Hlášení o stavu naplňování Akčního plánu k Národní strategii kybernetické bezpečnosti České republiky na období let 2015 až 2020

Kód	Úkoly	Subjekt	Časový rámec	Plnění
A.1.03	**Provádět technická i netechnická národní cvičení kybernetické bezpečnosti.**	NBÚ/NCKB ve spolupráci s: MO MV Zpravodajské služby	průběžně	**PLNĚNO** V roce 2016 byla provedena řada cvičení kybernetické bezpečnosti technického i netechnického charakteru. V polovině března zorganizovalo NBÚ/NCKB společně s Ústavem výpočetní techniky Masarykovy univerzity druhý běh cvičení s názvem Cyber Czech 2015. Dále v červnu 2016 proběhlo table-top cvičení Cyber Czech 2016, které navázalo na strategické cvičení, které bylo pořádáno NBÚ/NCKB ve spolupráci s European Cyber Security Initiative (ECSI) a European Defence Agency (EDA) v červnu 2015. Druhé technické cvičení s novými, unikátními scénáři se pak uskutečnilo v druhé polovině října pod názvem Cyber Czech 2016. Posledním cvičením v roce 2016 bylo národní cvičení komunikační, zaměřující se na ověření průchodnosti neklasifikovaných komunikačních kanálů a aktuálnosti údajů nahlášených povinnými subjekty dle § 16 ZKB. Cvičení se zúčastnili zástupci z řad subjektů státní správy a subjektů KII (blíže viz kapitola 5.8).
A.2.01	**Vytvořit jednotnou metodologii pro zvládání kybernetických bezpečnostních incidentů na základě ZKB a souvisejících právních předpisů.**	NBÚ/NCKB	Q1 2016	**SPLNĚNO** NBÚ/NCKB, resp. GovCERT.CZ vytvořil a disponuje jednotnou metodologií pro zvládání kybernetických bezpečnostních incidentů na základě ZKB a souvisejících právních předpisů.
A.2.04	**Vytvořit protokol osvědčených postupů v oblasti zajišťování kybernetické bezpečnosti.**	NBÚ/NCKB	Q2 2016	**SPLNĚNO** Úkol byl splněn formou vytvoření a poskytování podpůrných a metodických materiálů k problematice ISMS u KII a VIS (dostupné na webových stránkách www.govcert.cz) či problematice kontroly dodržování ZKB (např. dokument "Průvodce auditem"). Tyto materiály jsou pak použitelné i pro další subjekty, které nejsou povinnými subjekty dle ZKB. NBÚ proto doporučuje všem subjektům následovat prováděcí předpisy k ZKB, především tzv. "vyhlášku o kybernetické bezpečnosti" (vyhláška č. 316/2014 Sb.).

Kód	Úkoly	Subjekt	Časový rámec	Plnění
A.4.01	**Vytvořit efektivní model pro sdílení informací o zahraničních aktivitách mezi NBÚ a ostatními relevantními subjekty.**	NBÚ/NCKB ve spolupráci s: MZV MO MPO MV ÚZSI	Q2 2016	**SPLNĚNO** V ČR byl vytvořen efektivní model sdílení informací o zahraničních aktivitách a nastaven rámec spolupráce mezi NBÚ/NCKB a ostatními relevantními subjekty. K tomuto účelu došlo již v roce 2015 k vytvoření pracovní skupiny pro harmonizaci mezinárodních pozic (PS-MEZ) určené k harmonizaci mezinárodních aktivit na národní úrovni. Bilaterálně pak pravidelně zve MO zástupce NBÚ k dvoustranným jednáním se zahraničními partnery, které se dotýkají problematiky kybernetické bezpečnosti, dále probíhá úzká spolupráce mezi NBÚ a MO při řešení problematiky Cyber Defence v rámci NATO a subjekty se informují o závěrech jednání Cyber Defence Committee (také MV a MZV). V rámci MZV byla vytvořena pozice zvláštního zmocněnce pro kybernetický prostor, jehož úkolem je mimo jiné koordinovat pozice ČR na mezinárodním poli, přičemž MZV pokračuje v intenzívní spolupráci s NBÚ/NCKB a dalšími relevantními institucemi. Co se týká záležitostí ÚZSI, ten ve své strategii kybernetické bezpečnosti definuje model spolupráce s příslušnými domácími i zahraničními relevantními subjekty a počátkem 2017 předloží NBÚ k projednání první návrhy rámcové smlouvy a prováděcího ujednání pro stanovení pravidel při předávání zpravodajských informací v souladu se zákonem č. 153/1994 Sb., o zpravodajských službách České republiky. Spolupráce NBÚ/NCKB a MPO v mezinárodní oblasti byla již společně nastavena tak, aby umožňovala dotčeným institucím rychlou koordinaci stanovisek a spolupráci v oblastech společného zájmu. Dalším příkladem úspěšné mezirezortní koordinace v roce 2016 je např. realizace únorové návštěvy hodnotitelů v rámci sedmého kola vzájemných hodnocení pořádaných Pracovní skupinou pro obecné záležitosti (GENVAL), na níž se NBÚ/NCKB podílel s MV, MS, Policií ČR a Nejvyšším státním zastupitelstvím. Sdílení informací o zahraničních aktivitách pak probíhá i skrze veřejnou webovou platformu na www.govcert.cz, která by v blízké době měla obsahovat i neveřejnou část.

Kód	Úkoly	Subjekt	Časový rámec	Plnění
A.4.02	**Koordinovat a harmonizovat s ostatními resorty pozice v EU, NATO a dalších mezinárodních organizacích.**	NBÚ/NCKB ve spolupráci s: MZV MO MPO MV	od Q3 2015 průběžně	**PLNĚNO** Koordinace a harmonizace pozic v EU, NATO a dalších mezinárodních organizacích probíhá skrze nastavené komunikační kanály (viz např bod A.4.01). Celková spolupráce se zlepšila mimo jiné i vysláním cyber attaché do Bruselu, který zajišťuje lepší přehled o projednávaných otázkách souvisejících s kybernetickou bezpečností v EU a NATO. Již roku 2015 došlo také v rámci RKB k vytvoření PS-MEZ určené k harmonizaci mezinárodních aktivit na národní úrovni. MZV pak přispívalo k plnění tohoto úkolu především koordinací relevantních útvarů ústředí a sítě zastupitelských úřadů.
A.5.01	**Implementovat Bezpečnostní strategii České republiky s ohledem na zvyšující se kybernetické hrozby a v případě změny bezpečnostního prostředí navrhnout její revizi.**	NBÚ/NCKB MV MZV MO ÚV ČR Zpravodajské služby	průběžně	**PLNĚNO** Bezpečnostní strategie České republiky je naplňována všemi relevantními aktéry jednak plněním Akčního plánu, a jednak kontinuální reflexí hlavních bodů Bezpečnostní strategie ČR při přípravě strategických a koncepčních dokumentů, politik, analýz a stanovisek a při každodenní činnosti.
B.1.01	**Spolupracovat s EU v implementaci Strategie kybernetické bezpečnosti EU.**	NBÚ/NCKB MPO MZV MV	průběžně	**PLNĚNO** ČR kontinuálně spoluprace s EU v implementaci Strategie kybernetické bezpečnosti EU. Nejvýraznějším počinem v oblasti kybernetické bezpečnosti na evropské úrovni v roce 2016 bylo přijetí směrnice NIS, na jejíž transpozici se ČR v průběhu celého roku 2016 připravovala. V souladu se Strategií kybernetické bezpečnosti EU se ČR aktivně podílela na chodu agentury ENISA.

Kód	Úkoly	Subjekt	Časový rámec	Plnění
B.1.02	**Aktivně spolupracovat s EU, Evropskou komisí a jejími agenturami k zajištění větší koherence v kybernetických tématech v rámci EU.**	NBÚ/NCKB MPO MZV MV MO	průběžně	**PLNĚNO** V roce 2016 ČR aktivně spolupracovala s EU, resp. Evropskou komisí a jejími agenturami. ČR např. prostřednictvím NBÚ/NCKB a stálého zastoupení v Bruselu jednala i v roce 2016 v pracovní skupině Přátel předsednictví pro kybernetické otázky (Friends of Presidency of Cyber Issues), kde se mimo jiné draftoval Diplomatic Toolbox formulující možné diplomatické nástroje, které mají členské státy k dispozici při řešení závažných kybernetických útoků. Díky zřízení stálé pozice cyber attaché v Bruselu pak ČR získala lepší přehled o projednávání otázek souvisejících s kybernetickou bezpečností napříč jednotlivými orgány EU a pracovními skupinami Rady, což do budoucna umožní účinnější prosazování národních priorit a lepší koordinaci aktivit jednotlivých rezortů činných v oblasti kybernetické bezpečnosti a záležitostech s ní souvisejících. V prosinci 2016 se také uskutečnilo setkání stálých zástupců v Coreperu1 s komisařem Oettingerem, na kterém byla mimo jiné otázka koordinace diskutována. Z pozice MO se pak rozvíjí spolupráce s European Defence Agency (EDA). MO dále monitoruje aktivity EU v oblasti Cyber Defence a to především prostřednictvím Vojenského úseku Stálého zastoupení ČR při EU.

Kód	Úkoly	Subjekt	Časový rámec	Plnění
B.1.03	**Spolupracovat a aktivně se podílet na práci ENISA v oblasti informační a síťové bezpečnosti.**	NBÚ/NCKB	průběžně	**PLNĚNO** ČR je v ENISA zastoupena skrze účast na formálních a neformálních jednáních. Dva zástupci NBÚ/NCKB působí jako člen a alternát v představenstvu ENISA, kde se podílejí na schvalování programu, plánu prací a rozpočtu ENISA. Další zástupce NBÚ/NCKB je členem užší pracovní skupiny ENISA pro podporu tvorby a implementace národních strategií kybernetické bezpečnosti. V ČR slouží i tzv. National Liaison Officer (pracovník NBÚ/NCKB), který v každé členské zemi EU vykonává funkci referenčního bodu ve specifických otázkách kybernetické bezpečnosti, zprostředkovatele spolupráce a podporovatele aktivit ENISA.
B.1.04	**Aktivně se podílet v OBSE na vytváření a následné implementaci kybernetických opatření pro zvyšování důvěry mezi státy v kyberprostoru a případně dalších iniciativ v souladu s vizemi a principy NSKB ČR.**	NBÚ/NCKB ve spolupráci s: MZV	průběžně	**PLNĚNO** Práce OBSE v oblasti opatření pro budování důvěry a předcházení konfliktů v souvislosti s aktivitami v kyberprostoru, tzv. kybernetických CBMs („Confidence building measures“), dosáhla v roce 2016 dalšího milníku, když v březnu 2016 účastnické státy přijaly druhou sadu kybernetických CBMs. ČR, zastoupená NBÚ/NCKB a MZV, se aktivně na přípravě této druhé sady podílela a kontinuálně usiluje o implementaci a plnění obou sad.

Kód	Úkoly	Subjekt	Časový rámec	Plnění
B.1.05	**Spolupracovat se spojenci při implementaci politiky NATO v rámci kybernetické obrany.**	NBÚ/NCKB MO VZ	průběžně	**PLNĚNO** V roce 2016 proběhl NATO summit ve Varšavě, kde byl mimo jiné přijat také Cyber Defence Pledge, na jehož finální podobě se podílelo i NBÚ/NCKB. Na spolupráci s NATO se v oblasti kybernetické obrany podílí i MO. Spolu s NBÚ/NCKB spolupracují na přípravě pozic na jednání v Cyber Defence Committee (CDC), kde má MO stálé zastoupení prostřednictvím Stálé delegace ČR při NATO, a v případě potřeby i jiných orgánů NATO. Společně se v roce 2016 také účastnily aliančních cvičení Cyber Coalition a Locked Shields. Jednání Severoatlantické rady a CDC podpořilo NCKB v roce 2016 i přípravou analýz aktuálního dění v kybernetickém prostoru. ČR na půdě NATO pokračovala v aktivní účasti na dvou Smart Defence projektech a již třetím rokem se také aktivně podílela na činnosti NATO Cooperative Cyber Defence Centre of Excellence (CCDCoE), které se zaměřuje na výzkumnou a vědeckou činnost v oblasti kybernetické bezpečnosti a obrany (viz kapitola 5.3). MO realizuje požadavky NATO v oblasti Cyber Defence na základě závazků k plnění cílů výstavby schopností NATO CT 2013/E 5308 N „Information Assurance and Cyber Defence“. Plnění těchto požadavků rezort MO vyhodnocuje pravidelně 2x ročně. V měsíci listopadu 2016 přijalo MO nové cíle výstavby schopností CT 2017/E 6202 „Cyber Defence“, které po schválení ministry obrany v červnu 2017 nahradí CT z roku 2013. V předešlém roce 2015 bylo také rozhodnuto o vojenském zastoupení MO ve strukturách NATO CIRC. V roce 2016 probíhala příprava kandidátů z Centra CIRC na obsazení této pozice. VZ pak kontinuálně spolupracuje v rámci MO na připomínkách k dokumentům vytvářených v rámci NATO týkajících se problematiky kybernetické obrany. Do spolupráce a koordinace spjatých aktivit se také zapojuje MZV.

Kód	Úkoly	Subjekt	Časový rámec	Plnění
B.1.06	**Podporovat spolupráci s NATO v oblasti kybernetické obrany, zejména s ohledem na reakci na kybernetické bezpečnostní incidenty a výměnu technických informací o hrozbách a zranitelnostech.**	NBÚ/NCKB MO MZV VZ	průběžně	**PLNĚNO** ČR aktivně spolupracuje s NATO v oblasti kybernetické obrany. V souladu se závěry Varšavského Summitu byly rozpracovány návrhy budoucího vývoje kybernetické obrany NATO. Trvale se také spolupracuje na odborně-technické úrovni s NATO CIRC. Tato spolupráce vychází z memoranda o porozumění v oblasti kybernetické obranné spolupráce uzavřeného mezi ČR a NATO (CZE – NATO CD MOU). Schopnost spolupráce je prověřována při každoročních cvičeních NATO Cyber Defence Exercise Cyber Coalition. V rámci tohoto cvičení je testována i platforma MISP pro výměnu technických informací o hrozbách a zranitelnostech.

Kód	Úkoly	Subjekt	Časový rámec	Plnění
B.1.07	**Podporovat spolupráci s ITU ve věci tvorby a zavádění technických standardů v kybernetické bezpečnosti.**	NBÚ/NCKB MPO ČTÚ	průběžně	**PLNĚNO** ČR prostřednictvím ČTÚ i v roce 2016 plně podporovala veškeré aktivity a činnosti ITU, včetně vytváření technických standardů v oblasti kybernetické bezpečnosti. ČTÚ se pak v rámci svěřené gesce účastnil jednání v nejvyšším orgánu (standardizačního) sektoru ITU T - tj. Světového shromáždění pro standardizaci telekomunikací (WTSA – World Telecommunication Standardisation Assembly). Kybernetickou bezpečností se zabývá studijní skupina ITU-T SG 17 (security). ČTÚ na probíhajících jednání podpořil Společné evropské návrhy připravené organizací CEPT, mezi něž také patřil návrh struktury studijních skupin. Ten směřoval k zachování současného zaměření studijní skupiny SG 17 a pokračování její činnosti v oblasti kybernetické bezpečnosti v plném rozsahu. Z aktuální projednávané problematiky SG 17 lze např. uvést: - Přehled o výměně kyber-bezpečnostních informací. - Úprava technik při výměně strukturovaných kyber-bezpečnostních informací. - Pravidla zmírňující negativní dopady zavirovaných terminálů v mobilních sítích. - Zabezpečená aktualizace software pro komunikační zařízení inteligentního dopravního systému.

Kód	Úkoly	Subjekt	Časový rámec	Plnění
B.1.08	**Rozvíjet dialog skrze „cyber diplomacy“ mezi členskými zeměmi OSN týkající se norem vztahujících se k používání ICT v jednotlivých zemích s cílem snížit společné nebezpečí, chránit důležitou národní a mezinárodní infrastrukturu a budovat důvěru a stabilitu mezi zeměmi.**	MZV ve spolupráci s: NBÚ/NCKB	průběžně	**PLNĚNO** Vysoká úroveň legislativy v oblasti kybernetické bezpečnosti a ochota sdílení zkušeností poskytuje ČR silný nástroj pro rozvoj mezinárodních vztahů v této oblasti. Působení cyber attachés na vybraných zahraničních úřadech rovněž posiluje „cyber diplomacy“ České republiky. V neposlední řadě významně přispívá k rozvoji této problematiky i stálá účast odborníka NBÚ/NCKB v NATO CCD COE.
B.1.09	**Aktivně participovat národní expertizou a prostředky v CCDCOE a podílet se průběžně na výzkumných aktivitách centra.**	NBÚ/NCKB MO	průběžně	**PLNĚNO** ČR aktivně participuje na fungování CCDCOE skrze stálou účast odborníka NBÚ/NCKB v této instituci, národní expertizou a finančními prostředky. I v roce 2016 se průběžně podílela na jeho výzkumných aktivitách. ČR zároveň aktivně odpovídá na výzkumné dotazy CCDCOE a participuje na jejich projektech. V neposlední řadě se podílí na přípravě a organizaci cvičení kybernetické bezpečnosti Locked Shields. MO zatím nemá vojenské zastoupení ve strukturách CCDCOE a nepodílelo se proto prozatím na výzkumných aktivitách centra. Z tohoto důvodu bude MO vést diskuzi s NBÚ/NCKB o možnostech vyslání zástupce do struktur CCDCOE.
B.2.01	**Aktivně se podílet a podporovat spolupráci jak v rámci V4, tak ve Středoevropské platformě kybernetické bezpečnosti (CECSP).**	NBÚ/NCKB ve spolupráci s: MZV MO	průběžně	**PLNĚNO** Spolupráce v rámci V4 probíhala v roce 2016 jak na operační, technické, tak i strategické úrovni. Problematika kybernetické bezpečnosti byla např. jednou z hlavních agend jednání bezpečnostních ředitelů MO V4 v ČR v měsíci dubnu a předpokládá se zachování této agendy i pro další období. V rámci CECSP i v roce 2016 probíhala pravidelná jednání a ČR na nich prezentovala svůj vývoj v oblasti kybernetické bezpečnosti a pokračovala v diskuzi nad sdílením technických informací, včetně používaných standardů a nástrojů.

Kód	Úkoly	Subjekt	Časový rámec	Plnění
B.2.02	**Aktivně se podílet a podporovat spolupráci s národními bezpečnostními týmy ve středoevropském a východoevropském regionu.**	NBÚ/NCKB MO	průběžně	**PLNĚNO** NBÚ/NCKB v roce 2016 pokračoval v poskytování asistence státům, které budují svůj systém kybernetické bezpečnosti. Tento rok se v rámci dvou evropských projektů zaměřil na balkánské státy. V rámci pokračujícího projektu Enhancing Cyber Security český zástupce spoluorganizoval workshop pro členy makedonských, kosovských a moldavských CERT/CSIRT týmů, který se konal v Kišiněvě. Hlavním cílem bylo předat zkušenosti s budováním obdobného pracoviště v České republice. V rámci instrumentu TAIEX školili pracovníci NBÚ/NCKB představitele organizací ze šesti balkánských zemí, kteří se ve svých státech zabývají kybernetickou bezpečností. Čeští zástupci jim předávali zkušenosti s tvorbou koncepčních materiálů, ochranou KII či s tvorbou kybernetických cvičení. Z pozice MO je pak nutné uvést, že v roce 2016 nebyla aktivně rozvíjena spolupráce s národními vojenskými bezpečnostními týmy ve středoevropském a východoevropském regionu z důvodu nedostatku kapacit.
B.3.01	**Pokračovat a prohlubovat bilaterální spolupráci s vybranými státy v rámci kybernetické bezpečnosti.**	NBÚ/NCKB ve spolupráci s: MZV MO	průběžně	**PLNĚNO** V roce 2016 se pokračovalo v již zavedené spolupráci s vybranými partnery, k čemuž dopomohlo nejen působení cyber attachés (viz kapitola 4.7). MO kontinuálně spolupracuje s ozbrojenými silami USA v rámci programu Mil-to-Mil a rozvíjí spolupráci s Izraelem a dalšími státy. V roce 2016 proběhla bilaterální jednání MO s Gruzií a Korejskou republikou. MZV se rovněž významně podílelo na procesu posilování strategických partnerství s vybranými zeměmi (USA, Izrael, Korejská republika). S Korejskou republikou se uskutečnily kyberkonzultace (věcně připravené NBÚ/NCKB ve spolupráci s dotčenými resorty) na úrovni náměstků ministrů zahraničních věcí, a také se uskutečnil Česko-izraelský seminář ke kybernetické bezpečnosti mj. pod záštitou ministra zahraničních věcí ČR.

Kód	Úkoly	Subjekt	Časový rámec	Plnění
B.4.01	**Pravidelně se účastnit a aktivně se podílet na vytváření scénářů mezinárodních cvičení v oblasti kybernetické bezpečnosti.**	NBÚ/NCKB MO MV	průběžně	**PLNĚNO** ČR se i v roce 2016 zapojila do v pořadí již sedmého ročníku největšího mezinárodního technického cvičení kybernetické bezpečnosti Locked Shields, dále do cvičení NATO Crisis Management Exercise či Cyber Coalition a Cyber Europe (viz kapitola 4.12). U většiny těchto cvičení se ČR prostřednictvím svých zástupců (NBÚ/NCKB a MO) také podílela na přípravě jejich scénářů. Dále NBÚ/NCKB opět uspořádal dvě cvičení připravená na míru pro zahraniční partnery a to na zastupitelském úřadě ve Washingtonu, D.C. a na Velitelství pro transformaci NATO ACT v Norfolku. Akce se skládala ze specializovaného školení a návazného strategického table-top cvičení reflektující aktuální dění ve světě (viz kapitola 4.12.4).
B.5.01	**Účastnit se a organizovat mezinárodní školení, kurzy a semináře v oblasti kybernetické bezpečnosti.**	NBÚ/NCKB ve spolupráci s: MZV MO MV Zpravodajské služby	průběžně	**PLNĚNO** Značná část relevantních institucí ČR se prostřednictvím svých zástupců účastnila množství mezinárodních školení, kurzů či seminářů v oblasti kybernetické bezpečnosti. ČR v této souvislosti plně využívala svého aktivního zapojení v NATO CCDCOE, když část odborníků prošla školeními právě zde. Dále se zástupci relevantních institucí ČR účastnili i celé řady mezinárodních konferencí zaměřující se na problematiku kybernetické bezpečnosti a obrany. Vedle zvyšování expertízy přináší tato aktivita i potřebné kontakty s mezinárodními partnery na pracovní úrovni.
B.6.01	**Podporovat vytváření mezinárodních komunikačních a informačních kanálů mezi CERT/CSIRT pracovišti, mezinárodními organizacemi a akademickými centry.**	NBÚ/NCKB MO	průběžně	**PLNĚNO** V prvních měsících roku 2016 byla dokončena certifikace GovCERT.CZ, který se k 1. dubnu stal plným členem mezinárodní platformy FIRST (Forum for Incident Response and Security Teams) sdružující vládní a soukromé CERT/CSIRT týmy z celého světa. NBÚ/NCKB pak ostatní české CERT/CSIRT pracoviště podporuje v zapojení se do organizací FIRST a TI GÉANT (vládní CERT je členem od roku 2014) a zároveň podporuje technické nástroje a platformy určené ke sdílení a výměně informací.

Kód	Úkoly	Subjekt	Časový rámec	Plnění
B.6.02	**Aktivně se zapojit do výstavby a užívání NATO projektů pro řízení reakcí na kybernetické bezpečnostní incidenty a výměnu technických informací o škodlivých kódech mezi státy NATO.**	NBÚ/NCKB MO	od Q3 2015 průběžně	**PLNĚNO ČÁSTEČNĚ** Odpovědná pracoviště jsou zapojena do projektů sdílení informací v rámci NATO, které jsou mj. testovány v rámci cvičení kybernetické bezpečnosti. MO i NBÚ využívají pro sdílení technických informací o hrozbách a zranitelnostech NATO projekt Malware Information Sharing Platform (MISP). Již v roce 2014 byl podepsán za ČR Statement of Interest a MO je zastoupeno v projektovém týmu mnohonárodního Smart Defence projektu MISP. MO však není aktivně zapojeno ve výstavbě NATO projektů pro řízení reakcí na kybernetické bezpečnostní incidenty (např. projekt CIICS).
C.1.01	**Určovat průběžně subjekty KII a identifikovat VIS, jichž se dotýká ZKB a související právní předpisy.**	NBÚ/NCKB Ve spolupráci s: MV	průběžně	**PLNĚNO** V roce 2016 NBÚ/NCKB průběžně určoval subjekty KII a identifikoval VIS, jichž se dotýká ZKB a související právní předpisy. Na konci roku 2016 NBÚ/NCKB evidoval celkem 257 informačních či komunikačních systémů klasifikovaných jako KII či VIS, které spravuje celkem 88 správců (viz kapitola 2.1.3).
C.1.02	**Konzultovat, komunikovat a poskytovat metodickou podporu subjektům KII a VIS.**	NBÚ/NCKB	průběžně	**PLNĚNO** NBÚ/NCKB i v roce 2016 vytvářel a aktualizoval podpůrné materiály pro potřeby KII a VIS. Na požádání je v rámci metodické podpory poskytované pracovníky NBÚ/NCKB kontinuálně prováděn výklad povinností subjektů dle zákona č. 181/2014 Sb., o kybernetické bezpečnosti (ZKB). NBÚ/NCKB poskytuje i další metodickou pomoc. V roce 2016 NBÚ/NCKB opět vyvíjel bohatou přednáškovou činnost a konzultoval se subjekty problematiku kybernetické bezpečnosti.
C.1.03	**Podporovat a průběžně kontrolovat implementaci zákonných povinností u subjektů KII a VIS.**	NBÚ/NCKB	průběžně	**PLNĚNO** Začátkem roku 2016 byly u povinných osob zahájeny kontrol dodržování ZKB. NBÚ/NCKB provedl kontrolu u celkem 15 povinných subjektů (správců). Předmětem proběhlých kontrol bylo celkem 24 systémů (viz kapitola 2.2).

Kód	Úkoly	Subjekt	Časový rámec	Plnění
C.1.04	**Spolupracovat s mezinárodními partnery při hodnocení určování KII, zejména v oblasti přeshraničních závislostí**	NBÚ/NCKB	průběžně	**PLNĚNO ČÁSTEČNĚ** Spolupráce s mezinárodními partnery probíhala v roce 2015 především skrze poskytování a sdílení zkušeností při hodnocení a určování KII. Zástupci NBÚ tímto způsobem získávali další know-how ohledně určování a hodnocení KII zahraničními partnery. Hodnocení přeshraniční závislosti (resp. evropské kritické infrastruktury) v roce 2016 nebylo prioritou. Řešení tohoto úkolu bude aktuální až po úspěšné transpozici evropské směrnice NIS napříč státy EU.
C.2.01	**Informovat o výhodách a aktivně podporovat u soukromých subjektů (především spadajících pod KII) vznik CERT/CSIRT týmů k zajištění lepší spolupráce při řešení kybernetických bezpečnostních incidentů.**	NBÚ/NCKB	průběžně	**PLNĚNO** NBÚ kontinuálně informuje o výhodách a podporuje vznik dalších CERT/CSIRT týmů v České republice. Vznik nových CERT/CSIRT týmů u soukromých subjektů je NBÚ aktivně podporován, zejména poskytováním metodické podpory a know-how k jejich zřizování.
C.2.02	**Podporovat vznik CERT/CSIRT týmů v rámci resortů, dalších institucí státní správy a v rámci různých průmyslových odvětví.**	NBÚ/NCKB	průběžně	**PLNĚNO** Viz kód C.2.01. Zároveň lze zmínit příznivé působení národních cvičení kybernetické bezpečnosti jako jeden z podnětů příslušným subjektům k zajištění svého vlastního či sektorového CERT/CSIRT.
C.2.03	**Vybudovat resortní CERT/CSIRT pracoviště MV k ochraně základních registrů a nejdůležitějších systémů pro fungování e-Governmentu.**	MV ve spolupráci s: NBÚ/NCKB	Q1 2016	**SPLNĚNO** Bylo vybudováno resortní pracoviště MV k ochraně základních registrů a nejdůležitějších systémů pro fungování e-Governmentu.

Kód	Úkoly	Subjekt	Časový rámec	Plnění
C.3.01	**Průběžně navyšovat kapacity NCKB, potažmo GovCERT.CZ a reflektovat personální a znalostní nároky vyplývající z vývoje stavu kybernetické bezpečnosti ve státě**	NBÚ/NCKB	průběžně	**PLNĚNO** NCKB prošlo v roce 2016 důležitou organizační změnou. Zásadní událostí pro jeho další rozvoj bylo usnesení vlády ČR ze dne 19. prosince 2016 č. 1178, ve kterém vláda rozhodla o oddělení NCKB ze struktury NBÚ a vytvoření Národního úřadu pro kybernetickou a informační bezpečnost (NUKIB). Neméně důležité bylo i usnesení Vlády ČR ze dne 28. listopadu č. 1049, ve kterém vláda schválila návrh rozvoje kapacit a schopností NCKB; předpokládá navýšení personální kapacity na 300-400 zaměstnanců do roku 2025 a výstavbu nové budovy v Brně – Černých polích (viz kapitola 1). NCKB také pokračovalo v roce 2016 ve zvyšování kvalifikace svých pracovníků formou specializovaných školení, stáží a kurzů. Pracovníci GovCERT.CZ získali certifikace společnosti SANS, členové OKBP se účastnili celé řady školení a kurzů zaměřujících se na kybernetickou bezpečnost v kontextu mezinárodního práva, terorismu či metod analýzy informací z otevřených zdrojů.
C.3.03	**Udržovat aktuální evidenci kybernetických bezpečnostních incidentů, vyhodnocovat je a navrhovat opatření.**	NBÚ/NCKB	průběžně	**PLNĚNO** NBÚ/NCKB skrze GovCERT.CZ udržuje aktuální evidenci kybernetických bezpečnostních incidentů, vyhodnocuje je a navrhuje opatření (viz kapitola 7).
C.3.05	**Vytvořit a zavést honeypot systém k detekci kybernetických hrozeb.**	NBÚ/NCKB	Q3 2016	**ČÁSTEČNĚ SPLNĚNO** Honeypot systém k detekci kybernetických hrozeb byl již vytvořen v rámci GovCERT.CZ a na začátku roku 2017 proběhne jeho nasazení na NBÚ/NCKB. Komplexní nasazení ve státní správě je předpokládáno v letech 2017/2018.
C.3.06	**Mapovat vztahy mezi sítěmi veřejné správy a jejich ISP k zajištění efektivnější součinnosti v případě kybernetických bezpečnostních incidentů.**	NBÚ/NCKB	od Q4 2015 průběžně	**PLNĚNO** Prostřednictvím mapování a určování KII a identifikace VIS probíhal v roce 2016 proces mapování vztahů mezi sítěmi veřejné správy a jejich ISP. Tento úkol je kontinuálně prováděn na základě běžné činnosti GovCERT.CZ a v rámci kontroly dodržování ZKB subjekty KII a VIS.

Kód	Úkoly	Subjekt	Časový rámec	Plnění
C.3.08	**Vytvořit laboratoř pro detekci a testování dopadů malware na informační systémy.**	NBÚ/NCKB	Q2 2016	**SPLNĚNO** Laboratoř pro detekci a testování dopadů malware na informační systémy je v provozu a průběžně se navyšují její schopnosti i kapacity.
C.3.09	**Vytvořit a rozvíjet scénáře a programy simulace kybernetických bezpečnostních incidentů využitelné pro účely národních cvičení.**	NBÚ/NCKB ve spolupráci s: MO MV Zpravodajské služby	od Q3 2015 průběžně	**PLNĚNO** NBÚ/NCKB již několik let vytváří a rozvíjí scénáře a programy simulace kybernetických bezpečnostních incidentů, které využívá pro účely národních cvičení s názvem "Cyber Czech". Ostatní subjekty se aktivně podílejí na vyhodnocení národních a mezinárodních cvičení s cílem poskytnutí zpětné vazby pro využití k dalšímu rozvoji pro futuro vytvářených scénářů a simulací.
C.3.10	**Vytvořit a používat kapacity a schopnosti pro provádění kybernetických bezpečnostních testů.**	NBÚ/NCKB	od Q3 2015 průběžně	**PLNĚNO** Během roku 2016 bylo zahájeno poskytování služby formalizovaného penetračního testování. Tato služba je poskytována na základě smlouvy orgánům státní správy.
C.3.11	**Vytvořit kapacity a zlepšovat schopnosti forenzní analýzy a dalších podpůrných služeb v rámci kybernetické bezpečnosti pro potřeby ČR.**	NBÚ/NCKB	od Q3 2015 průběžně	**PLNĚNO** V rámci GovCERT.CZ nově vznikla v roce 2016 forenzní laboratoř. Jejím účelem je poskytnout prostředí a nástroje pro práci na zajištěných fyzických zařízeních (počítače, mobilní telefony, paměťová média aj.), jejich analýzu a uložení při zajištění požadované úrovně zabezpečení citlivých materiálů. Uvedení forenzní laboratoře do plného provozu je očekáváno v druhé polovině roku 2017.
C.3.12	**Podporovat projekt Fénix a zapojení významných sítí veřejné správy za účelem zachování funkcionalit a služeb během masivních kybernetických útoků.**	NBÚ/NCKB ve spolupráci s: MV	průběžně	**PLNĚNO** NBÚ/NCKB podporuje projekt FENIX i zapojení významných sítí veřejné správy do něj. Zástupci NBÚ/NCKB se účastní jednání pracovních skupin k projektu FENIX. S odpovědnými pracovníky NIX.CZ také dochází ke konzultacím s ohledem na další kybernetické bezpečnostní projekty NBÚ/NCKB. V současné době probíhají přípravy GovCERT.CZ na členství v NIX.CZ a posléze i v projektu Fénix.

Kód	Úkoly	Subjekt	Časový rámec	Plnění
C.4.01	**Provádět sběr a analýzu informací o hrozbách a rizicích, a tím zajišťovat aktuální přehled o situaci v kybernetické bezpečnosti jak v ČR, tak i ve světě.**	NBÚ/NCKB ve spolupráci s: Zpravodajské služby	průběžně	**PLNĚNO** Kapacity a schopnosti sběru a analýzy informací o hrozbách a rizicích technického směru jsou v rámci vládního CERT neustále rozvíjeny. Zpravodajské služby pak v rámci své působnosti sbírají a analyzují informace o hrozbách a rizicích s cílem mít přehled o situaci v oblasti kybernetické bezpečnosti jak v ČR, tak i ve světě.
C.4.02	**Detekovat anomálie v síťovém provozu a identifikovat potenciální kybernetické hrozby**	NBÚ/NCKB	Q1 2016	**SPLNĚNO ČÁSTEČNĚ** GovCERT.CZ dlouhodobě pracuje na rozvoji schopností detekce kybernetických útoků ve státní správě. Základním bodem této snahy je program nasazení síťových sond do klíčových státních institucí. Síťové sondy získávají a uchovávají popisná data o provozu a poskytují tak materiál pro analýzu a vyšetřování incidentů. Zároveň dovolují rozsáhlou automatizaci a rozpoznávání škodlivých a nebezpečných aktivit. Realizace tohoto projektu je očekávána v roce 2017.
C.4.03	**Rozvíjet schopnosti aktivně získávat informace v kyberprostoru o možných hrozbách a rizicích pro kybernetickou bezpečnost ČR.**	Zpravodajské služby	průběžně	**PLNĚNO** Zpravodajské služby v rámci své působnosti s ohledem na dostupné zdroje rozvíjí vlastní schopnosti aktivně získávat informace v kyberprostoru o možných hrozbách a rizicích pro kybernetickou bezpečnost ČR jak mezi sebou na národní úrovni, tak ve spolupráci se zahraničními zpravodajskými službami. V roce 2016 i nadále docházelo k rozvoji materiálně technického zázemí příslušných pracovišť zpravodajských služeb. Zároveň byly posilovány i jejich personální kapacity.
C.4.04	**Analyzovat obsah informací o hrozbách a rizicích pro důležité zájmy ČR získaných v kybernetickém prostoru včetně jejich manipulativního působení na veřejnost a vytvořit proces vzájemného efektivního informování o relevantních hrozbách a rizicích mezi příslušnými subjekty.**	Zpravodajské služby ve spolupráci s: NBÚ/NCKB	průběžně	**PLNĚNO** Zpravodajské služby analyzují informace získaných v kybernetickém prostoru o hrozbách a rizicích pro důležité zájmy ČR včetně jejich manipulativního působení na veřejnost a informují o nich ve svých výstupech oprávněným adresátům. Analýza obsahu informací o hrozbách a rizicích byla v roce 2016 prováděna v rámci zákonné působnosti zpravodajských služeb. Způsob předávání informací mezi zainteresovanými složkami, včetně pravidelných setkávání zástupců jednotlivých institucí, je rovněž nastaven.

Kód	Úkoly	Subjekt	Časový rámec	Plnění
C.4.05	**Podporovat koordinaci při preventivním působení v oblasti kybernetické bezpečnosti a získávání informací k plánování kybernetických útoků s cílem předcházení jejich provedení.**	BIS ÚZSI	průběžně	**PLNĚNO** ÚZSI a BIS kontinuálně spolupracují při preventivním působení v oblasti kybernetické bezpečnosti a získávání informací k plánování kybernetických útoků s cílem předcházení jejich provedení. Koordinace činnosti všech zpravodajských služeb je pak předmětem funkce Výboru pro zpravodajskou činnost, který je stálým orgánem Bezpečnostní rady státu.
C.4.06	**Modernizovat a personálně posílit jednotlivé specializované útvary zpravodajských služeb.**	BIS ÚZSI	od Q1 2016 průběžně	**PLNĚNO** ÚZSI usiluje o personální posílení specializovaných útvarů, personální otázka je zde vnímána jako prioritní. ÚZSI se také připojuje k iniciativám NBÚ/NCKB, které vedou k vytváření příslušných studijních programů a snížení platových rozdílů mezi státní správou a komercí. V rámci BIS je průběžně realizován rozvoj materiálně technického zázemí příslušných pracovišť, jakož i činnosti k zajištění odpovídajícího kvantitativního a kvalitativního personálního růstu na příslušných pracovištích.
C.4.07	**Nastavit a rozvíjet spolupráci mezi zpravodajskými službami ČR i zainteresovanými věcně příslušnými národními či mezinárodními subjekty.**	NBÚ/NCKB Zpravodajské služby	průběžně	**PLNĚNO** Spolupráce byla rozvíjena v mnoha ohledech; proběhlo množství pracovních schůzek či jednání zástupců jednotlivých subjektů jak na vedoucí tak i pracovní úrovni. Spolupráce mezi NBÚ/NCKB, BIS, ÚZSI a VZ je mj. rozvíjena také prostřednictvím cvičení kybernetické bezpečnosti (mezinárodních i národních), jichž se zástupci zpravodajských služeb pravidelně účastní.

Kód	Úkoly	Subjekt	Časový rámec	Plnění
C.5.01	**Zveřejňovat varování o kybernetických bezpečnostních hrozbách a incidentech s doporučením ke zvládání rizik.**	NBÚ/NCKB	průběžně	**PLNĚNO** NBÚ/NCKB pravidelně vydává informace o zranitelnostech a hrozbách prostřednictvím svého portálu www.govcert.cz. Zároveň provozuje twitterový účet, na kterém taktéž informuje o nejvážnějších hrozbách. V průběhu roku byla spuštěna nová verze veřejné části webových stránek sloužící jako informační portál širší a odborné veřejnosti. Neveřejná část je téměř dokončena a k jejímu předání a spuštění by mělo dojít na začátku roku 2017. Neveřejná část s kontrolou přístupu pak umožní sdílení informací ve větší míře směrem ke správcům systémů KII a VIS a také ke spolupracujícím bezpečnostním týmům. Jedná se zejména o informace, které není možné sdílet zcela veřejně.
C.6.01	**Průběžně vzdělávat a školit pracovníky NCKB v oblasti kybernetické bezpečnosti**	NBÚ/NCKB	průběžně	**PLNĚNO** Pracovníci NBÚ/NCKB se účastnili celé řady národních i mezinárodních školení a vzdělávacích aktivit a konferencí v oblasti kybernetické bezpečnosti.
C.6.02	**Prostřednictvím zahraničních kurzů udržovat aktuální povědomí o trendech v kybernetické bezpečnosti a hrozbách, kterým ČR jako aktivní člen EU a NATO čelí.**	NBÚ/NCKB	průběžně	**PLNĚNO** Pracovníci NBÚ/NCKB si prostřednictvím zahraničních kurzů udržují aktuální povědomí o trendech v kybernetické bezpečnosti a hrozbách, kterým ČR jako aktivní člen EU a NATO čelí (viz kód C.6.01).
C.6.03	**Navyšovat schopnosti GovCERT.CZ identifikovat povahu kybernetických bezpečnostních incidentů.**	NBÚ/NCKB	od Q2 2016 průběžně	**PLNĚNO** GovCERT.CZ průběžně navyšuje schopnosti identifikovat povahu kybernetických bezpečnostních incidentů. V tomto ohledu lze zmínit vývoj potřebných nástrojů, např. IntelMQ, stejně jako participaci na projektech SABU a PROKI a dalších.
C.6.05	**Zavést v GovCERT.CZ nepřetržitý provoz pohotovostní služby k monitorování a řešení kybernetických bezpečnostních**	NBÚ/NCKB	Q1 2016	**SPLNĚNO** Na GovCERT.CZ se již zavádí a je operačně schopný provoz pohotovostní služby k monitorování a řešení kybernetických bezpečnostních incidentů.

Kód	Úkoly	Subjekt	Časový rámec	Plnění
	incidentů.			
C.7.02	**Vypracovat a vládě předložit projekt státního cloudu včetně datových uložišť a další potřebné podklady (finanční, bezpečnostní, organizační a technické nároky).**	MV ve spolupráci s: MF NBÚ/NCKB	Q1 2016	**SPLNĚNO** Vláda svým usnesením č. 1050/2016 schválila „Strategický rámec Národního cloud computingu – eGovernment cloud ČR“ a zároveň schválila aktualizaci Akčního plánu Národní strategii kybernetické bezpečnosti ČR 2015 až 2020. Bod **C.7.02** se nahrazuje textem**:** **"Vypracovat a vládě předložit výstupy projektu „Příprava vybudování eGovernment cloudu“ definovaného Strategickým rámcem Národního cloud computingu – eGovernment cloud ČR včetně souhrnné analytické zprávy a souvisejících podkladů (finanční, bezpečnostní, organizační a technické nároky)".** S časovým rámcem: **4Q 2017.** Zároveň byly zahájeny práce na projektu „Příprava vybudování eGovernment cloudu“, za tímto účelem byla ustanovena pracovní skupina Rady vlády pro informační společnost, jejíž členové mají za úkol vypracovat komplexní analytickou zprávu v oblastech: - Legislativní/právní (L), - Bezpečnostní (B), - Ekonomická (E), - Provozní/obsahová (P), - Organizační/procesní (O), na základě které budou vydefinovány podmínky pro implementaci a vybudování eGovernment cloudu v ČR.

Kód	Úkoly	Subjekt	Časový rámec	Plnění
C.9.01	**V rámci Vojenského zpravodajství vytvořit Národní centrum kybernetických sil (NCKS), které bude schopné provádět široké spektrum operací v kyberprostoru a aktivity nutné pro zajištění kybernetické obrany ČR. NCKS bude schopné provádět vojenské operace v kyberprostoru, a to jak na podporu zahraničních operací AČR v rámci NATO nebo EU, tak i v případě hybridního konfliktu za účelem obrany ČR.**	VZ	od Q1 2016 průběžně	**PLNĚNO** V roce 2016 vzniklo Národní centrum kybernetických sil v rámci VZ, přičemž nyní dochází k jeho postupnému budování a získávání potřebných schopnosti pro naplnění úkolu.
C.9.03	**Zajištění vhodných prostor a nábor personálu pro NCKS.**	VZ	od Q4 2015 průběžně	**PLNĚNO** Kontinuálně probíhá zajišťování vhodných prostor a nábor personálu pro NCKS.
C.9.04	**Vybudování kompletní technické infrastruktury pro NCKS.**	VZ	od Q1 2016 průběžně	**PLNĚNO** Probíhá budování kompletní technické infrastruktury pro NCKS.
C.10.02	**Definovat soubor možných krizových situací a vytvářet krizové scénáře pro spolupráci, komunikaci a nasazení protiopatření v období krizových stavů.**	NBÚ/NCKB ve spolupráci s: MO VZ	od Q3 2015 průběžně	**PLNĚNO ČÁSTEČNĚ** Již v roce 2015 byly definovány prahy přechodů z normálního stavu do stavu kybernetického nebezpečí a byly zpracovány procesy jejich řešení. Aktuálně jsou krizové scénáře a situace procvičovány v rámci cvičení kybernetické bezpečnosti.
C.11.01	**Reflektovat v NCKB personální a znalostní nároky vyplývající z vývoje stavu kybernetické bezpečnosti ve světě a sdílet tyto své schopnosti a dovednosti s relevantními subjekty.**	NBÚ/NCKB	průběžně	**PLNĚNO** Mimo vzdělávání samotných pracovníků NBÚ/NCKB dochází kontinuálně i k předávání zkušeností a know-how relevantním partnerům a to jak mezinárodně (viz kód B.2.02), tak národně (zejména poskytováním metodické pomoci nebo organizováním či aktivní účastí pracovníků NCKB na odborných seminářích či konferencích).

Kód	Úkoly	Subjekt	Časový rámec	Plnění
C.11.02	**Reflektovat v NCKS personální a znalostní nároky vyplývající z vývoje stavu kybernetické obrany ve světě.**	VZ	průběžně	**PLNĚNO** VZ kontinuálně reflektuje v NCKS personální a znalostní nároky vyplývající z vývoje stavu kybernetické obrany ve světě.
C.12.01	**Zpracovat postup pro přechod mezi vyhlášeným stavem kybernetického nebezpečí dle zákona o kybernetické bezpečnosti a stavy dle ústavního zákona č. 110/1998 Sb., o bezpečnosti ČR.**	NBÚ/NCKB ve spolupráci s: MV MZV MO VZ ÚV ČR	Q1 2016	**SPLNĚNO** Postup pro přechod mezi vyhlášeným stavem kybernetického nebezpečí dle zákona o kybernetické bezpečnosti a stavy dle ústavního zákona č. 110/1998 Sb., o bezpečnosti ČR byl již zpracován a také procvičován na národní úrovni v rámci cvičení CMX.
D.1.01	**Navazovat kontakty a spolupráci se soukromým sektorem, a navyšovat tak povědomí o práci a možnostech spolupráce s NCKB prostřednictvím pravidelných jednání a vzájemného sdílení informací.**	NBÚ/NCKB	průběžně	**PLNĚNO** Předmětem spolupráce se soukromým sektorem v roce 2016 byla zejména účast na cvičeních kybernetické bezpečnosti či vzájemná účast na workshopech či jiných aktivitách jednotlivých subjektů. Mezi společností CISCO a NBÚ pak byla uzavřena na začátku roku dohoda o spolupráci v oblasti kybernetické bezpečnosti.
D.1.02	**Spolu s poskytovateli služeb elektronických komunikací a s poskytovateli služeb informační společnosti pracovat na shodném přístupu, jak lépe internetovým uživatelům v ČR pomoci rozpoznat a chránit se před škodlivými aktivitami v jejich systémech.**	NBÚ/NCKB	průběžně	**PLNĚNO** Pomocí webu a twitterového účtu dochází k informování veřejnosti o nejzásadnějších hrozbách a zranitelnostech. Zveřejnění zranitelností a hrozeb je v případě potřeby konzultováno s relevantními partnery.

Kód	Úkoly	Subjekt	Časový rámec	Plnění
D.2.01	**Spolupracovat se soukromoprávními subjekty KII při vytváření požadavků na bezpečnostní normy a povinné úrovně zabezpečení pro subjekty KII.**	NBÚ/NCKB	průběžně	**PLNĚNO** Návrhy a připomínky soukromoprávních subjektů byly v roce 2016 používány jako podklad pro novelizaci ZKB a jeho prováděcích právních předpisů, která bude provedena v souvislosti s nutností transpozice NIS směrnice do českého právního rámce (viz kapitola 3.2).
D.2.02	**Podporovat rozvoj norem v oblasti kybernetické bezpečnosti prostřednictvím národních a mezinárodní standardizačních a certifikačních orgánů a institucí a podporovat jejich přijetí u soukromých subjektů.**	NBÚ/NCKB	průběžně	**PLNĚNO** NBÚ/NCKB aktivně participuje v TNK UNMZ a prosazuje normy v oblasti kybernetické bezpečnosti na základě nejnovějších poznatků a praxe. Zároveň jsou propagovány existující standardy, zejm. normy řady ISO/IES 27000.
D.3.01	**Propagovat vysokou úroveň kybernetické bezpečnosti ve veřejných službách, a tím maximalizovat využívání systémů eGovernmentu ze strany soukromých organizací i široké veřejnosti.**	MPO MV	průběžně	**PLNĚNO** MV a MPO prosazují vysokou úroveň kybernetické bezpečnosti ve veřejných službách.
D.3.02	**Koordinovat přechod z protokolu IPv4 na IPv6 a informovat o bezpečnostních rizicích s tímto přechodem spjatých.**	MPO ve spolupráci s: MV	průběžně	**PLNĚNO** Relevantní subjekty průběžně pracují na zavádění protokolu IPv6. Úkol je průběžně plněn dle usnesení vlády ze dne 8. června 2009 č. 727 a ze dne 18. prosince 2013 č. 982.
D.3.03	**Podporovat rozšiřování DNSSEC pro zabezpečení webových prezentací a pravidelně monitorovat stav implementace DNSSEC jak ve veřejné správě, tak v národní doméně.cz**	MPO	průběžně	**PLNĚNO** MPO průběžně sleduje a podporuje zavádění DNSSEC ve státní správě. Úkol je průběžně plněn dle usnesení vlády ze dne 18. prosince 2013 č. 982.

Kód	Úkoly	Subjekt	Časový rámec	Plnění
D.4.01	**Poskytovat poradenství a organizovat vzdělávací a osvětové aktivity pro subjekty soukromé sféry**	NBÚ/NCKB	průběžně	**PLNĚNO** Osvěta a podpora vzdělávání v oblasti kybernetické bezpečnosti patří mezi hlavní oblasti činnosti NBÚ/NCKB. V roce 2016 NBÚ/NCKB navázalo na aktivity z předchozího roku, rozvinulo stávající spolupráci a připravilo nové projekty v této oblasti (viz kapitola 6).
D.4.02	**Podporovat malé a středně velké podniky prostřednictvím informační kampaně ohledně kybernetické bezpečnosti úzce zaměřené na potřeby a jejich možnosti.**	NBÚ/NCKB MPO	průběžně	**PLNĚNO** NBÚ i nadále informuje v této oblasti malé a středně velké podniky prostřednictvím svého webového portálu www.govcert.cz. Zároveň značná část standardů dostupných na tomto webovém portálu pro KII a VIS (nejrůznější podpůrné a metodické materiály zejména k problematice ISMS u KII a VIS) je použitelná i pro další subjekty, které nejsou povinnými subjekty dle ZKB. NBÚ/NCKB proto doporučuje i ostatním subjektům následovat prováděcí předpisy k ZKB, konkrétně tzv. "vyhlášku o kybernetické bezpečnosti" (vyhláška č. 316/2014 Sb.).
D.5.01	**Vytvořit mezi NCKB a subjekty KII a VIS platformu na sdílení informací o kybernetických hrozbách a zranitelnostech.**	NBÚ/NCKB	Q1 2016	**NESPLNĚNO** Neveřejná část webových stránek je téměř dokončena a k jejímu spuštění by mělo dojít na začátku roku 2017. Tato neveřejná část pak bude představovat platformu s kontrolou přístupu, která umožní sdílení informací ve větší míře směrem ke správcům systémů KII a VIS a také ke spolupracujícím bezpečnostním týmům. Bude se jednat zejména o informace, které není možné sdílet zcela veřejně, aby k nim nezískal přístup potenciální útočník.
E.3.01	**Iniciovat a podílet se na realizaci výzkumných projektů s partnery ze soukromé sféry**	NBÚ/NCKB	průběžně	**PLNĚNO** NBÚ/NCKB kontinuálně spolupracuje a podporuje výzkumné projekty s vybranými partnery ze soukromé sféry, kteří disponují prostředky na vědeckou a výzkumnou činnost.

Kód	Úkoly	Subjekt	Časový rámec	Plnění
E.4.01	**Spolupracovat s akademickou a soukromou sférou na výzkumných projektech, poskytovat jim potřebné informace a strategické vedení. Zapojit ČR a její akademickou i soukromou sféru do výzkumných programů (zahrnujících základní i aplikovaný výzkum a vývoj) na evropské i mezinárodní a transatlantické úrovni**	NBÚ/NCKB MŠMT	průběžně	**PLNĚNO** Již v roce 2015 byla zahrnuta oblast výzkumu a vývoje do dohod o spolupráci NBÚ. MŠMT pak poskytuje podporu na mezinárodní spolupráci ve výzkumu a vývoji, včetně spolupráce mezi akademickou a soukromou sférou. Tato podpora je poskytována na všechny vědní obory, mezi něž patří také oblast kybernetické bezpečnosti. Akademická i soukromá sféra jsou ze strany MŠMT pravidelně informovány o formách podpory a aktuálních výzvách k předkládání návrhů projektů, a to na webových stránkách MŠMT a na webových stránkách Národního kontaktního bodu ČR pro rámcové programy EU pro výzkum, vývoj a inovace (Technologického centra Akademie věd ČR) www.evropskyvyzkum.cz. Současně jsou potenciálním uchazečům o grantové projekty rámcových programů EU pro výzkum, vývoj a inovace poskytovány informačně a poradenské služby související s přípravou a řešením projektů (včetně právních a finančních aspektů).
E.4.02	**Podporovat a podílet se na publikační činnosti akademické sféry v oblasti kybernetické bezpečnosti.**	NBÚ/NCKB	průběžně	**PLNĚNO** Pracovníci NBÚ/NCKB publikovali v roce 2016 v několika periodicích. Dále pracovníci NBÚ/NCKB konzultovali několik diplomových prací a byla podporována publikační činnost vysokoškolských studentů.
F.1.01	**Podporovat iniciativy a osvětové kampaně, pořádat konference a workshopy pro veřejnost, respektive koncové uživatele.**	NBÚ/NCKB ve spolupráci s: MPSV	průběžně	**SPLNĚNO** NBÚ/NCKB kontinuálně podporuje iniciativy a osvětové kampaně, pořádá konference a workshopy pro veřejnost, respektive koncové uživatele (viz kapitola 6). Z hlediska MPSV lze zmínit středoškolská soutěž v kybernetické bezpečnosti (školní rok 2016/2017), kdy ministryně MPSV převzala záštitu nad soutěží a vedoucí oddělení bezpečnosti ICT se jako člen přípravného a soutěžního výboru aktivně podílí na realizaci. Na úrovni středních škol pak zároveň NBÚ/NCKB začalo spolupracovat při tvorbě pilotního oboru pro SŠ "Kybernetická bezpečnost". Obor bude vyučován na Smíchovské střední škole v Praze a Střední škole informatiky, poštovnictví a finančnictví v Brně.

Kód	Úkoly	Subjekt	Časový rámec	Plnění
F.1.02	**Provozovat a kontinuálně aktualizovat portál GovCERT.CZ jako informační platformu pro veřejnost ohledně aktuálních bezpečnostních hrozeb, rizik, zranitelností a dalších aktivit NBÚ.**	NBÚ/NCKB	průběžně	**PLNĚNO** V roce 2016 byla kontinuálně zajišťována aktuálnost zveřejněných informací na portálu www.govcert.cz. I nadále jsou získávány a kontinuálně doplňovány nové materiály a byla spuštěna nová verze veřejné části webových stránek sloužící jako informační portál širší a odborné veřejnosti.
F.1.03	**Vytvořit e-learningovou platformu pro vzdělávání širší a odborné veřejnosti.**	NBÚ/NCKB ve spolupráci s: MPSV	Q1 2016	**ČÁSTEČNĚ SPLNĚNO** E-learningová platforma byla v roce 2016 vytvořena. S ohledem na potřebu proškolení ústředních orgánů státní správy však byli v tomto roce prioritizování zaměstnanci veřejné správy před širší a odbornou veřejností.
F.2.05	**Zvyšovat povědomí ohledně zodpovědného, bezpečného používání internetu, ICT a nových médií.**	NBÚ/NCKB ve spolupráci s: MPSV	průběžně	**PLNĚNO** NBÚ/NCKB spolu s partnery dlouhodobě navyšují povědomí ohledně zodpovědného a bezpečného používání internetu, ICT a nových médií (viz kapitola 6).
F.2.06	**Podporovat u studentů rozvoj talentu v oblasti kybernetické bezpečnosti ve spolupráci s vysokými školami.**	NBÚ/NCKB	průběžně	**PLNĚNO** Spolupráce s vysokými školami zaměřená na vzdělávání v oblasti kyber bezpečnosti tvoří významnou složku činnosti NBÚ/NCKB. V roce 2016 došlo ke zmapování stavu možností vysokoškolského studia kybernetické bezpečnosti v ČR s cílem usnadnit orientaci uchazečům o studium tohoto oboru na vysoké škole. Aktuální přehled je dostupný na webových stránkách www.govcert.cz. Dále NBÚ/NCKB poskytuje stáže vysokoškolským studentům a možnost odborných konzultací. V neposlední řadě pracovníci NBÚ/NCKB vedli v roce 2016 několik diplomových prací.
F.2.07	**Zprostředkovávat vysokoškolským studentům možnost stáže v oblasti kybernetické bezpečnosti v ČR i zahraničí.**	NBÚ/NCKB MO	průběžně	**PLNĚNO** V uplynulém roce na NBÚ/NCKB absolvovalo stáž 7 studentů, kteří představovali technické, bezpečnostně politické i právní zaměření. Univerzita obrany pak zabezpečuje pro akreditované bakalářské studium ve studijním modulu „Kybernetická bezpečnost“ v oboru „Bezpečnostní management“ stáže v oblasti kybernetické bezpečnosti v ČR.

Kód	Úkoly	Subjekt	Časový rámec	Plnění
F.2.08	**Spolupracovat na vytváření nových vysokoškolských studijních oborů v oblasti kybernetické bezpečnosti a kybernetické obrany a spolupracovat s univerzitami a vysokými školami při zavádění těchto nových oborů, tvorbě učebních plánů apod.**	NBÚ/NCKB MO	průběžně	**PLNĚNO** NBÚ i MO kontinuálně spolupracují s univerzitami a vysokými školami a podporují vytváření nových vysokoškolských studijních oborů v oblasti kybernetické bezpečnosti a kybernetické obrany.
F.3.01	**Školit stávající zaměstnance veřejné správy v oblasti kybernetické bezpečnosti.**	NBÚ/NCKB MPSV MV	Od Q4 2015 průběžně	**PLNĚNO** NBÚ/NCKB provedlo v roce 2016 řadu školení pro zaměstnance veřejné správy týkajících se pravidel bezpečného využívání ICT technologií v zaměstnání a v soukromí (viz kapitola 6.2).
F.3.02	**Školit manažery kybernetické bezpečnosti ve veřejné správě ve věci rozpoznávání, (např. detekování anomálií), hlášení kybernetických bezpečnostních incidentů a další spolupráce s NCKB.**	NBÚ/NCKB MPSV	průběžně	**PLNĚNO** V oblasti školení manažerů ve veřejné správě lze zmínit např. dvoudenní školení s názvem „Kybernetická bezpečnost v organizacích“, které pravidelně vyučují pracovníci NBÚ/NCKB. Cílovou skupinou zde jsou manažeři IT bezpečnosti, manažeři kybernetické bezpečnosti, IT administrátoři, bezpečnostní architekti, implementátoři ISMS a další role vyplývající ze ZKB.
F.3.03	**Institucionalizovat další vzdělávání prostřednictvím získávání osvědčení za absolvování vzdělávacích programů.**	NBÚ/NCKB MPSV MV	průběžně	**PLNĚNO** V roce 2016 relevantní subjekty podporovaly institucionalizaci dalšího vzdělávání prostřednictvím získávání osvědčení za absolvování vzdělávacích programů.

Kód	Úkoly	Subjekt	Časový rámec	Plnění
F.3.04	**Pomocí moderních výukových metod zvyšovat úroveň vzdělanosti v oblasti kybernetické bezpečnosti.**	NBÚ/NCKB MPSV	průběžně	**PLNĚNO** NBÚ/NCKB již druhým rokem vedlo samostatně dva vysokoškolské předměty o kybernetické bezpečnosti na Masarykově univerzitě v Brně a Univerzitě Palackého v Olomouci. Ve spolupráci se studenty Pedagogické fakulty Masarykovy univerzity proběhla pilotní fáze interaktivního vzdělávacího modulu "Digitální stopa" (viz kapitola 6.9) a také bylo NBÚ/NCKB uspořádáno mnoho osvětových akcí, konferencí, apod. (viz kapitola 6).
G.1.01	**Personálně posílit pracoviště informační kriminality Policejního prezidia ČR o systemizovaná služební místa a systemizovaná pracovní místa, která budou sanovat stávající krizový stav a dále nyní naplní nezbytný lidský potenciál pro plnění vyžadovaných a stanovených činností.**	Policie ČR MV	do 2018	**PLNĚNO** Pracoviště informační kriminality bylo v rámci organizačních změn v roce 2016 přesunuto pod nově vzniklou sekci kybernetické kriminality Národní centrály proti organizovanému zločinu SKPV. Zde je odbor nově pojmenován jako odbor kybernetické kriminality a převzal veškeré činnosti předchozího pracoviště OIK. V roce 2016 bylo posíleno nově přidělenými služebními místy a cílového stavu bude dle předpokladů dosaženo v roce 2018. Mimo toto původní pracoviště byl v roce 2016 vytvořen nový odbor vyšetřování kybernetické kriminality, který se dělí na 3 oddělení. Tento odbor, který je rovněž samostatné personálně posilován, je zaměřen zejména na plnění úkolů policejního orgánu při vedení samostatného trestního řízení ve věcech nejzávažnějších projevů kybernetické kriminality – kybernetických útoků, které mají povahu kybernetického bezpečnostního incidentu, oznámených NBÚ. V této souvislosti úzce spolupracuje s pracovištěm NCKB při NBÚ. Existencí těchto dvou pracovišť je pokryta jak metodická, tak i výkonná činnost v oblasti kybernetické kriminality, na centrální úrovni. Definitivní vyřešení personálního posílení v letech 2017 a 2018, dalšího financování problematiky a s tím spojeného dodržení termínu realizace opatření je závislé na schválení příslušných finančních prostředků Vládou ČR.

Kód	Úkoly	Subjekt	Časový rámec	Plnění
G.1.02	**Personálně posílit o systemizovaná služební místa, ÚOOZ SKPV, ÚOKFK SKPV a NPC SKPV s ohledem na vyšetřování návazné trestné činnosti související s informační kriminalitou, včetně oblasti boje s terorismem zasahujícím i prostředí informačních technologií.**	Policie ČR MV	do 2018	**PLNĚNO** Součásti ÚOOZ a ÚOKFK SKPV byly v roce 2016 sloučeny do Národní centrály proti organizovanému zločinu SKPV, v rámci níž byla zřízena sekce kybernetické kriminality, která je postupně personálně posilována k cílovému personálnímu stavu v roce 2018. Personální posílení Národní protidrogové centrály SKPV není součástí přidělené kvóty tabulkových míst pro problematiku kybernetické kriminality, obsažené v materiálu Koncepce rozvoje schopností Policie ČR vyšetřovat kybernetickou kriminalitu. Tato místa budou rozdělována výhradně mezi NCOZ SKPV, KŘP, KÚP a ÚZČ. Národní protidrogová centrála SKPV bude personálně posilována v rámci samostatných, materiálem Koncepce rozvoje Policie ČR do roku 2020, této součásti vyhrazených, tabulkových míst. Definitivní vyřešení personálního posílení v letech 2017 a 2018, dalšího financování problematiky a s tím spojeného dodržení termínu realizace opatření je závislé na schválení příslušných finančních prostředků Vládou ČR.

Kód	Úkoly	Subjekt	Časový rámec	Plnění
G.1.03	**Personálně posílit jednotlivá regionální výkonná pracoviště SKPV určených pro informační kriminalitu o systemizovaná služební místa a systemizovaná služební místa v jednotlivých krajích. Tímto se sleduje reakce na lokální situaci v rámci regionálních součástí SKPV dle modelu respektujícího rozdělení na technický, operativní a procesní aspekt zastoupení na příslušném pracovišti informační kriminality, zajištěním dostatečné sanace stávajícího stavu, pokrytí vedení odborně náročného trestního řízení a zajištění akceschopnosti.**	Policie ČR MV	do 2018	**PLNĚNO** Výkonná pracoviště krajských pracovišť kybernetické kriminality jsou postupně posilována směrem k cílovému stavu v roce 2018. Pracoviště byla vytvořena na všech 14 KŘP, v rámci odborů analytiky. V další fázi je plánováno povinné vytvoření pracovišť kybernetické kriminality na úrovni územních pracovišť – územních odborů. Tímto bude zajištěno plné pokrytí regionů až k nejnižším článkům služby kriminální policie a vyšetřování. Články kybernetické kriminality KŘP a jejich personální posilování je součástí koncepčního řešení rozvoje schopností Policie ČR vyšetřovat kybernetickou kriminalitu. Připravován je rovněž společný komplexní systém financování těchto součástí – na základě principu periodické obnovy materiálně technického zabezpečení. Doposud byla rozdělena tabulková místa vyhrazená pro rok 2016. Definitivní vyřešení personálního posílení v letech 2017 a 2018, dalšího financování problematiky a s tím spojeného dodržení termínu realizace opatření, je závislé na schválení příslušných finančních prostředků Vládou ČR.
G.1.04	**Personálně posílit infastrukturu regionálních znaleckých pracovišť PČR o systemizovaná služební místa. Kriminalistický ústav Praha v souvislosti s jeho republikovou působností posílit o systemizovaná služební místa, která budou sanovat stávající nesoulad poměru zajišťované činnosti a personálních kapacit.**	Policie ČR MV	do 2018	**PLNĚNO** Znalecká pracoviště jsou postupně personálně posilována směrem k cílovému stavu v roce 2018, přičemž doposud bylo provedeno přidělení míst z kvóty pro rok 2016. Tabulková místa pro Kriminalisticky ústav Praha jsou součástí koncepčního řešení rozvoje schopností Policie ČR vyšetřovat kybernetickou kriminalitu. KÚP je rovněž součástí připravovaného společného komplexního systému financování – na základě principu periodické obnovy materiálně technického zabezpečení bude této součásti vyhrazena samostatná částka. Definitivní vyřešení personálního posílení v letech 2017 a 2018, dalšího financování problematiky a s tím spojeného dodržení termínu realizace opatření je závislé na schválení příslušných finančních prostředků Vládou ČR.

Kód	Úkoly	Subjekt	Časový rámec	Plnění
G.1.05	**Personálně posílit ÚZČ SKPV v oblasti programování o systemizovaná služební místa, v oblasti technické správy systémů o systemizovaná služební místa, která budou zajišťovat přijímání, zpracování a vyřizování rostoucích požadavků a zejména objemu dat charakteru provozních a lokalizačních údajů sítě Internet**	Policie ČR MV	do 2018	**PLNĚNO** Útvar zvláštních činností SKPV je postupně posilován tabulkovými místy pro problematiku kybernetické kriminality, směrem k cílovému stavu v roce 2018, přičemž doposud bylo provedeno přidělení míst z kvóty pro rok 2016. Tabulková místa pro Útvar zvláštních činností jsou součástí koncepčního řešení rozvoje schopností Policie ČR vyšetřovat kybernetickou kriminalitu. Definitivní vyřešení personálního posílení v letech 2017 a 2018, dalšího financování problematiky a s tím spojeného dodržení termínu realizace opatření je závislé na schválení příslušných finančních prostředků Vládou ČR.
G.1.06	**Personálně posílit o systemizovaná služební místa ÚSČ SKPV pro podporu speciálních činností v souvislosti s penetrací informačních technologií i do oblastí zajišťování úkonů souvisejících s vyšetřováním trestné činnosti**	Policie ČR MV	do 2018	**PLNĚNO** Útvar speciálních činností SKPV již v roce 2016 vyčlenil z vnitřních zdrojů několik systemizovaných služebních míst pro podporu vyšetřování kybernetické kriminality. Avšak stalo se tak na úkor ostatních činností tohoto útvaru.

Kód	Úkoly	Subjekt	Časový rámec	Plnění
G.1.07	**Personálně posílit technologickou správu dat a informační podporu zabezpečovanou pracovišti informatiky a provozu informačních technologií.**	Policie ČR MV	do 2018	**PROZATÍM NESPLNĚNO** Personální posílení součástí zabývajících se technologickou správou dat a informační podporou není součástí přidělené kvóty tabulkových míst pro problematiku kybernetické kriminality, obsažené v materiálu Koncepce rozvoje schopností Policie ČR vyšetřovat kybernetickou kriminalitu. Tyto budou rozdělovány výhradně mezi NCOZ SKPV, KŘP, KÚP a ÚZČ. V případě schválení personálních a finančních požadavků obsažených v materiálu Koncepce rozvoje Policie ČR do roku 2020 Vládou ČR, je možný předpoklad přidělení tabulkových míst i do těchto součástí. V takovém případě bude možné dodržet i termín v roce 2018.
G.2.01	**Nastavit povinnou a vynutitelnou minimální technologickou vybavenost všech pracovišť OIK SKPV a zajistit stanovenou techniku a technologie.**	Policie ČR MV	do 2018	**PLNĚNO** V rámci připravovaných nákupů materiálně technického vybavení jednotlivých pracovišť jsou vytvářeny standardy vybavenosti jednotlivých pracovišť, dle úrovně a specializace. Vzhledem ke skutečnosti, že rovněž čerpání prostředků na pořízení technického vybavení, softwaru a souvisejícího školení z evropských fondů, které by mělo být realizováno v roce 2017, je připravováno na centrální úrovni, je již i tímto postupně nastavena a zajištěna jednotnost technologického vybavení pracovišť. V rámci připravovaného systému periodické obnovy bude rovněž kladen důraz na dodržování standardů vybavenosti a to jak u policistů problematiky, tak i pracovišť samotných. Definitivní nastavení standardů a systému pořizování technologického vybavení do roku 2020 je závislé na schválení příslušných finančních prostředků Vládou ČR. V případě přidělení finančních prostředků bude opatření realizováno v termínu.

Kód	Úkoly	Subjekt	Časový rámec	Plnění
G.2.02	**Nastavit povinnou a vynutitelnou minimální technologickou vybavenost všech znaleckých pracovišť tzv. počítačové analýzy a zajistit stanovenou techniku a technologie.**	Policie ČR MV	do 2018	**PLNĚNO** V rámci připravovaných nákupů materiálně technického vybavení jsou rovněž pro znalecká pracoviště vytvářeny předpokládané standardy vybavenosti. Vzhledem ke skutečnosti, že rovněž čerpání prostředků na pořízení technického vybavení, softwaru a souvisejícího školení z evropských fondů, které by mělo být realizováno v roce 2017, je připravováno na centrální úrovni, je již i tímto postupně nastavena a zajištěna jednotnost technologického vybavení znaleckých pracovišť. V rámci připravovaného systému periodické obnovy bude KÚP jako expertnímu pracovišti vyhrazena samostatná částka pro pořizování materiálně technického vybavení. KÚP bude garantem příslušných standardů i pro regionální znalecká pracoviště. Definitivní nastavení standardů a systému pořizování technologického vybavení do roku 2020 je závislé na schválení příslušných finančních prostředků Vládou ČR. V případě přidělení finančních prostředků bude opatření realizováno v termínu.
G.2.03	**Společně plánovat jednotlivé nákupy pro výkonná pracoviště OIK a znalecká pracoviště počítačové analýzy s garancí vázanosti plánovaných prostředků v plánovaných rozpočtech pro další údobí.**	Policie ČR MV	do 2018	**PLNĚNO** Opatření souvisí s opatřeními G.2.01 a G.2.02. Pro výkonná i znalecká pracoviště je v současné době plánován společný nákup materiálně technického vybavení, v rámci čerpání evropských fondů. Obdobným způsobem bude postupováno i při pořizování majetku při budoucích nákupech z běžných rozpočtových prostředků. V tomto smyslu bude nastaven standardizovaný systém periodické obnovy. V rámci materiálu Koncepce rozvoje schopností Policie ČR vyšetřovat kybernetikou kriminalitu jsou stanoveny předpokládané vázané rozpočtové prostředky, které by měly být alokovány pro útvary linie kybernetické kriminality. Definitivní nastavení systému a plánování finančních prostředků je závislé na schválení nákladů Vládou ČR. V případě přidělení finančních prostředků bude opatření realizováno v termínu.

Kód	Úkoly	Subjekt	Časový rámec	Plnění
G.2.04	**Postupně realizovat vzájemnou blízkost dislokací výkonných a znaleckých pracovišť SKPV na jednotlivých úrovních v závislosti na vývoji stávajících dislokací.**	Policie ČR MV	do 2018	**PRŮBĚŽNĚ PLNĚNO** Uvedené opatření bude spojeno se zvýšenými náklady na pořízení nemovitostí, případně výstavbu nových. Případný přesun KÚP do stejné lokality jako je sídlo NCOZ SKPV a tedy i sekce kybernetické kriminality je v současné době ve fázi záměrů a příprav. Alespoň na úrovni centrálního výkonného pracoviště bylo realizováno sestěhování obou odborů (OKK a OVKK) do stejné lokality a budovy. Předpoklad realizace je spíše kolem po roce 2020.
G.3.01	**Vytvořit smluvní či obdobné vazby umožňující a garantující přímou a časově nejrychlejší spolupráci na prováděcí úrovni s bezpečnostními složkami BIS, ÚZSI a VZ a s prvky kritické infrastruktury, NCKB, GovCERT.CZ a národním CERT.**	Policie ČR MV ve spolupráci s: Vojenská policie	Q3 2016	**PLNĚNO** Realizace uvedeného opatření byla zpožděna v souvislosti s organizačními změnami u centrálního pracoviště sekce kybernetické kriminality, ke kterým došlo zejména v roce 2016. Ve finální fázi je uzavření memoranda mezi Policií ČR a Vojenským zpravodajstvím. V závěrečné fázi je rovněž smluvní ukotvení vztahů s provozovatelem národního CERTu sdružením CZ.NIC. V dalším období bude intenzivně pracováno na uzavření smluvních vztahů s dalšími partnery tak, aby uskutečnění tohoto opatření bylo uzavřeno nejpozději do konce roku 2017.
G.4.01	**Spolupracovat se zahraničními subjekty v oblasti výměny informací k informační kriminalitě a v oblasti vzdělávání.**	Policie ČR MV ve spolupráci s: Vojenská policie	průběžně	**PLNĚNO** Opatření je průběžně realizováno v plné míře. Pracovníci sekce kybernetické kriminality se účastní jednání v rámci struktur EUROPOLu, kde si vyměňují zkušenosti se zahraničními partnery. Účastní se rovněž zahraničních vzdělávacích kurzů. Se zahraničními partnery je spolupracováno rovněž v České republice, např. při účasti na vzdělávacím kurzu FBI ke kybernetické kriminalitě. Zkušenosti budou s partnery vyměňovány, v rozšířené míře, i v dalším období. Plánováno je pozvání specialistů z Německa, Rakouska, Slovenska a dalších, kteří by měli poskytnout své znalosti a zkušenosti v rámci některého z instrukčně metodických zaměstnání sekce kybernetické kriminality.

Kód	Úkoly	Subjekt	Časový rámec	Plnění
G.5.01	**Rozšířit kurzy kvalifikační přípravy o základní znalosti a dovednosti spojené s kriminalitou páchanou v prostředí informačních technologií a zavést elektronický nebo obdobně plošně nasaditelný systém průběžného vzdělávání.**	Policie ČR MV	průběžně, do Q2 2017	**PROZATÍM NEPLNĚNO** Realizace opatření je v počáteční fázi. V současné době je intenzivně pracováno na obsahovém rámci rozšíření základní odborné přípravy nově nastupujících policistů. Byly vydefinovány základní okruhy znalostí, kterými by měl každý policista disponovat a v současné době je připravován projektový záměr financování uvedeného rozšíření – bude spojeno se zvýšenými náklady na patřičné lektory, učební pomůcky a další. V této fázi bude realizována rovněž adekvátní forma proškolení již sloužících policistů – např. formou e-learningu. Předpoklad konečné realizace je spíše v roce 2018.
G.5.02	**Rozšířit specializační kurzy pro policisty SKPV o vyšší znalosti a dovednosti spojené s kriminalitou páchanou v prostředí informačních technologií.**	Policie ČR MV	průběžně, do Q2 2017	**PROZATÍM NEPLNĚNO** Realizace opatření je v počáteční fázi. V současné době je rovněž v tomto opatření intenzivně pracováno na obsahovém rámci rozšíření specializačních kurzů pro policisty nově nastoupivší na linii SKPV. Byly vydefinovány základní okruhy znalostí, kterými by měl každý policista SKPV disponovat a v současné době je připravován projektový záměr financování uvedeného rozšíření – bude spojeno se zvýšenými náklady na patřičné lektory, učební pomůcky a další. V této fázi bude realizována rovněž adekvátní forma proškolení již sloužících policistů SKPV – např. formou e-learningu. Předpoklad konečné realizace je spíše v roce 2018.

Kód	Úkoly	Subjekt	Časový rámec	Plnění
G.5.03	**Připravit odborné kurzy policejních specialistů na kriminalitu páchanou v prostředí informačních technologií.**	Policie ČR MV	průběžně, do Q2 2017	**PLNĚNO** V současné době je již plně realizován standardizovaný kurz zajišťování výpočetní techniky a dat pro specialisty systemizované na problematice kybernetické kriminality. V další fázi je připravován specializační kurz pro nově nastoupivší policisty do linie kyber. Tento kurz je součástí balíku opatření souvisejícího s opatřeními G.5.01, G.5.02 a rovněž G.5.04. Byly vydefinovány okruhy znalostí, kterými by měl každý policista problematiky kybernetické kriminality disponovat a v současné době je připravován projektový záměr financování uvedeného kurzu – bude spojeno se zvýšenými náklady na patřičné lektory, učební pomůcky a další. Další případné odborné kurzy i u mimorezortních partnerů, bude možno realizovat až po schválení finančních prostředků, definovaných Koncepcí rozvoje schopností Policie ČR vyšetřovat kybernetickou kriminalitu, Vládou ČR. Předpoklad konečné realizace je spíše v roce 2018.
G.5.04	**Vytvořit podmínky pro průběžné vzdělávání expertů PČR v oblasti informační kriminality v komerčním a akademickém prostředí.**	Policie ČR MV	průběžně, do Q2 2017	**PROZATÍM NEPLNĚNO** Opatření bude spojeno s vyššími náklady než u opatření G.5.01, G.5.02, G.5.03. Mimo společný balík ke všem uvedeným opatřením, v rámci kterého je připravován projektový záměr na 4 fázový systém vzdělávání, bude nutno rovněž financovat expertní kurzy v akademickém prostředí, ale zejména v komerčním prostředí. V některých případech bude realizován příjezd zahraničních expertů do ČR, případně budou tento typ vzdělávání realizován přímo v zahraničí. Definitivní realizace opatření je tak možná až po schválení finančních prostředků, definovaných Koncepcí rozvoje schopností Policie ČR vyšetřovat kybernetickou kriminalitu, Vládou ČR. Předpoklad konečné realizace je spíše v roce 2018.

Kód	Úkoly	Subjekt	Časový rámec	Plnění
G.5.05	**5 Kapacitně posílit a rozšířit podmínky pro jazykové studium specialistů ve formě všeobecné jazykové přípravy, odborné jazykové přípravy a zdokonalovacích kurzů a souběžně zohlednit další nábory s preferencí jazykové vybavenosti.**	Policie ČR MV	průběžně, do Q2 2017	**PLNĚNO** Všem specialistům problematiky kybernetické kriminality je, při respektování zájmů služby, umožněno účastnit se jazykových kurzů organizovaných rezortními zařízeními. Případné mimorezortní vzdělávací jazykové kurzy, zaměřené i na odborné jazykové znalosti, bude možné realizovat v případě přidělení patřičných finančních prostředků, definovaných Koncepcí rozvoje schopností Policie ČR vyšetřovat kybernetickou kriminalitu, Vládou ČR. Při náboru nových policistů je zohledňováno rovněž hledisko jazykové vybavenosti a případná ochota dalšího vzdělávání. V případě naplnění finančních požadavků bude dodržen termín realizace v roce 2017.
G.6.01	**Vybudovat multidisciplinární formalizované akademické prostředí rozvoje schopnosti bezpečnostních složek a zejména PČR postihovat informační kriminalitu a řešit s tím spojené bezpečnostní, standardizační, normotvorné, výzkumné a další provázané potřeby.**	Policie ČR MV	průběžně do roku 2018	**PROZATÍM NEPLNĚNO** V současné době je realizace tohoto opatření ve fázi přípravy. Určitou formu jeho naplnění představuje pravidelný workshop pořádaný Policejní akademií ČR k otázkám kybernetické kriminality, kde se setkávají specialisté z regionální i národní úrovně se zástupci akademického i komerčního prostředí a rovněž se zástupci justice. Tento se může stát základem budoucí širší platformy – mozkového trustu, kam by byly pravidelně zváni odborníci z dalších univerzit, soukromých IT společností a dalšího okruhu odborníků. Opatření je možno realizovat v termínu.

Kód	Úkoly	Subjekt	Časový rámec	Plnění
H.1.01	**Vytvářet v oblasti kybernetické bezpečnosti srozumitelné, efektivní a proporcionální zákonné a podzákonné právo.**	NBÚ/NCKB ve spolupráci s: MZV	průběžně	**PLNĚNO** NBÚ/NCKB v roce 2016 vytvořil dokument Bílá místa kybernetické bezpečnosti České republiky, jehož cílem bylo informovat o problémech, které byly zjištěny v prvním roce účinnosti ZKB. Tento materiál byl schválen usnesením vlády ČR ze dne 24. srpna 2016 č. 725. S nutností transpozice evropské směrnice NIS pak byla připravena transpoziční novela ZKB, která některé identifikované problémy reflektuje a řeší. Návrh novely vláda schválila dne 23. listopadu 2016 a dále byl postoupen k dalšímu projednání Poslanecké sněmovně Parlamentu ČR. Nová právní úprava by měla vejít v účinnost v roce 2017. Na národní úrovni lze také zmínit i návrh zákona, kterým se mění zákon č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů, který mění i ZKB s cílem zajistit dostatečnou úroveň úpravy vztahů mezi správci KII a VIS na straně jedné a dodavateli a subdodavateli ICT služeb na straně druhé.
H.1.02	**Analyzovat nezbytné zákonné regulace pro účinné zajištění kybernetické bezpečnosti v ČR.**	NBÚ/NCKB ve spolupráci s: MZV	průběžně	**PLNĚNO** Viz bod H.1.01.
H.2.01	**Kontinuálně se podílet na vývoji a implementaci evropského a mezinárodního právního rámce a pravidel v oblasti kybernetické bezpečnosti**	NBÚ/NCKB MZV	průběžně	**PLNĚNO** ČR se průběžně podílí na vývoji a implementaci evropského a mezinárodního právního rámce a pravidel v oblasti kybernetické bezpečnosti. Hlavním počinem v tomto ohledu byla příprava transpozice evropské směrnice NIS do českého právního rámce, konzultace k tzv. Tallinnskému manuálu 2.0 a v neposlední řadě i přijetí a implementace druhé sady CBMs členskými státy OBSE.

Kód	Úkoly	Subjekt	Časový rámec	Plnění
H.2.02	**Účastnit se diskuzí nad pojetím a významem konceptů kybernetické bezpečnosti a kybernetické obrany.**	NBÚ/NCKB MZV MO MV Zpravodajské služby	průběžně	**PLNĚNO** Zodpovědní aktéři se účastnili mnoha formálních i neformálních jednání, konferencí, seminářů a workshopů ohledně problematiky konceptů kybernetické bezpečnosti a kybernetické obrany. Diskuze probíhala v různých formátech s relevantními národními i zahraničními partnery. Konkrétně lze zmínit např. konzultace k tzv. Tallinnskému manuálu 2.0.
H.3.01	**Na základě průběžné analýzy efektivity účinné právní úpravy a jejího souladu s aktuálními poznatky z dotčených technických a společenskovědních oborů provádět příslušné změny a doplňování.**	NBÚ/NCKB	průběžně	**PLNĚNO** Viz bod H.1.01.
H.3.02	**Nastavovat povinnou úroveň zabezpečení pro subjekty KII pomocí aktualizace zákonného a podzákonného práva.**	NBÚ/NCKB	průběžně	**PLNĚNO** Viz bod H.1.01.
H.3.03	**Provést revizi a vytvořit návrh legislativních změn vybraných paragrafů trestního zákoníku a zákona o elektronických komunikacích, které by zefektivnily vyšetřování a postihování informační kriminality a reflektovaly aktuální situaci v problematice informační kriminality.**	MV Policie ČR ČTÚ ve spolupráci s: Zpravodajské služby	Q1 2016	**NESPLNĚNO** Realizace uvedeného opatření byla zpožděna v souvislosti s organizačními změnami u centrálního pracoviště sekce kybernetické kriminality, ke kterým došlo v roce 2016. V současné době je ve spolupráci s MV, které je hlavním garantem tohoto opatření, projednávána možná změna zákona o elektronických komunikacích. Připraveny jsou rovněž návrhy změn trestního řádu a zákona o mezinárodní justiční spolupráci ve věcech trestních – ve vztahu k zajišťování elektronických důkazů. Alespoň částečná realizace opatření bude možná, v závislosti na legislativním procesu, nejdříve v roce 2018.

Kód	Úkoly	Subjekt	Časový rámec	Plnění
H.4.01	**Pomocí vzdělávání soudců a státních zástupců ohledně kybernetické problematiky zajistit ukládání a vymáhání přiměřených sankcí v trestněprávních sporech, které zahrnují kybernetickou problematiku.**	NBÚ/NCKB MS MV Policie ČR	průběžně	**PLNĚNO** ČR aktivně vzdělává soudce a státní zástupce v oblasti kybernetické bezpečnosti a kybernetické kriminality. Justiční akademie uskutečnila v roce 2016 mnoho vzdělávacích aktivit ohledně této problematiky: kybernetické útoky a bezpečnost; sexuální zneužívání dětí a dětská pornografie prostřednictvím internetu; internetové podvody související s platebními kartami a trestná činnost z nenávisti a projevy na internetu, extremismus, terorismus a in a další. Konkrétně lze zmínit semináře na téma: Trestná činnost z nenávisti, Trestné činy proti lidské důstojnosti v sexuální oblasti, Ochrana autorských práv, Drogová problematika, Internetová kriminalita, Organizovaný násilný extremismus; trestná činnost z nenávisti; Terorismus, ve kterých byla vždy zahrnuta "kyber" problematika. Policie ČR se pak v rámci své činnosti snaží kontinuálně spolupodílet na průběžném vzdělávání zejména státních zástupců. Realizována jsou společná školení v rámci instrukčně metodických zaměstnání pro policisty problematiky kybernetické kriminality, kam jsou zváni rovněž zástupci justice, kteří jsou určeni jako specialisté pro "kyber". Státní zástupci a soudci budou zváni k účasti i na dalších případných odborných kurzech a školeních.

Kód	Nedokončené úkoly z roku 2015	Subjekt	Časový rámec	Plnění
C.3.04	**Určit minimální požadavky pro logy, které musí být zajištěny pro spolehlivou ex-post analýzu kybernetických bezpečnostních incidentů.**	NBÚ/NCKB	Q4 2015	**SPLNĚNO** Minimální požadavky pro logy, které musí být zajištěny pro spolehlivou ex-post analýzu kybernetických bezpečnostních incidentů jsou dostupné na webových stránkách www.govcert.cz.
C.5.02	**Vytvořit na základě dokončení mapování zabezpečovacích prvků u KII a VIS automatizovanou platformu na sdílení informací o kybernetických bezpečnostních hrozbách a incidentech vybraným ohroženým subjektům.**	NBÚ/NCKB	Q4 2015	**SPLNĚNO ČÁSTEČNĚ** Neveřejná část webových stránek, která bude fungovat jako automatizovaná platforma na sdílení tohoto typu informací mezi subjekty je téměř dokončena a k jejímu předání a spuštění by mělo dojít na začátku roku 2017 (viz bod D.5.01).
C.5.04	**Vytvořit na národní úrovni zabezpečenou platformu pro komunikaci při řešení rozsáhlejších kybernetických bezpečnostních incidentů.**	NBÚ/NCKB	Q4 2015	**SPLNĚNO ČÁSTEČNĚ** Úkol je realizován skrze projekt videokonferenčního systému mezi relevantními subjekty kybernetické bezpečnosti ČR. Tento projekt se na konci roku 2016 nacházel v poslední fázi testování a do poloviny roku 2017 bude již plně funkční.
F.2.04	**Vytvořit přehled vysokoškolských studijních programů v ČR i zahraničí zabývajících se kybernetickou bezpečností, průběžně jej aktualizovat a tento přehled v rámci propagace zveřejňovat.**	NBÚ/NCKB	Q4 2015	**SPLNĚNO** Přehled vysokoškolských studijních programů v ČR i zahraničí zabývajících se kybernetickou bezpečnostní je dostupný a průběžně aktualizovaný na webovém portálu www.govcert.cz.