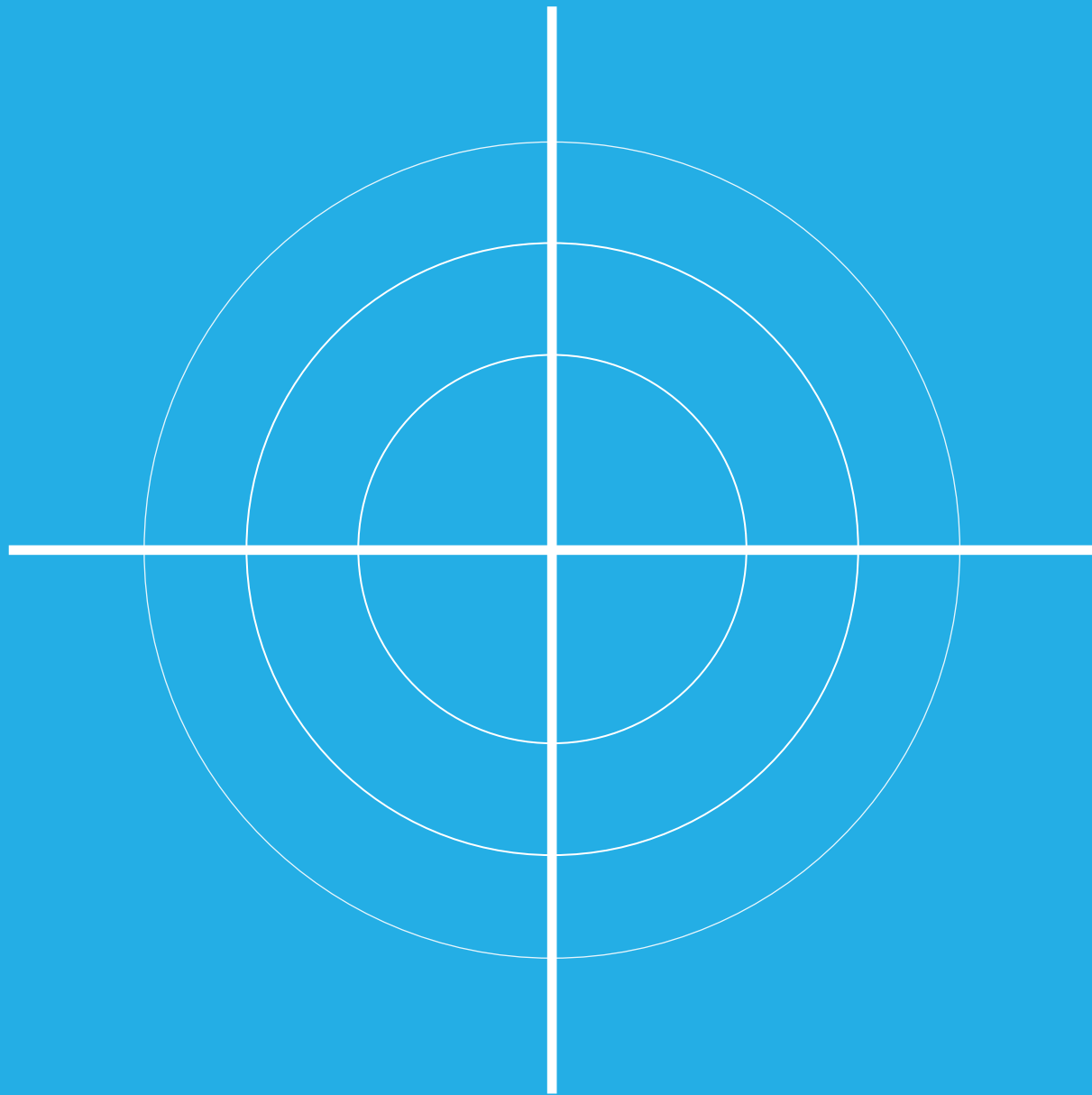
Navzdory pozitivním stránkám se zajišťování kybernetické bezpečnosti v Česku potýká s některými omezeními a nedostatky. **Nejvýznamnějším a dlouhodobým problémem pro kybernetickou bezpečnost Česka je nedostatek odborných personálních kapacit a nastavení systému financování.** Nedostatkem expertů, kterých chybí v celé EU až 300 000⁵, jsou v Česku poznamenány zejména malé a střední podniky a veřejná správa. Dlouhodobé prohlubování tohoto stavu je zejména u státní správy způsobeno nedostatečným přiřazením financí ze státního rozpočtu na platy expertů a rigidně nastaveným odměňováním. Také zdroje alokované na investiční a provozní výdaje spojené s kybernetickou bezpečností jsou ve veřejném i soukromém sektoru i přes postupné navyšování stále nedostatečné. Vlivem procesních překážek se jednotlivým organizacím nedaří dostatečně čerpat prostředky z národních nebo unijních zdrojů financování a problematické je zpravidla také zužitkování a nasazování výsledků výzkumu do praxe.

Nedostatek personálních kapacit a financování má přitom dalekosáhlé negativní dopady na bezpečnost infrastruktury i výkon ekonomiky. Jak ukazují nejen Zprávy o stavu kybernetické bezpečnosti vydávané NÚKIB⁶, chybějící zdroje již nyní ohrožují schopnost odolávat stále sofistikovanějším kybernetickým hrozbám a flexibilně reagovat na zvyšující se počet kybernetických bezpečnostních incidentů.

Zajišťování kybernetické bezpečnosti Česka nepříznivě ovlivňují i různorodá úroveň vyspělosti zabezpečení regulovaných subjektů a narůstající složitost a roztříštěnost regulačního prostředí, způsobená mimo jiné prudkým nárůstem legislativy EU s dopadem do kybernetické bezpečnosti v posledních letech nebo rozdílnými bezpečnostními požadavky sektorových regulací. Odolnost a reakční schopnost systému negativně ovlivňují též komplikované nebo chybějící procesy, například pro sdílení citlivých neutajovaných informací nebo pro koordinovanou reakci na rozsáhlé krize. Na jejich vhodném nastavení přitom závisí i schopnost Česka čelit krizím, bránit se v případě zapojení do ozbrojeného konfliktu a plnit spojenecké závazky vycházející z členství v NATO.



Vize a strategické cíle



Vize

Česko bude bezpečným a digitálně vyspělým státem s odolnou informační infrastrukturou, vzdělanou, kriticky myslící a inovativní společností a silnými mezinárodními i domácími partnerstvími, s jejichž pomocí zajistí efektivní ochranu a prosazování svých zájmů v kyberprostoru.



Strategická oblast: Bezpečná strategická infrastruktura

Česko bude posilovat své zdroje a rozvíjet své schopnosti k proaktivní a účinné reakci na kybernetické hrozby, včetně budování kapacit vlastní kybernetické obrany. Stabilní právní rámec a efektivní veřejná správa zajistí bezpečné a spolehlivé prostředí pro organizace i jednotlivce. Strategická infrastruktura bude připravena čelit aktuálním i budoucím výzvám, čímž podpoří stabilitu, rozvoj a bezpečnost Česka v kyberprostoru.

Ochrana a odolnost strategické infrastruktury před předvídanými i nepředvídanými hrozbami

Bude průběžně posilována ochrana a odolnost strategické infrastruktury proti širokému spektru hrozeb z kyberprostoru i fyzického prostředí, včetně hybridního působení s cílem minimalizovat z nich plynoucí rizika. Bude kladen důraz na zajištění vysoké bezpečnosti a spolehlivosti jak nových, tak stávajících IKT produktů prostřednictvím jejich pravidelných auditů, aktualizací a testování zranitelností.

Zabezpečení strategické infrastruktury nezbytné pro chod státu bude na úrovni aktuálního stavu poznání v této oblasti a bude využívat EDT, a to včetně ochrany před hrozbami, které plynou z těchto technologií samotných. S ohledem na pokrok v oblasti kvantových počítačů bude zajištěn přechod na kvantově odolnou kryptografii, která ochrání důvěrnost dat před dešifrováním v postkvantovém světě. Nástroje umělé inteligence budou využívány k detekci a ochraně i před útoky vedenými s pomocí těchto technologií.

V případech, kdy se útokům nepodaří zabránit, bude prioritou zajištění kontinuity nebo včasné obnovy poskytování služeb s minimálním dopadem na stát, organizace a jednotlivce. Odolnost infrastruktury bude zaměřena nejen na ochranu národních systémů (na celostátní i regionální úrovni) a jimi poskytovaných služeb, ale také na plnění spojeneckých závazků Česka.

Proaktivní přístup, efektivní detekce a účinná reakce na kybernetické útoky a krize, včetně kybernetické obrany a boje s kybernetickou kriminalitou

Budou rozvíjeny schopnosti efektivní detekce a rychlé a účinné reakce na kybernetické útoky jak na straně orgánů státu s působností v oblasti kybernetické bezpečnosti, obrany a boje s kybernetickou kriminalitou, tak na straně ostatní strategické infrastruktury.

Prostřednictvím aktivního monitoringu a analýzy aktuálních i potenciálních hrozeb v kyberprostoru, včetně proaktivního vyhledávání skrytých hrozeb a indikátorů kompromitace, bude zajištěna účinná detekce bezpečnostních událostí a incidentů. Na ty tak bude možné rychle a efektivně reagovat a předcházet jim nebo zmírňovat jejich dopady.

Česko posílí své kapacity pro efektivní odhalování, vyšetřování a potírání kybernetické kriminality. Budou rozvíjeny nástroje pro rychlou detekci a analýzu trestné činnosti v kyberprostoru, stejně jako právní, technologické a jiné mechanismy umožňující účinné postihování pachatelů, aniž by přitom docházelo ke snižování standardů kybernetické bezpečnosti a k nepřiměřenému zásahu do soukromí jednotlivců. V rámci boje s kybernetickou kriminalitou se Česko zaměří rovněž na prevenci a osvětu a bude se věnovat podpoře obětí této trestné činnosti.

Regulace vyvažující národní bezpečnost a individuální práva jednotlivců

Na kybernetické útoky bude Česko reagovat asertivně, a to v politické, ekonomické, diplomatické i trestněprávní rovině tak, aby se útočníkům škodlivé aktivity v dlouhodobém měřítku nevyplácely a ustoupili od nich. Ve vhodných případech bude Česko svoji reakci koordinovat se spojenci, zejména v rámci NATO, a součástí jeho reakce bude případné využití pasivní nebo aktivní kybernetické obrany. Pro tyto potřeby budou k zajištění bezpečnosti a obrany Česka nadále budovány ofenzivní a multidoménové kapacity. Čelení kybernetickým hrozbám prostředky kybernetické obrany bude vymezeno právním rámcem, umožňujícím efektivní působení v době míru i v případě přechodu do krizových stavů. Posílena bude za tímto účelem také spolupráce napříč veřejnými a soukromými subjekty strategické infrastruktury, a to včetně integrace schopností, sdílení informací, pořádání společných cvičení a využívání nestátních kapacit k řešení krizí.

Legislativní rámec a veřejné politiky v kybernetické bezpečnosti budou po vzoru současných příkladů dobré praxe maximálně přehledné, odborně srozumitelné, nadčasové a technologicky neutrální. Budou udržovat rovnováhu mezi zájmy společnosti a zájmy jednotlivců, na které dopadají. Důraz bude kladen na konsolidaci a sjednocení regulačních požadavků.

Regulace bude umožňovat pružnou, ale předvídatelnou reakci jejích tvůrců i adresátů na bezpečnostní a technologický vývoj tak, aby vytvářela bezpečné a spravedlivé konkurenční prostředí a podporovala efektivitu a inovace. Orgány státu budou mít potřebné nástroje a pravomoci k ochraně nedistributivních práv občanů a budou přitom kontrolovány tak, aby nebyla snížena účinnost výkonu těchto pravomocí.

Nové právní předpisy a politiky v kybernetické bezpečnosti budou připravovány s důrazem na provázanost s celkovým regulačním rámcem i na schopnost jejich adresátů je zavádět a dlouhodobě dodržovat. V tomto ohledu bude Česko adresáty regulace aktivně podporovat, poskytovat jim kvalitní metodické vedení, zároveň však bude důsledně kontrolovat a vymáhat plnění stanovených pravidel.

Posílení financování a efektivnější nakládání se zdroji ve veřejném sektoru

Veřejná správa bude systematicky plánovat a přidělovat investiční a provozní prostředky na kybernetickou bezpečnost podle reálných potřeb dané organizace, významu dotčené infrastruktury a aktuálních hrozeb. Financování bude nastaveno tak, aby nejen splňovalo legislativní požadavky a odvětvové standardy, ale také umožňovalo reagovat na technologický vývoj a zvyšující se nároky na dostupnost a bezpečnost digitalizovaných služeb státu.

Kromě průběžného navyšování objemu finančních prostředků bude potřebné úrovně kybernetické bezpečnosti dosahováno také optimalizací využívání stávajících kapacit a jejich efektivním sdílením, včetně využívání bezpečných centralizovaných řešení v oblasti služeb i zabezpečení. Tam, kde to právní předpisy umožní, budou zjednodušovány procesy čerpání veřejných prostředků k zajištění kybernetické bezpečnosti. Ve vhodných případech budou potřeby veřejné správy v této oblasti realizovány také prostřednictvím partnerství veřejného a soukromého sektoru (tzv. PPP projekty) nebo skrze financování z fondů EU nebo z jiných mezinárodních

Sjednocování veřejné IT architektury a posílení data governance s důrazem na bezpečnost

Bude sjednocována IT architektura a posilováno systematické řízení dat ve veřejném sektoru s cílem zvýšit jejich bezpečnost. Duplicitní bezpečnostní a jiná řešení, která generují nadbytečné náklady a nemají konkrétní přínos, budou omezována a bude prohlubována interoperabilita jednotlivých systémů státu skrze Projekt BIVOX a obdobná řešení. Veřejné instituce budou mít k dispozici základní nástroje pro bezpečné a efektivní zpracování informací v elektronické podobě ve formě ucelených aplikací, které lze s minimální dodatečnou konfigurací využívat v různých agendách a budou motivovány k jejich používání.

Pro správu, ochranu a využívání dat budou v rámci veřejné správy zaváděna jednotná pravidla, která posílí jak transparentnost veřejných dat, tak ochranu citlivých informací a koordinaci jejich sdílení mezi jednotlivými orgány veřejné moci. Bude stanovena odpovědnost za správu, kvalitu a zabezpečení dat ve veřejnoprávních systémech a agendách. Dojde k posílení analytické využitelnosti dat jak pro efektivní výkon státní správy, tak pro práci s otevřenými daty a pro zajištění dohledu nad veřejnou správou ze strany občanů.

Prosazování bezpečných a odolných dodávek nejen do strategické infrastruktury

Česko bude za předpokladu zachování otevřeného tržního prostředí omezovat závislost své strategické infrastruktury na rizikových technologiích a bude preferovat bezpečnostní řešení s tuzemským původem nebo s původem ze spolehlivých partnerských a spojeneckých zemí. Bude prosazovat zajišťování bezpečných a odolných dodávek, diverzifikace a řádné prověřování dodavatelů do strategické infrastruktury. Za účelem zvýšení ochrany svých systémů před kybernetickými hrozbami bude stát ve vybraných oblastech vytvářet nové nebo integrovat stávající bezpečné technologické alternativy k řešením, nad kterými nemá plnou kontrolu, včetně implementace otevřených softwarových a hardwarových řešení.

S ohledem na přicházející trend standardizace v kybernetické bezpečnosti bude Česko rovněž budovat kompetence v této oblasti a podporovat vznik certifikačních orgánů a zkušebních laboratoří.



Strategická oblast: Celospolečenská připravenost a rozvoj

Vysoká úroveň znalostí, schopností a kybernetické gramotnosti celé společnosti představují zásadní předpoklad pro bezpečnost kyberprostoru a předcházení porušení lidských práv, zejména u zranitelných skupin obyvatel. V souladu s Národním plánem vzdělávání v kybernetické bezpečnosti bude Česko usilovat o efektivní využívání digitálních technologií občany a kontinuální zvyšování schopností jednotlivců chránit sebe a své okolí před kybernetickými hrozbami prostřednictvím široce dostupného vzdělávání. Budování celospolečenské kybernetické odolnosti bude realizováno i prostřednictvím kvalitní a početné odborné základny a efektivní spolupráce napříč veřejným a soukromým sektorem, neziskovými organizacemi a akademickou sférou, jakož i civilně-vojenské spolupráce. Česko bude posilovat roli výzkumu a vývoje v kybernetické bezpečnosti se zaměřením na přenos znalostí do praxe a vznik bezpečných technologických alternativ.

Posilování počtů a motivace odborníků za účelem dlouhodobé udržitelnosti vysoké úrovně kybernetické bezpečnosti Česka

Prostřednictvím kvalitních a specializovaných vzdělávacích programů a kurzů v oblasti kybernetické bezpečnosti bude zvyšován počet kvalifikovaných absolventů a odborníků. Tyto programy a kurzy budou inkluzivní a nabídnou příležitosti pro různé sociální skupiny s cílem zvýšit jejich profesní zastoupení v kybernetické bezpečnosti. Propojováním počátečního a dalšího vzdělávání bude zároveň zajištěna větší flexibilita systému v reakci na reálné potřeby pracovního trhu v této oblasti.

Zvyšováním kvality pracovních podmínek se zaměřením na finanční a jinou motivaci na expertních a nedostatkových pracovních pozicích bude zvyšována atraktivita práce v oblasti kybernetické bezpečnosti pro stát a posilována profesionalita a stabilita lidských zdrojů ve veřejném sektoru. Ve spojení s možností kariérního růstu budou pracovní podmínky expertů ve veřejném sektoru směřovat k dosažení konkurenceschopnosti na celostátním pracovním trhu. Pozornost bude věnována i rovnosti pracovních příležitostí a podmínek pro ženy, odborníky bez vysokoškolského vzdělání či absolventy netechnických oborů na kyberbezpečnostních pozicích.

S personálními kapacitami na kybernetickou bezpečnost ve veřejném sektoru bude nakládáno hospodárně, efektivně a flexibilně. Nasazováním nových technologií a automatizací jednoduchých a rutinních činností bude usilováno o zvyšování přidané hodnoty a produktivity práce a takto uspořené prostředky bude umožněno převést na platové ohodnocení v rámci organizace.

Rozvoj celospolečenských digitálních kompetencí a bezpečnostní kultury

Posilováním vzdělávání, prevence a osvěty bude ve společnosti zvyšováno povědomí o bezpečném a zdravém využívání digitálních technologií a o jejich možných rizicích, včetně různých forem kyberkriminality, kyberšikany a násilí v online prostoru. Dojde k posílení schopnosti veřejných institucí, organizací i jednotlivců chránit se v kyberprostoru, kriticky analyzovat a vyhodnocovat informace a rozhodovat se zodpovědně. Díky začlenění kybernetické bezpečnosti do vzdělávání napříč všemi generacemi bude navýšena kultura kybernetické bezpečnosti v pracovním i soukromém životě.

Intenzivní spolupráce ke koordinaci a překonání rozdílů mezi sektory

Bude posílena výměna informací a komunikace v oblasti kybernetické bezpečnosti mezi veřejným, soukromým, neziskovým a akademickým sektorem a občanskou společností. Prostřednictvím systémově zakotvených platforem pro spolupráci a aktivního zapojení všech relevantních aktérů budou snižována kybernetická rizika pro stát i jednotlivce. Bude tak možné jednodušeji předcházet kybernetickým hrozbám a řešit krize s celospolečenským dopadem do kyberprostoru. Budování komunity a vzájemné důvěry, společná cvičení, sdílení informací a koordinovaná reakce posílí komplexní ochranu kyberprostoru a zvýší vzájemné porozumění a identifikaci s bezpečnostními potřebami státu. Posílena bude taktéž civilně-vojenská spolupráce s cílem navýšit situační povědomí státu a zlepšit efektivitu a koordinaci mezi klíčovými aktéry, včetně vzájemného předávání zkušeností a sdílení příkladů dobré praxe.

Rozvoj znalostí a schopností odborníků v kybernetické bezpečnosti

Budou vytvářeny podmínky pro rozvoj odborných kyberbezpečnostních kompetencí odborníků skrze formální i neformální vzdělávání, přičemž důraz bude kladen na praktickou využitelnost získaných znalostí.

Bude rozvíjen a modernizován vzdělávací systém a nabídka kurzů v oblasti dalšího vzdělávání, který zajistí přípravu odborné i široké veřejnosti na výzvy spojené s bezpečným pohybem v digitálním světě. Důraz bude kladen na aktualizaci výukových metod a dostupnost materiálů a kurzů tak, aby reagovaly na technologický pokrok a nové hrozby. Kvalitní a atraktivní specializované vzdělávací programy a kurzy přinesou jak více expertů na kybernetickou bezpečnost, tak větší bezpečnostní povědomí v jiných specializacích. Na rozvoji tohoto vzdělávání se bude aktivně podílet veřejný, soukromý, akademický i neziskový sektor.

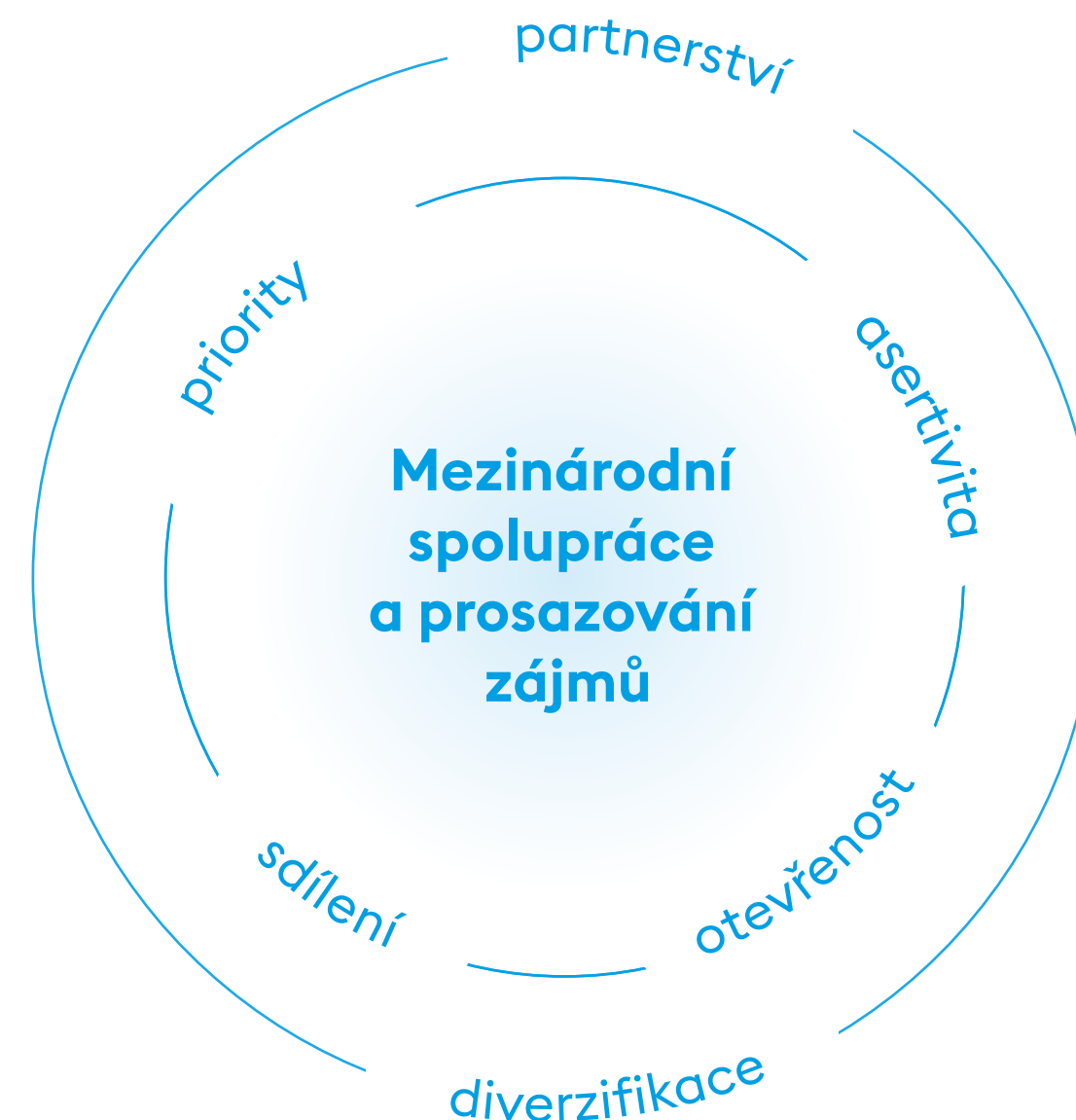
Podpora výzkumu a inovací v oblasti kybernetické bezpečnosti

Česko bude podporovat výzkum, vývoj a inovace v oblastech, kde má strategický zájem nebo konkurenční výhodu, s důrazem na dlouhodobou udržitelnost a bezpečnost výsledků výzkumu, jakož i jejich aplikovatelnost a přenos do praxe. Stát podpoří, nejen prostřednictvím role NÚKIB coby provozovatele Národního koordinačního centra, aktivity propojující akademickou sféru, inovátory a veřejný sektor s cílem posílit postavení Česka v evropském výzkumném ekosystému. K tomu bude zajištěna odpovídající součinnost orgánů státní správy, odborné kapacity a adekvátní financování.

Kybernetická bezpečnost bude jednou z prioritních oblastí účelové podpory výzkumu, vývoje a inovací. V této souvislosti bude NÚKIB budovat odborné zázemí pro poskytovatele státní podpory na výzkum a vývoj, jejichž gesční programy jsou zaměřeny na oblast kybernetické bezpečnosti.

Podpora vzniku bezpečných technologických alternativ

Česko bude podporovat vznik nových bezpečných technologických alternativ, které posílí odolnost jeho, ale i celé EU vůči kybernetickým hrozbám z dodavatelských řetězců. V rámci tohoto úsilí budou podporovány jak státní, akademické i neziskové subjekty, tak relevantní tuzemský průmysl a jeho konkurenceschopnost na domácím i zahraničním trhu. Za účelem minimalizace závislosti na dodavatelských rizikových technologiích bude Česko kromě vývoje vlastních alternativ aktivně hledat společná řešení v rámci EU, NATO a s dalšími mezinárodními partnery s cílem sdílení znalostí a zdrojů nezbytných pro naplnění principu otevřené strategické autonomie.



Strategická oblast:

Mezinárodní spolupráce a prosazování zájmů

Bezpečnost Česka je úzce spjata s mezinárodní stabilitou a členstvím v NATO a EU, které zůstává základem naší bezpečnosti a obrany i v kyberprostoru. Zodpovědné přispívání k aliančním schopnostem a kapacitám a aktivní zahraniční politika jsou a budou klíčové pro prosazování národních zájmů a bezpečnost kyberprostoru na národní i globální úrovni. Česko bude i ve vztahu ke kyberprostoru prosazovat dodržování mezinárodního práva veřejného s důrazem na univerzální hodnoty a respekt k lidským právům. Vůči kybernetickým hrozbám s původem v zahraničí bude Česko nadále aktivně zasahovat a nebude se zdrážet na ně odpovídajícím způsobem reagovat.

Navazování nových a posilování stávajících strategicky významných partnerství

Česko bude v oblasti kybernetické bezpečnosti posilovat a rozvíjet spolupráci s vybranými mezinárodními partnery, přičemž klíčová zůstává spolupráce v NATO a EU. Na půdě NATO bude Česko i nadále zachovávat svůj proaktivní přístup, podporovat akceschopnost a soudržnost Aliance a přispívat do aliančních aktivit.

Při navazování, prohlubování nebo naopak rozvolňování spolupráce bude Česko brát v potaz aktuální i dlouhodobý vývoj v mezinárodním prostředí a své národní zájmy stejně jako zájmy svých spojenců, včetně prosazování společných demokratických hodnot. Bude prohlubovat spolupráci zejména v rámci EU, v transatlantickém prostoru, v regionu Indo-Pacifiku se zaměřením na státy IP4, v regionu Blízkého východu, včetně svého mnohavrstevného vztahu s Izraelem, a s dalšími hodnotově podobně smýšlejícími partnery. Česko bude pokračovat v intenzivním diplomatickém působení prostřednictvím svých kybernetických atašé a zástupců v mezinárodních organizacích a unijních institucích, přičemž bude usilovat o zvýšení jejich počtu i míst jejich působení.

V rámci rozvoje mezinárodních vztahů a v reakci na vývoj mezinárodního bezpečnostního prostředí bude Česko nadále budovat i nové vazby ve výše uvedených i v dalších strategických regionech.

Aktivní prosazování zájmů, cílů a priorit Česka při utváření mezinárodních pravidel i práva EU

Česko se bude podílet na směřování mezinárodního vývoje bezpečného kyberprostoru. Důraz bude kladen na prosazování národních zájmů a aktivní účast při tvorbě mezinárodních právních norem a standardů. Zároveň bude všemi legálními i diplomatickými prostředky prosazovat jejich dodržování a nebude se zdrážet asertivně vystoupit proti jejich porušování.

Česko se bude nadále aktivně podílet na utváření legislativy EU a mezinárodních předpisů, úmluv, smluv nebo standardů v oblasti kybernetické bezpečnosti. Svou aktivní účastí napomůže tomu, že mezinárodní normy budou nastaveny jednoznačně, přiměřeně, srozumitelně a budou odrážet bezpečnostní a další zájmy i potřeby Česka. Tyto principy bude Česko prosazovat jak na úrovni EU a dalších mezinárodních organizací a uskupení, tak i při vnitrostátní implementaci unijního a mezinárodního práva. Aktivně bude podporovat také přímou aplikovatelnost mezinárodního práva veřejného v kyberprostoru v souladu se svou národní pozicí k interpretaci a aplikaci mezinárodního práva v kyberprostoru publikovanou v roce 2024, která bude vyhodnocována a případně aktualizována.

Česko se bude aktivně zasazovat o ochranu a podporu demokracie a lidských práv v kyberprostoru a proti ohrožování demokratických principů v této oblasti bude aktivně a cíleně vystupovat. Bude nadále požadovat, aby státy dodržovaly normy zodpovědného chování v kyberprostoru, na nichž se shodla mezinárodní komunita v rámci OSN a společné zásady aplikovatelnosti mezinárodního práva veřejného v kyberprostoru deklarované EU. Tyto aktivity budou zahrnovat nejen preventivní opatření, ale i odpovídající reakci na škodlivé aktivity a porušování lidských práv v kyberprostoru ze strany státních i nestátních aktérů.

Asertivní vystupování proti nepřátelskému působení škodlivých aktérů v kyberprostoru, včetně atribuce útoků, diplomatické reakce a uplatňování sankcí

Česko bude nadále využívat a posilovat své schopnosti a kapacity k atribuci kybernetických útoků vedených státními nebo na ně napojenými aktéry. Bude přitom spolupracovat a koordinovat své politicko-diplomatické kroky a bezpečnostní opatření se členy EU i NATO a s podobně smýšlejícími partnery na bilaterální úrovni a bude také vhodně využívat národních a mezinárodních sankčních mechanismů.

Prostřednictvím rychlé a asertivní národní i mezinárodní reakce na škodlivé aktivity v kyberprostoru bude Česko usilovat o odstranění a potrestání škodlivých aktérů a bude tím indikovat svou akceschopnost a odhodlanost vystupovat proti těm, kteří se snaží v kyberprostoru a skrze něj škodit. Tímto přístupem Česko demonstruje, že se škodlivým kybernetickým aktérům nevyplatí na něj cílit, jelikož reakce Česka a jeho spojenců předčí případné zisky spojené s nepřátelským a škodlivým jednáním. Česko bude své odstrašování škodlivých aktérů nadále posilovat a bude toto téma také aktivně prosazovat v prostředí NATO a EU.

Podpora otevřené strategické autonomie

Česko bude aktivně rozvíjet svou schopnost chránit a prosazovat národní zájmy v kybernetickém prostoru v souladu s principy otevřené strategické autonomie, aby mohlo lépe chránit svou digitální infrastrukturu a data. To zahrnuje i podporu diverzifikace technologií, budování expertízy, aktivní účast na formování mezinárodních politik zaměřených na ochranu dat, přístup ke zdrojům a technologiím a ochranu digitálních práv občanů. Tyto aktivity bude Česko podporovat jak v mezinárodních bilaterálních a multilaterálních vztazích, tak v rámci EU a NATO.

Ochrana globálního, otevřeného, bezpečného a svobodného kyberprostoru

Česko se bude podílet na udržování globálního, otevřeného, bezpečného a svobodného Internetu a kyberprostoru, který je založen na uplatňování mezinárodního práva a postaven na modelu více zainteresovaných stran (tzv. multistakeholder model) a bude vystupovat proti snahám o kontrolu a fragmentaci Internetu a aktivně se zasazovat o jeho transparentnost a důvěryhodnost, a to prostřednictvím spolupráce mezi státy i se soukromými a nevládními organizacemi.

Posilování mezinárodního sdílení informací a rozvojové spolupráce

Česko bude zkvalitňovat stávající mechanismy pro sdílení know-how, informací o kybernetických hrozbách, zranitelnostech a incidentech, stejně jako osvědčených postupů mezi státy, organizacemi a dalšími klíčovými aktéry na mezinárodní úrovni. Za tímto účelem bude využívat i relevantní alianční a unijní mechanismy, včetně integrovaného centra kybernetické obrany NATO (NATO Integrated Cyber Defence Centre), zodpovědného za navýšení situačního povědomí v Alianci. Tento přístup mimo jiné podpoří prevenci kybernetických útoků a umožní rychlou a koordinovanou reakci zejména v rámci NATO a EU.

Také s ohledem na vlastní bezpečnostní zájmy bude Česko přednostně rozvíjet strategickou spolupráci se zeměmi z regionu západního Balkánu a Východního partnerství. V odpovídající míře se bude podílet i na budování kapacit kybernetické bezpečnosti v rozvojových zemích ostatních regionů, jako je subsaharská Afrika, Indo-Pacifik, Blízký východ nebo Latinská Amerika. Tato spolupráce bude zahrnovat sdílení know-how, školení tamějších odborníků a vysílání vlastních expertů s cílem posílit stabilitu, bezpečnost a odolnost těchto regionů v kyberprostoru. Při rozvojové spolupráci bude ve vysoké míře využívat synergie a partnerství s dalšími rozvinutými zeměmi a financování z projektů EU, NATO a dalších vnějších zdrojů.

Významnou prioritou mezinárodního působení Česka v kyberprostoru zůstane podpora Ukrajiny, která zahrnuje mimo jiné pomoc s obnovou její digitální infrastruktury a poskytování technické pomoci.

Implementace

Strategické cíle k realizaci vize NSKB budou naplňovány skrze konkrétní, měřitelné, dosažitelné a časově vymezené úkoly s určenými gestory jejich plnění, které budou obsahem Akčního plánu k NSKB. Naplňování Akčního plánu k NSKB bude průběžně monitorováno NÚKIB, který předloží jednou ročně jeho vyhodnocení vládě České republiky.

Samotná NSKB konkrétní finanční požadavky k dosažení svých cílů nezakládá. Plnění úkolů Akčního plánu k NSKB bude financováno z příslušných kapitol státního rozpočtu, fondů a programů EU nebo prostřednictvím PPP projektů.

Ačkoliv plnění NSKB vždy závisí na aktuálních možnostech státního rozpočtu Česka a dalších zdrojů financování, investice do kybernetické bezpečnosti je pojistkou, která Česku vrátí násobně vyšší úspory oproti nákladům na řešení následků útoků a posílí jeho konkurenceschopnost a ekonomický růst.

Zdroje dat

1. Cybersecurity Ventures: The World's Third-Largest Economy Has Bad Intentions
<https://cybersecurityventures.com/the-worlds-third-largest-economy-has-bad-intentions-and-its-only-getting-bigger/>
2. ČBA: Češi a kyberbezpečnost 2024
<https://www.cbaonline.cz/clanky/cesi-a-kyberbezpecnost-2024>
3. Check Point: Počet kyberútoků na české firmy stoupl o 69 procent
<https://cesky.radio.cz/pocet-kyberutoku-na-ceske-firmy-stoupl-o-69-procent-8834152>
4. ENISA: Threat Landscape 2024
https://www.enisa.europa.eu/sites/default/files/2024-11/ENISA%20Threat%20Landscape%202024_0.pdf
5. EU: Cyber Skills Academy
<https://digital-skills-jobs.europa.eu/en/cybersecurity-skills-academy>
6. NÚKIB: Zprávy o stavu kybernetické bezpečnosti
<https://nukib.gov.cz/cs/infoservis/dokumenty-a-publikace/zpravy-o-stavu-kb/>



Národní úřad
pro kybernetickou
a informační bezpečnost

NÚKIB

