

**Implementační akční plán
Technologické platformy
„Energetická bezpečnost ČR“**

Obsah

1. Fáze (2012-2014)	4
1.1. Vhodné doplnění členské základny o vybrané subjekty pro realizaci klíčových aktivit TPEB 4	
1.2. Vytvoření vazeb na národní a mezinárodní organizace a spolupráce s nimi.....	4
1.3. Podpora VaVaI ve vybraných technologických oblastech	6
1.3.1. Iniciace VaVaI projektů v národních programech	6
1.3.2. Iniciace VaVaI projektů v mezinárodních programech	10
2. Fáze (2015+)	12
2.1. Cílená podpora VaVaI v oblasti klíčových technologií.....	12
2.2. Cílená podpora aktivit v oblasti tvorby bezpečnostní legislativy a standardů	13
2.3. Oblast propagace a vzdělávání	14

Implementační akční plán slouží k naplnění cílů Strategické výzkumné agendy Technologické platformy „Energetické bezpečnost ČR“.

IAP TPEB je konkrétně zaměřený na podporu technologického růstu bezpečnostního průmyslu v ČR úzce provázaný na podobné konkrétní aktivity v EU. Jde o první komplexní přístup a řešení od výzkumu a vývoje až do fáze normalizace a certifikace, standardizace a legislativní praxe.

Obsah IAP je rozdělen do dvou tematických celků popisujících vždy nejbližší dvou až tříleté období a předpokládané aktivity v následujícím střednědobém až dlouhodobém horizontu.

Dokument vychází ze Strategické výzkumné agendy a v návaznosti na její aktualizace bude probíhat také aktualizace IAP. Aktualizace jsou plánovány vždy v posledním roce krátkodobé fáze tak, aby bylo možno provést její vyhodnocení a zároveň upřesnit aktivity na nejbližší období. Na řešení a zpracování IAP se podílí tým zkušených odborníků z řad členů TPEB a spolupracujících subjektů.

Záměrem IAP v daném období je zajistit:

- Změny v členské základně umožňující splnění stanovených cílů
- Vytvoření konsorcií z řad členů za účelem řešení projektů VaVaI
- Podíl TPEB na přípravě a implementaci národních i mezinárodních dokumentů řešících problematiku energetické a kybernetické bezpečnosti

TPEB je přesvědčena, že opatření uvedená v tomto akčním plánu výrazně přispějí ke zlepšení konkurenceschopnosti českého i evropského bezpečnostního průmyslu. Cílem TPEB je zajistit, aby odvětví bezpečnosti v ČR a v EU mělo silnou domovskou základnu, ze které, budeme schopni expandovat do nových a rozvíjejících se trhů.,

Ochrana osobních údajů v tomto návrhu a dodržování základních práv musí být začleněna jako klíčový aspekt do všech bezpečnostních technologií v ČR a v EU.

1. Fáze (2012-2014)

1.1. Vhodné doplnění členské základny o vybrané subjekty pro realizaci klíčových aktivit TPEB

Cílem této aktivity je pružná obměna nebo doplnění členské základny v souladu s technologickými cíli. V tomto období bude činnost managementu TPEB zaměřena na získání členů z oblasti:

- Energetických subjektů (státních i privátních)
- Kooperujících subjektů zaměřených na technologie sledování prvků kritické infrastruktury
- Výzkumných a akademických pracovišť

1.2. Vytvoření vazeb na národní a mezinárodní organizace a spolupráce s nimi

Implementační akční plán bude naplňován v souladu s politikami EU. Ve smyslu sdělení EK k bezpečnostní průmyslové politice bude v ČR vytvářena silná strategická technologická základna pro bezpečnostní průmysl a realizaci jeho plánovaných výstupů. Jedná se zejména o tyto oblasti:

Standardizace

Standardy hrají zásadní roli ve fragmentovaném trhu a jejich zavedení a používání stimuluje ekonomický růst. Standardy mají rovněž důležitou úlohu při zajištění interoperability a vymáhání práva příslušnými orgány. Navíc standardy jsou naprosto zásadní pro zajištění jednotné úrovně kvality a jakosti pro bezpečnostní technologie

Připojení se k procesu vytváření evropských standardů a zapojení se do procesu jejich prosazování na světové úrovni je klíčovou formou podpory konkurenceschopnosti evropského bezpečnostního průmyslu.

Jedná se zejména o oblast ochrany kritické infrastruktury, energetiky a související kybernetiky se zaměřením na krizové řízení, komunikační interoperabilitu.

TPEB bude v souladu se zmíněnými prioritami EK spolupracovat s národními standardizačními institucemi a s evropskými standardizačními institucemi při sestavování detailních standardizačních cestovních map. Tyto standardizační mapy se stanou příštím nástrojem a aplikovanou technologií. V této činnosti budou muset být zapojeni koneční uživatelé tak, aby byla průkazná užitečnost a využitelnost těchto technologií.

Termín: **2013**

Certifikace – sjednocení procedur

V současnosti neexistuje v EU jednotný a rozšířený systém certifikace pro bezpečnostní technologie. Národní systémy se liší a jsou fragmentovány.

Vzhledem k uvedenému se TPEB připojí k iniciativě EK směřující vytváření certifikovaných produktů, které ponесou Bezpečnostní značku EU

Tato značka bude značkou kvality pro bezpečnostní produkty vyrobené a platné v EU Harmonizace certifikace v rámci programu „EU bezpečnostní značka“ přispěje k zvýšení konkurenceschopnosti bezpečnostního průmyslu ČR ve vztahu k americké a čínské konkurenci.

TPEB se zapojí do tohoto certifikačního procesu jak v oblasti legislativních úprav, tak i certifikačních norem, které budou aplikovány na oblasti jednotlivých technologií, které jsou popsány v záměru studie proveditelnosti a SVA.

Termín: **2013**

Hledání synergií mezi bezpečnostními a obrannými technologiemi

Bude nastartován proces analýzy průniku mezi bezpečnostním (civilním) a obranným (vojenským) trhem resp. technologiemi, které na obou stranách existují. Oba trhy jsou velmi fragmentovány, průmyslová základna není identická, stejně tak nejsou stejní koneční uživatelé. Shodu je třeba rozpoznat analyzovat a využít v samotném začátku, během procesu Vědy a výzkum, aplikovaného výzkumu. Během tohoto procesu dochází k největším překryvům. Tato situace se vzhledem k stávajícím rozpočtovým omezením stala neudržitelnou.

Proto se TPEB připojí k iniciativám EU a jejích technologických platforem, které hledají synergií mezi civilními a vojenskými technologiemi. Jedná se o součinnost s Evropskou obrannou agenturou prostřednictvím Evropského rámcového programu spolupráce, který se začal naplňovat již v průběhu 7 Rámcového programu. Cílem je synchronizace vědy a výzkumu, zabránění duplikací a využití vzájemných synergií. Tento program je zařazen do spolupráce v rámci projektu Horizon 2020.

Mezi konkrétní technologie, které budou podporovány ve zmíněné oblasti, patří technologie komunikační a letecké ve vztahu ke kritické infrastruktuře, jak je uvedeno v SVA. Zde budou připraveny a prosazovány tzv. „hybridní standardy“.

Předpokládá se, že tento postup zajistí nárůst trhu bezpečnostního průmyslu o cca 1mlrd€.

Termín sjednocení civilních a vojenských technologií v oblasti OKI: **2014**

Urychlení využití aplikovaného výzkumu na trhu

Zde se bude TPEB v souladu s politikami EU a jejich naplňováním aktivně využívat programy na profinancování technologií v uvedených oblastech zejména ty které jsou v kompetenci Generálního ředitelství vnitro EK a současně národního programu pro vědu a výzkum při MV ČR Zde se také chce soustředit na problematiku “ochrany duševního vlastnictví” pro bezpečnostní výzkum, která je pro danou záležitost klíčová i v souvislosti s “Evropskou bezpečnostní známkou”, standardy, certifikacemi apod.

Všechny uvedené kroky mají současně vést k vytvoření transparentního trhu veřejných zakázek pro bezpečnostní průmysl v EU, potažmo v ČR

V praxi se bude TPEB podílet na vytváření nových pravidel pro ochranu duševního vlastnictví v oblasti ochrany kritické infrastruktury, energetické a kybernetické bezpečnost. A bude prosazovat uplatnění tohoto instrumentu do připravovaných národních programů, resp. do veřejných zakázek.

Termín: **2014**

Aplikace postupů před zadáváním veřejných zakázek

TPEB se bude podílet na přípravě a realizaci postupů, které mají předcházet zadávání veřejných zakázek. Primární zásady těchto postupů jsou obsaženy v zakládající dokumentaci

Programu Horizon 2020; vychází ze směrnic 2004/18 EK a 2009/81 EK o veřejných zakázkách. Cílem je zjednodušit veřejné zakázky a současně udržet jejich transparentnost a dostupnost pro vybraný segment trhu. To bude stimulovat konkurenceschopnost a zaměstnanost a současně to výrazně přispěje k udržení kvality zakázek.

Tento proces byl již zaveden v USA a první odhady jsou, že by měl podpořit exportní kapacity bezpečnostního průmyslu o cca 2 mld. € do roku 2020.

Termín: **2014**

1.3. Podpora VaVaI ve vybraných technologických oblastech

Aktivity TPEB budou zaměřeny v rámci výše uvedených programů na harmonizaci legislativy, standardizace a zkušebnictví a dále pak na podporu rozvoje nových technologií a propojování (technologické, komunikační) jednotlivých zmíněných oblastí. Důraz bude položen na aplikovaný výzkum a demonstrační projekty v následujících čtyřech tematických oblastech důležitých z hlediska energetické a kybernetické bezpečnosti a to jak z hlediska legislativy, tak technologií:

- Komunikační technologie
- Kybernetická bezpečnost
- Technologie sledování prvků KI
- Fyzická bezpečnost

1.3.1. Inicie VaVaI projektů v národních programech

Projekt z oblasti komunikačních technologií

Způsob iniciace

Na základě výzvy třetí veřejné soutěže ve výzkumu, experimentálním vývoji a inovacích PROGRAMU BEZPEČNOSTNÍHO VÝZKUMU ČESKÉ REPUBLIKY V LETECH 2010 – 2015 (BV II/2-VS) inicioval TPEB přípravu projektu v oblasti komunikačních technologií v návaznosti na ochranu KI.

Očekávaný dopad

Projekt bude zaměřen na návrh mobilního vysílacího střediska, které představuje velice účinný způsob přenášení informací k civilnímu obyvatelstvu především při mimořádných událostech. Obzvláště události poslední doby ve světě nám ukazují, že je zapotřebí mít k dispozici relativně snadný způsob pro šíření místně a časově aktuálních informací i při poničení stávající infrastruktury, přerušení dodávek el. energie apod.

Hlavním přínosem bude zvýšení bezpečnosti občanů při živelných či průmyslových pohromách nebo hrozbě teroristického útoku prostřednictvím umožnění distribuce místně cílené informace nezávisle na existující infrastruktuře.

Harmonogram přípravy

Žádost byla vypracována týmem specialistů složeným z řad zaměstnanců budoucích řešitelů v uplynulých měsících a byla podána dle podmínek zadávací dokumentace do 16. 7. 2012. V současné době probíhá příprava na zahájení projektu tak, aby v případě úspěšného posouzení žádosti mohla být neodkladně zahájena realizace.

Zapojené subjekty TPEB

VUT v Brně, Fakulta elektrotechniky a komunikačních technologií

Partneři

TESLA Electrontubes, s.r.o.

V rámci řešení projektu se předpokládá úzká spolupráce se složkami IZS a regulačními úřady (ČTÚ).

Financování

Financování bude realizováno v souladu s Rámcem společenství pro státní podporu výzkumu, vývoje a inovací (2006/C 323/01).

Projekt z oblasti kybernetické bezpečnosti

Způsob iniciace

Na základě výzvy třetí veřejné soutěže ve výzkumu, experimentálním vývoji a inovacích PROGRAMU BEZPEČNOSTNÍHO VÝZKUMU ČESKÉ REPUBLIKY V LETECH 2010 – 2015 (BV II/2-VS) inicioval TPEB přípravu projektu v oblasti kybernetické bezpečnosti v návaznosti na ochranu KI.

Očekávaný dopad

Cílem projektu je komplexní analýza hrozeb a následný návrh souboru opatření pro Smart Grid (inteligentní sítě) zajišťující kybernetickou bezpečnost jak z hlediska provozovatelů, tak i uživatelů.

Bude provedena komplexní analýza kybernetických hrozeb v prostředí Smart Grid (SG) po stránce technologické i právní, jejíž výsledky budou využitelné při vytváření nových standardů a norem pro implementaci smart technologií. Navržené bezpečnostní postupy budou testovány v laboratorních podmínkách VUT v Brně a Masarykovy univerzity v Brně na funkčních vzorcích SG, resp. rozsáhlých výpočetních sítích. Vznikne modulární aplikační systém schopný v reálném čase dohledovat komplexní infrastrukturu SG s důrazem na identifikaci narušení, autorizaci služeb, autentizaci uživatele a další rizikové oblasti.

Úspěšné dokončení projektu bude znamenat vytvoření komplexních analytických podkladů pro zahájení standardizačních či legislativních procesů pro vytvoření právního prostředí při zavádění SG technologií. Zároveň vznikne modulární aplikační základna pro zabezpečení kybernetické bezpečnosti SG systémů, která přímo souvisí s ochranou proti hrozbám ohrožujícím bezpečnost kritických infrastruktur v oblasti energetiky.

Harmonogram přípravy

Žádost byla vypracována týmem specialistů složeným z řad zaměstnanců budoucích řešitelů v uplynulých měsících a byla podána dle podmínek zadávací dokumentace do 16. 7. 2012. V současné době probíhá příprava na zahájení projektu tak, aby v případě úspěšného posouzení žádosti mohla být neodkladně zahájena realizace.

Zapojené subjekty TPEB

VUT v Brně, Fakulta elektrotechniky a komunikačních technologií

CNS, a.s.

Icontio ltd.

INVEA-TECH a.s.

Mycroft Mind, a.s.

Unicorn systems a.s.

Partneři

V rámci řešení projektu se předpokládá úzká spolupráce s provozovateli inteligentních sítí (ČEZ) a standardizačními úřady (ÚNMZ).

Financování

Financování bude realizováno v souladu s Rámcem společenství pro státní podporu výzkumu, vývoje a inovací (2006/C 323/01).

Projekt z oblasti sledovacích technologií

Způsob iniciace

Na základě výzvy třetí veřejné soutěže ve výzkumu, experimentálním vývoji a inovacích PROGRAMU BEZPEČNOSTNÍHO VÝZKUMU ČESKÉ REPUBLIKY V LETECH 2010 – 2015 (BV II/2-VS) inicioval TPEB přípravu projektu v oblasti sledování prvků KI v návaznosti na jejich ochranu a bezpečnost.

Očekávaný dopad

Hlavním přínosem této technologie bude zkvalitnění procesu monitorování prvků kritické infrastruktury použitím technologie automatizovaného dohledu za pomoci bezpilotních letových prostředků. Jejich nasazení umožní zintenzivnit monitorovací mise a snížit náročnost misí na letovou posádku a na vyhodnocování dat ze senzorových systémů sloužících k monitorování kritických infrastruktur. Navrhovaný systém povede ke zkvalitnění identifikace, prevence a ochrany proti hrozbám ohrožujícím bezpečnost kritických infrastruktur a to hlavně z hlediska automatické identifikace podezřelého chování v kritických infrastrukturách. Dalším pozitivním dopadem aplikace technologií, které budou předmětem výzkumu projektu, je automatické monitorování energetických a strategických provozů (například provozy rozvodů vysokého napětí, provozy chemického a jaderného průmyslu) a tím pádem prevence jejich fatální poruchy či poškození. Občané ČR a prvky IZS budou díky automatickému a včasnému varování v případě nestandardního stavu těchto provozů lépe chráněni v případě nutnosti zásahu či fatální poruchy.

Bezpečnost kritické infrastruktury je klíčová pro správné fungování státu a pro komfort a bezpečnost občanů. Aplikací technologií RPAS je možné zvýšit bezpečnost při současném snížení nákladů na její zajištění. Technologie vyvíjené v tomto projektu mají aplikovatelnost na následující scénáře ochrany infrastruktury:

- Ochrana a monitorování rozvodů vysokého napětí (ČEPS)
- Monitorování postižených oblastí po živelných katastrofách (požáry, povodně, atd.) nebo teroristických útocích (složky IZS)
- Ochrana a monitorování zařízení pro výrobu elektřiny ((ČEZ)

Harmonogram přípravy

Žádost byla vypracována týmem specialistů složeným z řad zaměstnanců budoucích řešitelů v uplynulých měsících a byla podána dle podmínek zadávací dokumentace do 16. 7. 2012. V současné době probíhá příprava na zahájení projektu tak, aby v případě úspěšného posouzení žádosti mohla být neodkladně zahájena realizace.

Zapojené subjekty TPEB

VUT v Brně, Fakulta elektrotechniky a komunikačních technologií

Partneři

Řešitelem projektu je Honeywell International spol. s r.o., který úzce spolupracuje s TPEB, ale zatím není členem.

V rámci řešení projektu se předpokládá úzká spolupráce s provozovateli prvků KI (složky IZS, ČEZ, ČEPS) a regulačními úřady (ČTÚ, NARFA CZE, ÚCL, OVL MO).

Financování

Financování bude realizováno v souladu s Rámcem společenství pro státní podporu výzkumu, vývoje a inovací (2006/C 323/01).

Projekt z oblasti ochrany KI

Způsob iniciace

Na základě druhé výzvy TAČR Centra kompetence plánované v roce 2013 bude iniciována příprava projektu na vznik specializovaného Centra kompetence zaměřeného na ochranu KI.

Očekávaný dopad

Předpokládáme vytvoření specializovaného centra výzkumu, vývoje a inovací v progresivním oboru ochrany KI s vysokým aplikačním potenciálem a perspektivou pro značný přínos k růstu konkurenceschopnosti ČR. Vzniklé centrum vytvoří podmínky pro rozvoj dlouhodobé spolupráce ve výzkumu, vývoji a inovacích mezi veřejným a soukromým sektorem.

Vznikem strategického partnerství podniků a výzkumných organizací dojde ke zvýšení konkurenceschopnosti ČR, posílení interdisciplinarity výzkumu, vývoje a inovací a zvýšení horizontální mobility výzkumných pracovníků (zejména začínajících výzkumníků). Důraz bude kladen na skutečnou realizaci výsledků v praxi.

Činnost centra bude v souladu s SVA.

Harmonogram přípravy

Harmonogram přípravy bude v souladu se zadávací dokumentací, která bude zveřejněna v průběhu příštího roku 2013, tak aby žádost byla podána v požadovaném termínu.

Zapojené subjekty TPEB

Na základě detailního rozpracování věcné náplně projektu bude následně vybrána skupina relevantních subjektů z řad členů TPEB a to jak z akademické tak privátní sféry.

Partneři

Na základě detailního rozpracování věcné náplně projektu bude následně vybrána skupina relevantních partnerů umožňující splnění cílů projektu.

Financování

Financování bude realizováno v souladu s Rámcem společenství pro státní podporu výzkumu, vývoje a inovací (2006/C 323/01).

Projekty z oblasti ochrany KI

V roce 2014 je předpoklad vyhlášení výzev do pokračujících programů „ALFA“ (TAČR) a „Bezpečnostní výzkum ČR“ (Ministerstvo vnitra ČR) na další programové období.

TPEB předpokládá iniciaci minimálně dvou projektů navazujících na průběžné výsledky projektů zahájených v roce 2013 v rámci těchto programů. Jejich tematické zaměření, rozsah a výběr partnerů bude vycházet z aktualizace IAP provedené v 1. polovině roku 2014.

1.3.2. Inicie VaVaI projektů v mezinárodních programech

Mezinárodní projekt z oblasti KI

Způsob iniciace

VUT v Brně jako člen TPEB v součinnosti s univerzitami v Krakově a Žilině připraví společný projekt v rámci programu Visegrad Funds.

Očekávaný dopad

Projekt bude zaměřen na příhraniční spolupráci v oblasti energetické bezpečnosti.

Harmonogram přípravy

Žádost projektu bude zpracována ve 3. čtvrtletí 2012 a následně podána.

Zapojené subjekty TPEB

Přípravou žádosti projektu a jeho následnou realizací bude pověřena VUT v Brně.

Partneři

AGH University of Science and Technology, Krakov, Polsko

Univerzity of Zilina, Žilina, Slovenská republika

Financování

Financování bude realizováno v souladu s Rámcem společenství pro státní podporu výzkumu, vývoje a inovací (2006/C 323/01).

Mezinárodní projekt z oblasti KI

Způsob iniciace

VUT v Brně jako člen TPEB v součinnosti s univerzitami v Polsku, Slovensku a Maďarsku připraví společný projekt v rámci programu Visegrad Funds.

Očekávaný dopad

Projekt bude zaměřen na příhraniční spolupráci v oblasti energetické bezpečnosti.

Harmonogram přípravy

Žádost projektu bude zpracována v 1. čtvrtletí 2013 a následně podána.

Zapojené subjekty TPEB

Přípravou žádosti projektu a jeho následnou realizací bude pověřena VUT v Brně.

Partneři

AGH Univerzity of Science and Technology, Krakov, Polsko

Univerzity of Zilina, Žilina, Slovenská republika

Financování

Financování bude realizováno v souladu s Rámcem společenství pro státní podporu výzkumu, vývoje a inovací (2006/C 323/01).

Mezinárodní projekt z oblasti ochrany KI

Způsob iniciace

TPEB ČR se v součinnosti s rakouským bmvit (Bundesministerium für Verkehr, Innovation und Technologie - Spolkové ministerstvo dopravy, inovací a technologií) bude účastnit výzvy 7. Rámcového programu Evropské komise v rámci mezinárodního projektu řešícího problematiku bezpečnosti inteligentních sítí (Smart Grids).

Na základě vzájemné koordinace mezi TPEB a bmvit bude vytvořen tým specialistů z řad členů TPEB, kteří se budou podílet na řešení projektu.

Očekávaný dopad

Řešení problematiky bezpečnosti inteligentních sítí jak z hlediska legislativy, tak i zaváděných nových technologií.

Harmonogram přípravy

V průběhu podzimních měsíců letošního roku proběhne iniciační schůzka mezi TPEB a bmvit, kde bude stanoven harmonogram přípravy projektu v základních rysech.

Zapojené subjekty TPEB

Na základě detailního rozpracování věcné náplně projektu bude následně vybrána skupina relevantních subjektů z řad členů TPEB a to jak z akademické tak privátní sféry.

Partneři

Hlavním partnerem bude rakouský bmvit.

Financování

Financování bude realizováno v souladu s Rámcem společenství pro státní podporu výzkumu, vývoje a inovací (2006/C 323/01).

2. Fáze (2015+)

V tomto období bude TPEB pokračovat v rozvoji národních a mezinárodních aktivit zaměřených na:

- Iniciaci VaVaI projektů v rámci národních i mezinárodních programů
- Tvorbu norem a související legislativy
- Oblast propagace a vzdělávání

TPEB předpokládá spolupráci s evropskými partnerskými organizacemi uvedenými níže a spolu s nimi se podílet na projektech v rámci bezpečnostního výzkumu ve výzvách Horizon 2020 a dalších komunitárních programech.

Seznam evropských partnerských organizací:

- **ERNICIP** (European Reference network for Critical Infrastructure protection)
- **CEN** (European Committee for Standardization)
- **CENELEC** (European Committee for Electrotechnical Standardization)
- **EOS** (European Organisation on Security)

Projekty budou opět zaměřeny jak technologicky, tak i legislativně. Výběr klíčových technologických oblastí, na které budou projekty zaměřeny, bude upřesněn v souladu s aktualizovanou SVA na počátku této fáze implementačního akčního plánu.

Současně se budeme podílet na přípravě nižších právních norem souvisejících s legislativou EK pro ochranu kritické infrastruktury, resp. energetické a kybernetické bezpečnosti. Zde předpokládáme nezbytnost implementace výstupů pro jasně vymezenou skupinu, která se pohybuje ve zmíněné oblasti a je reprezentantem konečného uživatele, jako jsou:

- výrobci energií
- distributoři energií
- vlastníci KI
- provozovatelé KI
- atd.

S tím souvisí i oblast vzdělávání a propagace, v rámci které bude TPEB organizovat odborné konference a to jak na národní, tak i mezinárodní úrovni.

2.1. Cílená podpora VaVaI v oblasti klíčových technologií

V rámci výzkumných a vývojových aktivit budou sledovány aktuální národní a mezinárodní programové výzvy s cílem iniciovat projekty za účasti členů TPEB v oblasti energetické a kybernetické bezpečnosti.

Z národních aktivit se jedná zejména o programy:

- Program bezpečnostního výzkumu ČR v letech 2015+
- Programy TA ČR

V rámci mezinárodních aktivit plánujeme účast v programech:

- HORIZON 2020
- V případě tematických a finančních možností v programech specializovaných ETP:
 - o ENIAC
 - o ARTEMIS
 - o EDA

Iniciované projekty budou v souladu s klíčovými technologiemi identifikovanými v SVA. V rámci plánované aktualizace IAP v roce 2014 dojde k podrobnému rozpracování aktivit TPEB v následujících dvou letech (2015 - 2016). Na základě aktualizované SVA dojde k upřesnění:

- Technologické náplně a stanovení cílů projektů na základě identifikovaných požadavků na nové technologie
- Legislativních oblastí vyžadující dopracování souvisejících norem pro zavedení nových technologií

2.2. Cílená podpora aktivit v oblasti tvorby bezpečnostní legislativy a standardů

TPEB zajistí aktivní účast v pracovních skupinách následujících subjektů formou delegovaných zástupců:

- **ERNICIP** (European Reference network for Critical Infrastructure protection).

Jedná se o poradní orgán EK. Zástupce TPEB je ve skupině ERNCIP Industrial Automated Control Systems and Smart Grids Thematic Group, která má do konce roku předložit EK první dílčí doporučení jak postupovat v uvedené problematice, zejména s ohledem na vytváření norem a standardů a nových technologických aplikací.

Rozvoj spolupráce ve skupině umožní aktivně se podílet na tvorbě a rozpracování následujících dokumentů:

- Analýza existujících standardů Ochrany kritické infrastruktury (OKI)
- Vytvoření evropského obchodního modelu pro testování a standardizaci

- **CEN/CENELEC** - poradní orgán standardizačního úřadu EK

TPEB zajistí účast vybraného zástupce v „Koordinační skupině kybernetické bezpečnosti“. Bude se aktivně podílet na aktivitách evropského standardizačního úřadu v souvislosti s harmonizací a vytvářením nových norem pro oblast ochrany kritické infrastruktury, včetně energetické a kybernetické bezpečnosti.

Na základě provedené analýzy aktuální standardizace v oblasti bezpečnostních norem v jednotlivých členských státech EU bude rozpracován návrh postupu pro jejich harmonizaci, zpracování a zavedení nových norem úzce souvisejících se zaváděním nových technologií.

Seznam národních norem v uvedené oblasti a soupis mezinárodních norem poskytující přehled o evropských a světových standardech a existujících databázích bude v pravidelných termínech aktualizován, aby bylo možné identifikovat nedostatečné legislativně pokryté oblasti.

- **EOS** (European Organisation on Security)

EOS je bruselskou platformou sjednocující 39 špičkových výzkumných ústavů, firem a institucí z 13 evropských států a představujících cca 65% průmyslového bezpečnostního trhu.

Problematika, ve které TPEB bude spolupracovat, je zaměřena na otázky energetické a kybernetické bezpečnosti. Na základě výsledků dokumentů zpracovaných do konce roku 2014

v rámci Bílé knihy uvedené níže, budou stanoveny další aktivity EOS, na kterých se bude TPEB aktivně podílet:

- Bezpečnost energetické infrastruktury
- Postupy pro implementaci strategie evropské kybernetické bezpečnosti.

2.3. Oblast propagace a vzdělávání

V oblasti propagace a vzdělávání TPEB v uvedeném období zajistí přístup široké veřejnosti k relevantním informacím z oblasti energetické a kybernetické bezpečnosti. Aktivity TPEB vedoucí ke splnění těchto cílů budou soustředěny do následujících oblastí:

- Aktualizace webových stránek TPEB s ohledem na publikaci veřejně dostupných dokumentů z oblasti energetické a kybernetické bezpečnosti. Jedná se jak o národní dokumenty zveřejněné orgány státní správy, tak o relevantní dokumenty evropských institucí a organizací, zejména těch, ve kterých máme své zástupce, jak je uvedeno v předchozí kapitole 2.2.
- Pořádání odborných setkání za účasti národních a mezinárodních expertů, formou
 - o Kulatých stolů
 - o Diskusních fór
 - o Technologických dní
 - o Demonstračních akcí s cílem předvedení nových technologií nebo identifikace nových hrozeb v oblasti energetické a kybernetické bezpečnosti
 - o Atd.
- Pořádání odborných konferencí s národní i mezinárodní účastí zaměřených na řešení vybraných technologických oblastí souvisejících se zajištěním energetické a kybernetické bezpečnosti.

Dalším krokem je spolupráce s MŠMT a jednotlivými vzdělávacími subjekty na zapracování problematiky energetické a kybernetické bezpečnosti do výuky na různých stupních vzdělávacího systému ČR. Pro zahájení jednání jsou jako výchozí metody zvoleny:

- Poskytnutí externích lektorů z řad vlastních expertů TPEB;
- Organizace odborných seminářů s cílem zajistit předávání odborných informací profesionálním lektorům.