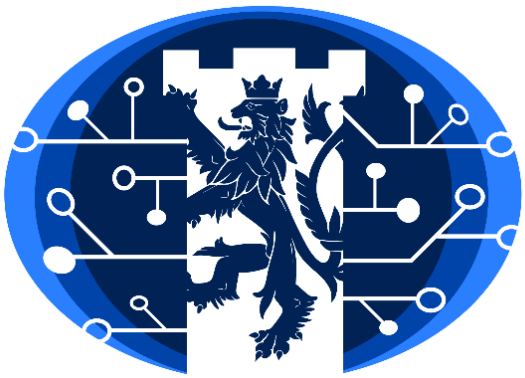

Strategie kybernetické obrany ČR

2018 – 2022

Národní centrum kybernetických operací

Úvod

Mezi základní funkce státu patří zajišťování bezpečnosti občanů, obrana svrchovanosti, územní celistvosti, principů demokracie a právního státu. Jedním z pilířů pro udržení těchto hodnot je komplexní systém obrany státu s dlouhodobou vizí.

S ohledem na významný celospolečenský a technologický vývoj je potřebné změnit zažité formy a způsoby zajišťování obrany. V současné době je totiž na vzestupu forma asymetrického vedení konfliktů, kde významnou roli hraje využívání kyberprostoru. Nelze opomenout ani rychlé tempo vývoje umělé inteligence a robotických systémů.

Budování obranných schopností v kyberprostoru je pro ČR vhodné i s ohledem na členství v NATO, neboť kyberprostor byl uznán jako plánovací a operační doména s tím, že kybernetický útok je způsobilý aktivovat čl. 5 Severoatlantické smlouvy. Proto v souladu s požadavkem zakotveným v čl. 3 Severoatlantické smlouvy by smluvní strany měly udržovat a rozvíjet jak individuální, tak kolektivní schopnosti odolat i kybernetickým útokům.

ČR výše uvedené skutečnosti reflektuje a postupně přijímá potřebná opatření. Přístup k řešení kybernetických útoků je však zatížen systémovými nedostatky. Ačkoliv v oblasti kybernetické bezpečnosti je dosaženo vysoké úrovně, systémové řešení kybernetické obrany je teprve na svém počátku. Navíc chápání a rozlišování těchto pojmů je nejednotné.

Pro vysvětlení je vhodné uvést, že podle vládního přístupu k dané problematice je kybernetická obrana autonomní a specifickou oblastí širšího konceptu kybernetické bezpečnosti. Zajišťováním kybernetické obrany se v tomto kontextu totiž myslí zajišťování obrany státu ve smyslu zákona o zajišťování obrany ČR. Podle jeho obsahu se obranou státu rozumí souhrn opatření k zajištění svrchovanosti, územní celistvosti, principů demokracie a právního státu, ochrany života obyvatel a jejich majetku před vnějším napadením. Tato obrana v sobě zahrnuje výstavbu účinného systému obrany státu, přípravu a použití odpovídajících sil a prostředků a účast v kolektivním obranném systému.

Oproti tomu se kybernetickou bezpečností rozumí souhrn prostředků směřujících k zajištění ochrany kybernetického prostoru. Tyto prostředky mohou být různého charakteru – právní, organizační, vzdělávací, technické apod. Zjednodušeně řečeno, kybernetickou bezpečností se v tomto smyslu myslí zajištění důvěrnosti, integrity a dostupnosti informací a dat v kyberprostoru.

Působnost kybernetické obrany se od bezpečnosti liší především povahou a intenzitou útoků, aniž by bylo možné vymezit úplně přesná kritéria. Připravenost na kybernetické útoky proto musí být komplexní a nemůže se zaměřit pouze na sféru bezpečnosti, ale je nutné vybudovat schopnosti i proti útokům, které lze vyhodnotit jako způsobilé aktivovat obranu státu. Aktivace kybernetické obrany tak bude přicházet v úvahu pouze v případě těch nejintenzivnějších útoků. Specifikem kybernetické obrany bude skutečnost, že bude prováděna jak v případě vyhlášení mimořádných stavů, především formou součinnosti s ostatními složkami zajišťujícími obranu ČR, tak i nepřetržitě mimo tyto stavy.

Základním kamenem pro vybudování účinného systému kybernetické obrany ČR byl požadavek vlády uvedený v rámci akčního plánu k Národní strategii kybernetické bezpečnosti pro období 2015 až 2020, kde byl stanoven jako úkol vybudování a posilování schopností kybernetické obrany. Jako odpovědný subjekt za zajišťování kybernetické obrany bylo určeno Národní centrum kybernetických operací (dále NCKO). Zvolená koncepce vychází z racionálního reflektování rozdílnosti mezi zajišťováním kybernetické bezpečnosti a obrany.

Koncepční podmínky pro řádné zajišťování obrany státu v kyberprostoru stanovuje tato strategie kybernetické obrany, která je rozdělena na veřejnou a neveřejnou část. V rámci veřejné části je uvedena základní vize a v obecné míře i jednotlivé cíle, které popisují plánovaný stav v dílčích oblastech řešeného problému. Míra obecnosti veřejné části je dána povahou dané problematiky, kdy teprve neveřejná část obsahuje souhrn konkrétních opatření, jejichž implementací budou jednotlivé cíle naplněny. Stanovená opatření vychází z principů obranné politiky ČR, reflektují současné trendy moderních obranných doktrín a jsou souladná se základními principy demokratického právního státu. Při jejich koncipování bylo bráno v potaz, že objektem obrany je zachování a ochrana základních práv a svobod jednotlivce, stejně jako výše uvedených principů a hodnot, neboť bezpečí a svoboda nejsou vzájemně se vylučujícími hodnotami. Bez bezpečí není svobody. Bez svobody není bezpečí. Obranná opatření jsou proto koncipována v duchu principu proporcionality takovým způsobem, aby ČR byla státem demokratickým a bezpečným, disponujícím schopnostmi si tyto hodnoty bránit.

Klíčové výzvy z hlediska kybernetické obrany ČR

Potencionálních útočníků způsobilých provést kybernetický útok v rozsahu umožňujícím aktivaci kybernetické obrany ČR je opravdu velké množství. Jedná se jak o státní, tak i nestátní aktéry. Kybernetické útoky jsou totiž ideálním nástrojem pro poškození politických, obchodních či dalších obdobných cílů a také silným nástrojem pro vynucení vlastní vůle. Zároveň je ve většině případů velmi obtížné rozkrýt původce útoku, a to především v reálném čase. Tím se snižuje riziko spjaté s případnou adekvátní reakcí. Tyto skutečnosti, v kontextu s relativní absencí geografických a obdobných omezení, představují pro útočníka značnou výhodu.

Primárním cílem takto motivovaných kybernetických útoků mohou být především systémy, které představují úzké propojení mezi počítačovým systémem a fyzickou infrastrukturou, ať už vodního hospodářství, energetiky či jinou. Cílem mohou být i přímo prvky infrastruktury obranné.

Z hlediska kybernetické obrany ČR lze za nejvýznamnější hrozbu považovat navyšování ofenzivních kybernetických schopností potenciálně nepřátelských států. Mezi další významné patří narůstající hrozba kyberterorismu a soustavné upevňování struktur kybernetického zločinu, jakož i vzájemné propojování státních a nestátních útočníků.

V oblasti kybernetických zranitelností se priority z hlediska kybernetické bezpečnosti a kybernetické obrany do značné míry protínají. Za nejvýznamnější zranitelnosti lze považovat nízkou digitální gramotnost a nedostatečné povědomí jednotlivých uživatelů o bezpečnostních zásadách v kybernetickém prostoru, především v kontextu s rostoucím počtem zařízení internetu věcí. Z hlediska vedení kybernetické obrany se stále významnějšími stávají zranitelnosti související s narůstající závislostí bezpečnostních složek státu na informačních a komunikačních technologiích.

Nejdůležitejší výzvy podrobněji:

Nové trendy prosazování vlivu

V současné době neustále roste úloha nekonvenčních a dosud nepoužívaných způsobů dosahování politických a strategických cílů. Vedení boje probíhá asymetrickou formou. Je stále obtížnější odlišit útoky vnější od vnitřních. Nástroje prosazení mocenského vlivu již často nejsou typicky vojenské, ale spíše informační. Významnou roli zde hraje využívání možností kyberprostoru, jakožto součásti širšího pojetí prosazování vlivu. Reálnou hrozbou se stává nasazení moderních robotechnických vojenských, ale i nevojenských systémů či umělé inteligence pro tyto účely. Výrazně stoupá riziko ohrožení svrchovanosti, územní celistvosti, principů demokracie a právního státu.

Státní aktéři

V poslední dekádě dochází ve světě opakovaně k útokům, které jsou díky své sofistikovanosti a rozsahu přisuzovány ať už přímo, nebo nepřímo státním aktérům. Jednotlivé státy budují silné kybernetické schopnosti různých forem, od ofenzivních vojenských schopností, až po skupiny pracující v utajení ve prospěch těchto států. Účelem jejich použití mohou být průmyslové špionáže, získávání zpravodajských informací, šíření dezinformací, ale i útoky zacílené na způsobení ztrát na životech, zdraví i majetku. Tato hrozba je prioritní z hlediska kybernetické obrany vzhledem k dostatečnému hmotnému i finančnímu zajištění útočníků, které umožňuje provádění těch nejintenzivnějších útoků.

Kyberterorismus

Ačkoli pod pojmem teroristický útok je většinou míněna fyzická hrozba, stále častěji se objevují deklarace ze stran různých teroristických skupin o posilování aktivit v kyberprostoru. Ten je zatím využíván zejména jako rekrutační nebo informační platforma. Lze však předpokládat, že v blízké budoucnosti budou teroristické skupiny schopny provést i relativně pokročilé útoky.

Rostoucí počet zařízení internetu věcí

Ke konci roku 2017 bylo celosvětově připojeno k internetu cca 20 miliard zařízení. Podle predikcí by se do konce roku 2020 mohl počet zařízení navýšit až na 30 miliard s navazujícím dalším exponenciálním růstem. Hrozbu nepředstavuje přímo množství připojených zařízení, ale jejich často slabé, nebo žádné zabezpečení, které umožňuje snadné ovládnutí těchto zařízení pro vedení kybernetických útoků.

Nízká míra digitální gramotnosti a nedostatečné povědomí uživatelů o zásadách bezpečnosti v kybernetickém prostoru

Tento problém je dlouhodobý, se vzrůstající závislostí společnosti na informačních a komunikačních technologiích se však stává čím dál více patrným. Ve vztahu ke kybernetické obraně ČR je vhodné zdůraznit nízké povědomí o zásadách chování v kyberprostoru a jeho fungování mezi významnými státními činiteli, nebo mezi vedoucími pracovníky ozbrojených složek. Spear phisingové kampaně, kompromitace malwarem a kompromitace za použití technik sociálního inženýrství, či manipulací legitimních uživatelských účtů jsou vůbec nejrozšířenějšími vektory působení útočníků všech úrovní v kybernetickém prostoru.

Vzrůstající závislost obranných složek státu na informačních a komunikačních technologiích

Obranné složky státu jsou stále závislejší na použití informačních technologií, které jsou využívány např. pro komunikaci, jako podpora plánování a rozhodovacích procesů nebo jako základ bojových systémů. Schopnost obrany těchto složek v kyberprostoru, ale zároveň i schopnost aktivního působení v kyberprostoru nabývá tedy čím dál více na významu.

Vize

Strategie kybernetické obrany je tvořena s vizí, že ČR bude schopna čelit i těm nejzávažnějším kybernetickým útokům. Pro naplnění vize je nutné disponovat plnohodnotnými schopnostmi kybernetické obrany, použitelnými jak při obraně, tak při podpoře vojenských operací. Pro tyto účely je zásadní, aby zajišťování kybernetické obrany bylo vnímáno jako součást komplexní obrany ČR. Dále bude třeba vybudovat silné mezinárodní vazby v oblasti kybernetické obrany, a tím posílit schopnosti předcházení i řešení kybernetických útoků. Nutností bude i připravenost k aktivní pomoci mezinárodním partnerům při plnění závazků vyplývajících z členství v mezinárodních organizacích.

Základní strategické směřování

Strategie kybernetické obrany za svůj globální cíl považuje dosažení takového stavu, kdy NCKO bude zajišťovat kybernetickou obranu ČR, bude schopné provádět vojenské operace v kybernetickém prostoru a zároveň plnit aktivní úlohu v mezinárodním prostředí.

Globálního cíle bude dosaženo v případě plnění následujících strategických cílů:

1. Nastavení právního rámce

2. Vybudování a rozvoj infrastruktury NCKO

3. Vybudování schopností obrany v kyberprostoru

4. Nastavení spolupráce a provádění vzdělávání a cvičení

5. Podílení se na zajištění kybernetické bezpečnosti v rezortu MO

1. Nastavení právního rámce

Organizování kybernetické obrany ČR je teprve na samotném začátku. V této fázi je proto potřebné využít nástrojů administrativně právní regulace, kterými se určí základní pravomoci a působnost jednotlivých zainteresovaných orgánů veřejné moci, především NCKO, stejně jako práva a povinnosti osob výkonem těchto pravomocí dotčených. Zásadním krokem bude i nastavení účinného systému kontroly činností souvisejících se zajišťováním kybernetické obrany ČR. Následovat bude přijetí navazujících právních norem pro zajištění komplexní právní regulace. Smyslem přijímaného právního rámce bude podpora rozvíjení všech ostatních potřebných oblastí a dovedností k zajištění kybernetické obrany ČR. Splněním tohoto cíle budou vymezeny základní právní aspekty kybernetické obrany. Důležitým prvkem bude i podílení se na právní úpravě kybernetické obrany v mezinárodním měřítku.

2. Vybudování a rozvoj infrastruktury NCKO

Zásadním krokem ke splnění globálního cíle je vybudování sil NCKO. Jednou z priorit bude obsazení NCKO kvalitním personálem, na což přímo navazují opatření přispívající k vyškolení a následnému udržení vycvičeného a zkušeného personálu. Další prioritou bude pořízení a vývoj špičkových technologií, které umožní efektivní využití lidského potenciálu. Vzhledem k provázanosti kyberprostoru bude nezbytné využívat externích zdrojů, zejména pak v personální a technologické oblasti. Splněním tohoto strategického cíle bude vybudováno adekvátní zázemí pro činnost NCKO.

3. Vybudování schopností obrany v kyberprostoru

Pro zajištění obrany ČR je nezbytně nutné vytvoření schopností k provádění operací v kyberprostoru. Ty budou prováděny jak v rámci kybernetické obrany ČR, tak jako součást vojenských operací. Dále bude potřebné získat schopnosti předvídat potencionální útoky, lépe lokalizovat útoky již probíhající a analyzovat možné způsoby jejich odražení. Nabyté schopnosti budou následně ukotveny v doktrinálním rámci. Důležitou oblastí kybernetické obrany ČR bude rovněž vytvoření tzv. „cyber deterrence“ strategie. Splněním třetího strategického cíle nabude NCKO schopnosti aktivně působit v kybernetickém prostoru.

4. Nastavení spolupráce a provádění vzdělávání a cvičení

Funkční zajištění kybernetické obrany ČR si nelze představit bez spolupráce se státními i nestátními entitami, a to jak na národní tak i mezinárodní úrovni. Izolovanost by byla sama o sobě značným bezpečnostním rizikem. Asymetrickým hrozbám a kybernetickým útokům je nutné čelit komplexně. NCKO se proto aktivně zapojí do zajišťování kybernetické bezpečnosti ČR. Dále musí vybudovat silná spojenectví v mezinárodním prostředí, zejména v rámci NATO, EU a s okolními zeměmi. Pro potřeby zdárného zajištění kybernetické obrany ČR bude nutné rozvíjet i spolupráci se soukromým sektorem, především v oblasti vědy a výzkumu. Významným aspektem spolupráce bude organizování či účast na různých cvičeních a vzdělávacích aktivitách, neboť se jedná o významný zdroj informací a zkušeností o technických i právních souvislostech provádění kybernetické obrany ČR. Naplněním čtvrtého strategického cíle bude dosaženo významného zkvalitnění zajišťování kybernetické obrany ČR. Schopnosti NCKO budou zároveň přispívat k zvýšení bezpečnosti kyberprostoru v ČR i spojenců.

5. Podílení se na zajištění kybernetické bezpečnosti v rezortu MO

Závislost bezpečnostních složek státu na informačních technologiích stále stoupá. Úkolem všech složek v rámci rezortu MO tedy musí být celkové navýšení úrovně kybernetické bezpečnosti. Prvořadým úkolem NCKO bude zajištění kybernetické bezpečnosti vlastních prostředků a sítí. Speciální schopnosti NCKO však budou využity i k posílení obranyschopnosti ostatních prvků a také příslušníků rezortu MO. Splněním tohoto cíle bude zajištěna spolehlivost a důvěryhodnost informačních systémů NCKO, potažmo dalších informačních systémů v rámci rezortu MO.

Cíle jednotlivých startegických oblastí

1. Nastavení právního rámce

1.1. Vymezení působnosti a pravomocí

V první řadě je třeba jasným a nezpochybnitelným způsobem vymezit pravomoc a působnost zainteresovaných orgánů veřejné moci, především NCKO, stejně jako práva a povinnosti osob výkonem těchto pravomocí dotčených. Významné bude i vymezení momentů aktivace kybernetické obrany ČR. Teprve na těchto základech je možné dále stavět účinnou kybernetickou obranu s ohledem na ústavní principy a zásady právního státu. Bude tedy nutné připravit návrh nutných legislativních změn pro potřeby plné funkčnosti NCKO tak, aby zdárně prošly legislativním procesem.

1.2. Vymezení kompetencí v rámci rozhodovacího procesu pro použití schopností kybernetické obrany ČR

Zdárné zajišťování kybernetické obrany ČR musí vycházet z jednoznačně určených kompetencí, což se v budoucnu projeví především v rámci rozhodovacího procesu pro použití schopností kybernetické obrany ČR. Bude tedy nutné přijmout pravidla, kde se tyto mechanizmy vymezí. Především bude potřeba vytvořit plán kybernetické obrany ČR. Zároveň s tím bude třeba přijmout předpisy na zákonné úrovni a také uzavřít jednotlivé dohody o spolupráci. V návaznosti na to bude potřebné přijetí jednotlivých dokumentů krizového či kooperačního charakteru, na základě kterých bude mimo jiné konkrétně řešena spolupráce se státními i zahraničními partnery.

1.3. Tvorba a revize vnitřní právní úpravy NCKO

Důležitým aspektem bude i tvorba navazující vnitřní právní úpravy NCKO. Ta bude konkretizovat plnění jednotlivých úkolů, vzájemné vztahy, návaznost na vnitřní předpisy v rámci rezortu MO a odpovědnost jednotlivých osob vykonávajících kybernetickou obranu ČR.

1.4. Podílení se na tvorbě a revizi legislativy v oblasti regulace kyberprostoru

Znalosti a zkušenosti z fungování NCKO budou využity při revizi a tvorbě návrhu legislativních změn souvisejících s kybernetickou bezpečností ČR a obecně kybernetickým prostorem. Důležité bude aktivně se účastnit diskuzí nad pojetím a významem konceptů kybernetické bezpečnosti a kybernetické obrany ČR.

1.5. Podílení se na právní úpravě kybernetické obrany v mezinárodním měřítku

Vzhledem k povaze kyberprostoru bude významnou skutečností mající vliv na kybernetickou obranu ČR i otázka mezinárodní regulace. Proto bude potřebné aktivní podílení se na tvorbě právní úpravy kybernetické obrany v mezinárodním měřítku, především v otázkách jurisdikce, odpovědnosti a práva na sebeobranu.

2. Vybudování a udržení infrastruktury NCKO

2.1. Zajištění vysoké technologické úrovně prostředků NCKO

Zavádění špičkových technologií je nezbytné pro efektivní výkon kybernetické obrany ČR. Jednou z priorit NCKO bude monitoring nových trendů v oblasti technologického vývoje a jejich následný pružný a cenově výhodný nákup a implementace ve vlastních strukturách. V oblastech, ve kterých nelze plnohodnotně spoléhat na komerční produkty, bude rovněž kladen důraz na investice do vlastního vývoje a následného zavádění vlastních technologií.

2.2. Početně a kvalitně dostatečné personální obsazení NCKO

NCKO, stejně jako většina obdobných institucí v ČR, bude muset čelit nedostatku vhodného personálu. Další prioritou NCKO tedy bude zefektivnění náboru. Důležitým krokem bude přiblížení přijímacího procesu moderním personálním trendům v oblasti IT. Nezbytné bude také nastavení a udržení konkurenceschopných pracovních podmínek v oblasti finančního odměňování a nabídky moderních benefitů. V dlouhodobém horizontu se NCKO zaměří na alternativní způsoby rekrutace. V dnešním pracovním prostředí, zejména pak v oblasti IT je jednou z největších výzev udržení a motivování personálu. Základním opatřením bude tvorba systému finančního ohodnocení a kvalitního, soustavného vzdělávání. Důležité bude rovněž nastavení motivačního systému odměňování a povyšování dle výkonnosti a v souvislosti s tím i aplikace moderních manažerských postupů.

2.3. Zajištění infrastruktury

Nezbytným opatřením bude zajištění vhodné infrastruktury a potřebné logistické podpory, které budou umožňovat efektivní výkon kybernetické obrany ČR.

2.4. Využití externích zdrojů

Výměna cenných zkušeností mezi odborníky z civilního sektoru a příslušníky NCKO může být velice přínosnou při navyšování kvalifikace personálu. Snahou bude uvedení do praxe různých výměnných programů s civilními společnostmi. Jednou z forem využití externích zdrojů bude zapojení aktivních záloh a jejich příprava pro případné nasazení. NCKO bude také usilovat o využití externích prostředků a prostor pro vývoj technologií nebo výcvik svých příslušníků.

3. Vybudování schopností obrany v kyberprostoru

3.1. Vybudování schopností pro provádění operací v kyberprostoru v rámci obrany ČR

Ústředním cílem pro zajištění kybernetické obrany ČR bude vytvoření schopností pro provádění operací, které bude možné použít v případě nutnosti obrany proti významným kybernetickým útokům. NCKO vytvoří sadu schopností poskytujících širokou škálu možností odpovědi na kybernetické útoky různé povahy.

3.2. Vybudování schopností pro provádění operací v kyberprostoru pro podporu vojenských operací

Kromě zajišťování kybernetické obrany ČR bude úkolem NCKO vytvoření schopností pro podporu vojenských operací. Ty budou cíleny na operační až taktickou úroveň a budou zahrnovat jak podporu boje v jiných doménách, tak provádění operací výhradně v kyberprostoru.

3.3. Posílení schopností predikce a analýzy útoků v kyberprostoru

V kybernetickém prostoru patří schopnost rozpoznat útok, správně definovat protivníka, jakož i znát jeho motivace, taktiky a techniky působení, mezi nejsložitější a zároveň zcela nejzásadnější úkony. NCKO bude posilovat schopnosti sběru a analýzy informací o hrozbách, rizicích a útocích v kyberprostoru. Tyto schopnosti budou založeny na třech hlavních pilířích. Na komplexní analýze kybernetických hrozeb – „Cyber Threat Intelligence“, vyspělé forenzní analýze a bezpečnostním operačním centru kybernetické obrany NCKO. Získané informace

budou nezbytným podkladem pro výkon efektivní kybernetické obrany ČR, vybrané informace mohou být sdíleny s ostatními národními i mezinárodními relevantními subjekty.

3.4. Vytvoření doktrinálního rámce pro použití schopností kybernetické obrany ČR

Utváření operačních schopností musí být doprovázeno začleněním všech nově vytvořených schopností v doktrínách na všech úrovních – strategické, operační i taktické.

3.5. Vytvoření „cyber deterrence“ strategie

Důležitou schopností je odrazování potenciálních útočníků od provádění nepřátelských akcí. Na „cyber deterrence“ se podílí řada činitelů, jako například schopnost odhalování útoků a dohledání jejich původců, celková úroveň kybernetické obrany, nebo postihy hrozící při dopadení. Pokud však jednotlivé prvky působí samostatně, je jejich účinnost nesrovnatelně nižší než v případě uceleného a systémového přístupu. Jelikož se jedná o komplexní víceoborové téma, je vhodné na národní úrovni vytvořit samostatnou strategii.

4. Nastavení spolupráce a provádění vzdělávání a cvičení

4.1. Spolupráce v rámci rezortu MO

Klíčová spolupráce bude nutně probíhat v rámci rezortu MO jako součást komplexního zajišťování obrany ČR. Úzká spolupráce bude probíhat s AČR v rámci podpory vojenských operací. Bude nutné vybudovat ve spolupráci s ostatními složkami rezortu MO bezpečné komunikační kanály.

4.2. Spolupráce na národní úrovni

NCKO se bude účastnit tvorby funkčního systému spolupráce organizací podílejících se na zajišťování kybernetické bezpečnosti ČR. Zásadní bude kooperace s NÚKIB, PČR - NCOZ národním CERT a ostatními pracovišti typu CERT/CSIRT. Vzhledem k tomu, že kybernetické hrozby mají mnoho podob, měl by se posilovat soulad mezi civilními a vojenskými přístupy k ochraně kritických aktiv. Tyto snahy je třeba podpořit užší spoluprací mezi NCKO, soukromým sektorem a akademickou sférou. Významná bude rovněž spolupráce v rámci vědy a výzkumu. Spolupráce na národní úrovni bude podporována vhodnou strategickou komunikací.

4.3. Spolupráce na mezinárodní úrovni

Vzhledem ke globální povaze kybernetického prostoru musí NCKO vybudovat silná a důvěrná spojenectví v mezinárodním prostředí. Hlavní spolupráce bude probíhat v rámci struktur NATO a EU, kde se předpokládá rovněž aktivní účast příslušníků NCKO. Úzká spolupráce bude navázána zejména s CCD COE. Samozřejmostí musí být rovněž utužování partnerství v rámci spolupráce se sousedními zeměmi. Dalším významným aspektem bude rozvíjení spolupráce v mnohem větším globálním měřítku.

4.4. Cvičení

Důležitou součástí spolupráce je organizování či účast na cvičeních. Pomocí cvičení lze ověřit a zdokonalit schopnosti čelit reálným hrozbám. Cvičení budou zaměřena nejen na připravenost technických struktur, ale i právní a rozhodovací aspekty. Stejné aktivity je nutné vyvíjet jak na národní, tak i mezinárodní úrovni.

4.5. Vzdělávání

Zajištění kybernetické obrany ČR notnou dávkou přispěje i vzdělávání osob podílejících se na jejím zajišťování, stejně jako osvěta jiných zainteresovaných osob prostřednictvím příslušníků NCKO. Typicky se bude jednat o účast na školeních, seminářích a konferencích. Důležitým aspektem bude podpora a kooperace při vzniku vzdělávacích programů zaměřených na oblast kybernetické obrany. I zde platí, že je nutné stejné aktivity vyvíjet jak na národní, tak i mezinárodní úrovni.

5. Podílení se na zajištění kybernetické bezpečnosti rezortu MO

5.1. Zajištění kybernetické bezpečnosti NCKO

NCKO se stane pravděpodobným cílem pro různě motivované kybernetické útoky. Jejich snahou bude získávání informací, zpochybnění důvěryhodnosti, nebo přímo úplné vyřazení NCKO, tedy i oslabení obranyschopnosti ČR. NCKO proto musí zavádět veškerá opatření nutná pro zajištění maximálního stupně vlastní kybernetické bezpečnosti.

5.2. Podílení se na detekování hrozeb a zranitelností sítí v rámci rezortu MO

NCKO bude disponovat obšírnými informacemi o hrozbách v kyberprostoru, na základě kterých bude dávat doporučení k přijetí opatření v rámci zajištění kybernetické bezpečnosti rezortu MO. Operační schopnosti NCKO budou využity rovněž jako jeden z prostředků pro odhalování kybernetických zranitelností prvků v rámci rezortu MO. Pro zjišťování zranitelností mohou být využity rovněž moderní metody založené na spolupráci se širokou veřejností.

5.3. Podílení se na zajištění kybernetické bezpečnosti sítí a příslušníků rezortu MO

Bezpečnostní operační centrum kybernetické obrany NCKO musí navázat úzkou spolupráci s obdobnými pracovišti v rámci rezortu MO, především pak s Centrem CIRC MO. V rámci této kooperace musí docházet k aktivní výměně informací a ke koordinaci činností jeho jednotlivých prvků. NCKO se rovněž musí aktivně podílet na stanovování zaváděných standardů kybernetické bezpečnosti. Dalším opatřením bude podílení se na obraně příslušníků rezortu MO, kteří by se mohli stát terčem kybernetických útoků různých forem a motivací. Jejich obrana může mít například povahu školení, ale i aktivní výpomoci v případě jejich přímého ohrožení kybernetickými útoky.

5.4. Podílení se na odborných školeních pro ICT odborníky rezortu MO

Příslušníci NCKO budou nadstandardně vyškoleni a zároveň budou svou činností získávat jedinečné zkušenosti. Nabyté znalosti a zkušenosti budou předávány prostřednictvím školení relevantním příslušníkům rezortu MO s cílem celkového navyšování digitální gramotnosti personálu.

Implementace

Tato strategie je rozpracována do úrovně specifických cílů, které jsou popsány v míře umožňující její zveřejnění pro širší odbornou i laickou veřejnost. Na základě zde uvedených cílů je vypracován neveřejný implementační plán, který obsahuje podrobný popis opatření pro splnění jednotlivých cílů, odpovědnosti, termíny jejich plnění a způsob hodnocení.

Plnění strategie bude průběžně kontrolováno a vyhodnocováno. S ohledem na dynamiku rozvoje moderních technologií bude průběžně sledováno, zda takto nastavená strategie odpovídá aktuální situaci. Reflektována bude i diskuze, za jejímž účelem bude zřízen i veřejnosti přístupný kontaktní bod ve formě emailové adresy. V případě potřeby je tedy počítáno s provedením nutných revizí.

Průběh implementace bude průběžně vyhodnocován formou výročních zpráv, které budou předkládány prostřednictvím ředitele Vojenského zpravodajství odpovědným orgánům.

Závěrečné slovo

Předkládaná strategie má spíše povahu organizační a slouží k vybudování účinného systému kybernetické obrany ČR. Poznatky a zkušenosti získané v průběhu zajišťování kybernetické obrany ČR budou stěžejním podkladem pro plánování dalšího rozvoje a strategického směřování s tím, že navazující strategie může být jistě ambicióznější, třeba tím směrem, že ČR bude vyvíjet snahu patřit mezi nejvýznamnější světové hráče na poli zajišťování kybernetické obrany.

Seznam použitých zkratek

AČR – Armáda České republiky

CCD COE - NATO Cooperative Cyber Defence Centre of Excellence

CERT – Computer Emergency Response Team

CIRC – Computer Incident Response Capability

EU – Evropská unie

MO – Ministerstvo obrany

NATO – North Atlantic Treaty Organization

NCKO – Národní centrum kybernetických operací

NÚKIB – Národní úřad pro kybernetickou a informační bezpečnost

Příloha

Grafické znázornění cílů.

Strategie kybernetické obrany ČR pro období 2018 - 2022

1 Nastavení právního rámce

- působnost a pravomoce
- rozhodovací proces
- vnitřní předpisy
- mezinárodní právo
- právní aspekty kyberprostoru

2 Infrastruktura

- technické zázemí
- personál
- infrastruktura
- externí zdroje

3 Schopností kyb.obrany

- operace v kyberprostoru
- podpora vojenských operací
- predikce a analýza
- doktríny
- cyber deterrence

4 Spolupráce, vzdělání a cvičení

- rezortní, národní, mezinárodní
- cvičení
- vzdělávání

5 Rezortní kyb. bezpečnost

- Kyb. bezpečnost NCKO
- podílení se na:
  - detekci hrozeb a zranitelností
  - zajištění bezpečnosti
  - školení

Strategie kybernetické obrany ČR pro období 2018 - 2022

znázornění cílů

NCKO 2018