

Zpráva o činnosti v letech 2020 s výhledem roku 2021

TPEB v daných letech aktivně naplňovala svůj dlouhodobý záměr, který vychází z představy významně stimulovat národní kapacity v oblasti ochrany kritické infrastruktury prostřednictvím VaVal projektů a expertního dialogu s relevantními stakeholdery z prostředí strategických infrastrukturních firem, utilitních firem, státní správy a výzkumných institucí. TPEB dále přispívá k vzájemné koordinaci aktivit a informovanosti subjektů státní správy, subjektů výzkumu a vývoje a dodavatelů bezpečnostních technologií, a to v návaznosti na národní i nadnárodní programy. Ve zmíněném duchu TPEB také spolupracuje i s řadou subjektů, které nejsou členy platformy.

Ve své činnosti se TPEB soustředí především na podporu podávání projektů v oblasti aplikovaného výzkumu a vývoje, expertní aktivity v oblasti strategií, normotvorby a standardizace (prostřednictvím svého člena České agentury pro standardizaci (ČAS)) a osvětovou činnost propojující znalosti a schopnosti jednotlivých pilířů public-private-partnership (PPP) projektu. Všechny tyto aktivity vykonává v národním i evropském kontextu, často v úzké součinnosti s institucemi a orgány Evropské komise. Expertní dosah platformy potvrzují zejména národně a nadnárodně zaměřené projekty výzkumu, vývoje a inovací. TPEB je usazena jako relevantní aktér u českých poskytovatelů a byla přizvána již do 20 konsorcií usilujících o projekty H2020. Právě v kontextu evropských projektů, kde je neustále kladen důraz na spolupráci mezi institucemi státní správy, samosprávy a firmami i výzkumnými institucemi, patří s výjimkou etablovaných univerzit či velkých výzkumných pracovišť mezi nejaktivnější hráče.

TPEB působí v duchu PPP platformy a propojuje zájmy jednotlivých výše zmíněných segmentů. Kromě projektové činnosti se aktivně věnuje sledování významných strategických a legislativních trendů. V tomto kontextu lze zmínit Cyber Security Act, Nařízeních evropského parlamentu o opatřeních na zajištění bezpečnosti dodávky plynu, o rizikové připravenosti v odvětví elektroenergetiky, týkající se především otázek certifikace v oblasti informačních a komunikačních technologií, kde v současnosti dochází k několika konkrétním aktivitám či problematiku související s energetickou bezpečností ve vztahu k evropským i národním iniciativám.

Hlavními cíli platformy je:

- a) S ohledem na mnohaleté působení ve strukturách EK umožnit tuzemským subjektům zúčastňovat se programů a projektů EK, zejména Horizon Europe
- b) Stimulovat spolupráci mezi firmami, výzkumnými institucemi a státem v klíčové strategické oblasti zvyšování ochrany a odolnosti kritické infrastruktury.
- c) Napomáhat definici zájmů a potřeb českých subjektů v oblasti ochrany a odolnosti kritické infrastruktury ve vztahu k národním i nadnárodním institucím a relevantní legislativě.
- d) Podporovat využití českých kapacit, know-how a best practices.
- e) Koordinovat a podporovat činnost členů platformy ve vztahu k Národnímu programu energetické odolnosti ČR. Stimulovat a kultivovat expertní i veřejnou diskusi o ochraně kritické infrastruktury.
- f) Zapojovat do uvedených aktivit malé a střední podniky či startupy.

I. Projekty v oblasti výzkumu, vývoje a inovací

A) Projekty H2020

Mezinárodní projekty VaVal, především program H2020, patří mezi nejdynamičtější agendy činnosti TPEB v posledních letech, kdy platforma aktivně vstoupila a pomohla procedurálně i substantivně zformovat celkem 20 konsorcií, která úspěšně zareagovala na konkrétní projektové výzvy. Všechny podané projekty souvisely s budováním spolupráce a technologickými inovacemi v širší oblasti ochrany kritické infrastruktury. Platforma v projektech staví na dlouhodobě kultivovaných vztazích s end-usery a ve spolupráci s Českou agenturou pro standardizaci buduje profil v oblasti normotvorby.

V zásadní konkurenci, která v rámci H2020 existuje, platforma uspěla s projekty:

SecureGas

Projekt získal podporu ve výzvě SU-INFRA-01-2018-2019-2020: Prevention, detection, response and mitigation of combined physical and cyber threats to critical infrastructure in Europe. Projekt se soustředí na zabezpečení plynárenských sítí před kybernetickými hrozbami. Úctyhodné multidisciplinární konsorcium čítá 21 mezinárodních partnerů. Skládá se z integrované energetické společnosti (ENI S.p.A), plynárenské korporace (Public Gas Corporation of Greece S.A.), TSO – Transmission system operator (provozovatele přenosové soustavy AB Amber Grid) a provozovatele distribuční soustavy DSO – Distribution system operator (Attiki Natural Gas Distribution Company SA), spravující dohromady + 15000 km plynovodů; poskytovatelů technologií působících v oblasti bezpečnosti a kritické infrastruktury (Leonardo S.p.A, Guardtime A.S., Elbit Systems Ltd., WINGS ICT Solutions, IDEMIA Identity & Security Germany AG, EXUS, GAP Analysis S.A., Innov-Acts Ltd. a Disaster Management, Advice and Training Consulting KG), výzkumných a akademických institucí v oblasti energetiky, bezpečnosti a odolnosti (Fraunhofer-Gesellschaft zur Förderung der angewandten Forschung, Kentro Meleton Asfaleias, Joint Research Centre Ispra, Technická univerzita v Rize, Technologická platforma Energetická bezpečnost ČR). Platforma zúčastněných stran (Stakeholder Platform), vedená Agenzia per la Promozione della Ricerca Europea, bude poskytovat zázemí k zajištění dlouhodobého šíření výstupů projektu. Projektová role TPEB obsahuje aktivity v oblasti standardizace a evaluace vyvíjených řešení.

S4AllCities

Projekt S4AllCities (Smart Spaces Safety and Security for All Cities) byl zahájen v září 2020. Zaměřuje se na systémy zajišťující bezpečnost a ochranu obyvatel měst. Inteligentní města mají hlavní zodpovědnost za zajištění bezpečného fyzického a digitálního ekosystému podporujícího soudržnost a udržitelný rozvoj měst pro blaho občanů EU. S4AllCities integruje pokročilé technologie a organizační řešení v tržně orientovaném sjednoceném rámci Cyber - Physical Security Management, zaměřeném na zvyšování úrovně odolnosti městských infrastruktur, služeb, ICT systémů, IoT a podporu sdílení informací a informovanosti mezi zainteresovanými složkami městských aglomerací v oblasti bezpečnosti. Tři pilotní případy se zapojením celkem 5 měst ve 4 zemích (Španělsko, Rumunsko, Česká republika, Řecko), umožní systému S4ALLCITIES System of Systems nasazení a ověření jeho inteligentních komponent a funkcí ve skutečném životním prostředí, zajištění dodávek řešení a služeb v souladu s novými požadavky inteligentních měst, zaměřené na: řízení bezpečnosti otevřených rizikových prostorů ; kybernetické zabezpečení; sledování podezřelých aktivit a chování; identifikace objektů bez dozoru; odhad cyber-fyzických rizik v reálném čase na více místech a měření aktivace pro efektivní řešení krizových situací.

S4AllCities bude využívat přítomnosti TPEB ČR, jedinečného neziskového subjektu veřejného a soukromého partnerství v České republice, který se zaměřuje na oblast ochrany kritické infrastruktury, při posilování spolupráce veřejného a soukromého sektoru v oblasti ochrany veřejných prostor. TPEB bude pořadatelem jedné ze 3 akcí, které projekt povede, se zaměřením přesně na posílení spolupráce veřejných a soukromých subjektů. TPEB ČR, v rámci účasti na projektu významně těží tím, že se postupně vedle energetiky zaměří na širší oblast kritické infrastruktury a bude rozvíjet své postavení v oblasti standardizace sloužící jako brána pro české standardizační orgány.

STAMINA

Projekt STAMINA byl zahájen v září 2020. Zaměřuje na strategický a krizový management v případě pandemie. Nabídne použití nových konceptů v prediktivním modelování a obecně v řešení pandemických krizí, které potenciálně pomohou zefektivnit národní zdravotnické plánovací systémy, a to od úrovně strategických plánovačů až po první respondenty. Stávající krizové rámce budou posíleny zpravodajskými informacemi získanými z datových souborů a modelů o pandemiích a pokročilými vizualizačními technologiemi, které a) umožní predikci šíření nemocí, b) odhadnou dopady (socioekonomické) pandemické krize na veřejné zdraví obecně a c) budou podporovat subjekty s rozhodovací pravomocí při provádění nejuhodnějších strategií reakce, včetně plánování zdrojů a celkového řešení krizí. Každá demonstrace bude obsahovat několik simulačních cvičení zahrnujících kompletní řetězec zúčastněných stran nezbytný k testování a validaci nového navrhovaného konceptu end-to-end, včetně přeshraniční spolupráce. Cílem rozsáhlých demonstrací bude poskytnout zúčastněným stranám přímou příležitost ke spolupráci při validaci nových konceptů, a tím významně zlepšit schopnost situačního uvědomění a schopnosti podpory rozhodování příslušných organizací v oblasti strategického a krizového zdravotnického managementu ve velkém počtu členských států EU. Výsledkem projektu bude závazek zúčastněných stran sdílet a uplatňovat strategie připravenosti a řešení krizí vyvinuté v projektu a provádět ověřené nové koncepce na vnitrostátní i přeshraniční úrovni.

TPEB je v projektu zodpovědná za českou demonstraci a aktivity v oblasti standardizace a veřejného dosahu.

Další projekty, na kterých se TPEB ČR podílí, a které byly podány v rámci programu H2020/Horizon Europe v roce 2020 a na podzim 2021:

Ve druhé polovině roku 2020 TPEB ČR vstoupila do dalších čtyř projektových konsorcií v rámci nových výzev programu H2020. Jedná se o projekty SCANNER, PowerProtect, EUROCAP a SMARPOL.

Na podzim roku 2021 TPEB vstoupila do tří projektových konsorcií projektů ELEMENTAL, SecurEnergies a PRETECO v rámci nového programu Horizon Europe.

Projekty úspěšně podané v roce 2020 :

Projekt **SCANNER** navrhuje automatizovaný mechanismus pro kontrolu bezpečnosti a ochrany softwarových řešení a aplikací. Výsledný mechanismus podpoří vývojářskou práci a zjednoduší certifikační proces v oblasti bezpečnosti a ochrany dat. Specifičtěji dojde v rámci projektu implementována sada modelů a technik identifikace hrozeb, která se bude opírat o různé statické a dynamické analýzy kódu. Inovativnost projektu SCANNER spočívá v nástrojích využívajících nejnovějších metod na poli umělé inteligence.

Projekt **PowerProtect**

Energetické systémy (EPES) v celé EU procházejí proměnou díky integraci různých informačních a komunikačních technologií (založených na IP), které odkrývají nové možnosti monitorování a kontroly, ale zároveň představují celou řadu nově vznikajících rizik, hrozeb a zranitelných míst. PowerProtect se zaměřuje na řešení zvýšené potřeby kybernetické bezpečnosti a ochrany dat v těchto systémech: (i) homogenizací sběru a zpracování dat z heterogenních a systémových komponent s podporou IP, (ii) vývojem sady technologií pro kybernetickou bezpečnost, jako je fotonický Physical Unclonable Functions, Trusted Execution Environments, and Blockchain-based logging and auditing databases, (iii) zlepšování detekce incidentů narušení (a obecně neobvyklého chování) pomocí technik strojového učení, (iv) zlepšování povědomí o stavu zabezpečení EPES pomocí velkých dat analytika a (v) budování automatizovaného systému podpory a odezvy na rozhodování zahrnujícího analýzu rizik v reálném čase. PowerProtect využije průmyslový multi-iterační cyklus k vývoji těchto inovativních řešení na úrovni TRL 7 a zajistí přechod z laboratoře na trh s minimálním zpožděním. Vyvinuté systémy budou během svého vývoje validovány dodržováním zákonných a etických pravidel pro ochranu údajů a přispíváním k průmyslovým standardům v energetickém sektoru. Pro účely testování a vyhodnocení bude rovněž poskytnuto zkušební zařízení pro emulaci energetického systému.

Projekt **EUROCUP**

Pořádání významných sportovních akcí, jako jsou mistrovství světa ve fotbale FIFA, olympijské a paralympijské hry nebo mistrovství Evropy ve fotbale UEFA a mistrovství světa v ragby, je pro každé hostitelské město jedinečnou výzvou a příležitostí. Miliony návštěvníků z celého světa vytvářejí bezprecedentní potřeby v oblasti bezpečnosti. S příklady nešťastných událostí souvisejících s bezpečností na olympijských hrách v Mnichově v roce 1972, v Atlantě v roce 1996 či bombových útoků během maratonů na Srí Lance v roce 2008 a v Bostonu v roce 2013 má ochrana těchto symbolických událostí prvořadý význam. Každý odpovědný orgán činný v trestním řízení (LEA) má nevyhnutelně společně s hostitelským městem nelehký úkol posoudit rizika, stanovit komplexní strategii veřejné bezpečnosti, definovat efektivní organizační strukturu a poskytnout dostatek zdrojů na podporu plánování a zajištění účinného bezpečnostního a zabezpečovacího provozu během významných sportovních akcí. Cílem projektu EUROC@P je vytvářet znalosti a poskytovat pokročilé technologie pro podporu a zlepšování schopností LEA v oblasti ochrany občanů a veřejných činitelů. Pokud jde o životní cyklus zabezpečení/ochrany, zaměřuje se EUROC@P na fáze IDENTIFIKACE, OCHRANY a

DETEKCE, ačkoli ostatní fáze (REAKCE a OBNOVA) budou také těžit z technologií vyvinutých v rámci projektu. Všechna řešení založená na nejnovějších technologiích EUROC@P budou předvedeny v realistickém prostředí ve čtyřech pilotních projektech a ověřeny sedmi partnery LEA, což usnadní integraci řešení EUROC@P do jednotné platformy pro plánování zabezpečení a monitorování velmi rozsáhlých událostí.

Projekt **SMARPOL**

Evropa, její občané a její hodnoty jsou zkoušeny na mnoha úrovních, přičemž členské státy EU jsou svědky neustále rostoucího spektra hrozeb. Terorismus ohrožuje naši bezpečnost, hodnoty našich demokratických společností a práva a svobody evropských občanů. V reakci na současné teroristické prostředí příslušné orgány stále více začleňují zpravodajské informace do operací vymáhání práva. Je třeba vyvinout účinné mechanismy pro přenos kritických zpravodajských informací donucovacím orgánům, zejména v případech, kdy jednání na základě těchto zpravodajských informací pomůže zachránit životy nevinných lidí. Aby bylo možné bojovat proti rostoucí diverzifikaci hrozeb, je třeba rozšířit možnosti relevantních aktérů o inovativní a robustní technologické kapacity. Kromě toho je nutné údaje pečlivě spravovat, protože na citlivý obsah mohou platit legislativní omezení a záruky. Pro řešení těchto výzev projekt SMARPOL navrhuje nástroj Smart Policing Toolbox, který poskytne

vylepšené možnosti pro účinný boj proti trestné činnosti a terorismu. Projekt poskytne inovativní, robustní a uživatelsky přívětivé inteligentní policejní nástroje umožňující pokročilou vizualizaci dat, aplikaci rozšířené reality, řešení pro detekci a sledování bez rušivých vlivů, analýzu videa a obsahu, aplikaci AI pro včasnou identifikaci a detekci neobvyklé činnosti, autonomní a mobilní platformy typu plug-and-work edge, vylepšenou a rychlou extrakce znalostí, vylepšené možnosti školení, efektivní sdílení informací, správu dat a funkce spolupráce s cílem rozšířit a vylepšit funkce LEA a plně využívat schopnosti založené na datech pro prevenci, vyšetřování reakce v boji proti terorismu a organizovanému zločinu v souladu s národními i evropskými právními a etickými předpisy.

Projekty úspěšně podané v roce 2021 :

ELEMENTAL

HORIZON-HLTH-2021-ENVHLTH-02 - HORIZON-RIA - podaný 21.9.2021

Projekt ELEMENTAL bude provádět interdisciplinární technické a vědecké inovační činnosti, které uspokojí potřeby klíčových stakeholderů v oblasti boje se zdravotními výzvami souvisejícími s globálními změnami klimatu. Navrhovaná řešení projektu ELEMENTAL umožní tvůrcům politik a systémů veřejného zdraví proaktivně řešit globální zdravotní problémy v oblasti duševního zdraví, které jsou umocněny environmentálními stresory vyplývajícími ze změny klimatu. Toho bude dosaženo vývojem sady prediktivních modelů pro i) vývoj rizik způsobených klimatem, ii) prevalenci duševního zdraví související se stresory vyvolanými klimatem, iii) integrované modely hodnocení kvantifikovaných ekonomických nákladů, iv) analýzu dat pro reakce podle socioekonomických a regionálních faktorů.

SecurEnergies

HORIZON-CL3-2021-INFRA-01 - HORIZON-IA – podaný 23.11.2021

Projekt SecurEnergies si klade za cíl vyvinout společnou evropskou strategii na ochranu evropské energetické infrastruktury před hybridními hrozbami, a zajistit tak energetickou suverenitu EU. SecurEnergies si klade za cíl řešit výše uvedené problémy tím, že se zaměří na energetické infrastruktury EU a jejich vzájemné provázanosti s telekomunikačními, vodohospodářskými a finančními sektory primárně, stejně jako se zeměmi mimo EU, s cílem odhalit zranitelnost a systémová rizika a hybridní hrozby, kterým čelí celá propojená přeshraniční CI síť. Projekt si klade za cíl pomoci vládním agenturám, sdružením a společnostem a být si vědom hybridních hrozeb, pochopit jejich potenciální dopad a kaskádové efekty a připravit účinnou společnou strategii odolné obrany a reakce.

PRETECO

HORIZON-CL3-2021-FCT-01

Projekt počítá s vytvořením digitální platformy, která může nabídnout tvůrcům politik, místním manažerům, LEA a bezpečnostním pracovníkům schopnosti plánovat scénáře spolupráce, analyzovat zranitelná místa a rizika v případě teroristického útoku a pomáhat jim při zavádění účinných odstrašujících a zmírňujících opatření, jakož i výcvikových cvičení, směrem ke zvýšení odolnosti veřejných prostranství.

Platforma PRETECO nabídne realistický trojrozměrný (3D) virtuální analog města spolu s modelováním infrastruktury (vodovodní síť, síť plynovodů, energetická síť, telekomunikační síť, dopravní síť) a simulačními schopnostmi (virtuální útoky, virtuální senzory, simulace pohybu davů a vozidel, vzájemné závislosti kaskádových efektů), které umožní rozsáhlé hodnocení zranitelnosti proti různým hrozbám a scénářům, přičemž podrobnosti přizpůsobí specifikům každého města. Jediný přístup PRETECO je založen na otevřené architektuře, kde:

a) městští (bezpečnostní) plánovači mohou přidat bezpečnostní prvky (silniční nárazníky/zábrany, nastavení jednosměrného provozu, více únikových cest), vše v kontextu security-by-design & ethical-by-design přístupu

b) LEA a PSC mohou nastavit řadu zranitelností města na základě jejich integrovaného souboru nástrojů pro hodnocení zranitelnosti

c) LEA, PSC, místní úřady, FR a další agentury mohou navrhovat scénáře spolupráce pro simulaci kaskádového teroristického útoku scénáře pro testování různých preventivních a reakčních opatření při současném posílení vzájemné spolupráce.

B) Projekt OPPIK – Ochrana kritické infrastruktury II

Od poloviny roku 2020 TPEB ČR pracuje na realizaci projektu podpořeného v rámci OP Podnikání a inovace pro konkurenceschopnost s názvem **Ochrana kritické infrastruktury II**. Dominantním cílem projektu bylo stimulovat mezinárodní spolupráci a formování konsorcií usilujících o projekty z evropského programu H2020. Projekt navazoval na úspěšně vyřešený projekt **Ochrana kritické infrastruktury a Energetická a kybernetická bezpečnost**. V rámci těchto úspěšně realizovaných projektů započal proces aktivního budování mezinárodní kooperativní sítě subjektů působících v široce pojaté oblasti ochrany kritické infrastruktury. Projekt **Ochrana kritické infrastruktury II** dále rozvíjí trend spolupráce v rámci H2020/Horizont Europe.

C) Bezpečnostní výzkum MV

Projekt CIRFI 2019: Indikace narušení resilience kritické infrastruktury Předmětem projektu CIRFI 2019: Indikace narušení resilience kritické infrastruktury je výzkum v oblasti resilience kritické infrastruktury. V rámci projektu budou determinovány indikátory narušení resilience vybraných subsystémů kritické infrastruktury a bude vytvořen nástroj na jejich včasnou identifikaci a posouzení vhodnosti předmětných indikátorů pro konkrétní infrastrukturní subsystémy. Zástupci členů TPEB ČR se podílejí na realizaci tohoto projektu.

D) Technologická agentura TAČR

TPEB započala strategický dialog s agenturou TAČR, jehož cílem je efektivněji nasměrovat aplikovaný výzkum ve sféře kritické infrastruktury do oblastí hlavních sektorových zájmů. Na základě iniciativy TAČR zvažuje účast ve výzvách programu Théta, jehož zaměření vychází z aktualizované Státní energetické koncepce, kterou TPEB připomínkovala. Specifickou součástí strategického dialogu

s TAČRem jsou bilaterální programy, kde došlo k uzavření funkční spolupráce mezi ČR a Jižní Koreou. Společná témata se týkají především otázek energetické bezpečnosti, a to například stability, efektivity a bezpečnosti dodávek elektrické energie, vč. politického a institucionálního zabezpečení či rozvoje inovačního potenciálu v daném sektoru.

Projekt „Projektování a bezpečné provozování LNG čerpacích stanic“ v rámci programu Théta

Cílem projektu je přispět k odblokování současné situace, kdy na trhu není poptávka po nákladních vozidlech na LNG z důvodu nedostatečně rozvinuté infrastruktury čerpacích stanic. Infrastruktura se nerozvíjí z důvodu chybějících informací a stavebně technických předpisů pro výstavbu a provoz. Prosazení stavebních předpisů tak vytvoří základní impuls pro urychlení rozvoje a vytvoření nabídky, která povede k rozšíření LNG v nákladní přepravě i jinde. Proces bude také znamenat významný příspěvek pro naplnění směrnice Evropského parlamentu 22/2014 o zavádění infrastruktury pro alternativní paliva. Stanoveného cíle bude dosaženo realizací navazujících etap: sestavení monografie (06/2019), uspořádání odborné konference (05/2020), návrh příslušné ČSN (12/2020) a certifikace metodiky (08/2021). TPEB je členem projektového konsorcia. Projekt byl schválen k realizaci, která započala 1. listopadu 2018 a byla úspěšně zakončena 30.zářím 2021

II. Podpora expertního dialogu

Národní program energetické odolnosti ČR

TPEB hájí a snaží se naplnit zájmy svých členů z řady end-userů ve vztahu k východiskům zvyšování stability a dostupnosti dodávek elektrické energie.

Jedním z hlavních východisek ke zvyšování stability a dostupnosti dodávek elektrické energie je Státní energetické koncepce ČR schválené dne 18. května 2015, zejména oblast výkonu státní správy v podobě Národního programu energetické odolnosti. Zmiňovaný program byl v prvotní fázi zaměřen na analýzu dopadů a formulaci vybraných nástrojů zvyšujících energetickou odolnost ve vazbě na harmonizaci schopnosti ostrovních provozů územních celků, ochranu kritické infrastruktury a klíčové systémy energetiky v širších souvislostech.

Mezi další východiska definující potřebu posílení energetické bezpečnosti ve vztahu k zajištění ochrany obyvatelstva patří Bezpečnostní strategie, Koncepce ochrany obyvatelstva do roku 2020 s výhledem do roku 2030 a Strategický rámec udržitelného rozvoje. Zde je důraz kladen na zvýšení ochrany a odolnosti prvků kritické infrastruktury, spolupráci zainteresovaných subjektů a zajištění energetické bezpečnosti České republiky, jakožto dalších významných zájmů státu.

V oblasti zvyšování energetické odolnosti ČR je cílem TPEB podporovat spolupráci se společnostmi ČEZ, a.s. a ČEPS, a.s. v kontextu potřeby:

- a) Formulace územních energetických koncepcí v souladu s reálnými možnostmi z hlediska procesu zvyšování stability a odolnosti dodávek strategických služeb,
- b) Potřeby precizace systému ochrany kritické infrastruktury,
- c) Vytvoření platformy pro vzájemnou výměnu dat, informací a zkušeností pro posílení pozitivního dopadu Státní energetické koncepce a Národního programu energetické odolnosti ČR

- d) Zvýšení postavení a aktivizace ČR při tvorbě a implementaci evropských a mezinárodních norem a pravidel.
- e) Přípravy energetického odvětví kritické infrastruktury na implementaci Nařízení EP a Rady EU (Cyber Security Act, Nařízeních evropského parlamentu o opatřeních na zajištění bezpečnosti dodávky plynu, o rizikové připravenosti v odvětví elektroenergetiky)

Konference - XIX. ročník mezinárodní konference Ochrana obyvatelstva – Zdravotní záchranářství 2020

Ve dnech 5.2. – 6.2.2020 se v Ostravě konala významná celorepubliková konference – XIX. ročník mezinárodní konference Ochrana obyvatelstva – Zdravotní záchranářství 2020, kterou pořádala VŠB – Technická univerzita Ostrava – Fakulta bezpečnostního inženýrství a Sdružení požárního a bezpečnostního inženýrství, z.s. ve spolupráci s Ministerstvem vnitra – generálním ředitelstvím Hasičského záchranného sboru ČR a Fakultní nemocnicí Ostrava. Konference se zúčastnil jako přednášející JUDr. Richard Hlavatý s tématem Průmysl 4.0 ve vazbě na energetickou bezpečnost a odolnost.

On-line pracovní setkání s názvem „Zákon o soukromých bezpečnostních službách ve vazbě na ochranu kritické infrastruktury“

Technologická platforma „Energetická bezpečnost ČR“ ve spolupráci s aktivním členem Platformy společností ČEPS, a.s., dne 10.12.2020 organizovali on-line pracovní setkání s názvem „Zákon o soukromých bezpečnostních službách ve vazbě na ochranu kritické infrastruktury“. Pracovního setkání se účastnili představitelé Samostatného oddělení soukromých bezpečnostních služeb Ministerstva vnitra ČR, představitelé odborných a profesních sdružení – Český klub bezpečnostních služeb, České asociace bezpečnostních manažerů a v neposlední řadě zástupci subjektů kritické infrastruktury E.ON Distribuce, a.s., Pražská energetika, a. s. a ČEPS, a.s. Akademický a výzkumný sektor byl reprezentován doc. Ing. Martinem Hromadou, Ph.D. členem správní rady Platformy, který setkání současně moderoval. Předmětem setkání byla odborná diskuze o očekávaném vlivu přijetí zákona na celkovou kvalitu a cenovou politiku poskytovaných bezpečnostních služeb s vazbou na specifické potřeby subjektů kritické infrastruktury. Problematika ochrany kritické infrastruktury je ústředním mottem i v rámci realizovaných a připravovaných projektů i v programech jako je Horizont2020, kde se TPEB ČR aktivně zapojuje prostřednictvím odborníků z řad svých členů, ale i z dalších institucí a firem.

Toto on-line setkání je jedním z dalších důležitých kroků v rozvíjení spolupráce na tomto vysoce aktuálním tématu, jehož řešení je podporováno i v rámci projektu Ochrana kritické infrastruktury II., jehož hlavním cílem je v návaznosti na již úspěšně vyřešené projekty Energetická a kybernetická bezpečnost (OPPI) a Ochrana kritické infrastruktury (OPPIK) propojovat schopnosti a potřeby firemní a výzkumné sféry reflektující strategické potřeby a zájmy infrastrukturních společností a státní správy v kontextu projektů výzkumu a vývoje.

Workshop „MOŽNOSTI ÚSPĚCHU I V TÉTO DOBĚ“ konaný dne 20.5.2021

Cílem tohoto workshopu byla prezentace úspěšných forem spolupráce mezi soukromým, akademickým a komerčním sektorem, často naplňujícím koncepty efektivních PPP projektů. Byly zde

prezentovány aktivní členové TPEB ČR a jejich portfolio činností vzhledem k strategickým zájmům Platformy, které reflektují aktuální výzvy společnosti, nejenom v oblasti bezpečnosti. Byly zde prezentovány zkušenosti z působení v mezinárodních konsorciích projektů SECUREGAS, STAMINA, S4ALLCITIES, které do jisté míry a ve specifických oblastech aplikují trendy a nástroje Průmyslu 4.0 s využitím aspektu digitalizace. Diskuze reflektovala proces tvorby a vstupu do národních i evropských konsorcií, vzhledem k preferencím členů Platformy s orientací na průmyslové subjekty a podniky.

První konference o LNG v ČR v rámci projektu Projektování a bezpečné provozování LNG čerpacích stanic pořádána VUT v Brně společně s plynaři z GasNetu a TPEB ČR

Zástupci Fakulty stavební Vysokého učení technického v Brně společně s největším tuzemským distributorem zemního plynu společností GasNet uspořádali vůbec první konferenci o využití LNG v nákladní dopravě v České republice, jejíž spoluorganizátorem byla i TPEB ČR. Kromě představitelů VUT a GasNetu na konferenci vystoupili zástupci Ministerstva dopravy i dalších subjektů podílejících se na rozvoji tohoto efektivního a ekologického paliva v nákladní dopravě. Účastníci konference potvrdili dobrou perspektivu LNG v České republice. První konference o využití zkapalněného zemního plynu (LNG) v nákladní dopravě se konala formou videokonference za účasti více než 50 zástupců Ministerstva průmyslu a obchodu, Ministerstva dopravy, dopravců i dalších odborníků z oblasti nákladní dopravy a požární bezpečnosti staveb.

Na základě prezentovaného lze konstatovat, že obecným cílem platformy v oblasti rozvoje expertního dialogu je:

- a) podpora hledání inovačních či legislativních řešení v oblasti efektivnější spolupráce v rámci národních PPP projektů.
- b) formování národní pozice vůči nadnárodním iniciativám.
- c) zkvalitňování veřejné i expertní diskuze o ochraně a odolnosti kritické infrastruktury.
- d) vytváření expertní sítě napříč státním, soukromým a veřejným sektorem.
- e) organizování a příprava projektů výzkumu, vývoje a inovací a budování aplikační báze v národním i evropském kontextu.

III. Perspektiva dalšího vývoje

TPEB v uplynulých letech jednoznačně prokázala, že má potenciál posouvat české schopnosti a zájmy na evropskou úroveň. V dalších letech plánuje rozvíjet projektovou aktivitu s cílem ještě více zapojovat členskou základnu. Se vzrůstající legitimitou také hodlá aktivněji působit v národním kontextu v rámci strategických a expertních debat.

TPEB ČR stala v roce 2021 řádným členem Evropské technologické platformy NetworldEurope ETP

NetworldEurope je novou Evropskou technologickou platformou (ETP) soustředící se na komunikační sítě a služby. Platforma navazuje na NetWorld2020 a její úspěšné působení při podpoře politik zvyšujících evropskou konkurenceschopnost v této dynamické oblasti. Komunikační sítě a služby

umožňují interakci mezi uživateli různých typů zařízení, mobilních nebo pevných, a naplňují tak požadavky na propojení moderní, digitální společnosti. **NetworldEurope ETP sdružuje 968 členů** z odvětví komunikačních systémů: 148 předních průmyslových společností, 356 inovativních malých a středních podniků, 331 předních akademických institucí a 133 dalších spolupracujících členů.

Hlavním cílem NetworldEurope ETP je pravidelně aktualizovanou výzkumnou agendou přispívat ke společným výzkumným programům na evropské a národní úrovni. V této souvislosti je třeba zdůraznit, že výzkum a vývoj v oblasti mobilních a bezdrátových, pevných a satelitních komunikačních sítí prostupuje mnoha dalšími technologickými sektory.

Členství v NetworldEurope dává všem členům možnost ovlivnit směr výzkumu související s budoucími komunikačními systémy v oblasti mobilních a bezdrátových sítí či nacházet příležitosti pro spolupráci v rámci výzkumu a vývoje v celé EU. Členové také získávají aktuální zprávy o výzkumných aktivitách a výsledcích, nabídky účastí v konsorciích či informace o možné finanční podpoře výzkumu a vývoje. V neposlední řadě se mohou účastnit konzultací a tvorby zpráv ETP NetworldEurope, které jsou komunikovány Evropské komisi. Řádní členové mají hlasovací práva na valné hromadě. Členové mají také možnost přispět a poskytnout zpětnou vazbu ke strategickému programu výzkumu a inovací NetworldEurope (SRIA).