


EVROPSKÁ UNIE
EVROPSKÝ FOND PRO REGIONÁLNÍ ROZVOJ
INVESTICE DO VAŠÍ BUDOUCNOSTI


# Projekt:

# Energetická a kybernetická bezpečnost

Etapa IV. - Legislativa

Praha , leden 2015

***Tento projekt je financován z ERDF prostřednictvím OPPI a ze státního rozpočtu ČR.***

# Shrnutí III. etapy

V rámci závěrečné čtvrté etapy projektu Energetická a kybernetická bezpečnost TPEB naplnila cíle uvedené ve Strategické výzkumné agendě a zároveň dále upřesnila akční plán svého působení v následujícím období. Klíčové aktivity této etapy byly trojího typu. První představovalo pokračování procesu nastartovaného především ve třetí etapě, který spočívá ve vytváření projektových konsorcií a vytváření projektových žádostí směřujících do českých i zahraničních výzev. V tomto kontextu TPEB vstoupila do konsorcia vedeného Univerzitou Tomáše Bati, které se uchází o účelovou podporu v rámci výzvy Bezpečnostního programu Ministerstva vnitra ČR.

Další konsorcia pak vycházejí z druhé aktivity TPEB v tomto období, kterou představuje další internacionalizace projektových a expertních aktivit. Zde TPEB navázala kontakty s izraelskými a čínskými partnery, přičemž cílem těchto snah je vytvořit další inovační konsorcia, která by zahrnovala instituce a firmy z těchto zemí.

Vstupem do projektových konsorcií v oblasti výzkumu, vývoje a inovací a jejich formováním TPEB naplňuje svůj nejvýznamnější dlouhodobý cíl, kterým je propojování výzkumné, vývojové a inovační základny s komerčním sektorem a koncovými uživateli, kteří většinou patří mezi státní instituce. V tomto smyslu se plně naplňují poslání a charakteristika TPEB jako public-private-partnership platformy.

Třetí zásadní aktivitou ukotvenou ve Strategické a výzkumné agendě a Implementačním akčním plánu bylo uspořádání velké projektové konference, na níž byla diskutována témata, která vzešla z práce projektového týmu na prvních třech etapách. Samotná konference se konala v prostorách PSP ČR za účasti mnoha českých a zahraničních expertů a reprezentantů relevantních institucí státní správy. Jedním z klíčových témat konference byla i implementace kybernetického zákona, který zároveň představoval jeden z pilířů činnosti projektového týmu v posledních měsících trvání projektu.

Tak jako v minulých etapách došlo i v závěrečné etapě k navázání nové spolupráce s českými i zahraničními institucemi, zejména pak s Národním bezpečnostním úřadem, The Israeli-Europe R&D Directoriate či Česko-izraelskou smíšenou obchodní komorou a Smíšenou česko čínskou komorou vzájemné spolupráce.

# Shrnutí výsledků III. etapy

Jak již bylo zmíněno v předchozích zprávách, Strategická výzkumná agenda a Implementační akční plán TPEB v kontextu projektu energetická a kybernetická bezpečnost počítají s aktivitami rozdělenými do 4 hlavních oblastí – komunikační technologie, kybernetická bezpečnost, technologie sledování prvků kritické infrastruktury a fyzická bezpečnost. Jakkoli je toto dělení analyticky vhodné, na úrovni konkrétních projektových žádostí se hranice mezi těmito jednotlivými oblastmi logicky stírají. Nejvýznamněji se to týká kybernetické bezpečnosti a komunikačních technologií, které jsou povětšinou v projektových výzvách vedeny pod společnou hlavičkou ICT.

V souladu s implementačním plánem a v rámci naplňování Strategické výzkumné agendy došlo v rámci první fáze projektu prostřednictvím analýz stávajícího stavu daných oblastí k identifikaci klíčových priorit, které by měly být nadále rozvíjeny. Ve druhé fázi pak byla v rámci studií rozvinuta problematika standardizace spojená s těmito prioritami. Tato expertní činnost umožnila přikročit ve třetí fázi k iniciaci projektových žádostí a k formování mezinárodních konsorcií. Finální čtvrtá fáze pak měla v návaznosti na předchozí etapy věnovat pozornost problematice legislativy. Do čtvrté etapy se však výrazně přenesla také projektová dynamika, která charakterizovala etapu třetí.

## Dosažené cíle:

- V rámci oblastí kybernetické bezpečnosti, komunikačních technologií a fyzické bezpečnosti byl úspěšně podán projekt **Resilience 2015: dynamické hodnocení odolnosti souvztažných subsystémů kritické infrastruktury**, který soutěží o účelovou podporu v rámci programu Bezpečnostního výzkumu Ministerstva vnitra ČR.

- V rámci všech oblastí byla uspořádána velká projektová mezinárodní konference **Energy & Cyber Security in EU**, která proběhla 9. listopadu 2014 v prostorách PSP ČR.

- TPEB v součinnosti s Národním bezpečnostním úřadem připravuje **systém analýzy připravenosti infrastrukturních firem na požadavky kybernetického zákona**, který vstoupil v platnost 1. 1. 2015.

- TPEB připravila několik dalších iniciálních verzí projektových žádostí, které budou v návaznosti na výzvy poslány do projektových soutěží Technologické agentury ČR a dalších programů.

- TPEB pracovala na vytváření dalších projektových žádostí a konsorcií, která budou usilovat o projekty v rámci výzev programu H2020

- TPEB nadále rozpracovávala výzkumně-vývojovou nabídku pro vznikající programy česko-čínské a česko-izraelské spolupráce.

Zástupci TPEB se účastnili několika konferencí a workshopů, kde prezentovali schopnosti, aktivity a postoje TPEB k otázkám týkajícím se ochrany kritické infrastruktury.

# Shrnutí aktivit v rámci jednotlivých kapitol

## Kybernetická bezpečnost

Kyberkriminalita se stala společenským problémem, denně jsme informováni o různých formách zcizení citlivých dat – může se jednat o přístupová data k účtům on-line her nebo čísla platebních karet i s jejich ochrannými údaji. Pomalu si zvykáme na změnu, kdy nelze útokům zcela zabránit. Změnila se i otázka z dříve používané pokud na nás zaútočí na kdy na nás zaútočí. Dnes všichni víme, že je otázkou času kdy na prostředky společnosti bude směrován kybernetický útok. Bohužel, se nejedná jen o „zábavu“ hrstky hackerů, ale o výnosný mezinárodní obchod. Vzájemné propojení lidí, zařízení a organizací otevírá nová a nová zranitelná místa. Nové technologie a měnící se obchodní požadavky vyžadují zcela odlišný přístup k bezpečnostním opatřením.

Bezpečnost počítačové sítě byla historicky budována na jejím perimetru. Všichni vnímali nebezpečí přicházející z internetu. Nejinak tomu bylo u administrátorů jednotlivých systémů, kteří nastavovali systémy tak, aby byly chráněny proti vnějšímu nepříteli. Velká část informačních systémů, někteří analytici ve svých studiích uvádějí až 100%, jsou infikovány škodlivými a nebezpečnými kódy. Koncové body se tak stávají součástí sítí útočníků. Prostřednictvím těchto programů nainstalovaných v koncových stanicích útočníci získávají citlivé údaje, popřípadě je využívají k rozesílání spamu a vedení útoků na ostatní uživatele.

Postupem času jsme zvykli, že v každé síti se na zajištění bezpečnosti podílejí řada zařízení - Firewaly, IDS, IPS jejichž hlavní funkce si připomeneme v následujících odstavcích.

### *Firewall.*

Firewally, česky něco jako „bezpečnostní brána“, jsou to zařízení nebo software jejichž úkol je poměrně jednoduchý oddělit provoz mezi dvěma sítěmi. Typicky mezi naší domácí sítí a internetem. Podle předem definovaných pravidel propouští jedním nebo druhým směrem data. Brání tak zejména před neoprávněnými průniky do sítě a odesílání dat ze sítě bez vědomí a souhlasu uživatele. V prostředí domácností a malých firem je instalace bezpečnostní brány nejefektivnějším a nejdůležitějším prvním krokem při ochraně počítačové sítě. Firewall pracuje na 3. a 4. vrstvu tzv. OSI modelu - kontroluje procházející provoz na základě IP adres a TCP/UDP portů. K tomu kontroluje například také to, jestli procházející provoz odpovídá standardům podle RFC (správná velikost paketu, pořadí jednotlivých částí paketu, atd.). .

Na co klasické firewally nestačí? Firewally byly první široce použité zařízení využívané k ochraně před útočníky od začátků Internetu. Úkolem firewallu je kontrolovat provoz a rozhodnout, jaký provoz může projít zvenčí dovnitř a zevnitř ven. Zatímco síťový provoz se v posledních deseti letech významně změnil. Velká část provoz na internetu je web-based. A to je jeden z důvodů proč se tradiční port-based firewally v podstatě stávají "slepé". To znamená, že nemohou rozlišovat různé typy provozu, které používají stejný port, nemohou odhalit aplikace tunelované v jiných aplikacích a oni nemohou analyzovat obsah v

zašifrovaných paketech. Firewally již neodpovídají potřebám řízení provozu a firemní bezpečnosti.

Na tuto situaci reagují Next Generation Firewally. Veškerý provoz je řízen na úrovni aplikací a nikoliv na úrovni TCP/UDP protokolu. Firewally využívají databází aplikací, která je pravidelně aktualizována, podobně jako databáze antiviru, nebo IPS/IDS. Databáze aplikací je alfou a omegou NG firewallů.

### *Intrusion Detection System*

Další z používaných systémů je Intrusion Detection System (IDS), jenž ve svých počátcích monitoroval provoz v počítačových síti. Klíčovým prvkem IDS je senzor, který obsahuje mechanismy pro detekci škodlivých a nebezpečných kódů. Později byl doplněn o funkcionalitu aktivní reakce na případné bezpečnostní hrozby. IDS systémy se liší v závislosti na mnoha kritériích. Například je možné rozdělit tyto systémy[1] podle systému, který monitorují na:

a) Network based IDS - jsou zařízení které mohou sledovat celou síť z několika vhodně vybraných zařízení. Většinou jsou tato zařízení pasivní, průběžně sledují veškerý provoz na síti. Zařízení jsou velice jednoduché na instalaci, jsou odolná vůči útokům a dokonce neviditelná pro útočníky.Network-based IDS nemusí být schopen sledovat a analyzovat veškerý provoz na velké, zatížené síti a proto může přehlédnout útoky jež se během špičky objeví. Další nevýhodou je omezení týkající se vysokorychlostních sítí, tzv. switched base networks které neumí monitorovat. Velkou překážkou pro tato zařízení jsou i šifrovaná data. Zařízení vyžaduje aktivní zapojení správců sítí.

b) Host-based IDS analyzuje aktivity na zařízení na kterém je nainstalován. Může určit, který procesor nebo uživatelé se podílí na škodlivých aktivitách. Host-based IDS dokáže detekovat útoky nezjistitelné zařízením network-based IDS. Dokáže analyzovat i zakódovaný provoz. Mezi nevýhody patří poměrně velký provoz který zařízení generuje na sledované síti v jehož důsledku dochází ke snížení výkonu sítě. Cílem útočníků bývá samotné zařízení, kdy útočníci taková zařízení vyřadí z provozu.

c) Application based IDS, jak samotný název napovídá toto zařízení se zaměřuje na analýzu událostí které nastaly při běhu konkrétní aplikace. Útoky odhaluje za pomoci analýzy logů aplikace, dokáže identifikovat mnoho typů útoku nebo podezřelé aktivit. Nevýhody jsou podobné jako u předcházejícího typu zařízení tj. náchylnost k útoku a velké zatížení zařízení na kterém je nainstalován.

[1] "Deploying and Tuning Network Intrusion Detection Systems." Intrusion.com White Paper

IDS analyzuje[2] získávané informace a porovnává je s již známými hodnotami. Svým způsobem funguje podobně jako antivirové programy, které pracují s databází známých škodlivých kódů. IDS je v takovém případě vybaven signaturami známých útoků.

a) IDS detekující anomálie sleduje odchylující se segmenty - to zpravidla bývají varovné příznaky, že se děje něco "nenormálního".Tento systém je schopen na rozdíl od systému detekce známých útoků detekovat nové, doposud v datových vzorcích nespecifikované útoky.

b) Speciální případ pak představuje heuristická analýza, jenž využívá statistik získaných z provozu. V případě vyhledávání výjimek z pravidel systém IDS kontroluje komunikaci a konfrontuje ji s definovanými pravidly. Toto řešení umožňuje vyhledávání anomálií na poli záměrné deformace komunikace mezi útočníkem a jeho potencionálním cílem.

c) Systémy IDS dále dělíme podle místa působnosti na host-based a network-based. Dalším způsobem dělení IDS pasivní a aktivní systémy.

Některé systémy IDS mají implementovány určité obranné mechanismy (ukončení TCP spojení, jiná konfigurace firewallu po zjištění útoku aj.), ale zpravidla nejsou schopné reagovat s dostatečnou rychlostí, protože mezi detekcí útoku a pokusem o jeho zablokování uplyne krátká, leč významná doba.

### *Intrusion Prevention System*

Intrusion Prevention System (IPS) - je v podstatě pokračovatelem systému IDS. Hlavním rozdílem je schopnost ve velmi krátké době aktivně blokovat identifikovaná nebezpečí tj. IPS proaktivně brání průniku. Systémy IPS zvládají nejen monitoring a reporting zejména pak přijímají různé protiakce. Nepoužívají k likvidaci útoků žádné další systémy, ale s nebezpečím se vypořádají sami.

K základním úkolům systémů IPS patří:

a) Identifikovat neautorizovaný provoz založený na signaturových vzorcích

b) Identifikovat neautorizovaný provoz založený na detekci anomálií v protokolech

c) Ukončit nebo znesnadnit služby spojené s nežádoucí činností. V této oblasti spočívá hlavní těžiště činnosti IPS. V případě odhalení útoku přijmout odpovídající protiopatření, a to bez prodlení.

IPS potřebuje dohled v podobě správce, který bude systém průběžně dolaďovat na základě dosažených výsledků (falešné poplachy, resp. nezaregistrované útoky). Stejně tak je nutné IPS stále doplňovat o nové informace, aby byl schopen se vypořádat se všemi aktuálními hrozbami.

[2] Eagle, Liam. "Enabling the Defense in Depth Security Strategy." The Web Host Industry Review.

Výše uvedené systémy jsou založené na signaturách, tedy databázi známých hrozeb. Na kvalitě této databáze záleží účinnost těchto systémů, které jsou sice téměř bezchybné, ale nemohou být schopny reagovat na nové hrozby neobsažené v databázi. Nejenom z tohoto důvodů získávají na popularitě systémy založené na Network Behavioral Analysis tedy analýze chování.

### *Network Behavior Analysis (NBA)*

Řešení je založené na vyhodnocování provozních statistik, pomoci kterých upozorňuje na neobvyklé chování. Hlavní výhodou proti používaným řešením je orientace na celkové chování systému, což umožňuje získat ucelený pohled na celou IT infrastrukturu a reagovat i na dosud neznámé či specifické hrozby v síti.

Nejlépe jsou rozdíly viditelné při porovnání systémů Intrusion Detection a Anomaly Detection. Oba systémy hledají tzv. "špatné věci" v systému nebo síti, situace které mohou být potenciální bezpečnostní incidenty. Výsledky jsou stejné - podezřelé chování je označeno a předáno správci systému k dalšímu prošetření. Nicméně i přes tyto podobnosti, každý nástroj funguje zcela odlišně. IDS používá definovaný soubor pravidel a filtrů, které byly vytvořeny tak, aby rozpoznal konkrétní hrozby. Oproti tomu ADS porovnává získané údaje s údaji získanými dlouhodobým provozem a upozorňuje na případné odlišnosti. Zatímco IDS hledá rozdíly oproti známým hrozbám (signaturám) ADS hledá neobvyklé chováni porovnáním se statistikami . ADS má potenciál odhalit nové, neznámé, nebo neveřejné hrozby.

### Anomaly Detection System

Jak můžete vidět, ADS je mocný nástroj, který doplňuje stávající systémy jako je IDS, firewall nebo IPS. Ale jak to zjistit, co je normální chování? Podle čeho označuje činnost divné? Odpověď na tyto otázky je klíčem k efektivní ADS. Rozdíl spočívá v metodách pro stavbu profil systému. K dnešnímu dni, modelování normálního chování je založeno na dvou přístupech: statistickém a specifikacím. Obojí lze aplikovat na jednotlivé stroje, sítě, protokoly nebo dokonce aplikace. Nicméně techniky používané pro generování profilu jsou zcela odlišné.

a) Založené na statistikách.

Tento přístup používá statistik k nastavení referenční bodu chování systému. Proces začíná učením. Jsou sledovány konkrétní události ve sledovaném prostředí, jako jsou systémová volání, síťový provoz či aplikace po určenou dobu. S využitím matematických metod se definuje referenční bod. Výsledkem je základní nastavení pro některé proměnné chování daného systému. Zaznamenaná data jsou převedena do stejné kvantitativní metriky a porovnávána s výchozí hodnotou. Pokud odchylka překročí určitou hranici, událost je označena jako anomální.

Princip ADS založeného na statistikách vypadá jednoduše, ale pouze na první pohled. První náročný úkol je rozhodování o nejvhodnější metodě pro měření odchylek. Dalším těžkým úkolem je vícerozměrná korelace. Zjednodušené vysvětlení je uvedeno výše, kde jsme měřili pouze jeden prvek komplexního systému. Aby bylo možné generovat skutečně užitečná data je nutná znalost více proměnných a jejich vztahů. Následně pomocí protokolové analýzy zjistit, zda-li útočník získal platný účet k přenosu souborů. Jak je patrné učení ADS je velice obtížný úkol. Ale je tu ještě větší problém pro detekci anomálií na bázi statistik - měnící se prostředí. Uživatelé jsou přidáváni, služby jsou odstraněny, nová zařízení jsou implementována. Každý z těchto faktorů vyžaduje aktualizaci profilu. Ve velkém, různorodém prostředí ADS se neustále učí.

b) Založené na specifikacích

Metoda založená na specifikacích závisí méně na matematice a více na lidském pozorování a zkušenostech. Tato metoda používá logického popisu očekávaného chování při sestavení profilu. S využitím těchto postupů by mohl správce sestavit seznam podobný pravidlům a podpisům užívaných v systémech IDS.Stav který vybočuje z očekávaného chovaní by byl označen za anomální. Je to koncept podobný postupu známého z nastavení firewallů "Deny-all", kde je blokována veškerý nežádoucí provoz a je povolen jen výslovně specifikovaný provoz. A ADS založené na specifikacích rozšiřuje tuto myšlenku více prvků systému - aplikace, servery, síťový provoz a tak dále. Místo blokování událost, by vytvořil upozornění.

Přínosy systémů využívající NBA

a) Efektivnější procesy - problémy jsou odhaleny včas. IT odborníci se mohou věnovat rozvoji infrastruktury a poskytovaných služeb místo toho aby řešili operativními problémy.
b) Úspora nákladů - významné snížení pracnosti správy IT infrastruktury minimalizace nákladů vyplývajících z náprav škod způsobených bezpečnostními incidenty v síti.
c) Bezpečnější infrastruktura - infrastruktura je lépe chráněna před novými bezpečnostními hrozbami (sociální inženýrství, útoky zevnitř, úniky dat, odchozí SPAM, …).

### *České řešení FlowMon ADS*

FlowMon ADS[3] je moderní systém detekce anomálií a nežádoucích vzorů chování v síti založený na standardu NetFlow, jež má za úkol zvýšení vnější i vnitřní bezpečnosti počítačové sítě. Jeho hlavní výhodou oproti běžným systémům je orientace na chování zařízení nasíti, nikoliv vlastní obsah komunikace, což umožňuje reagovat na dosud neznámé nebo specifické hrozby, pro které není dostupná signatura.

Jako základní stavební kámen FlowMon ADS byl zvolen databázový systém CACHÉ od společnosti InterSystems. InterSystems CACHÉ je inovativní objektová databáze vyznačující se extrémním výkonem. CACHÉ umožňuje rychlý vývoj webových aplikací, mimořádnou

[3] https://www.invea.com/cs

rychlost zpracování transakcí, masivní rozšiřitelnost a dotazy na transakční údaje v reálném čase, a to vše s minimálními požadavky na

administraci. Otevřenost a unikátnost architektury CACHÉ nám umožňuje dosahovat takové průchodnosti dat proudících datovou sítí, které jiné databáze jednoduše nemají šanci v reálném čase byť jen načíst, natožpak zaindexovat a průběžně aplikovat detekční algoritmy“.

Za bezpečnou je dnes považována taková organizace, která má nasazen nejen firewall a intrusion prevention systém, ale také systém pro automatickou detekci anomálií na základě statistik o síťovém provozu. Systémy tohoto typu se souhrnně nazývají NBA (Network Behavior Analysis) a umožňují detekovat hrozby, proti kterým jsou ostatní bezpečnostní nástroje neúčinné – jedná se například o malware psaný na míru, viry a botnety nepodchycené antiviry, sociální inženýrství a další hrozby spojené s rizikem od vlastních vnitřních uživatelů sítě. Informace o neobvyklých chování zařízení v síti mohou indikovat i potenciální nebezpečí hrozící ostatním organizacím se kterými je daná organizace "propojena". A tak se daná organizace může stane důvěryhodnější v dnešním on-line světě.

### *Přístup k informačním systémům.*

V dnešní dynamické době kdy být "on-line" je prakticky nutností a zajištění bezpečnosti systémů je jedním z klíčových úkolů pro odborníky v IT. IT odborníci vykonávají řadu činností jenž jsou nezbytné pro zajištění správné a bezpečné činnost řady systémů, aplikací. Z pohled těchto pracovníků se jedná o nepříliš zajímavou a vzrušující práci jako je aktualizace všech systémů, šifrování citlivých dat, pravidelné zálohování a mnoho dalších.

Podle studii předních konzultačních společností, mezi všemi aktivitami získává na důležitosti řízení přístupu k síťovým prostředkům (Network Access Control - NAC). Každý uživatel se setkal s nepříjemnou situací, kdy nemůže spustit aplikaci nebo nemá přístup k firemním datům. Navíc zaměstnanci požadují přístup k firemním datům nejen s využitím zařízení zaměstnavatele ale i vlastních. Všude přítomné mobilita, cloud a řešení jako BOYD (z anglického "Bring Your Own Device" ) požadavky na pracovníky IT neustále zvyšují. Na rozdíl od rozpočtů, které v lepším případě zůstávají stejné.

Na první pohled rozporuplné požadavky nemají jednoduché řešení. Jediná možnost je maximum činnosti zautomatizovat a tím snížit požadavky na IT odborníky, kteří mohou soustředit na jiné oblasti. Z praxe víme, že není možné do budoucna spoléhat a řešení založené na Excelu a tištěných tabulkách.

#### Network Access Control

Network Access Control (NAC) je řešení zabezpečení sítě navržené tak aby umožňovalo poskytnout, omezit nebo zakázat přístup k síťovým zdrojům prostřednictvím politik definovaných uživateli.

### Next-Gen NAC

Next-gen NAC[4] není lék na všechny neduhy, ale umožňuje v reálném čase monitorování, řízení a tím pomáhá řešit četné IT výzvy. Co je Next-Gen NAC? Next-Gen NAC rozšiřuje možnosti současných NAC produktů přidáním multi-dimenzionální řídící platformy, která nabízí interoperabilitu v oblastech bezpečnosti sítě a architektury. Next-Gen NAC nabízí tři hlavní funkce:

a) Visibility Network. Next-gen NAC poskytuje uživatelům bezprecedentní, okamžitou a inteligentní správu majetku. To zahrnuje všechna síťová zařízení - PC, notebooky, servery, virtuální stroje, mobilní zařízení a síťovou infrastrukturu. Poskytuje informace o typu zařízení, uživateli, jeho umístění, aplikacích a řadu dalších detailů.
b) Granular policies. Next-gen NAC umožňuje konfigurovat cokoliv dle výběru politik založených na specifických potřebách organizace. Politiky mohou být použity pro uživatele (a skupiny jednotlivé uživatelé), zařízení ale i kategorie zařízení nebo pro aplikace.
c) Mittigation. Uživatelé Next-gen NAC mají téměř neomezené množství způsobů jak snížit riziko vytvořené neoprávněným nebo nevyhovující zařízení.

### *DDI*

Co je ukryto za zkratkou DDI - jedná se o tři velice důležité systémy DNS, DHCP a IPAM (Domain Name System - DNS, Dynamic Host Configuration Protocol - DHCP, Internet Protocol Address Management - IPAM.

Jsou to systémy, které pomáhají organizacím jednak efektivně spravovat jejich IP adresní prostor jednak zlepšují celkovou dostupnost a snižují provozní náklady Existuje několik různých typů dodavatelů DDI - velcí výrobci Microsoft, Cisco, Alcatel-Lucent a BT a středně velcí dodavatelé Infoblox a BlueCat a menší nebo regionální dodavatelé EfficientIP, Nixu Software. V Čechách se této problematice úspěšně věnuje společnost Novicom.

Jak se pozná dobře fungující systém? Vůbec o něm nevíte a přesto se s ním setkáváte každý den v podnikových sítích. Pomalý server DHCP zkomplikuje komunikaci mezi lidmi připojenými k síti a tak přispívá k vytváření neproduktivního pracovní prostředí. V případě výpadku DHCP serveru je vstup lidem do sítě zabráněn úplně, což při dnešní závislosti na systémech znamená praktické zastavení činnosti Správně fungující systém DDI pružně a efektivně přiděluje IP adresy. Je zdrojem všech informací, jenž potřebují zařízení připojené do podnikové sítě. Rychle a bez námahy překládá názvy sítí na IP adresy.

Řešení DDI mohou být samostatná zařízení, software nebo dokonce řízené služby. Mohou také být integrovány s několika dalšími virtuálními službami. Administrátoři ovládají pomocí webového GUI a (Graphical User Interface) téměř každý aspekt jejich DNS, DHCP a správu IP adres.

Důležitým parametrem pro řešení přístupu je vysoká dostupnost tzv. High Availability Pro dosažení vysoké dostupnosti je využíváno více zařízení z nichž jedno je hlavní a jedno nebo více vedlejších. I databáze, které se používají pro DNS, DHCP jsou navrženy tak splňovaly

[4] ForeScout Releases Definitive Guide to Next-generation Network Access Control

požadavky na vysokou dostupnost. Jsou sjednoceny a aktualizovány současně v celé síti. Což vede k zajištění jejich efektivnosti a redundance, to vše pro minimalizaci výpadků a zajištění jednotnosti.

*DNS / DHCP:*

Jak již bylo zmíněno, řešení DDI sjednocuje a centralizuje služby DNS / DHCP a zajišťuje vysokou dostupnost těchto služeb. Mnoho řešení DDI umožňují DNS a DHCP službám sdílet jednu databázi s cílem pro lepší integraci mezi těmito dvěma službami. DDI mimo jiné umožňuje rozložení zátěže na více zařízení. V praxi velmi využívanými pomocníky jsou tzv. "šablony" umožňující společnostem automatizovat a standardizovat vytváření konfigurací v síti.

*IP Address Management:*

Většina řešení DDI je dodávána s přehledným grafickým uživatelským rozhraním, který graficky zobrazuje všechny IP adresy v síti. Tato řešení umožňují administrátorům lokalizovat IP adresy zařízení kdekoli ve své síti. Pokud administrátoři mají takovýto jednotný a centralizovaný nástroj pro správu IP adres k dispozici lze snadno zjistit kdo, co a kdy v síti udělal. IP adresy jsou hierarchicky uspořádány. Některá řešení dokonce nabízejí API, které se integrují s externími aplikacemi jako Google Maps . Lze tak snadno zjistit kde přesně se libovolná IP adresa nachází.

Pro každou IP adresu, IPAM (IP Address Management) modul spravuje jednotlivé záznamy, které obsahují informace jak hostitelských jmen, MAC adresy, odpovídající portů přepínače, info o zařízení, datum a čas zadání zařízení, atd. IPAM modul kontroluje nekonzistence a překrývající se IP adresy a označuje konflikt IP adres, které musí být dořešeny správcem. Pomáhají také identifikovat nepoužívané IP adresy v síti. Dále IPAM modul sleduje využití IP adres, tedy situace kdy se blíží jejich plné využití v každém sub-síť. Správci mohou rozdělit, a znovu přidělovat IP adresní prostor bez obav z IP adres konfliktů.

Bez pečlivého řízení, základ síťových služeb - DNS, DHCP a IP správa Adres (DDI) může velmi rychle stát nepřehledná a obtížně zvladatelná. Jakákoliv změna v síti se stane noční můrou. Bez spolehlivého DDI kritické aplikace, včetně e-mailů, webových služeb, ERP, CRM nemohou fungovat. Integrace do jediného systému vede jak ke snížení chybovosti, zvýšení efektivity, zajištění kontinuity služeb a zcela zásadním způsobem ovlivňuje bezpečnost sítě.

***Bezpečnost dat v cloudu.***

Cloud computing ještě stále řada odborníků považuje za méně bezpečný než klasické řešení. Analytici upozorňují, že až dosud došlo k jen velmi nízkému počtu narušení bezpečnosti dat ve veřejných cloudech – naopak většinou k němu dochází právě v datových centrech přímo u zákazníků.

V podstatě si pod tímto termínem skrývají dvě zásadní otázky, kde jsou firemní data uložená, jak jsou tato data zabezpečená.

### Firemní data a jejich umístnění

Lokalita ve kterém mají organizace uložená data je stále velice důležitá i když analytici předpovídají pokles důležitosti. Ve svých předpovědích uvádějí, že v roce 2020 bude (fyzické) místo ve kterém má daná organizace uložena svá data nahrazeno logickou lokalitou v kombinaci s právní a politickou lokalitou. Manažeři společností musí učinit rozhodnutí a ohodnotit rizika společně s vlastníky, právníky, zákazníky, regulačními orgány, zástupci zaměstnavatelů, obchodníky a veřejností.

Prakticky existují čtyři typy umístění dat[5]:

a. Fyzické umístění: Historicky, lidé přirovnáván fyzickou blízkost s fyzickou kontrolu nad daty a bezpečnost. I když každý ví, že k lokálně uloženým datům lze přistupovat vzdáleně. Touha po fyzické kontrole stále existuje a to zejména u regulačních orgánů..
b. Právní umístění: Mnoho IT odborníků si stále nejsou vědomi konceptu právního umístění. Právní poloha je určena právnickou osobou, která kontroluje data. "Prohlášení jako" je nelegální ukládat data v zahraničí, jsou často výklady právního jazyka, který je mnohem méně jasný.
c. Politická umístění: otázky mezinárodní politické rovnováhy jsou důležité pro subjekty veřejného sektoru, nevládních neziskových organizací (NNO), společnosti, které slouží milionům spotřebitelů.
d. Logické umístění: To se ukazuje jako nejpravděpodobnější řešení mezinárodních dohod o zpracování dat které určuje kdo má přístup k datům. Například Česká společnost podepíše smlouvu s Irskou dceřinou společností poskytovatele cloudových služeb USA si plně uvědomuje že zálohováná data jsou fyzicky uložena v datovém centru v Indii. Zatímco právní umístění poskytovatele by Irsko, politický umístění by USA a fyzické umístění bude Indie, logické umístnění všech data je stále v České republice. V tomto případě stalo, všechna přenášená data a všechny uložené údaje v Indii bude muset být šifrovány s klíči, které jsou uložené v České republice. Takovéto uspořádání zvýší náklady a složitost a zároveň sníží použitelnosti funkcí jako je náhled a vyhledávání, mobility a latence.

"Žádný z typů umístění dat neřeší sám o sobě problém s jejich uložení," uvádí pan Casper. Budoucností jsou tzv. hybridní organizace. To jsou takové organizace které budou používat více lokalit s více modely poskytování služeb.

### Bezpečnost uložených dat

Mnohé podniky ověřují jak mohou profitovat z cloud computingu. Cloudové služby jako jsou Saas, PaaS a IaaS přinesou zákazníkům řadu výhod, včetně úspor z rozsahu, optimalizaci řešení a úspory nákladů. Model zaplať za využitou kapacitu služeb je velmi atraktivní,

[5] Gartner press release Physical Location of Data Will Become Increasingly Irrelevant in Post-Snowden Era

protože umožňuje organizacím plánovat budoucnost bez obrovských počátečních investic do infrastruktury.

Přes velký zájem o tyto služby se doposud nepodařilo přesvědčit velkou část zákazníků o bezpečnosti uložených dat. Ubezpečení poskytovatelů služeb, která se objevují po úspěšném útoku na data zákazníků uložená v cloudu se míjejí účinkem.

Data uložená v cloudech poskytují tolik požadovanou flexibilitu tj. jsou přístupná prostřednictvím internetového prohlížeče v libovolném zařízení (jakémkoliv počítači, mobilním telefonu, tabletu). Další nezbytnou funkcionalitou je synchronizace mezi všemi zařízeními uživateli. Velká část aplikací je sice připravena pracovat se šifrovanými daty, ale jen malá část úložišť je připravena pracovat s šifrovanými daty. A tak otázky bezpečnosti týkající se sdílení médií s jinými společnostmi, přenosy dat mezi virtuálními stroji jsou stále nedořešené. Další nedořešenou oblastí je přesun dat mezi poskytovateli (při změně poskytovatele služeb).

### *Bezpečnost v nejběžněji používaných úložištích*

Služby dnes nejběžněji používaných úložišť jako je Dropbox, Google Drive, One Drive jsou praktické, efektivní ale jak je velmi dobře známo ne příliš bezpečné. Soubory nejsou šifrované, služby šifrují přenos souborů mezi uživatelem a úložištěm. Toto zabezpečení chrání před datovým odposlechem, ne však před zcizením dat z úložiště. Svým způsobem se na tomto stavu podílejí i sami uživatelé, kteří vyžadují komfortní práci s uloženými dat.

### Ověření identity

Jednofaktorové nebo dvoufaktorové ověření identity? Odborníci na bezpečnost v odpovědi na tuto otázku jasno. Jednofaktorové ověření identity je nedostačující. Pokud některá úložiště nabízejí dvoufaktorové ověření identity, tak pouze volitelně. Pohodlí nás uživatelů těchto služeb dostává přednost před bezpečností.

Například Google dvoufaktorové ověření identity pro své služby, včetně Google Drive nabízí, ale pouze volitelně. Microsoft již aktivně na dvoufaktorové ověření identity přešel, ovšem zatím jen pro citlivé operace. Plošné využívání například pro přístup k úložišti zůstává volitelné. Apple pro iCloud a další služby rovněž nabízí dvoufaktorové ověření identity ale opět pouze volitelně.

Odborníci dlouhodobě upozorňují na další slabé místo ochrany řady služeb (nejen úložišť). Tím je změna hesla po zodpovězení kontrolní otázky. Dříve tuto ochranu mohl obejít útočník, který svou oběť dobře znal. Dnes kdy jsou odpovědi na nejčastější kontrolní otázky dohledatelné na sociálních sítích je i tato forma pomoci dalším bezpečnostním rizikem.

## Šifrování

Dvoufaktorové ověření identity snižuje možnost zneužití hesla, ale v žádném případě nepomůže v případě, kdy k datům uloženým v cloudovém úložiště získá přístup nepovolaná osoba.V tomto případě ochranu uložených dat lze zajistit výhradně šifrování. Pro uložená data šifrování prakticky nabízí každý poskytovatel těchto služeb, ale skutečnost je jiná. Například populární služby Dropbox, Google Drive či OneDrive šifrují pouze přenos souborů mezi zařízením uživatele a cloudovým úložištěm. Pokud však selže zabezpečení, může nešifrované soubory teoreticky získat kdokoliv.

# Komunikační technologie

## *Úvod*

Vzhledem k inženýrským činnostem, na něž se technické univerzity soustřeďují, bývá náš pohled dominantně zaměřen na řešení technologických problémů souvisejících s elektronickou komunikací. Do sféry těchto problémů přirozeně patří zajištění bezpečnosti a spolehlivosti komunikace, ochrana komunikace před úmyslným či neúmyslným narušením či neautorizovaným přístupem.

Studovaná technická řešení následně procházejí procesem ověřování, validace a evaluace se snahou dospět k všeobecně přijatelným standardům a normám. Problematika standardizace a normotvorby v oblasti elektronických komunikací byla podrobně diskutována v předchozí etapě projektu.

Znatelně však chybí přesah technického pohledu do legislativní oblasti a snaha o mezioborový přístup k řešení souvisejících problémů. Zmíněným dvěma aspektům se proto věnujeme v následujících odstavcích.

## *Legislativní aspekty*

Lídrem ve vývoji informačních a komunikačních technologií jsou Spojené státy americké. Vzhledem k vyspělosti amerického vývoje a výroby informačních a komunikačních systémů a vyspělosti trhu informačních a komunikačních služeb se americké právní prostředí s jistým předstihem setkává s potřebou definování právního prostředí provozu a poskytování informačních a komunikačních služeb. Je proto vždy dobré seznámit se s příklady amerických právních norem, které s oblastí informačních a komunikačních technologií souvisejí.

V následujících odstavcích proto zmíníme zákon na ochranu soukromí v elektronické komunikaci (*Electronic Communications Privacy Act*, ECPA) a zákon o vnitřní komunikaci (*Stored Communications Act*, SCA). Následně navážeme českými zákony – zákonem o ochraně osobních údajů a zákonem o kybernetické bezpečnosti.

### Zákon na ochranu soukromí v elektronické komunikaci

Zákon na ochranu soukromí v elektronické komunikaci (*Electronic Communications Privacy Act*, ECPA) byl přijat v roce 1986, aby rozšířil vládní pravidla týkající se telefonních hovorů na přenos elektronických dat mezi počítači a nově přidal pravidla zabraňující přístupu k obsahu vnitřní elektronické komunikace.

Primární motivací k přijetí zákona na ochranu soukromí v elektronické komunikaci bylo zabránit neautorizovanému přístupu vládních úřadů k obsahu soukromé elektronické komunikace.

Elektronická komunikace je v zákoně definována jako libovolný přenos znaků, signálů, písma, obrazů, zvuků, dat či myšlenek libovolným fyzikálním mechanismem – po vedení, bezdrátově, elektromagneticky, foto-elektronicky či foto-opticky. Vyloučeny jsou orální komunikace, pípání pageru a další atypické neplnohodnotné formy komunikace.

Zákon dominantně upravuje legislativní aspekty přenosu informace. Aspekty uchovávání informace legislativně upravuje zákon o vnitřní komunikaci.

### Zákon o vnitřní komunikaci

Zákon o vnitřní komunikaci (*Stored Communications Act*, SCA) je zákonem, který se vztahuje k dobrovolnému i nucenému zveřejnění obsahu vnitřní drátové a elektronické komunikace a přenosových záznamů, jež jsou v držení poskytovatelů internetových služeb. Zákon vstoupil v platnost v říjnu 1986.

Čtvrtý dodatek ústavy USA chrání právo občana na ochranu osobních údajů. Z pohledu online zpracování informací se tento dodatek jeví jako nedostatečně silný, neboť se vztahuje ke konkrétnímu času a prostoru, takže postihnout virtuální kybernetický prostor je problematické.

Navíc uživatelé obecně svěřují bezpečnost online informací poskytovatelům internetových služeb jako třetí straně. To bývá chápáno jako vzdání se nároku na soukromí. Proto byl přijat zákon o vnitřní komunikaci, který zesiluje ochranu osobních údajů ve vztahu k emailové a jiné digitální komunikaci.

Zákon o vnitřní komunikaci zavádí trestní postihy osob, které vědomě a bez autorizace nebo díky zneužití autorizace získají, pozmění či znepřístupní informace přenášené či uložené v elektronických komunikačních systémech.

Zákon o vnitřní komunikaci popisuje podmínky, za kterých může poskytovatel internetových služeb dobrovolně odkrýt komunikaci či záznamy svého zákazníka. Obecně má poskytovatel zakázáno odkrýt další osobě (fyzické či právní) jakoukoli část obsahu komunikace, jež probíhá v rámci poskytované služby. Zveřejnit lze pouze informace, které nesouvisejí s obsahem komunikace (např. emailové adresy komunikujících), a to výhradně vládním úřadům. Neomezeně lze zveřejnit informace nesouvisející s obsahem pouze v případě komunikace veřejných institucí, univerzit a podobných institucí.

V zákoně jsou rovněž specifikovány podmínky, při jejichž splnění může vláda přinutit poskytovatele internetových služeb k prozrazení identity zákazníka a informace nesouvisející s obsahem.

Zákon rovněž definuje, jak dlouhou dobu může poskytovatel uchovávat neotevřené, nepřečtené emailové zprávy. V zákoně o vnitřní komunikaci byla tato lhůta stanovena na 180 dnů.

Z pohledu možností vlády vynutit si zveřejnění obsahu komunikace rozlišuje zákon o vnitřní komunikaci mezi službami elektronické komunikace (je vyžadováno povolení k domovní prohlídce) a vzdálenými výpočetními službami (postačuje soudní obsílka).

### Zákon o ochraně osobních údajů

V České republice lze považovat za obdobu zákona na ochranu soukromí v elektronické komunikaci a zákona o vnitřní komunikaci zákon o ochraně osobních údajů, který vstoupil v platnost v červnu roku 2000. Zákon o ochraně osobních údajů je základním právním předpisem upravujícím ochranu osobních údajů a činnost Úřadu pro ochranu osobních údajů.

Smyslem zákona o ochraně osobních údajů je Listinou základních práv a svobod zaručené právo na ochranu občana před neoprávněným zasahováním do jeho soukromého a osobního života neoprávněným shromažďováním, zveřejňováním nebo jiným zneužíváním osobních údajů. V současné společnosti je vlivem rozvoje informačních technologií toto právo stále více narušováno. Na druhou stranu, zákon občana neochrání, dokud si lidé neuvědomí své chování při používání internetu a nebudou sami zásahům do soukromí předcházet.

Národní legislativa týkající se ochrany osobních údajů je harmonizována s právem evropským. Jedná se zejména o následující zákonné normy:

- Úmluva o ochraně osob se zřetelem na automatizované zpracování osobních dat; pro Českou republiku nabyla účinnosti dne 1. listopadu 2001.
- Dodatkový protokol k Úmluvě o ochraně osob se zřetelem na automatizované zpracování osobních dat; pro Českou republiku nabyl účinnosti dne 1. července 2004.
- Směrnice Evropského parlamentu a Rady 95/46/ES ze dne 24. října 1995, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů
- Směrnice Evropského parlamentu a Rady 2000/31/ES ze dne 8. června 2000, o určitých aspektech služeb informační společnosti, zejména elektronického obchodního styku v rámci vnitřního trhu
- Směrnice Evropského parlamentu a Rady 2002/58/ES ze dne 12. července 2002, o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací.
- Nařízení Komise (EU) č. 611/2013 ze dne 24. června 2013 o opatřeních vztahujících se na oznámení o narušení bezpečnosti osobních údajů podle směrnice Evropského parlamentu a Rady 2002/58/ES o soukromí a elektronických komunikacích.
- Doporučení Komise 2009/387/ES ze dne 12. května 2009, o zavedení zásad ochrany soukromí a údajů v aplikacích podporovaných identifikací na základě rádiové frekvence.
- Doporučení Komise 2014/724/EU ze dne 10. října 2014, o šabloně pro posouzení dopadů inteligentních sítí a inteligentních měřicích systémů na ochranu údajů.

### Zákon o kybernetické bezpečnosti

Od ledna 2015 platí v České republice zákon o kybernetické bezpečnosti, díky kterému by měl být stát odolnější vůči případným elektronickým útokům na důležité počítačové systémy v zemi.

Primárním úkolem zákona o kybernetické bezpečnosti je sjednocení elektronické komunikace. Sjednotit by se tak měla výměna informací nejen ve státní, ale částečně i soukromé sféře; zákon přímo stanovuje i jejich vzájemné dorozumívání. Kontrolní i exekutivní pravomoci má mít centrální orgán (Národní centrum kybernetické bezpečnosti CERT se sídlem v Brně). Aktivovat a hlavně sjednotit by se tak měla dnes pasivní počítačová ochrana státu a Česko by tak mělo být schopno nejen snadněji rozpoznat, ale přímo aktivně bojovat s útoky na elektronické úrovni. Lepší ochrany by se tak mohla dočkat i osobní data občanů registrovaných například na úřadech nebo bankách. Pomoci by měl zákon i samotné české ekonomice; měl by totiž zatraktivnit tuzemské prostředí pro zahraniční investice (nejen IT), na druhé straně by měl podporovat světově uznávané české dodavatele ICT technologií.

Zákon je postaven na třech pilířích: bezpečnostní opatření, hlášení kybernetických bezpečnostních incidentů a protiopatření (reakce na incidenty). Odpůrci zákona se nejčastěji bojí třetího pilíře: zákon dle jejich názoru dává státu velkou moc regulovat informační sektor a potenciálně mu umožňuje odposlouchávat či přímo odpojovat nepohodlné osoby či organizace.

### Závěr

Od zákonných norem upravujících provozování informačních a komunikačních systémů a poskytování souvisejících služeb očekáváme:

- Definování jednoduchých, jednoznačných, jasných a co možná nejobecnějších pravidel provozování komunikačních a informačních systémů a poskytování souvisejících služeb (ochrana soukromí uživatelů je jejich nedílnou součástí);
- Definování sankcí za porušování těchto pravidel;
- Definování způsobu, jakým je dodržování pravidel vymáháno;
- Specifikaci veřejných institucí, zodpovědných za dohlížení dodržování pravidel a inicializaci sankčních řízení.

Zákonné normy by měly mít co možná největší nezávislost na existujících systémech a technických řešeních. Technologický vývoj v oblasti informačních a komunikačních systémů je totiž natolik dynamický, že legislativní procesy nejsou schopny na tuto dynamiku adekvátně reagovat.

V současnosti můžeme považovat zákonné prostředí v České republice za vhodně nastavené, a to díky existenci zákonu o kybernetické bezpečnosti, zákonu o ochraně osobních údajů a jejich harmonizaci s právem Evropské unie.

### *Mezioborový přístup*

Problematika bezpečnosti elektronické komunikace zahrnuje dvě hlediska – hledisko technické a hledisko sociální. Technickými prostředky lze znesnadnit neautorizovaný přístup k přenášené či uložené informaci (šifrování, autorizace, diverzitní komunikace), avšak bez sociologické identifikace kyberneticky nebezpečného chování uživatelů je síla technického řešení významně oslabena.

Mezioborovost problematiky informačních a komunikačních technologií reflektují výzvy evropského rámcového programu HORIZON 2020 v oblasti společenských výzev, jejichž zveřejnění je plánováno na rok 2015. Jedná se o podprogram *Societal Challenges* (SC)

*SC7: Secure societies – Protecting freedom and security of Europe and its citizens*

a jeho výzvy

- DS 3 – 2015: Role ICT v ochraně kritické infrastruktury
- DS 4 – 2015: Bezpečné sdílení informací
- DS 5 – 2015: Důvěryhodné elektronické služby

Mezioborový přístup k řešení problematiky zabezpečení komunikačních a informačních systémů je nesmírně důležitý jak z hlediska vývoje nových systémů, ale též z hlediska zavádění nových standardů a norem, a současně z pohledu případných legislativních aktivit.

Proto je zapotřebí věnovat intenzivní pozornost přípravě nových výzkumných projektů mezinárodního charakteru, které budou mít ambici celoevropského dopadu na zvýšení úrovně bezpečnosti komunikačních a informačních systémů nejen jako klíčové kritické infrastruktury moderní informační společnosti, ale rovněž jako soukromého statku občanů České republiky a Evropské unie.

*Literatura*

[1] Electronic Communications Privacy Act of 1986 (zákon na ochranu soukromí v elektronické komunikaci) [online], Justice Information Sharing, U.S. Department of Justice, Office of Justice Programs, [cit. 4. ledna 2015], dostupné na: https://it.ojp.gov/default.aspx?area=privacy&page=1285

[2] Stored Communications Act of 1986 (zákon o vnitřní komunikaci) [online], Justice Information Sharing, U.S. Department of Justice, Office of Justice Programs, [cit. 4. ledna 2015], dostupné na: https://it.ojp.gov/default.aspx?area=privacy&page=1285

[3] Zákon o ochraně osobních údajů [online], Úřad pro ochranu osobních údajů, [cit. 4. 1. 2015], dostupné: https://www.uoou.cz/vismo/zobraz_dok.asp?id_ktg=1261&p1=1261

[4] Zákon o kybernetické bezpečnosti [online], Bureau Veritas Czech Republic, [citováno 4. ledna. 2015], dostupné na: http://www.bureauveritas.cz/wps/wcm/connect/bv_cz/local/home/news/press-releases/zakon-o-kyberneticke-bezpecnosti

# Sledování prvků kritické infrastruktury

### *Evropský program na ochranu kritické infrastruktury*

V prosinci 2005 Rada pro spravedlnost a vnitřní věci vyzvala Komisi, aby navrhla **Evropský program na ochranu kritické infrastruktury (EPCIP)**. V reakci na to Komise přijala toto sdělení a návrh směrnice o určení a označení evropské kritické infrastruktury pro zlepšování ochrany takové infrastruktury.

Sdělení stanovuje zásady, procesy a nástroje navržené pro provádění programu EPCIP. Ohrožení, na něž má program reagovat, se netýkají jen terorismu, ale patří sem také trestné činnosti, přírodní nebezpečí a další důvody nehod na principu stejného přístupu pro veškerá ohrožení.

Obecným cílem EPCIP je zlepšování ochrany kritické infrastruktury v Evropské unii (EU). Toho bude dosaženo prováděním evropských právních předpisů stanovených v tomto sdělení.

Legislativní rámec pro EPCIP obsahuje následující:

- postup pro určení a označení evropské kritické infrastruktury a společný přístup k posuzování potřeb zlepšování ochrany takové infrastruktury. Stane se tak formou směrnice;
- opatření, která mají usnadnit provádění EPCIP, včetně akčního plánu EPCIP, Výstražné informační sítě kritické infrastruktury (CIWIN), vytvoření skupin odborníků na ochranu kritické infrastruktury na úrovni EU, procesů sdílení informací o ochraně kritické infrastruktury a určení a analýzy vzájemných závislostí;
- poskytování podpory zemím EU v oblasti vnitrostátních kritických infrastruktur, které by na základě zvážení mohla příslušná země EU využít, a pohotovostní plánování;
- vnější prostředí;
- doprovodná finanční opatření, a zvláště navržený program EU „Prevence, připravenost k obraně proti terorismu a jiným souvisejícím bezpečnostním rizikům a zvládání jejich následků“, pro období 2007–2013, která poskytnou příležitosti financovat opatření týkající se ochrany kritické infrastruktury.

Akční plán EPCIP má tři hlavní pracovní oblasti:

- první se zabývá strategickými aspekty EPCIP a rozvojem opatření horizontálně použitelných na veškerou práci v oblasti ochrany kritické infrastruktury;
- druhá se zabývá evropskými kritickými infrastrukturami a jejím cílem je snížit jejich zranitelnost;
- třetí je vnitrostátní rámec, který podporuje země EU v ochraně jejich vnitrostátních kritických infrastruktur.

Mezi nejdůležitější pasáže předmětného sdělení patří zejména:

***„Výstražná informační síť kritické infrastruktury (CIWIN):***

*Výstražná síť (CIWIN) bude zřízena samostatným návrhem Komise za účelem bezpečné výměny osvědčených postupů a mohla by také poskytnout platformu pro výměnu rychlých výstrah propojenou se systémem Komise ARGUS.*

***Skupiny odborníků:***

*Pokud je zapotřebí specifických odborných znalostí, může Komise zřizovat skupiny odborníků na ochranu kritických infrastruktur na úrovni EU, které se budou zabývat jasně definovanými otázkami. Podle odvětví kritické infrastruktury mohou funkce odborníků zahrnovat následující úkoly:*

- *pomoc při určování zranitelných míst, vzájemných závislostí a osvědčených postupů v odvětví;*
- *pomoc při rozvoji opatření ke snížení zranitelných míst a při rozvoji metriky plnění;*
- *formulování případových studií.*

***Sdílení informací o ochraně kritické infrastruktury***

*Zainteresované subjekty musí sdílet informace o ochraně kritické infrastruktury, zejména o opatřeních týkajících se bezpečnosti kritických infrastruktur a chráněných systémů, studie vzájemných závislostí a posuzování zranitelnosti, ohrožení a rizik souvisejících s ochranou kritické infrastruktury. Zároveň musí být zajištěno, aby nedošlo ke zveřejnění sdílených vlastnických, citlivých nebo osobních informací a aby veškerý personál pracující s utajenými informacemi byl prověřen na příslušný stupeň utajení od příslušné země EU.*

***Určení vzájemných závislostí***

*Pro lepší vyhodnocování slabých míst, ohrožení nebo rizik týkajících se kritických infrastruktur je nutné určit a analyzovat vzájemné závislosti zeměpisné i odvětvové povahy.*

***Kontaktní skupina pro ochranu kritické infrastruktury***

*Komise plánuje vytvořit kontaktní skupinu pro ochranu kritické infrastruktury. Kontaktní místa, určená každou zemí EU, budou zodpovědná za koordinaci otázek týkajících se ochrany kritické infrastruktury s ostatními zeměmi EU, Radou a Komisí.*

***Ochrana vnitrostátních kritických infrastruktur***

*I když Komise uznává, že ochrana vnitrostátních kritických infrastruktur je odpovědností vlastníků, provozovatelů a zemí EU, poskytuje v této oblasti podporu na vyžádání zemí EU. Všechny země EU by měly vytvořit vnitrostátní program ochrany včetně těchto bodů:*

- *klasifikace vnitrostátních kritických infrastruktur s přihlédnutím k dopadům narušení nebo zničení určité infrastruktury (zeměpisný rozsah škod a závažnost důsledků);*
- *určení zeměpisných a odvětvových vzájemných závislostí;*
- *pohotovostní plánování.*

***Vnější prostředí***

*Vnější prostředí ochrany kritické infrastruktury je důležitým aspektem EPCIP. Aspekt propojenosti a vzájemné závislosti současného hospodářství znamená, že narušení nebo zničení určité infrastruktury by mohlo mít vážný dopad na země mimo Unii a naopak. Je proto velmi důležité posilovat mezinárodní spolupráci v této oblasti prostřednictvím odvětvových dohod.*

***Doprovodná finanční opatření***

*EPCIP bude spolufinancován programem Společenství „Prevence, připravenost k obraně proti terorismu a jiným souvisejícím bezpečnostním rizikům a zvládání jejich následků“ pro období 2007–2013.*

***Historické souvislosti***

*Ve dnech 17. a 18. června 2004 Evropská rada požádala Komisi o přípravu celkové strategie na vylepšení ochrany kritické infrastruktury. Komise v reakci na to přijala 20. října 2004 sdělení „Ochrana kritické infrastruktury v boji proti terorismu“.*

*Evropská rada ve dnech 16. a 17. prosince 2004 ve svých závěrech o předcházení, připravenosti a reakci na teroristické útoky a v Programu solidarity přijatých Radou 2. prosince 2004 přijala záměr Komise předložit Evropský program na ochranu kritické infrastruktury (EPCIP) a Výstražnou informační síť kritické infrastruktury (CIWIN).*

*V roce 2005 se na EPCIP intenzívně pracovalo. Dne 17. listopadu 2005 Komise přijala Zelenou knihu o Evropském programu na ochranu kritické infrastruktury.*

*Dne 15. září 2005 bylo přijato rozhodnutí o financování pilotního projektu obsahujícího soubor přípravných akci s cílem posílit boj proti terorismu. Potom, 26. října 2006, následovalo druhé rozhodnutí o financování pilotního projektu EPCIP.*

*Dne 12. prosince 2006 Komise představila návrh směrnice o určení a označení evropských kritických infrastruktur a společný přístup k posuzování potřeb zlepšování jejich ochrany. Ve stejný den Komise přijala i toto sdělení. Tyto dokumenty jasně ukazují, jak Komise navrhuje řešit problematiku ochrany kritické infrastruktury v EU.*

*Nakonec, dne 12. února 2007, byl přijat navržený program EU „Prevence, připravenost k obraně proti terorismu a jiným souvisejícím bezpečnostním rizikům a zvládání jejich následků“.“*

## Národní program ochrany kritické infrastruktury

Hlavním cílem **Národního programu ochrany kritické infrastruktury** je rozpracování obecných záměrů nastíněných v Komplexní strategii k řešení problematiky kritické infrastruktury do konkrétních kroků určených příslušným nositelům úkolů.

Obecně lze tyto úkoly shrnout do následujícího přehledu:

a. určení významu fungování subjektů kritické infrastruktury,
b. stanovení dopadů nefunkčnosti prvků kritické infrastruktury,
c. analýzu ohrožení a určení způsobu jak zabránit nebo minimalizovat dopady nefungování některých prvků kritické infrastruktury,
d. stanovení úkolů gestorům za řešení problematiky v jednotlivých odvětvích či subjektům kritické infrastruktury za řešení problémů vzniklých u prvků kritické infrastruktury,
e. vypracování přehledu zákonných norem upravujících odpovědnost v oblasti ochrany kritické infrastruktury, tj. stávajících i chybějících,
f. vypracování rozborů ekonomických dopadů na veřejné rozpočty.

Samotný Národní program ochrany kritické infrastruktury zahrnuje tyto okruhy řešení problematiky kritické infrastruktury:

1. Stanovení zásad určování prvků kritické infrastruktury (odvětvová a průřezová kritéria týkající se kritické infrastruktury České republiky (dále jen „ČR) a případně vybraných subjektů evropské kritické infrastruktury),
2. Provedení legislativních úprav ve vazbě na právní předpisy ČR v oblasti bezpečnosti (zákon o krizovém řízení a související právní předpisy) a závazné mezinárodní dokumenty, zejména EU,
3. Stanovení konkrétních nositelů úkolů se zřetelem na jejich stanovené působnosti,

4. Vypracování programů pro ochranu kritické infrastruktury pro jednotlivé oblasti a podoblasti kritické infrastruktury („resortní programy“),

   a) zpracování analýz ohrožení celostátně významných prvků kritické infrastruktury, jako např. v energetice, dopravě a komunikacích a stanovení vzájemných vazeb a závislostí s cílem odkrýt a posílit zranitelná místa oblastí a prvků kritické infrastruktury,

   b) provedení úprav metodik pro zpracování plánů v oblasti bezpečnosti (krizové plány, plány krizové připravenosti, plány bezpečnosti vlastníka/provozovatele prvků kritické infrastruktury apod.),

   c) projednání otázek souvisejících se zabezpečením plánů kontinuity činnosti subjektů kritické infrastruktury s cílem zachovat minimální funkčnost subjektů kritické infrastruktury včetně stanovení hlavní a klíčové činnosti pro zajištění kontinuity fungování subjektů kritické infrastruktury,

   d) projednání možnosti úprav vnitřních předpisů, norem a standardů pro příslušné oblasti kritické infrastruktury z hlediska jejich dostatečnosti pro ochranu kritické infrastruktury,

   e) zabezpečení informování (vyrozumění) hlavních vlastníků/provozovatelů dodávajících a poskytujících relevantní zboží a služby v oblasti kritické infrastruktury,

5. Vytvoření podmínek pro financování opatření ochrany kritické infrastruktury, včetně projektů uplatňovaných v rámci programů EU ,
6. Podpora výstupů a výsledků vědeckého rozvoje zaměřeného na ochranu prvků a systémů kritické infrastruktury,
7. Zajištění vzdělávání v oblasti ochrany kritické infrastruktury.

Z výše uvedeného přehledu vystupují zřetelně do popředí otázky související se zásadami určování prvků a systémů kritické infrastruktury, úkoly klíčových účastníků procesu, legislativa a financování ochrany kritické infrastruktury.

Pokud budeme vycházet z poznatků současného stavu v oblasti standardizace a certifikace v civilní letecké dopravě tak si musíme nejprve určit jednotlivé úrovně systému dozoru nad certifikaci v civilní letecké dopravě.

Dotčené subjekty v ČR, které dozorují a dohlížejí na správní postup při standardizaci a certifikaci v ČR zastávají:

Ministerstvo dopravy ČR - Odbor civilního letectví (MD ČR/OCL)

Nejvyšším orgánem pro civilní letectví v ČR je Ministerstvo dopravy, kde leteckou dopravu zastřešuje Odbor civilního letectví. Na základě Úmluvy o mezinárodním civilním letectví, která byla Českou republikou uveřejněna jako závazný právní předpis ve Sbírce Zákonů má Ministerstvo dopravy právo uveřejňovat letecké předpisy rady L. Letecké předpisy řady jsou uveřejňovány prostřednictvím Letecké informační služby státního podniku Řízení letového provozu. Tyto předpisy jsou určeny pro aplikaci doporučení a standardů Mezinárodních organizací pro civilní letectví.

Ministerstvo dopravy je centrální institucí státní správy v oblasti civilního letectví v ČR. Zajišťuje provádění přijatých zákonů a mezinárodních smluv, které schválila vláda České republiky v civilním letectví a přispívá k realizaci dopravní politiky. Rozhodovací pravomoc je v souvislosti se vznikem Úřadu pro civilní letectví omezena pouze na oblasti, ve kterých je nutné uplatňovat pouze širší zájmy.

Úřad pro civilní letectví (dále jen ÚCL) - Sekce letových standardů - Odbor standardizace a regulace

- **Sekce letových standardů je ve své působnosti v rámci Úřadu pro civilní letectví ČR odpovědná za:**
  a. výkon státní správy a státního dozoru v oblasti ověřování technické a provozní způsobilosti vyjmenovaných leteckých zařízení, v oblasti zajištění bezpečného vzdušného prostoru a navigačního prostředí nad územím České republiky harmonizovaného s okolními státy a v oblasti ochrany navigačního prostředí nad územím České republiky proti interferenci jiných než leteckých zařízení;
  b. výkon státní správy a státního dozoru v oblasti způsobilosti řídících letového provozu a plnění úkolů vnitrostátního dozorového orgánu;
  c. výkon státní správy a státního dozoru v oblasti způsobilosti syntetických výcvikových zařízení;
  d. provádění měření a letového ověřování leteckých zařízení;
  e. zajištění způsobilosti letadel ÚCL ;
  f. výkon státní správy a státního dozoru nad způsobilostí k provozu a provozem civilních a vojenských letišť, používaných pro civilní letecký provoz, dle platného legislativního rámce;
  g. výkon státní správy a státního dozoru jako speciálního stavebního úřadu pro civilní letecké stavby, dle platného legislativního rámce;

h. výkon státní správy a státního dozoru v oblasti ověřování technické a provozní způsobilosti vyjmenovaných bezpečnostních zařízení, dle platného legislativního rámce;
i. spolupráci s MD na tvorbě návrhů civilních leteckých předpisů ČR a analýzu a návrhy úprav civilních leteckých předpisů tak, aby nebyly v rozporu s právními předpisy ES a požadavky EASA a aby v maximální možné míře splňovaly standardy a doporučené postupy ICAO;
j. dosažení a zajištění jednotného stanoviska ÚCL k dané problematice v oblasti předpisových požadavků, jejich návrhů a změn, včetně koordinace postupu k jeho dosažení, a předání tohoto stanoviska příslušným organizacím;
k. účast v odborných skupinách ES, EASA, Eurocontrol, ICAO apod. při vývoji mezinárodních leteckých předpisů a ve spolupráci s jednotlivými útvary ÚCL za přípravu nezbytných podkladů pro účast generálního ředitele ÚCL na jednáních správní rady EASA a dalších příslušných jednáních;
l. zapracování příslušných požadavků regulace oblasti bezpilotních systémů do systému leteckých předpisů ČR a prvotní posouzení žádostí týkajících se certifikace nebo povolení k provozování bezpilotních systémů s ohledem na koncepci regulace bezpilotních systémů;
m. činnosti související s pozicí šéfredaktora webových stránek ÚCL;
n. vedení knihovny dokumentů ICAO v rámci ÚCL a zajištění přístupu ÚCL do mezinárodní elektronické databáze leteckých předpisů;

- **Odbor standardizace a regulace (REG) je ve své působnosti v rámci Sekce letových standardů**

Odbor standardizace a regulace připravuje návrhy znění českých leteckých předpisů, které uveřejňuje Ministerstvo dopravy (MD), a plní další úkoly dle níže uvedených specifikací.

V rámci svých kompetencí odbor zejména:

a) spolupracuje s MD na tvorbě návrhů civilních leteckých předpisů ČR;
b) analyzuje a navrhuje úpravy českých leteckých předpisů tak, aby nebyly v rozporu s právními předpisy ES/EU a požadavky EASA a aby v maximální možné míře splňovaly standardy a doporučené postupy ICAO;
c) v rámci standardizace zajišťuje dosažení jednotného stanoviska ÚCL k dané problematice v oblasti předpisových požadavků, jejich návrhů a změn, včetně koordinace postupu k jeho dosažení. Je-li to použitelné, zasílá stanovisko ÚCL cestou generálního ředitele ÚCL, případně Ř/SLS nebo Ř/REG, příslušným organizacím;
d) ve spolupráci s jednotlivými útvary ÚCL připravuje nezbytné podklady pro účast generálního ředitele ÚCL na jednáních správní rady EASA, výboru EASA a dalších jednáních a koordinuje průběh vyjadřování souvisejících připomínek;
e) organizuje práci externích spolupracovníků a interní připomínková řízení ke změnám předpisů;
f) organizuje jménem ÚCL odborná připomínková řízení k návrhům českého znění civilních leteckých předpisů, které vznikly pod jeho řízením;

g) zpracovává připomínky vzešlé z připomínkových řízení organizovaných OLP a předává konečné návrhy MD;
h) zpracovává informační bázi předpisů a souvisejících dokumentů pro potřeby ÚCL;
i) ve spolupráci s odbornými odděleními připravuje výklad ustanovení leteckých předpisů, osvětluje záměry sledované změnami předpisů resp. novými předpisy a v oblasti zpracovávaných předpisu se účastní provádění auditů a inspekcí v rámci státního dozoru;
j) sleduje vydávání příloh k Úmluvě o mezinárodním civilním letectví, dokumentů vydávaných ICAO, EASA, ECAC a právních dokumentů ES/EU jako vodítek pro tvorbu návrhů národních leteckých předpisů;
k) sleduje vývoj předpisů a další dokumentace týkající se regulace oblasti bezpilotních systémů (včetně modelů) zpracovávaných v EU, EASA, ICAO, FAA a podobně. Vyhodnocuje získané poznatky s koncepcí regulace oblasti bezpilotních systémů v ČR a připravuje návrhy zapracování příslušných požadavků do systému leteckých předpisů ČR;
l) připravuje prvotní stanoviska žádostí týkajících se bezpilotních systémů;
m) prověřuje jednotné uplatňování leteckých předpisů pracovníky ÚCL a účinnost předpisů ke zvyšování bezpečnosti leteckého provozu;
n) v případě potřeby připravuje návrhy na změny AIP v těch částech, které se týkají leteckých předpisů v jeho působnosti;
o) účastní se práce v odborných skupinách EU, EASA, ICAO, ECAC atd. při vývoji mezinárodních leteckých předpisů;
p) spolupracuje na zabezpečení úkolů vyplývajících z mezinárodních smluv a z členství v mezinárodních organizacích v oblasti leteckých předpisů;
q) vede knihovnu dokumentů ICAO v rámci ÚCL;
r) zajišťuje přístup ÚCL do mezinárodní elektronické databáze leteckých předpisů;
s) podílí se na sestavování podkladů pro rozbor činnosti ÚCL;
t) plní další úkoly z příkazu generálního ředitele ÚCL a ředitele sekce.

K zajištění výkonu činností jsou na odboru zřízeny následující organizační útvary:

- oddělení leteckých předpisů (OLP)
- dokumentační středisko.

V návaznosti na Nařízení č. 216/2008 (1592/2002) Evropského parlamentu a Rady o společných pravidlech v oblasti civilního letectva a o ustanovení EASA kterým se doplňuje a kterým se*: „stanoví prováděcí pravidla pro certifikaci letové způsobilosti letadel a souvisejících výrobků, letadlových částí a zařízení a certifikaci ochrany životního prostředí, jakož i pro certifikaci projekčních a výrobních organizací"*.

Komise Evropského společenství přijala nařízení Komise (ES) č. 748/2012 (1702/2003) na základě nařízení Evropského parlamentu a Rady (ES) č. 1592/2002 (o společných pravidlech v oblasti civilního letectví a o zřízení Evropské agentury pro bezpečnost letectví). Obě nařízení jsou závaznými zákonnými normami členských států EU.

Nařízením Komise (EU) č. 748/2012 ze dne 3. srpna 2012, kterým se stanoví prováděcí pravidla pro certifikaci letové způsobilosti letadel a souvisejících výrobků, letadlových částí a zařízení a certifikaci ochrany životního prostředí, jakož i pro certifikaci projekčních a výrobních organizací.

Problematikou certifikace letadel a ostatních výrobků a částí letadlové techniky se zabývá nařízení Komise (ES) č. 748/2012 kde podrobné požadavky a postupy vycházející již z přílohy Part 21 k Nařízení 748/2012. Tato příloha je taky nazvaná Část 21 a zabývá se postupy certifikace letadel a ostatních výrobků a částí letadlové techniky.

## Předpisová základna

Před začátkem certifikace nové letadlové techniky je nutné určit, kde bude letadlová technika provozována, zda jen v ČR nebo i v zahraničí, a podle toho pak postupovat ve výběru vhodné předpisové základny. Výrobce předpokládá, že největší distribuce letadlové techniky bude hlavně pro zahraniční zákazníky, a je tedy nutné pro uznání Typového certifikátu v zahraničí (státech EU) postupovat dle předpisů EU, konkrétně postupovat dle přílohy **Part 21 Nařízení komise (ES) 748/2012**.

Dále je vhodný postupovat dle obecné zásady postupů „Rozhodnutí správní rady č. 7-2004 Postupy certifikace výrobků- **EASA MB 02/04**", který vydal výkonný ředitel EASA

Taky nemožno opomenut národní předpisovou základnu, zde se bude vycházet z:

## Předpis L-8/A (Předpis Letová způsobilost)

Účelem tohoto předpisu je stanovit národní požadavky na letovou způsobilost pro letadla včetně jejich motoru, vrtule a vybavení. Dále pro letadla včetně jejich motoru, vrtule a vybavení, jejichž Typová osvědčení nebyla převedena do kompetence EASA.

Pokud je některá položka vybavení schválená dle EASA, pokládá se, jako by byla schválená i podle tohoto předpisu. Tento předpis je důležitý z hlediska doplňujících informací.

*Zákon o civilním letectví č. 49/1997 sb.*

Tento zákon zpracovává a upravuje příslušné předpisy Evropských společenství v oblasti civilního letectví, tedy i podmínky letecké stavby a certifikace.

*Různé doporučené postupy a směrnice ÚCL*

- postupy pro získání oprávnění výrobků, letadlových částí a zařízení nebo jejich změn a oprav, které nespadají pod působnost Nařízení komise (ES) č. 748/2012
- Poradní oběžník k předpisu L8A pro způsoby prokazování jednotlivých požadavků předpisové základny
- Postupy pro získání oprávnění k projektování výrobků, letadlových částí Nařízení komise (ES) č. 748/2012
- Postupy pro vydání oprávnění k provádění zkoušek letecké techniky
- Směrnice pro vypracování technické specifikace vybavení letadel
- Směrnice pro nakládání se zkušebními vzorky po provedené zkoušce
- Atd.…

## Analýza možností certifikace

Aby mohla být letecká technika provozována za normálních provozních podmínek u budoucích zákazníků, musí projít schvalovacím procesem nazývaným certifikace. Cílem certifikace je ověření zda konstrukce a všechny ostatní parametry jsou vyhovující a nevytváří žádné nebezpečí či už pro posádku nebo provoz v letecké dopravě.

### Kategorie způsobilosti

Před samotnou certifikací je nutné určit a definovat, k čemu vyvíjená letecká technika bude používána, a podle toho zvolil kategorii způsobilosti. Příloha Part 21 konkrétně HLAVA B rozeznává dva základní typy způsobilosti:

standardní typová osvědčení

zvláštní typová osvědčení

### Podaní žádosti

Pro zahájení certifikace musí nejprve výrobce (žadatel) vyplnit a odeslat formulář Žádosti o typové osvědčení. Žádost o typové osvědčení nebo typové osvědčení pro zvláštní účely musí být podána formou a způsobem stanovenými EASA.

Žádost bude poslána přímo na ÚCL. ÚCL přijme žádost pouze od žadatele, který je držitelem Oprávnění organizace k projektování.

K žádosti o typové osvědčení musí být doložena požadovaná výkresová dokumentace s popisem vlastností konstrukce, předběžné základné údaje, popis provozních charakteristik zahrnujíce i navrhované provozní charakteristiky a omezení.

**Sestavení certifikačního programu**

Žadatel si sestaví na základě doporučení vlastní program certifikace, který lze rozdělit do 3 částí:

Seznámení - Výrobce popíše, co je účelem certifikace a co požaduje, aby bylo výsledkem certifikace.

Certifikační základna - Žadatel popíše, pro jakou certifikační základnu se rozhodl a podle kterého předpisu bude celá certifikace probíhat.

Příprava certifikačních programů - Jak žadatel doloží daný bod předpisu (navrhnutí typu zkoušek, metodika zkoušky + výsledek zkoušky, atd.)

**Odeslání zprávy ÚCL na EASA**

Po úspěšném dokončení certifikačního programu ÚCL odešle na EASA. Na základě návrhu žadatele EASA přezkoumá a nakonec přijme certifikační program, který bude určovat významné mezníky programu a příslušné předměty plnění. Tento program musí zejména určovat:

- způsoby průkazu;
- zapojení certifikačního týmu do procesu určování vyhovění;
- potřebu dosvědčení zkoušek;
- důležitá rozhodnutí ovlivňující výsledek certifikačního procesu.
- Po úspěšném přijatí certifikačního programu EASA sestaví certifikační tým, který bude dozorovat navržený program.

**Provedení zkoušek**

Certifikační tým EASA se musí účastnit řádných technických instruktáží uspořádaných žadatelem k certifikačnímu programu výrobku, aby byl důkladně obeznámen s návrhem, novými technologiemi a všemi specifickými nebo neobvyklými vlastnostmi nebo zamýšleným neobvyklým použitím výrobku, jak je nezbytné k určení certifikační předpisové základny.

Certifikační tým je povinen ověřit, zda žadatel dosáhl vyhovění požadavkům certifikační předpisové základny a požadavkům k ochraně životního prostředí v souladu s odsouhlaseným certifikačním programem

**Vydání osvědčení**

Po uznání všech nutných průkazů vyhovění provedených žadatelem, včetně prohlášení o vyhovění, je výkonný ředitel EASA povinen vydat platné osvědčení. Toto rozhodnutí bude žadateli oznámeno dopisem.

### Návrh dokumentace a zpráv

Žadatel při podání žádosti o provedení certifikace musí ÚCL předložit tuto dokumentaci:

1. **typový návrh**

Výrobní dokumentace typu: Výkresová dokumentace, popis ostatních výrobků

Popis: příslušenství, vybavení a systémů: omezení, technické parametry...

Technologické parametry: postupy výroby, montáže, parametry a doklady použitého materiálu.

Zachování letové způsobilosti

Ostatní informace: (např. doklady výroby, doklady způsobilosti, přílohy).

2. **program zkoušek**

Program zkoušek je popisuje, jak se samotná zkouška provede. Tento postup nesmí být v rozporu s předpisovou základnou a musí splňovat všechny její požadavky.

3. **Prokazované body předpisu**

Jedná se o přehled prokazovaných bodů předpisu. Každý bod by měl obsahovat paragraf předpisové základny, aby byl jednoduše dohledatelný. Tento seznam prokazovaných bodů se pak dále využije při sestavení časového rozvrhu zkoušek (Harmonogram zkoušek).

4. **časový rozvrh zkoušek**

Všechny zkoušky musí být předem naplánovány. Musí být vytvořen tzv. Harmonogram zkoušek. Ten je pak předán ÚCL, který si naplánuje účast na jednotlivých zkouškách. Harmonogram dále slouží k názornějšímu přehledu provedených zkoušek, zpoždění, změn, atd.

5. **metodika zkoušek**

Měla by podrobně definovat podmínky, vyhodnocení, potřebné přístrojové zařízení pro jednotlivé zkoušky. Dále popisuje všechny konfigurace a režimy, pro které bude prováděna zkouška. Je zde popis i prostředí zkoušky, např. požadavky meteorologických podmínek (teplota, vlhkost, výška, ve které bude prováděna zkouška, hustota vzduchu, tlak, atd.). Nakonec zde musí být uvedeno, jak bude provedeno vyhodnocení zkoušky.

6. **letovou příručku – pro letadla**

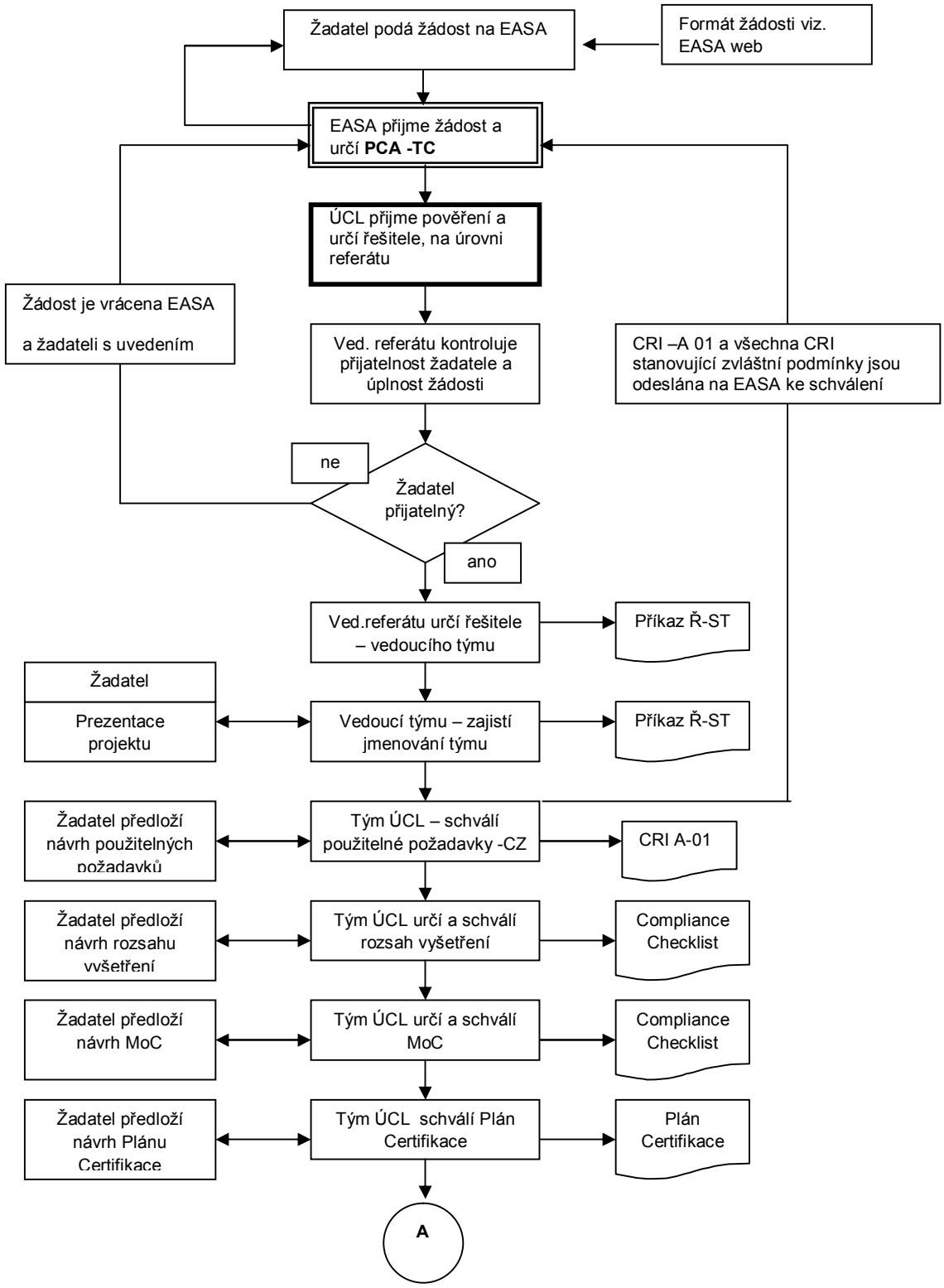
Výrobce by měl mít již zpracovanou alespoň předběžnou letovou příručku pro daný letoun. Je vhodné v průběhu zkoušek letovou příručku doplňovat (v případě zjištění

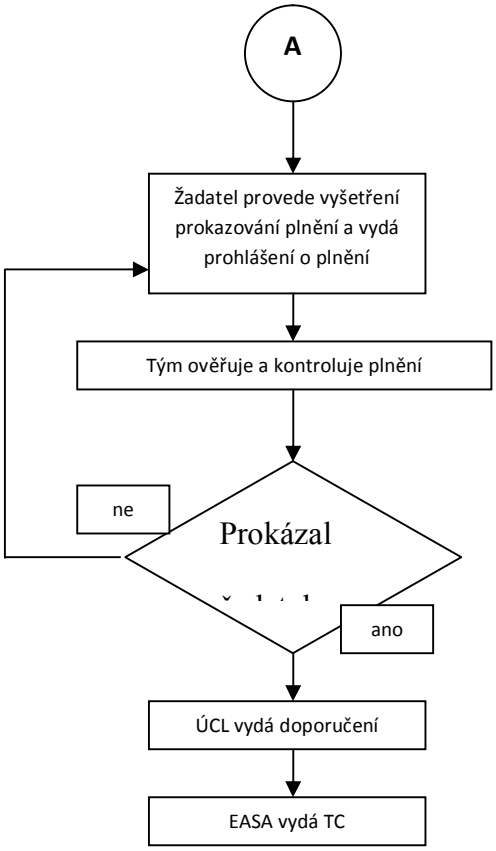
důležitých skutečností). Předpisem není požadováno předložení Letové příručky při podání žádosti o certifikaci (až dále).

**7. jiné specifické dokumenty**

Sem je možno zahrnout Průkaz shody s typovou dokumentací a Průkaz shody zkušebního zařízení s typovou dokumentací. Kde inspektor ÚCL nebo jiná pověřená

## Postupový diagram TC




A
Žadatel provede vyšetření prokazování plnění a vydá prohlášení o plnění
Tým ověřuje a kontroluje plnění
ne
Prokázal
ano
ÚCL vydá doporučení
EASA vydá TC

Současná velká mezinárodní letiště tvoří jeden z charakteristických symbolů moderní pospolitosti. Stejně jako mohou být velké průmyslové podniky jedním z hlavních terčů potenciálních útočníků, blíží se i letiště svými ekonomickými vztahy a povahou vykonávaných činností měřítkům takových podniků. Pro letiště jako objekt počátku přepravního procesu to znamená zatraktivnění z pohledu možných primárních cílů teroristických skupin, jejichž hlavním cílem je za pomoci protiprávních akcí narušit standardní chod společnosti, vyvolat ekonomické ztráty a zmatek. Z toho důvodu nejsou hrozby teroristických útoků podceňovány a naopak jsou každou zúčastněnou stranou, od výrobce technologií až po provozovatele letiště brány nadmíru vážně.

Všechny předpokládané bezpečnostní hrozby vyžadují od provozovatelů letišť realizovat řadu bezpečnostních opatření, která jsou velice nákladná a představují proto nemalou nákladovou položku v rozpočtech chodu letišť. Tato opatření kromě toho také komplikují logistická zabezpečení vzdušného i pozemního provozu a značným způsobem rovněž negativně ovlivňují osobní pohodlí a spokojenost zákazníků. Vzhledem k předpovědím, že se letecká doprava v Evropě do roku 2030 zdvojnásobí lze předpokládat, že tyto rozmanité a nákladné problémy nevyhnutelně porostou ještě více. A to již nyní, podle literárních zdrojů, stojí zajišťování bezpečnosti přibližně 25-30% z celkových provozních nákladů letišť. Do budoucna bude také potřeba navíc zavádět náročnější kontrolní technologie, potřebné k detekci sofistikovanějších způsobů terorismu. Celý tento nově koncipovaný proces však nesmí výrazněji narušit leteckou dopravu. Trvale nezbytnou podmínkou bude zachování, v řadě případů pak i zvýšení propustnosti cestujících i nákladu.

## Legislativní rámec ochrany před protiprávními činy

Nařízení Evropského parlamentu a Rady (ES) č. 300/2008 pojednává o ochraně letišť následujícím způsobem:

***„Působnost:***

*Toto nařízení by se mělo vztahovat na letiště sloužící civilnímu letectví, která se nacházejí na území členského státu, na provozovatele poskytující služby na těchto letištích a na subjekty dodávající zboží nebo poskytující služby na tato letiště nebo jejich prostřednictvím.*

*Toto nařízení se vztahuje na:*

*a)všechna letiště nebo části letišť umístěné na území členského státu, které nejsou využívány výhradně pro vojenské účely;*

*b)všechny provozovatele, včetně leteckých dopravců, kteří poskytují služby na letištích podle písmene a);*

*c)všechny subjekty uplatňující normy ochrany letectví před protiprávními činy, které provozují činnost z prostorů nacházejících se uvnitř či vně letiště a které poskytují zboží nebo služby pro letiště podle písmene a) nebo jejich prostřednictvím*

***Bezpečnostní program letiště***

*Každý provozovatel letiště vypracuje, uplatňuje a zachovává bezpečnostní program letiště.*

*V tomto programu se popíší metody a postupy, kterými se musí provozovatel letiště řídit, aby dodržoval toto nařízení a národní bezpečnostní program ochrany civilního letectví před protiprávními činy členského státu, v němž se letiště nachází.*

*Program musí obsahovat ustanovení o vnitřním řízení kvality popisující způsob, jakým má provozovatel letiště sám sledovat dodržování těchto metod a postupů.*

*Bezpečnostní program letiště se předloží příslušnému orgánu, který může případně přijmout další opatření.*

***Bezpečnost letišť***

*Požadavky na projektování letiště*

*1.1 Při projektování a stavbě nových letištních zařízení nebo úpravách stávajících letištních zařízení musí být plně zohledněny požadavky na provádění společných základních norem stanovené v této příloze a v prováděcích předpisech k ní.*

*Na letištích se vymezí tyto oblasti:*

*a) veřejný prostor letiště;*

*b) neveřejný prostor letiště;*

*c) vyhrazené bezpečnostní prostory a*

*d) kritické části vyhrazených bezpečnostních prostorů.*

*1.2 Kontrola vstupu*

*1.Vstup do neveřejného prostoru letiště se omezí s cílem zabránit vstupu neoprávněných osob a vjezdu vozidel bez povolení k vjezdu do tohoto prostoru.*

*2.Vstup do vyhrazených bezpečnostních prostorů se kontroluje s cílem zajistit, aby do těchto prostorů nevstoupily žádné neoprávněné osoby a nevjela žádná vozidla bez povolení k vjezdu.*

*3.Osobám a vozidlům může být udělen přístup do neveřejného prostoru letiště a do vyhrazených bezpečnostních prostorů pouze tehdy, pokud splňují požadované bezpečnostní podmínky.*

*4.Osoby, včetně členů posádky letadla, musí před vydáním identifikačního průkazu člena*

*posádky letadla nebo letištního identifikačního průkazu opravňujících k přístupu bez doprovodu do vyhrazených bezpečnostních prostorů úspěšně absolvovat ověření spolehlivosti.*

*1.3 Detekční kontrola osob jiných než cestujících a detekční kontrola vnášených předmětů*

*1. Osoby jiné než cestující se spolu s vnášenými předměty při vstupu do vyhrazených bezpečnostních prostorů podrobují nepřetržité namátkové detekční kontrole s cílem zabránit vnesení zakázaných předmětů do těchto prostorů.*

*2. Všechny osoby jiné než cestující se spolu s vnášenými předměty při vstupu do kritických částí vyhrazených bezpečnostních prostorů podrobují detekční kontrole s cílem zabránit vnesení zakázaných předmětů do těchto částí.*

*1.4 Kontrola vozidel*

*Vozidla vjíždějící do vyhrazeného bezpečnostního prostoru se kontrolují s cílem zabránit vnesení zakázaných předmětů do těchto prostorů.*

*1.5 Dozor, hlídky a jiné fyzické kontroly*

*Na letištích a případně ve veřejně přístupných přilehlých prostorech se provádí dozor, hlídky a jiné fyzické kontroly s cílem zjistit podezřelé chování osob, nalézt slabiny, které by mohly být využity ke spáchání protiprávního činu, a osoby od páchání těchto činů odradit.“*

V souladu s výše uvedeným nařízením pojednává také o ochraně letišť národní legislativa představující zejména část 8 Zákona 49/1997 sb.

***„Působnost:***

*Provozovatel letiště, letecký dopravce, poskytovatel letových provozních služeb a poskytovatel služeb při odbavovacím procesu na letišti jsou před zahájením svého provozu povinni mít schválený bezpečnostní program ochrany civilního letectví před protiprávními činy (dále jen "bezpečnostní program"). Bezpečnostní program schvaluje na písemnou žádost osob podle věty první Ministerstvo dopravy.*

***Povinnosti a oprávnění provozovatel letiště***

*(1) Provozovatel letiště je povinen přijímat opatření k zabránění vstupu nepovolaných osob a nedovolenému vjezdu vozidel do jím určených prostorů letiště. Za tímto účelem provozovatel letiště nebo jím pověřená osoba vydává a odebírá*

*a) letištní identifikační průkazy a vede jejich evidenci,*

*b) povolení k vjezdu vozidel a vede jejich evidenci.*

*(2) Provozovatel letiště je dále povinen*

*a) vytvořit na letišti, na kterém je provozována obchodní letecká doprava, podmínky k provádění bezpečnostních kontrol,*

*b) zajistit, aby osoby, které vstupují do jím určených prostorů letiště, byly podrobeny bezpečnostní kontrole,*

*c) zajistit, aby vozidla, která vjíždějí do jím určených prostorů letiště, byla podrobena bezpečnostní kontrole,*

*d) vydat a do 30 dnů od vydání vhodným způsobem zveřejnit podmínky pro vstup a pobyt cestujících, ostatních osob a vozidel v prostoru letiště,*

*e) odepřít vstup do jím určeného prostoru letiště nebo z něj vykázat osoby, které se nemohou prokázat platným letištním identifikačním průkazem nebo u nichž nebyla provedena bezpečnostní kontrola,*

*f) zabránit vjezdu vozidel, která se nemohou prokázat platným povolením k vjezdu nebo která nebyla podrobena bezpečnostní kontrole.*

*(3) Povinnosti podle písmen e) a f) se vztahují rovněž na osobu pověřenou provozovatelem letiště k výkonu činností souvisejících s ochranou civilního letectví před protiprávními činy.*

*(4) Provozovatel letiště nebo jím pověřená osoba jsou oprávněni*

*a) vydávat cestujícím a ostatním osobám, které vstupují do prostorů určených provozovatelem letiště nebo se v těchto prostorech zdržují, pokyny a příkazy k zajištění bezpečnosti na letišti,*

*b) omezit cestující a ostatní osoby v další činnosti, popřípadě je vykázat z prostoru letiště, pokud neuposlechnou pokynů nebo příkazů provozovatele letiště nebo jím pověřené osoby,*

*c) odepřít vstup do prostorů určených provozovatelem letiště nebo z něj vykázat osoby, které se nemohou prokázat platnou letenkou a palubní vstupenkou nebo u nichž byly zjištěny zakázané předměty nebo které jsou pod vlivem alkoholu, omamných nebo psychotropních látek,*

*d) vyzvat cestující a ostatní osoby, které vstupují do prostorů určených provozovatelem letiště nebo se v těchto prostorech zdržují, neuposlechnou-li pokynu nebo příkazu provozovatele letiště nebo jím pověřené osoby, aby tyto prostory opustily,*

*e) provádět bezpečnostní kontrolu.*

*(5) Náležitosti letištního identifikačního průkazu, způsob jeho vydávání a užívání, náležitosti povolení k vjezdu vozidel do prostorů letiště určených provozovatelem letiště a rozsah bezpečnostní kontroly vozidel stanoví prováděcí právní předpis.“*

## Organizace a řízení procesu přípravy bezpečnostních pracovníků

### Školení podle NPBV

Každý výcvik probíhá podle požadavků a osnov **Národního programu bezpečnostního výcviku** v civilním letectví České republiky a **předpisu L17** – Ochrana před protiprávními činy. Výcvikové centrum, druhy školení a samotný průběh výcviků jsou popsány v následujících kapitolách, s ohledem na utajované části **NPBV** a vnitřní předpisy a postupy Letiště Praha a.s.

**Výcvikové centrum a poskytovaná školení**

Na Letišti Praha - Ruzyně jako na největším letišti v České republice, působí velké množství pracovníků nejrůznějších profesí. Letiště Praha, a.s. Jako největší provozovatel civilní letecké dopravy je odpovědný za zajištění bezpečnosti. Přímo v areálu letiště, konkrétně ve spojovacím objektu, se nachází Školící a výcvikové centrum Letiště Praha a.s., ve kterém probíhají potřebná školení a výcviky nových pracovníků, jakož i přeškolování a aktualizační školení pracovníků stávajících. Toto centrum organizačně patří pod úsek bezpečnosti Letiště Praha a.s. Škála poskytovaných výcviků je široká a jednotlivé druhy se od sebe liší podle oblasti působnosti pracovníků, náročnosti na provedení a dalších faktorů. NPBV obsahuje školení a výcviky, pokrývající celou oblast bezpečnosti v letecké dopravě. Od obecných příprav, přes odborné přípravy kontroly osob, zavazadel, vstupů, obsluhu rentgenových zařízení až po přípravu posádek, pracovníků státní správy a auditorů.

**Organizační struktura pracovníků na letišti**

V kapitole Prováděné kontroly bylo zmíněno, že o ochranu letiště jako celku, se stará skupina specializovaných bezpečnostních pracovníků. Dále bude uvedena struktura, použitá na Letišti Václava Havla Praha (na jiných letištích se použitá struktura může lišit). Bezpečnostní kontrola (BEK) zajišťuje kontroly cestujících a jejich zavazadel. Počet takovýchto pracovníků se pohybuje okolo 400. Na druhé straně úkolem ostrahy letiště (OLE) je ochrana vnějšího perimetru letiště, provádění kontrol na služebních vchodech a hlídková činnost. Pracovníků v tomto útvaru je přibližně 350. Výcviky obou těchto útvarů se liší podle jejich budoucí specializace s ohledem na prováděné činnosti. Všichni bezpečnostní pracovníci spadají pod úsek Bezpečnost na Letišti Praha a.s., který zajišťuje, aby jak výcviky, tak prováděné kontroly a další činnosti byly v souladu s bezpečnostními programy a právními předpisy. Dále dohlíží, aby všem pracovníkům na dané pracovní pozici bylo zajištěno takové školení, které jim umožní vykonávat své povinnosti na odpovídající úrovni. Samozřejmostí je jistá hierarchie a rozdělení odpovědností a kompetencí.

**Vlastnosti a nábor bezpečnostních pracovníků**

Na letišti existují prostory s různým stupněm zabezpečení a s tím spojené kontroly (veřejné prostory, neveřejné prostory, vyhrazené bezpečnostní prostory). Postup přijímání pracovníků, kteří se nepodílejí na zabezpečení a ani nemají přístup do vyhrazených bezpečnostních prostor (SRA) řídí sám provozovatel letiště. Rozdílné přijímací postupy se týkají pracovníků, kteří se sice na zabezpečení přímo nepodílejí, ale mají přístup do těchto zabezpečených prostor. Poslední skupiny, která přímo provádí výkon bezpečnostních opatření, jejich kontrolu nebo za ni nese odpovědnost, se samozřejmě týká nejvyšší prověření a příslušný výcvik.

Do poslední jmenované skupiny patří i bezpečnostní pracovníci a to jak bezpečnostní kontroly (BEK), tak i ostrahy letiště (OLE). Při náboru nových pracovníků jsou kladeny požadavky na osobní vlastnosti i fyzický stav uchazeče o místo bezpečnostního pracovníka, ale důležitou složku v přijímacím procesu hraje i minulost takového uchazeče. Toho se dosahuje ověřením spolehlivosti, které dokládá beztrestnost a upřesňuje předchozí pracovní pozice u jiných zaměstnavatelů. Podrobnější kritéria pro nábor nových pracovníků jsou následující:

- požadované vzdělání
- pohovor s odpovědným pracovníkem
- lékařské potvrzení o schopnosti vykonávat stanovenou službu nebo činnost
- psychologický test
- jazykové znalosti (podle místa působení pracovníka)
- ověření spolehlivosti

Při posuzování, zda je daný uchazeč vhodný na místo bezpečnostního pracovníka, se přihlíží ke všem výše vyjmenovaným kritériím. Někteří specializovaní pracovníci mohou projít procesem dodatečného ověření, zda je taková práce pro ně vhodná. Jedná se např. o obsluhu rentgenových zařízení, tzv. screener, kde jedna z prvních zkoušek, kterou uchazeči podstupují, ještě před začátkem samotného výcviku, je tzv. pre-employment testing. Ten se skládá z několika vzorových rentgenových snímků, na kterých je ukryt nebezpečný nebo zakázaný předmět. Úkolem je najít jej v omezeném časovém limitu. Test ověří, zda má daný člověk rozpoznávací schopnosti nezbytné při dalším výcviku.

**Průběh výcviku**

Detailněji se zaměříme na výcvik pracovníků, kteří provádějí kontrolu osob a obsluhují rentgenová zařízení pro detekční kontrolu kabinových zavazadel. Celkový výcvik bezpečnostního pracovníka se skládá z několika částí. Jedno z prvních školení, které je na programu, je školení o používání identifikačních karet (IDC), následují 3 dny účasti na pracovišti, kde se daný budoucí pracovník seznamuje s prostředím, používanými výrazy a prostředky. Dalším velkým blokem je 12 denní školení (podle specializace pracovníka), které je zakončeno standardizovanou zkouškou. Po zácviku na pracovišti, kde pracovník provádí výkon své práce samostatně, ale stále pod dohledem nadřízené osoby, je mu vydáno osvědčení Ministerstva dopravy. Tím se pracovník stává plnohodnotným členem pracovního útvaru a může samostatně vykonávat službu.

Teoretické školení probíhá v malých skupinách (cca 13) pracovníků. Realizováno je formou přednášek školitelem z připravených prezentací. Všechny probírané prezentace a materiály jsou k dispozici i v tištěné podobě, takže je možno si do nich dělat vlastní poznámky, popř. se k nim vrátit později. Toto je důležité, protože je kladen důraz na individuální přístup každého z pracovníků. Opuštěním školící místnosti tedy zdaleka vzdělávání nekončí. Je vhodné a v řadě případů i nutné znát předpisy, postupy a doplňkové materiály, které jsou předmětem samostudia. V průběhu školení školitel přednáší připravená témata od používané techniky, přes postupy ať již v rutinních nebo krizových situacích až po příklady z praxe. To je velice důležité, protože právě na ně reagují pracovníci velice pozitivně

a pamatují si je. Součástí jsou tedy i rady a představení případů, které se již staly. Kde všude se dají ukrýt zakázané předměty a jak je nutno v takových případech postupovat. V případě nejasností na pracovišti, potřeby ověřit jisté skutečnosti apod., mají pracovníci možnost volat tzv. dispečink. Jedná se o specializované pracoviště, které je podpůrným prostředkem všem pracovníkům v případě potřeby. Může však také organizovat nouzové postupy a další.

Další částí, která je úzce spojena s výcvikem, jsou praktické ukázky a cvičení. Zde záleží na specializaci pracovníka. Podle toho jsou voleny praktická cvičení. Mezi hlavní však patří obsluha rentgenových zařízení a osobní prohlídka cestujících a jejich zavazadel. Tyto ukázky a cvičení probíhají přímo na rentgenových zařízeních. Mezi hlavní používané značky patří Heimann a Rapiscan. Školitel má k dispozici celou škálu předmětů, které vkládá do zavazadel. Sami pracovníci si poté osvojují jak obsluhu samotného zařízení, tak detekci předmětů a postupy při jejich odhalení. I zde jsou dávány příklady z praxe, jak je možné odhalit i poměrně dobře ukryté předměty apod. Zavazadla však nejsou jediným předmětem kontroly, nutná je i znalost fyzické kontroly osob. Ta probíhá na figurantech, na kterých se pracovníci učí samotnou prohlídku, ale i postupy při odhalení zakázaných předmětů.

Ve volném čase mezi školeními (nejméně však 1 hodinu denně) pracovníci procvičují detekci zavazadel, tentokrát však ve speciálním simulátoru, nazývaný X-Ray Tutor. Ten umožňuje rychlé a efektivní procvičení a zdokonalení se v odhalování nástražných výbušných zařízení, střelných zbraní, nožů apod. Zároveň je možné zpětné porovnání případných chyb, vedení statistik úspěšnosti a další funkce.

Po ukončení výcviku následuje již zmíněná standardizovaná zkouška. Ta se skládá z písemného testu, fyzické kontroly tří figurantů a zavazadel, kde se hledí na dodržení metodiky, stanoveného času a postupů při nalezení zakázaného předmětu. Dále příprava osoby na bezpečnostní kontrolu a obsluha technických zařízení, jako jsou rentgen a průchozí a ruční detektor kovů. Nezbytnou znalostí bezpečnostních pracovníků je také určení, zda daná identifikační karta má umožněn přístup do daného prostoru, i toto je součástí zkoušky, kdy za pomoci losu je třeba určit rozsah přístupných prostor pro vylosovanou kartu. Poslední částí zkoušky je vyhodnocení 100 ks snímků v softwaru X-Ray Tutor.

### Analýza charakteristik lidského činitele ve vztahu k procesům řešení krizových situací v systémech ochrany

V Evropě byl v letech 2009 až 2012 řešen projekt BEMOSA (Behavioral Modeling for Security in Airports), spolufinancovaný Evropskou komisí v rámci 7. Rámcového programu pro výzkum a technický rozvoj v Evropské Unii. Hlavním cílem projektu byl vývoj modelu chování lidí, čelících tváří v tvář bezpečnostním otázkám v normálních rutinních i krizových situacích a postupu při rozhodovacím procesu na letištích. Přijetím projektem rozpracovaného modelu v praxi může být zvyšována míra bezpečnosti, snižováno procento falešných poplachů a v neposlední řadě také zvyšována efektivita a tím i ziskovost. Konsorcium projektu BEMOSA rovněž vytvářelo předpoklady pro vypracování nově koncipovaného balíčku školení pro zaměstnance letiště. Tato školení se zaměřují na přípravu bezpečnostních pracovníků ve vztahu ke zvyšování bezpečnosti a ekonomické efektivnosti bezpečnostních

procesů. Projekt předpokládal, že speciálně přizpůsobené vzdělávací programy pomohou výrazně zvýšit úroveň dovedností všech lidských zdrojů v rámci letiště a jejich přípravu pro citlivé rozhodování. Hlavním cílem přípravy tak je zvýšit efektivnost letecké dopravy snížením falešných poplachů, stejně jako zlepšit bezpečnost a koordinaci v případech nouze a ohrožení bezpečnosti.

K získání údajů a popisů, jaké jsou předpoklady vzniku mimořádných událostí a jaké bezpečnostní hrozby byly řešeny v praxi, byla v rámci projektu provedena hloubková studie uvedené problematiky u několika vybraných evropských letišť. Výsledky získané z dotazníkových šetření, osobních pohovorů a panelových studií pak byly podle svého kvantitativního nebo kvalitativního charakteru vhodným způsobem dále tříděny a vyhodnocovány. Data sebraná během průzkumu umožnila vytvoření modelu chování bezpečnostních pracovníků na letišti.

V nejrůznějších situacích, které mohou nastat při bezpečnostních kontrolách, se začal stále více vyskytovat jev, který dokazoval, že bezpečnostní rozhodování na letištích jsou orámována pravidlem shody (Rule Compliance). Jedná se o nedostatek ve výcviku pracovníků. V podstatě jde o to, že pravidla a protokoly pro kontrolu jsou často přímo dané pokyny v rozhodovacím procesu, který určuje konečný výsledek bezpečnostních rozhodnutí. Ne ve všech situacích je však možné nalézt správné řešení v předepsaných postupech. Klíčový prvek v celém rozhodovacím procesu pak hraje lidský faktor a jeho úsudek v daném místě, čase i situaci. Tento chybějící prvek se tedy stal hlavním cílem výzkumu projektu BEMOSA. Pilotní průzkum, se zaměřením na pravidlo shody „zkombinoval výsledky více než 700 skriptů případové studie, 518 odpovědí do strukturovaných dotazníků a téměř 700 jednočlenných rozhovorů a prokázal, že pravidlo dodržování zásad bezpečnosti zdaleka neposkytuje plnou ochranu.“

Již od prvních zjištění o nedostatcích výcvikových programů bylo jasné, že bude zapotřebí důkladnějších hloubkových výzkumů. Za spolufinancování Evropskou unií (TRANSPORT - AAT.2009.5.2.3 – Grant Agreement 234049)3, započal projekt BEMOSA. Řešení projektu probíhalo od 1. září 2009 do 30. října 2012. Jeho název vznikl spojením slov BEhavioral MOdeling for Security in Airports. Vedení projektu se ujal známý izraelský odborník na disaster management prof. Alan Kirschenbaum. V rámci řešení projektu: „Důraz byl kladen na první a nejdůležitější zjištění skutečných bezpečnostních chování letištních zaměstnanců a cestujících. Letiště jsou složité ekonomické a sociální organizace, je jasné, že bezpečnostní rozhodnutí jsou založena na zaměstnancích v jejich interakci s cestujícími a nařízenými pravidly a technologiemi.

Tato trilogie, ve které se zaměstnanci ocitnou je rozhodující, a ovlivňuje, jak udělají jejich bezpečnostní rozhodnutí.“ Základ pro výzkum tvořil pohled na letiště jako na velkou a složitou organizaci, ve které existují formální i neformální vazby mezi jednotlivými subjekty a jemnější sada komunikačních sítí, která usnadňuje každodenní práci. Důležité bylo odhalit, jak se zaměstnanci chovají v běžných a v nestandardních situacích.

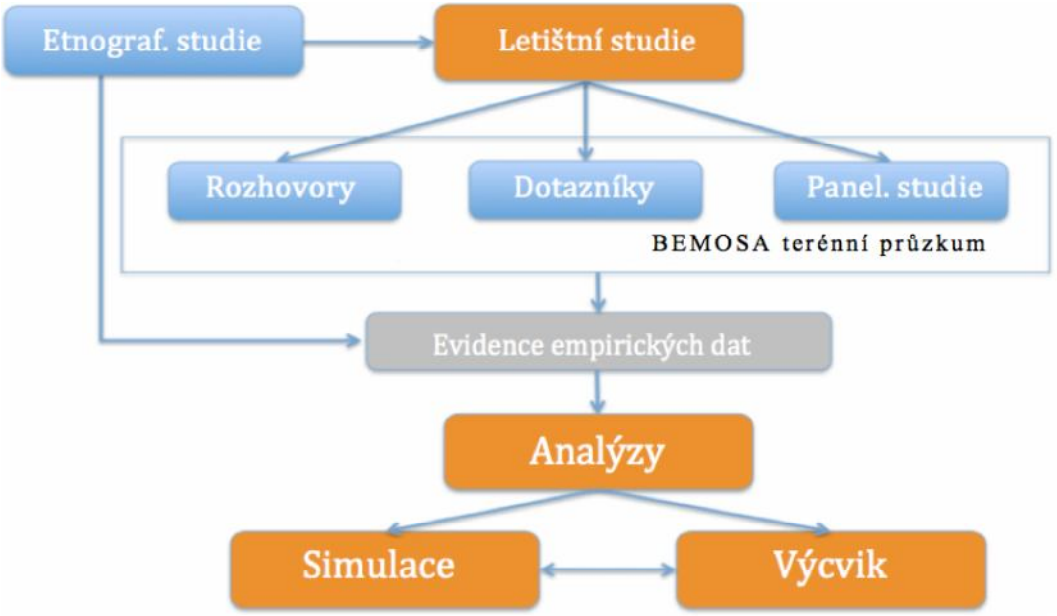
Filozofií projektu BEMOSA byla myšlenka, že jak porozumění, tak i evidence umožňuje pochopení bezpečnostních rozhodnutí – což znamená: na příkladech se učí nejlépe.

Projekt předpokládá, že na základě modelových řešení pak budou zúčastněné strany moci předvídat, kontrolovat a měnit mnoho problémových překážek, které až dosud byly nákladné a neefektivní pro provoz letiště.

Cílem tedy bylo navrhnout takový balíček školení, který by byl pro přípravu bezpečnostních pracovníků letiště bezpečnější, jistější a vzhledem k vyšší účinnosti samozřejmě ekonomičtější. V důsledku kvalitnějšího průběhu v rámci procesu bezpečnostních kontrol by se celkově tedy zvýšila spokojenost a komfort cestujících.

Prvním úkolem při řešení projektu BEMOSA bylo získání základních údajů o provozu letiště. Nezbytnou podmínkou pro bližší analýzu jednotlivých rozhodnutí totiž je pochopení, jak administrativně i logisticky složitá organizace ve skutečnosti letiště je. Toto vedlo k etnografické studii, která měla zachytávat chování bezpečnostních pracovníků i cestujících. Do průzkumu bylo zapojeno osm vzorků z mezinárodních i regionálních letišť v Evropě a jedno školící centrum. Zapojena byla jak menší, tak větší letiště. Seznam letišť, kde průzkum probíhal je uveden v tabulce.

Jednotlivé fáze výzkumu jsou uvedeny ve Schématu. Jak již bylo řečeno, nejdříve proběhla etnografická studie, jejímž cílem byla deskripce chování bezpečnostních pracovníků na letištích. Po získání dostatku informací o fungování letiště jako sociální organizace se přešlo k dalšímu kroku. Tím byla studie vybraných letišť. Použité metody je lišily v různých oblastech výzkumu. Kvantitativní metody byly využity pro sumarizování výsledků od zaměstnanců a bylo tedy možné zobecnit jistá fakta a doložit je statistickými údaji. Naopak pro budování scénářů a záznam výpovědí pracovníků o prožitých situacích bylo zapotřebí zvolit kvalitativní metody výzkumu.



Sběr dat probíhal třemi různými způsoby. Prvním zvoleným způsobem byly osobní rozhovory, kdy buď byly kladeny konkrétní otázky tazatelem, nebo bezpečnostní pracovník vyprávěl sám na bázi volného rozhovoru. Druhým způsobem techniky sběru dat byla dotazníková šetření. Data byla sbírána do standardizovaných archů, které se daly následně jednoduše strojově vyhodnotit. Posledním, třetím způsobem byly panelové výzkumy, prováděné na určitých vzorcích specializovaných pracovníků. Celkovým cílem projektu byl sociotechnický výzkum a odhalení kauzality chování bezpečnostních pracovníků. Po ukončení sběru dat byla provedena velká analýza těchto získaných empirických dat. Odvozené závěry přispěly k budování scénářů, simulací alternativních situací a následné návrhy tréninkových programů.

## Faktory ovlivňující výkonnost a chybovost pracovníků bezpečnostní kontroly

Práce je dominantní činností v životě každého člověka, respektive nejvýznamnější formou interakce člověka s předmětným světem. Z psychologického hlediska pracovní činnost definujeme jako specificky lidskou, cílevědomou činnost, zaměřenou na uspokojování jednak existenčních, jednak sociálně-psychologických potřeb.

Pracovní činnost člověka ovlivňují faktory, které ve vztahu k plnění pracovních úkolů vystupují jako určující. V psychologii jsou tyto činitele předmětem studia a nazýváme je determinanty pracovní činnosti. Obecně rozlišujeme mezi objektivními a subjektivními determinanty pracovní činnosti. Faktory ovlivňující výkonnost a chybovost pracovníka lze rovněž rozdělit na vnitřní, tedy psychické, a vnější, tedy faktory pracovního prostředí.

### *Psychické faktory*

Psychické faktory práce zahrnují psychosociální stres na pracovišti, psychickou pracovní zátěž, patologické vztahy - mobbing, bossing, šikanu a v neposlední řadě lze zmínit třeba syndrom vyhoření. Ve většině rozvinutých zemí se psychosociální faktory a faktory spojené s organizací práce stávají hlavními pracovními riziky.

#### Psychická pracovní zátěž

Psychická zátěž na pracovišti je jedním z nejsledovanějších a nejvíce hodnocených faktorů, které ovlivňují pracovní podmínky.

Výzkumem a dlouholetou praxí byla ověřena rizikovost několika základních kriterií a oblastí pracovních podmínek z hlediska psychické zátěže.

Patří k nim:

1. časový tlak a intenzita práce
2. vynucené pracovní tempo
3. monotonie
4. nároky v oblasti komunikace a kooperace
5. práce v třísměnném a nepřetržitém pracovním režimu a noční práce

6. vlivy narušující soustředění (nejčastěji hluk-nutné posouzení nejen z hlediska intenzity, ale i kvality)
7. odpovědnost hmotná a organizační
8. riziko ohrožení vlastního zdraví a zdraví jiných osob
9. pracovní podmínky (práce vykonávané na dislokovaných pracovištích, spojené se sociální izolací)
10. šikana, mobbing a další problémy ve vztazích na pracovišti.

Jednotlivá kritéria a oblasti pracovních podmínek jsou využívána ke kategorizaci prací z hlediska faktoru psychické zátěže (obsahuje je i platná legislativa).

Kvalifikované posouzení psychické zátěže náleží odborníkovi, neboť se, kromě zmíněných kritérií, hodnotí i další stresory, obsah práce, její časové charakteristiky a další nezbytné okolnosti včetně posuzování osobnostních charakteristik zaměstnanců, jež náleží psychologovi.

Psychický pracovní stres

Pracovní stres je normální a běžný, zatímco nadměrný stres může ovlivnit produktivitu a může mít dopad na fyzické a duševní zdraví. Schopnost vypořádat se s ním znamená ve většině rozdíl mezi úspěchem a neúspěchem. Nelze úplně ovládat všechno v pracovním prostředí, ale to neznamená, že se jedná o bezmoc, dokonce i když nastane obtížná a zdánlivě neřešitelná situace. Způsob, jak zvládat pracovní stres není o tom dělat obrovské změny, nebo přehodnotit kariérní ambice, ale spíše o zaměření se na jednu věc, která je vždy tou hlavní příčinou.

Psychickou zátěž na pracovišti lze rozdělit do jednotlivých kategorií, které zatěžují duševní kondici pracovníka:

1. směnová práce
2. práce v noci
3. monotónní práce – pohybová, úkolová
4. práce ve vynuceném tempu
5. Psychosociální stres na pracovišti vzniká při nevhodném způsobu řízení podniku a nevhodných způsobech chování na pracovišti:
6. Špatná organizace práce
7. Dlouhá či nepravidelná pracovní doba
8. Požadavky na vysoký výkon
9. Velká zodpovědnost
10. Malé možnosti rozhodovat o práci
11. Špatná komunikace mezi nadřízenými a pracovníky
12. Malá informovanost pracovníků o záměrech vedení
13. Špatné kolegiální vztahy – konkurence, kliky, šikana
14. Násilí na pracovišti
15. Nepřiměřeně nízká odměna
16. Nedostatek času na soukromé záležitosti, rodinu
17. Obavy o zdraví na pracovišti – nedostatečná ochrana, apod.

## Mobbing

Pojem mobbing je odvozen z anglického výrazu „to mob“, který můžeme přeložit jako napadat, spílat, útočit, urážet, utlačovat, vrhat se na někoho. Termín mobbing jako první použil ve svých studiích chování zvířat etolog Konrád Lorenz, který zkoumal útoky zvířecí smečky na vetřelce.

Za mobbing se tedy považuje souhrn takových jednání na pracovišti, která mají za cíl nějakou osobu znevážit, poškodit její pověst, narušit její sebeúctu a sebevědomí a mohou způsobit škody na jejím zdraví. Podle německého psychologa a odborníka na problematiku mobbingu Hanse-Jurgena Kratze, je mobbing „řada negativních komunikativních jednání, jichž se pravidelně dopouští jednotlivec nebo několik osob vůči určitému člověku po určitou dobu (nejméně půl roku)“.

S občasnými neshodami a výměnami názorů v pracovním kolektivu se lidé zpravidla umějí bez následků vyrovnat. Nebezpečné však začínají být mezilidské vztahy tehdy, když někdo systematicky, cíleně a často i protiprávně zasahuje do pracovního i soukromého života druhého člověka. Útočník nepřátelsky napadá jiného zaměstnance a podrobuje ho ponižujícímu psychickému deptání, upřesňuje Kratz.

Mobbing může mít více podob. Mobbing provozovaný nadřízeným, kdy vedoucí pracovník vyvíjí na podřízeného tlak tak, aby si vynutil jeho přizpůsobení a poslušnost nebo ho dostal z pracovního místa, se nazývá bossing. Naopak útoky zaměstnanců vůči vedoucím pracovníkům s cílem je zničit či poškodit, se označují jako staffing. Mobbingem je ale i úmyslná manipulace s informacemi, se kterými člověk pracuje, s cílem mu ublížit a způsobit problémy. Mobbingem je také pomlouvání, obtěžování některého z kolegů, snaha vyloučit ho z kolektivu nebo z firmy.

Obětí mobbingu se může stát prakticky kdokoliv bez ohledu na věk nebo obor činnosti. Některé výzkumy však ukázaly vyšší riziko ve zdravotnictví, školství a ve státní správě, ve velkých podnicích a u zaměstnanců středního a staršího věku. Terčem mobbingu mohou být jak lidé nesmělí, neprůbojní, málo výkonní či psychicky slabí, kteří k šikanování svým způsobem vyzývají, tak i sebejistí, samostatní a schopní zaměstnanci, kteří ostatní převyšují, a proto se jich kolegové chtějí zbavit. „Systematické intrikování, útoky, které proti nim vedou nadřízení nebo kolegové, je postupně připravují o sebevědomí i pracovní výkon.“

### *Bossing*

Bossing je jakousi podskupinou mobbingu. Je specifický tím, že šikany se dopouští nadřízený pracovník. Bossing je psychická šikana v zaměstnání, které se dopouští na svém podřízeném nadřízený pracovník. Jedná se tedy o chování nadřízeného, které poškozuje podřízeného před jeho kolegy, znesnadňuje či znemožňuje mu jeho práci. Bossing se samozřejmě vyvíjí a stupňuje. Tato šikana zhoršuje vztahy na pracovišti a zvyšuje kult osobnosti vedoucích.

Za šikanu (bossing) může být považováno:

- přehnané kontrolování plnění povinností či docházky,
- neschválení dovolené,
- arogantní chování,
- slovní urážky,
- nedocenění práce či častá a neoprávněná kritika,
- zesměšňování před kolegy,
- zadávání příliš složitých úkolů (na které nemá podřízený kvalifikaci nebo jsou nesplnitelné),
- zabraňování přístupu k informacím např. od nadřízených-vede k neinformovanosti,
- nemožnost vyjádřit svůj názor nebo navrhnout své návrhy
- přisvojení si práce podřízeného jeho šéfem,
- sexuální obtěžování,
- bezdůvodné vyhrožování výpovědí (ukončením služebního poměru),
- různé naschvály (odebrání kancelářských potřeb, apod.),
- přemíra přesčasů
- probírání drobných chybiček, které jsou u ostatních přehlíženy, atd.

Šikana

Šikana – to je nemoc, nemoc toho, kdo šikanuje. Je to „nemocné“, tedy patologické chování. Většina projevů šikany naplňuje skutkovou podstatu trestných činů. Při posuzování toho, co je a co není šikana, musíme mít na zřeteli především to, jak uvedené projevy působí na toho, komu jsou určeny, tedy na oběť šikany. Důležitým znakem šikany je nepoměr sil mezi agresorem a obětí. U šikany je typickým znakem samoúčelnost převahy agresora nad obětí. To odlišuje šikanu od běžných „chlapeckých šarvátek“ mezi spolužáky. K tomu, abychom mohli hovořit o šikaně, musí existovat agresor, oběť a prostředí, ve kterém se šikana uskutečňuje. Šikanování je velice závažný, společensky nebezpečný jev, ohrožující oběť fyzicky, ale zejména psychicky. To jsou důvody, proč nesmíme šikanu přehlížet nebo zlehčovat. Šikanování je nutno chápat jako poruchu vztahů. A to nejen mezi agresorem a obětí. Šikana se nikdy neděje ve „vzduchoprázdnu". Šikana vzniká tam, kde existují ve skupině, ve třídě, nezdravé vztahy, kde je silná diferenciace na silné a slabé. Ve školních kolektivech existuje vážné nebezpečí, že i pedagog, často neúmyslně, ale mnohdy záměrně dá „zelenou“ silnějšímu jedinci, který pak začne vykonávat to, co vede k šikaně. Problém šikany tedy nelze léčit jako problém vztahu mezi agresorem a obětí, aniž bychom léčili celou skupinu. To je jedna z nejčastějších chyb, ke které při řešení problému šikany dochází.

Syndrom vyhoření

Syndrom vyhoření (burn-out syndrome) znamená ztrátu profesionálního zájmu nebo osobního zaujetí u pracovníka některé z psychicky náročných profesí. Nejčastěji se spojuje se ztrátou činorodosti a smyslu práce, projevuje se pocity zklamání, hořkosti při hodnocení minulosti, postižený ztrácí zájem o svou práci, spokojuje se s každodenním stereotypem a rutinou, nevidí důvod pro další sebevzdělávání a osobní růst, snaží se pouze přežít a nemít problémy. Ve vývoji lze definovat několik stadií:

1) jedinec by chtěl pracovat co nejlépe, touží po úspěchu, ale ten nepřichází,
2) nic nestíhá, je stále v časové nouzi, jeho práce začíná ztrácet systém,
3) výskyt běžných symptomů neurózy, provázený pocitem, že něco musí pořád dělat, výsledkem je chaos,
4) pocit „musím“ se ztrácí a obrací ve vzdor: „nemusím nic.“

Nakonec kolegové obtěžují už jen svou přítomností, pryč jsou zbytky zájmu, nadšení, zůstala jen únava a zklamání.

Zodpovědná práce pracovníka bezpečnostní kontroly patří k rizikovým profesím, při nichž se osobnost člověka opotřebovává. Pracovník bezpečnostní kontroly přichází do kontaktu s lidmi, s cestujícími. Práce s lidmi je všeobecně považována za psychicky náročnou. Obzvláště tehdy, když cestující vnímají průběh bezpečnostní kontroly za značně obtěžující a zdržující. Pracovník je tedy v očích cestujících mnohdy vnímán negativně. U této pozice se tedy vyskytuje značný psychický nápor, který musí denně pracovníci při vykonávání svého zaměstnání překonávat, což může vést až k rozvoji syndromu vyhoření.

### *Vnější faktory pracovního prostředí*

Pracovní prostředí je všeobecně dáno stavebním, prostorovým a přístrojovým vybavením pracoviště, estetickou úrovní a organizací práce spolu s vhodnou tepelnou, ventilační, světelnou a zvukovou pohodou.

Pracovní prostředí je pro člověka světem, ve kterém tráví přibližně třetinu svého života, proto je důležité, aby se v něm cítil příjemně a svou pracovní činnost vykonával se spokojeností, zájmem.

Úspěch v pracovní činnosti je nutným předpokladem pocitu spokojenosti. Všechny faktory pracovního prostředí mají současně vliv na zdraví a dopad na psychiku, na pohodu a pracovní výkon osobnosti. Jsou to nejen materiální podmínky, např. architektonické řešení pracovních prostor, urbanistické řešení komplexu provozních budov, estetická úroveň řešení pracovních interiérů a exteriérů, stav technického rozvoje, přístupové komunikace, čistota prostorů, osvětlení, barevná úprava, hluk, mikroklimatické podmínky, ale i sociální pracovní podmínky, např. motivace, uspokojení z práce, typ pracovní skupiny, vztahy v ní, psychosociální klima a typ řízení. Celé chování pracovního subjektu se nazývá kultura a image.

Špatně řešené pracovní prostředí může vést k pocitům nespokojenosti, subdeprese až deprese, k úzkostem, k pocitům únavy, až vyčerpanosti a k duševním poruchám a samozřejmě k celkové pracovní nevýkonnosti.

Vedle psychických faktorů působících na pracovníka existuje i řada dalších neméně důležitých faktorů tvořících pracovní prostředí. Mezi nejdůležitější faktory působící na pracovníka tedy podle Státního zdravotního ústavu (2013) patří:

- hlučnost
- osvětlení
- barevná psychologie
- tepelné podmínky
- vůně a pachy na pracovišti.

Hlučnost

Jedná se o směsici nejrůznějších tónů a šumů. Tiché pracoviště je pro psychiku i osobnost velkou výhodou. Vykonává-li člověk jednoduchou činnost, není účinek hluku na tuto činnost většinou příliš velký. Rušivý účinek hluku je však dobře patrný při vykonávání složitější duševní činnosti. Dlouhodobá expozice hluku dokonce u mnoha pracovníků způsobuje po létech nervovou labilitu s typickými znaky neurózy. K oslabené odolnosti vůči hluku přispívají i sociální konflikty na pracovišti. Pro pracovníky bezpečnostní kontroly je tento prvek obzvláště důležitý. V okolí prostor, kde probíhá bezpečnostní kontrola, se shromažďuje mnoho cestujících, kteří čekají na možnost absolvování bezpečnostní kontroly s cílem pokračovat v odbavovacím procesu. Mnohdy se jedná i počty přibližujícím se stovkám osob. Pro bezpečností pracovníky tak vzniká nepříjemné hlučně pracovní prostředí. Lidé spolu komunikují, řeší pracovní záležitosti, telefonují, střídají se zde různé jazyky,…, což na pracovní psychiku působí značně negativně. Bohužel zamezení tohoto nežádoucího vlivu je neovlivnitelné a zcela nemožné.

Osvětlení

Podmínky pro osvětlení pracovišť upravuje Nařízení vlády č. 361/2007 Sb. Osvětlení pracovišť denním, umělým, popřípadě sdruženým osvětlením musí odpovídat nárokům vykonávané práce na zrakovou činnost, pohodu vidění a bezpečnost zaměstnanců v souladu s konkrétními technickými požadavky obsaženými v příslušných českých technických normách. Špatné osvětlení může totiž zapříčinit nejen bolesti hlavy, má vliv na psychiku pracovníka, ale je dokázáno, že vlivem špatného osvětlení bývá snížena výkonnost při tělesné a duševní práci až o 30 %. Lampy a zářivky by měly být klinicky testovány, aby nezatěžovaly zrakový nerv. Psychická pohoda je u bezpečnostních pracovníků považována za velice důležitou. Zvolení vhodného osvětlení by tedy mělo být tedy samozřejmostí a to nejen v okolí pracoviště bezpečnostní kontroly, ale i v areálu celého letiště.

Barevná psychologie

Použití barev v pracovním prostředí nejen příznivě ovlivňuje pracovní pohodu, ale má i ekonomické důsledky. Usnadňuje a urychluje orientaci, zvyšuje bezpečnost práce a usnadňuje rozlišovací (diferenciační) procesy.

Z hlediska psychologického účinku se barvy dělí na studené a teplé. Mezi studené barvy patří modrá a zelená a mezi teplé barvy patří červená, oranžová a některé odstíny žluté. Barevné změny jsou citlivými osobami vnímány i povrchem kůže, nejen zrakem. Lidé se liší mírou citlivosti na barvy. Často se uvádí, že ženy dávají přednost teplým a sytým barvám a muži zase barvám tlumeným. Předpokládá se, že barvy mohou ovlivnit i zdravotní stav člověka, a to jak kladně, tak i záporně. V pracovním prostředí bezpečnostních pracovníků

převládají většinou barvy světlé, které působí spíše chladně a formálně, což splňuje svůj účel, neboť v lidech evokují pocit pořádku a jakéhosi řádu.

Tepelné podmínky

Významný vliv na zdraví pracovníků, pracovní pohodu a výkonnost, mají také mikroklimatické, neboli tepelné podmínky. Tepelný stav pracovního prostředí není určen jen teplotou vzduchu, nýbrž i dalšími důležitými faktory, a to vlhkostí vzduchu, rychlostí proudění vzduchu a teplotou okolních ploch a předmětů. V České republice jsou optimální hodnoty mikroklimatických podmínek zakotveny v hygienických předpisech. V těchto směrnicích jsou uvedeny hodnoty pro vnitřní teplotu a intenzitu výměny vzduchu na různých pracovních či hygienických zařízeních, např. kancelářské místnosti mají mít teplotu od 18°C do 21°C, vzduch se v nich má vyměňovat dvakrát až třikrát za hodinu

Vůně a pachy

Pracovní výkon také ovlivňují vůně, ale i pachy na pracovišti. Existuje obor, který se zabývá vlivy vůní na různé výkony a situace na pracovišti, který se nazývá „vonný marketing“. Marketing zabývající se vůněmi využívá poznatku, že vůně a pachy působí na limbický systém lidského mozku. Ten nepodléhá vědomé kontrole, a proto na podvědomé úrovni ovlivňuje naše pocity a chování. Protože takto popsaný mechanismus působení je příliš zjednodušený a jednotlivé vůně a pachy připomínají a vyvolávají v každém člověku individuální vzpomínky (ať už na něco příjemného či nepříjemného), je důležité, aby se pracovalo s vůněmi pod prahem lidského vnímání – tzv. podprahové koncentrace. Správně zvolená vůně odbourává pocit strachu, vytváří příjemnou atmosféru, podporuje koncentraci a vnímavost a již zmíněnou výkonnost. Pracovníci bezpečnostní kontroly jsou samozřejmě mnohdy vystaveni i negativně vnímaným vůním, tedy pachům.

Obsluha počítače

Za zcela běžnou je dnes již považována práce s počítačem. I pracovník bezpečnostní kontroly přijde do styku s informačními technologiemi, které dlouhodobě nepůsobí na psychickou pohodu zaměstnance pozitivně. Dle dnešních znalostí a zkušeností prakticky nelze pochybovat o tom, že masové používání počítačů s sebou přináší i řadu zdravotních potíží.

Jedná se např. o:

1. Problematiku elektromagnetického pole generovaného zobrazovací jednotkou
2. Zrakové obtíže
3. Obtíže pohybového aparátu
4. Psychosomatické obtíže.

Myšlenka Air Transport Security Knowledge Centre neboli Znalostního centra pro oblast Security v letecké dopravě vznikla za účelem vytvoření vhodného prostředku na podporu institucí, zabývajícími se problematikou ochrany civilního letectví před protiprávními činy.

Jen na území České a Slovenské republiky najdeme řadu firem a nejrůznějších subjektů, které se svou vědecko-výzkumnou, nebo jinou činností, snaží předcházet stále se zvyšující možnosti hrozeb ze strany terorismu a dalších osob či skupin, které by se mohli podílet na protiprávním jednání proti civilnímu letectví.

K usnadnění a zefektivnění činnosti těchto institucí bude založeno Air Transport Security Knowledge Centre (ATSKC) a to především k podpoře získávání a předávání kontaktů, informací a v neposlední řadě k rozvoji spolupráce mezi institucemi, při řešení problémů v této citlivé oblasti. ATSKC bude držitelem pouze takových dat, které v případě úniku nebudou moci být zneužity v takovém měřítku, které by mohlo vyvolat jakékoliv ohrožení projektů nebo civilního letectví vůbec.

Velice zjednodušeně lze o Znalostním centru hovořit, jako o jakési bance - o databázi, kde budou shromážděny kontakty na instituce se základními informacemi nejen o právě probíhajících projektech, ale zároveň o projektech, které již byly řešeny v minulosti. Tímto by se také omezilo, nebo v ideálním případě úplně předešlo duplicitním činnostem a s tím souvisejícím plýtváním peněžními prostředky a časem institucí, které si mohou být v řešení projektů vzájemně prospěšné.

Aby projekt mohl vůbec začít existovat, bylo potřeba najít vhodné místo, odkud by se databáze co nejefektivněji dala spravovat. Tímto místem se stala Vysoká Škola obchodní v Praze, jakožto instituce s řadou odborníků nejen v letectví, s potřebnými kontakty a tedy i předpokladem pro správné fungování a rozvoj Centra.

### Cíle a úkoly ATSKC

Mezi hlavní cíle a činnosti Centra patří:

- Správa elektronické databáze, která zahrnuje i pravidelnou aktualizaci, kontrolu a zpracovávání vkládaných dat. Tato data budou administrátoři projektu dále šířit v rámci portálu tak, aby neporušovala autorská práva a případně aby neprezentovala data, která by mohla jakýmkoliv způsobem ohrozit bezpečný provoz letecké dopravy. ATSKC bude schraňovat a prezentovat pouze značně omezené informace, aby v případě napadení a úniku dat z databáze nemohla třetí strana žádným způsobem těžit či jinak zneužít těchto informací.
- Pravidelné pořádání vědeckých konferencí, na které jsou zváni zástupci institucí, přispívajících nebo jiným způsobem využívajících portál. Konference by ideálně měly

mít časem mezinárodní charakter a měly by být zaměřeny nejen na provoz Centra a souvisejících otázek, ale také na otázky samotných výzkumů a hrozeb letecké dopravy.

Nápad využít bezpilotní vzdušný prostředek k užitečné činnosti je v podstatě velmi starý a jeho primární určení bylo, tak jako u mnoha jiných vynálezů, veskrze mírumilovné. Již před koncem devatenáctého století, v roce 1883, bylo použito upoutaného létajícího draku s instalovaným fotoaparátem k pořizování leteckého snímkování krajiny pro soukromé účely. Samotná spoušť závěrky aparátu pak byla tehdy ovládána napřímo operátorem pomocí dlouhé struny. Let draka, konstrukcí připomínajícího současné draky dětské, nebylo možno prakticky nijak řídit. Choval se jako klasické vztlakové těleso bez aerodynamických kormidel a tak byly směr a výška letu dány převážně směrem a silou větru, jakož i délkou vypouštěného lana. O patnáct let později bylo už obdobné techniky využito ve španělsko-americké válce k prvnímu leteckému průzkumu, a to snímkováním pozic protivníka za bojovou linií.

## Legislativní omezení bezpilotních prostředků

Cílem leteckých předpisů je zajištění ochrany posádky, cestujících, osob a majetku na zemi. V případě bezpilotních letadel odpadá problém s ochranou posádky a cestujících.

S žádným letadlem není možné létat, aniž by bylo příslušnou institucí pro provoz schváleno, a proto je potřeba, aby existovaly postupy pro schvalování letové způsobilosti pro všechny kategorie letadel – tzv. certifikaci.

Zároveň je nutné, aby byla daná kategorie přesně a jednoznačně vymezena. Takové požadavky je rovněž nutné přenést i na bezpilotní letadla. Tyto postupy, spolu s požadavky leteckých předpisů, by měly vždy zajistit maximální možnou bezpečnost dané letadlové konstrukce a následného provozu letadla.

Provozní požadavky kladené na bezpilotní letadla musí být stejné jako pro klasická pilotovaná letadla, aby se mohla při svém provozu bez problémů zařadit do vzdušného prostoru a riziko nehody bylo stejné nebo menší, než jaké je u pilotovaných letadel. Trendem je nevytvářet nové předpisy speciálně pro bezpilotní letadla, ale přizpůsobit bezpilotní letadla tak, aby byla rovnocennými elementy v řízeném vzdušném prostoru. Nicméně v některých případech, kde je podstatná odlišnost, se budou muset stávající přepisy upravit nebo vytvořit nové. I přes rychlý vývoj elektronických senzorů a programového vybavení umožňující automaticky vyhodnocovat krizové situace, nedokážu počítačové systémy zcela nahradit lidské rozhodování.

Z pohledu certifikace je vhodné BP rozdělit na dvě skupiny - do 150kg a nad 150kg. Letadla nepřesahující hmotnost 150kg, která nejsou regulována EASA, se mají certifikovat na státní úrovni. Letadla o hmotnosti vyšší než 150kg mají být certifikována na mezinárodní úrovni.

V současnosti se v celosvětovém měřítku problematika civilních bezpilotních letadel zastavila, jsou sice vytvořené speciální komise v rámci ICAO, EUROCONTROL. Situace na národní úrovni je postupném rozvoji. V několika státech jsou již civilní úkoly pomocí bezpilotních prostředků plněny, v řadě dalších států se na vytvoření podmínek pro civilní provoz intenzivně pracuje. Pomocí těchto aktivit se postupně zasahuje do různých částí problematiky civilních bezpilotních prostředků (certifikace, vyhýbání se srážkám, integrace …) Získané zkušenosti se předávají vytvořeným komisím pro rozvoj civilních bezpilotních letadel, ty všechny informace shromažďují a analyzují. Postupně se tak zaplňují neprozkoumané oblasti, ale až když bude většina problémů vyřešena a ověřena, dojde k vydání jednotných celosvětových požadavků a doporučení.

Tyto předpisy způsobí velmi intenzivní zrychlení rozvoje civilních BP. Proto již v dnešní době řada výrobců provádí vývoj a výrobu civilních bezpilotních letadel. Právě jejich výrobky budou pak mít na trhu velký náskok.

### Platná legislativa ČR

V současné době český **Zákon o civilním letectví 49/1997 sb. § 52** řeší základní požadavky na létání letadel bez pilota:

„*Letadlo způsobilé létat bez pilota může létat nad územím České republiky jen na základě povolení vydaného Úřadem pro civilní letectví se sídlem v Praze (dále jen "Úřad") a za podmínek v tomto povolení stanovených. Úřad povolení vydá, nebude-li ohrožena bezpečnost létání ve vzdušném prostoru, stavby a osoby na zemi a životním prostředí.*"

Postup zpracování žádosti o povolení k létaní dle **§ 52 leteckého zákona č.49/1997 Sb.**:

- vedení evidence UAS;
- vyhodnocení parametrů UAS, bezpečnostní dokumentace, způsobu provozu, dokladu o pojištění, čestná prohlášení pilota;
- v závislosti na kategorii přezkoušení teoretických znalostí a praktických dovedností pilota a letových vlastností UAS;
- výběr správního poplatku;
- vydání povolení;
- v případě leteckých prací následuje žádost o provádění leteckých prací; povolení k létání slouží jako doklad splnění zákonných požadavků na zápis do rejstříku, kvalifikace personálu a letovou způsobilost.

Naproti tomu **Úmluva o mezinárodním civilním letectví (Chicagská úmluva), článek 8** stanovuje:

„*Žádné letadlo, které je způsobilé být řízeno bez pilota, nesmí létat bez pilota nad územím smluvního státu, leč se zvláštním zmocněním tohoto státu a v souhlase s podmínkami takového zmocnění. Každý smluvní stát se zavazuje zajistit, aby let takových letadel bez pilota byl v*

*oblastech, přístupných civilním letadlům, řízen tak, aby bylo vyloučeno nebezpečí pro civilní letadla.*“

Jak je vidět, oblast legislativy v České republice není nijak rozsáhlá. Podle mého názoru je to dáno tím, že požadavky se budou stanovovat až na konkrétní letadlo, které se bude využívat pro civilní provoz. Tento stav se rychle blíží, v ČR se již za pomoci grantů uskutečňuje vývoj civilních bezpilotních letadel.

Na základě **článek 8 Chicagské úmluvy** byl doplnění ICAO Annex 2, který řeší obsah a podmínky žádosti o povolení dle čl. 8 Úmluvy).

ICAO Annex 7 - klasifikace letadel.

ICAO Annex 13 - letecké nehody a incidenty.

S ohledem na rozvoj letectví v oblasti bezpilotních systémů a leteckého modelářství a z důvodu potřeby dalšího posilování úrovně bezpečnosti letového provozu, osob a majetku na zemi byla ve spolupráci **Ministerstva dopravy, Úřadu pro civilní letectví** a dalších subjektů státní správy, zástupců leteckého průmyslu a letecké veřejnosti, vypracována **koncepce regulace bezpilotních systémů**.

Ta vychází z platné legislativy a mezinárodních standardů a doporučení a je zaváděna v několika krocích. **Základní pravidla** vychází z předpisu **L2 - Pravidla létání**, který definuje mezinárodní standardy o létání. Zde jsou však definována pouze obecná **pravidla létání**, bez hlubšího zaměření na problematiku UAV.

V roce 2005 byl vydán Řízením letového provozu ČR **oběžník s označením AIC C 13/08**. Ten byl reakcí na připravované doplnění předpisu L2, tzv. **doplňku X**, který nabyl platnosti 1. 3. 2012 a kterým se do předpisu **L2 zapracovávají zásady pro létání s bezpilotními prostředky a směrnice CAA/S-SLS-010-n/2012 zveřejněná Úřadem pro civilní letectví**.

Letecký předpis L2 řeší podrobnější úprava regulace letadel a pilotů zapojených do leteckých prací a taky omezení nezkoordinovaného provozu modelů letadel v blízkosti letišť.

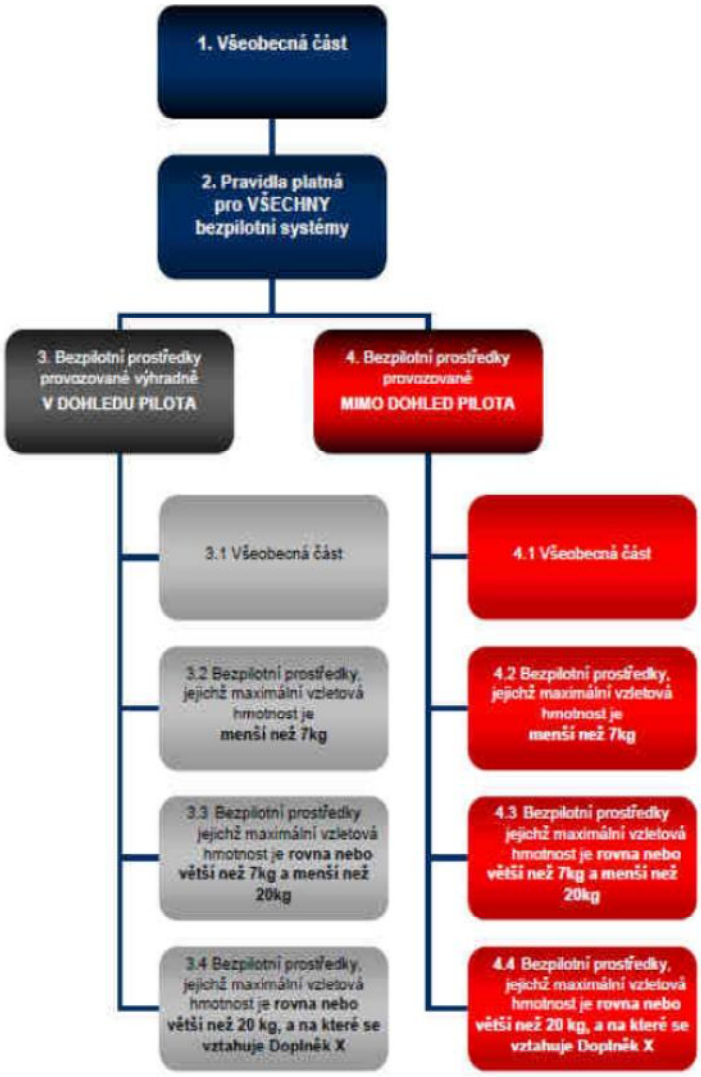
Podle oběžníku AIC se za bezpilotní prostředek považuje letadlo, které je konstruováno pro provoz bez pilota - člověka na palubě. Nesmí však dojít k omylu, že bezpilotní prostředek nemá pilota. Pilot je ten, kdo je za bezpilotní prostředek odpovědný a nepohybuje se vůči zemi tzn., že není na palubě jiného létajícího objektu, ze kterého bezpilotní prostředek řídí.

Za bezpilotní systém se považuje systém skládající se z bezpilotního prostředku, řídicí stanice a jakéhokoliv dalšího prvku nezbytného k umožnění letu, jako například komunikačního spojení nebo prvku pro vypuštění a návrat. Bezpilotních prostředků, řídících stanic nebo prvků pro vypuštění a návrat může být v rámci bezpilotního systému více.

Podle **ustanovení doplňku předpisu L2**, Pravidla létání, který právě prochází veřejným připomínkovým řízením, je za bezpilotní systém považován i model letadla, včetně

vybavení nezbytného pro jeho provoz. Tato specifikace byla zavedena na základě nutnosti zabezpečit jednotnost regulace všech UAV, ať jsou používány pro profesionální (komerční) účely, anebo rekreační a sportovní účely a rovněž bere v úvahu mezinárodní vývoj regulačních požadavků.

Vzhledem k **nutnosti zajistit bezpečnost civilního letectví**, osob a majetku na zemi jako celku byla přijata forma regulace všech bezpilotních prostředků bez ohledu na jejich hmotnost a využití. Doplněk X předpisu L2 je strukturován podle následujícího obrázku.




Z výše uvedené struktury je patrné základní a podrobné členění doplňku. Dělení podle hmotnosti je už pouze jakýmsi rozšířením základních pravidel platných pro všechny. S různou hmotností UAV jsou rozdílné požadavky, jako např. nutnost provozovat model pod dohledem, s vykonanými zkouškami ÚCL, pojištěním atd.

Tabulka omezení a povinností pilota je uvedena v příloze této práce.

Současně s přijetím platnosti tohoto dokumentu - doplňku X vyšly také postupy pro vydávání povolení k létání letadla bez pilota. Kromě seznamu nutných technických a

teoretických znalostí pro udělení oprávnění pro pilota a stroj jsou zde uvedena i kritéria, kdy je oprávnění nutné:

- pokud má model letovou hmotnost pod 20 kg a je využíván ke sportovním a rekreačním účelům, není oprávění nutné,
- pokud má model letovou hmotnost nad 20 kg, je nutné oprávnění pro jakýkoliv způsob použití,
- model jakékoliv hmotnosti, který je využíván k vědeckým a komerčním účelům, podléhá registraci a nutnosti získat oprávnění.

V následujícím odstavci jsou uvedena základní pravidla pro provoz UAV na území ČR:

*„ let bezpilotního letadla smí být prováděn jen takovým způsobem, aby nedošlo k ohrožení bezpečnosti létání ve vzdušném prostoru, osob a majetku na zemi a životního prostředí „*

*„ s výjimkou provozu bezpilotního prostředku mimo dohled pilota musí pilot trvale udržovat vizuální kontakt s bezpilotním prostředkem, přičemž prostředek musí zůstat pro pilota viditelný i bez vizuálních pomůcek ve všech fázích letu*

*Za vizuální pomůcky se nepovažují brýle a kontaktní čočky na lékařský předpis“*

*„ provoz bezpilotního prostředku mimo dohled pilota je možný pouze v rezervovaných nebo vyhrazených vzdušných prostorech. Žadatel o využití takového vzdušného prostoru postupuje v souladu s postupy uvedenými v Letecké informační příručce ČR, části ENR 1.1.9 „*

*„bezpilotní prostředek se nesmí použít k přepravě nebezpečných látek nebo zařízení, které by mohly způsobit obecné ohrožení“*

*„bezpilotní prostředek se nesmí použít ke shazování předmětů za letu“*

*„lety bezpilotních prostředků se nesmí provádět v noci,“*

*„s výjimkou provozu bezpilotního prostředku mimo dohled pilota se nesmí lety*

*bezpilotních prostředků provádět ve výšce větší než 100 m nad zemí,“*

s výjimkou, kdy tak povolí Úřad na základě předchozího souhlasu příslušného správního orgánu či oprávněné osoby, se lety bezpilotního prostředku nesmí provádět v ochranných pásmech, zejména pak v ochranných pásmech:

- podél nadzemních dopravních staveb
- podél tras nadzemních inženýrských sítí
- podél tras nadzemních telekomunikačních sítí
- v okolí vodních zdrojů
- podél hranic zvláště chráněných území
- v okolí nemovitých kulturních památek, památkových rezervací, památkových zón
- v blízkosti přírodních léčivých zdrojů a zdrojů nerostného bohatství.

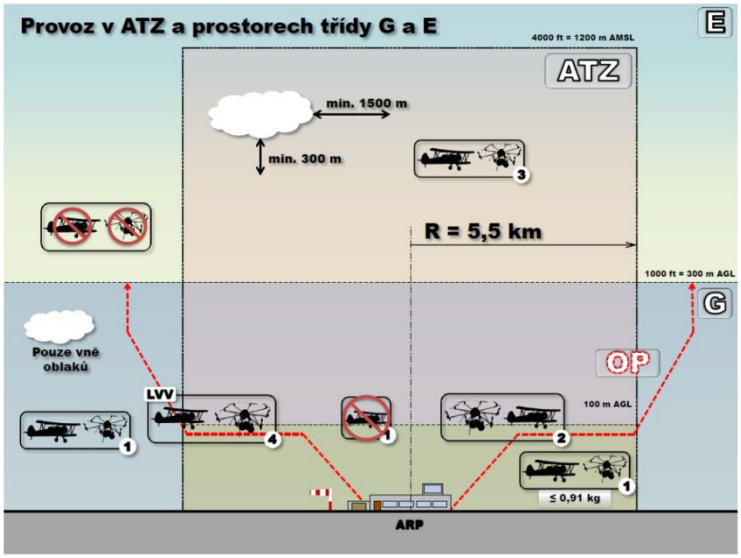
Na základě doplňku X předpisu L2 je sestavená tabulka. V tabulce V tabulce jsou kroky, které každý pilot modelu, UAV či UAS musí provést, aby jeho činnost byla v souladu

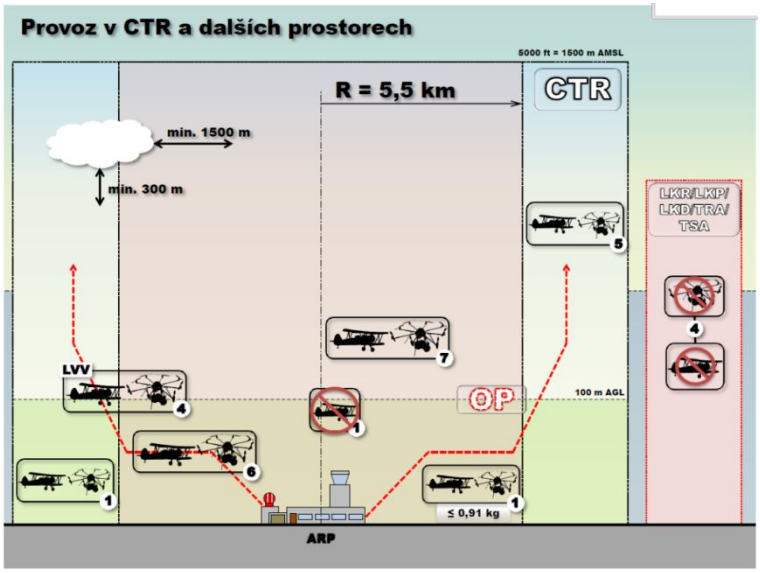
se zákony platnými v České republice. Vždy záleží na dvou základních parametrech, a to sice na maximální vzletové hmotnosti (MTOW) a na druhu činnosti. Činnost prováděná s letounem je rozčleněna dále do tří podskupin: rekreační a sportovní činnost; výdělečná, experimentální a výzkumná činnost; bezpilotní letadla provozovaná mimo dohled pilota. Nutno upozornit, že UAV, UAS a modely spadají legislativně pod ÚCL.

| MTOW [kg] | ≤ 0,91 | | > 0,91 a < 7 | | ≤ 7 a ≤ 20 | | > 20 | | UAV provozované mimo dohled pilota |
|---|---|---|---|---|---|---|---|---|---|
| účel | rekreačně sportovní | ostatní | rekreačně sportovní | ostatní | rekreačně sportovní | ostatní | rekreačně sportovní | ostatní | |
| evidence pilota | NE | ANO | NE | ANO | NE | ANO | ANO | ANO | ANO |
| evidence letadla | NE | ANO | NE | ANO | NE | ANO | ANO | ANO | ANO |
| test teor. znalostí pilota | NE | NE | NE | NE | NE | ANO | ANO | ANO | ANO |
| povolení k létání | NE | ANO | NE | ANO | NE | ANO | ANO | ANO | ANO |
| povolení k provádění LP a LČPVP | NELZE | ANO | NELZE | ANO | NELZE | ANO | NELZE | ANO | NELZE |
| označení ID štítkem | NE | ANO | ANO | ANO | ANO | ANO | ANO | ANO | ANO |
| poznávací značka | NE | NE | NE | ANO | NE | ANO | NE | ANO | ANO |
| použití „failsafe“ | NE | NE | ANO | ANO | ANO | ANO | ANO | ANO | ANO |

Podrobnější a přesné definování pojmů lze dohledat v doplňku X předpisu L2 a dále v **směrnici CAA/S-SLS-010-n/2012** zveřejněné úřadem pro civilní letectví.

Předpis L2 taky stanovuje let bezpilotního letadla a/nebo modelu letadla prováděn jen v následujících prostorech:






V současné době probíhá Novela leteckého zákona č.49/1997 Sb., kde budu právě komplexní podmínky implementace UAS.

Mimo přímou angažovanost ÚCL spadá:

- letová způsobilost UAS spadající pod EASA (zejména nad 150 kg MTOM)
- provoz modelů letadel do 20 kg mimo CTR a ATZ (koordinační dohody)
- státní RPA (vojenská, policejní, celní) – příslušná ministerstva zajišťují splnění závazku z Chicagské úmluvy: „Smluvní státy se zavazují, že vydávajíce předpisy pro svá státní letadla, budou náležitě dbáti bezpečnosti létání civilních letadel.“

Modely letadel spadají do definic letadla a dálkově řízeného letadla dle ICAO Annex 7

Modely letadel nejsou vyjmuty z Úmluvy o mezinárodním civilním letectví, avšak:

- UASSG a Sekretariát ICAO rozhodly, že není zapotřebí stanovovat celosvětově harmonizované standardy pro modely letadel, a
- je ponecháno na odpovědnosti každého členského státu, aby vyvinul vlastní regulační rámec vztahující se na provoz modelů letadel v oblastech přístupným jiným civilním letadlům

## Vojenské využití

Entuziasmus konstruktérů a leteckých průkopníků v počátcích dvacátého století byl ovšem cílen především na zvládnutí pilotovaného a řízeného letu s letadlem těžším vzduchu s vlastním pohonem, posléze korunovaný úspěšným letem bratří Wrightů v prosinci 1903. První pokusy o řízený let bezpilotního prostředku pak proběhly v další dekádě. Potřeby válečné mašinérie za první světové války podnítily pokusy s rádiem řízenými bezpilotními prostředky různých typů, v té době určených především pro potřeby průzkumu bojiště. Ale zůstalo pouze u experimentů, žádná konstrukce dálkově řízeného letadla nepřekročila hranici pokusů. Až ve třicátých letech minulého století vyvinuli inženýři Britského Královského

Námořnictva prakticky použitelný, rádiem dálkově řízený bezpilotní letoun Queen Bee, dosahující rychlosti 160km/h. I tento typ trpěl řadou nedostatků a jeho nasazení jako útočného dálkového stroje bylo víc než problematické, ale jako první prokázal skutečnou provozuschopnost, a kdyby nic jiného, dokázal britským pilotům sloužit jako funkčně létající výcvikový vzdušný terč.

Rovněž další vývoj bezpilotních prostředků je bohužel spojen především s válečným využitím. Během druhé světové války vyvíjelo Německo, jako takzvané zbraně odplaty, více druhů bezpilotních systémů. Jednalo se prvořadně o křídlaté létající bomby V-1, poháněné pulsačním náporovým motorem a vybavené gyroskopicky ovládaným aerodynamickým řízením. Jak mimořádně výkonný pohon, tak spolehlivé autonomní řízení prokázaly nebezpečnou efektivitu takovýchto bezpilotních systémů. Ještě sofistikovanější a ve svém dopadu nebezpečnější, byl vývoj raketových střel V2, vedený v Peenemünde konstruktérem Wernherem Von Braunem. Oba tyto bezpilotní systémy prokázaly, že UA prostředky nemusí být jen podpůrným systémem, ale mohou sloužit jako plně autonomní a funkční celky. Ale i spojenci vyvíjeli bezpilotní létající bomby. Kupříkladu USA vyvíjely v rámci operace Afrodita bezpilotní verze těžkých bombardérů Boeing B-17 Flying Fortress a Consolidated PB4Y-1 Liberator. Tyto letouny byly zbaveny výzbroje a posádky a měly být po mez nosnosti naplněny trhavinou, což byl více než dvojnásobek nosnosti bomb. Následně měly být pomocí rádiového řízení a sledování televizním přenosem na dálku, navedeny na cíl, kde měly explodovat. Samotný start byl proveden klasicky pilotovaný, protože rádiové ovládání bylo ještě nedostatečně komplexní pro bezpečné provedení vzletu. Posádka, tvořená pouze dvojicí pilotů, pak měla, po nastoupání do určené letové hladiny a uvedení letadla do požadovaného směru, vyskočit s padáky. Následující let a navedení na cíl měl na starosti operátor, letící v upraveném bombardéru B-17, sledující let díky televiznímu přenosu. O těchto bezpilotních letounech se také již mluvilo jako o dronech. Ovšem technicky i technologicky byly tyto letounové bomby velmi nespolehlivé a technické poruchy měly za následek smrt více posádek. Mezi dalšími při jedné misi s přestavěným Liberatorem BQ-8 zahynul i poručík Joseph P. Kennedy, nejstarší bratr budoucího amerického prezidenta Johna. F Kennedyho. Ačkoli bylo po zkušebním programu minimálně deset dronů použito na vytipované cíle, jejich úspěšnost byla velmi nízká, zatímco nebezpečí pro posádky extrémně vysoké a tak byla celá operace Afrodita ukončena.

S vypuknutím studené války nedlouho po německé kapitulaci, započala firma Ryan Aeronautical s vývojem bezpilotního letounu poháněného proudovým motorem. V roce 1951 představila a úspěšně zalétala plně řiditelný typ XQ-2 Firebee, který se tak v podstatě stal prarodičem současných vojenských bezpilotních letounů. Tento bezpilotní prostředek byl vypouštěn za letu z nosiče tvořeného upraveným bombardérem a byl dálkově řízen pilotem, letícím v mateřském letadle. Z prvního prototypu vyvinula firma Ryan úspěšně použitelný dron typ BQM – 34 Firebee, který se v průběhu šedesátých let osvědčil během vietnamského konfliktu jako velmi spolehlivý a efektivní prostředek s celkem více než 34 000 odlétaných misí. I když se jednalo o vojenský typ, byl to historicky první bezpilotní prostředek skutečně široce nasazovaný a tak zde uvádím jeho technickou specifikaci.

Ryan BQM – 34 Firebee

- délka 6,9 m
- rozpětí 3,9 m
- výška 2,1 m
- max. vzletová hmotnost 1406,2 kg
- maximální rychlost 0,97 M
- dostup 18,3 km
- výdrž 1:55 h
- pohon GE J-85-100, 12,93 kN

Obdobný vývoj vojenských bezpilotních prostředků probíhal i v tehdejším sovětském svazu v konstrukčních kancelářích Lavočkin a Tupolev. Typ La-17 byl technicky i výkony plně na úrovni svého amerického protějšku, byť měl menší výdrž. Tupolevovy konstrukce, například Tu-143 byly používány nejen Sovětským svazem, ale využívala je jako průzkumné například Sýrie v roce 1982 nad Izraelem v Libanonské válce.

Ostatně kromě soupeřících mocností USA a SSSR byly bezpilotní prostředky vyvíjeny i v jiných zemích, od 70. let kupříkladu také v Izraeli. Byly to úspěšné bezpilotní letouny Scout a Pioneer. A právě tyto typy posunuly cílení vývoje směrem k menším a lehčím letadlům. Objevily se prvky lehčí kluzákové konstrukce, letouny byly menší, jejich produkce byla levnější a snazší bylo i ovládání. IAI Scout (v hebrejštině zvaný Žluva), byl průzkumný bezpilotní prostředek poháněný pístovým motorem a mimo jiné mohl nést i kameru s 360° úhlem záběru. Tento UA byl se vzletovou hmotností 159 kg prakticky o řád lehčí, než soudobé proudové drony a s 38 kilogramy užitečné zátěže měl výdrž přes 7 hodin letu. Obdobné parametry měl konkurenční Tadiran Mastiff. (Zde je vhodné zmínit, že se v současnosti jen na půdě Izraele vyvíjí, či už je v provozu zhruba 45 typů UA všech kategorií, zatímco v USA a v Číně se již může mluvit o stovkách typů.) Byť tyto bezpilotní letouny nedosahovaly vysokých rychlostí, ukázaly se jako dobře využitelný, efektivní a relativně velmi levný prostředek pro pěchotní průzkum, operující přímo z bojiště. Jejich úspěšnost byla natolik přesvědčivá, že o podobný menší typ projevily zájem i ozbrojené složky obou supervelmocí. Spojené státy ovšem, a to nejen díky legislativnímu omezení nákupu zahraniční bojové techniky, logicky stály především o vývoj vlastních prostředků. Od osmdesátých let tak kromě rychlých a těžkých proudových UA dostaly ve vývoji zelenou i střední typy, umožňující vyšší výdrž a řádově levnější pořizovací náklady i provoz. Miniaturizace ovšem zasáhla i do vývoje bezpilotních prostředků a tak zaznamenáváme v poslední dekádě největší rozmach vývoj právě u jejich nejmenších typů. Tyto takzvané mikro drony mají specifické rozměry od jednotek do desítek centimetrů a hmotnost se u nejmenších z nich počítá již na pouhé gramy. Jejich malé rozměry, nepatrná hmotnost a vysoká automatizace ovládání, umožňují jejich nasazení přímo v první linii minimálně školeným personálem. A právě vývoj a rozmach levnějších a menších typů bezpilotních prostředků nabízí i efektivní a ekonomické využití v civilní a komerční sféře.

## Počátky civilního a komerčního využití dronů

Společně s vývojem vojenským, se zvláště v posledních desetiletích začínají objevovat a prosazovat i konstrukce čistě civilní. Jakkoli by bylo pro výrobce logické použít konverze stávajících vojenských typů, jiné specifické požadavky na užití v komerčně-civilní oblasti působily na výrobce tlak k vývoji nových konstrukcí. A tak se začaly objevovat UA spíše subtilnější, než jejich soudobé vojenské protějšky. Tyto malé bezpilotní prostředky často původně vznikaly jako rádiem řízené modely, nebo sofistikované hračky a díky jejich velkosériové výrobě bylo brzy dosaženo velmi nízkých prodejních cen, přirozeně vedoucí k vyššímu obratu výrobců. A v komerční sféře to byly často právě výrobci modelářské techniky, kteří přicházeli na trh se stále dokonalejším řešením automatických systémů, sledujících a zabezpečujících jak stabilitu a směr letu UA, tak zjednodušujících jejich dálkové řízení. Levnější pořizovací cena, společně se snazším řízením a dostupnými přídavnými systémy, především sledovacími, postupně v komerčním sektoru zvedla poptávku po bezpilotních prostředcích všech typů. Malé komerční UA tak přestaly být doménou nadšenců a modelářů, ale v mnoha oblastech jejich působnosti se postupně nabízejí jako plnohodnotná varianta pilotovaných strojů, nebo i jiných sledovacích systémů. Kromě leteckého snímkování a filmování, začaly být bezpilotní prostředky nasazovány na monitoring požárů, pro sledování výšky hladin vodních toků, pátrání po zmizelých, bezpečnostní monitoring i ochranu národních parků. Ovšem díky poněkud živelnému růstu počtu létajících UA v civilní sféře, začalo být leteckým dohlédacím úřadům jasné, že i toto mladé letecké odvětví bude třeba regulovat a to dříve, než dojde k mimořádným událostem.

## Nutná legislativa a certifikace pro civilní letecký provoz

Rychlý rozvoj výroby a čím dál širší uplatnění bezpilotních prostředků v civilním sektoru, vyústil v potřebu koordinace jejich pohybu ve vzdušném prostoru a zavedení příslušných právně provozních předpisů. Jednotlivé státy sdružené v ICAO řešily tuto problematiku primárně sami, ale brzy bylo jasné, že bude třeba koordinovaného postupu.

### *Formování právního rámce*

V září roku 2002 vytvořila JAA / Eurocontrol pracovní skupinu UA Task Force k legislativnímu řešení požadavků regulace pohybu létajících bezpilotních prostředků. Úkolem bylo vyřešit pro UA otázky technické bezpečnosti, ochrany před protiprávními činy, zachování letové způsobilosti, provozní spolehlivosti, údržby a licencování. Pracovní skupina byla složena z 55 zástupců vlád a průmyslu, včetně jednoho zástupce FAA. První zpráva skupiny byla publikována v červnu roku 2004. Smyslem této zprávy byla pomoc ICAO, tedy Mezinárodní organizaci pro civilní letectví, pro podporu budoucích ICAO UA iniciativ a poskytování poradenství agentuře EASA pro bezpečnost letectví ve vývoji budoucích předpisů letové způsobilosti vztahujících se k civilním bezpilotním prostředkům.

Aby byl umožněn pohyb UA již v současné době v legislativním rámci příslušné země, ICAO vydala pokyn národním leteckým dohlédacím úřadům, aby vytvořily patřičné předpisy a případná omezení. Takto byl umožněn jak vývoj, tak provoz bezpilotních letadel již v současné době, ovšem s omezeními, která sníží pravděpodobnost nehod na přijatelnou úroveň. V České republice vydal v květnu 2013 Úřad pro civilní letectví Doplněk X k předpisu L2, který rozpracovává výše zmíněný požadavek Úmluvy a Postupy, stanovující podrobnosti pro jeho uvedení do praxe. Doplněk X definuje provoz bezpilotních leteckých prostředků, stanovuje podmínky jejich provozu a s ohledem na probíhající vývoj UA částečně v některých ohledech změkčuje tvrdost předpisů týkajících se nepilotovaných letadel. Je to například možnost nižší výšky letu malých UA nad terénem atd. Současně tento doplněk také přesně pojmenovává jednotlivé druhy UA a zavádí jejich kategorizaci.

*Kategorie létajících bezpilotních prostředků*

- Autonomní letadlo

Bezpilotní letadlo, které neumožňuje zásah pilota do řízení letu.

- Bezpilotní letadlo UA

Letadlo určené k provozu bez pilota na palubě. V mezinárodním kontextu se jedná o nadřazenou kategorii dálkově řízených letadel, autonomních letadel i modelů letadel. Pro účely Doplňku X k předpisu L2 se bezpilotním letadlem rozumí všechna bezpilotní letadla kromě modelů letadel s maximální vzletovou hmotností nepřesahující 20 kg.

- Bezpilotní systém (UAS)

Systém skládající se z bezpilotního letadla, řídicí stanice a jakéhokoliv dalšího prvku nezbytného k umožnění letu, jako například komunikačního spojení a zařízení pro vypuštění a návrat.

- Model letadla

Letadlo, které není schopné nést člověka na palubě, je používané pro soutěžní, sportovní nebo rekreační účely, není vybaveno žádným zařízením umožňujícím automatický let na zvolené místo, a které, v případě volného modelu, není dálkově řízeno jinak, než za účelem ukončení letu nebo které, v případě dálkově řízeného modelu, je po celou dobu letu pomocí vysílače přímo řízené pilotem v jeho vizuálním dohledu.

***Provoz dronů dle současné legislativy ČR***

Již v současnosti se civilní drony běžně pohybují ve vzdušných prostorech vyspělých států a samozřejmě je tomu tak i v České republice. U naprosté většiny komerčních bezpilotních prostředků je předpokládán provoz v nízkých výškách do 100 m nad terénem, přesto jsou výška letu a vzdálenost od pilota, či operátora UA řídícího, dalším podstatným faktorem, který je třeba legislativně řešit. A to nejen ve vztahu k ostatnímu letovému provozu, ale rozhodně i ve vztahu k bezpečnosti osob a majetku na zemi. ÚCL již v současnosti řeší i tuto problematiku zmíněným Doplňkem X a myslím, že je důležité zdůraznit současnou

hlavní myšlenku Doplňku a to, že se bezpilotní prostředek nesmí ocitnout v žádné fázi letu mimo dohled jeho pilota (až na výjimky, kdy ÚCL povolí jinak) a ten zároveň nesmí být sám mobilní. V současnosti tedy nelze dron naprogramovat, aby se pohyboval sám podle určeného algoritmu, ani jej nemůže jeho pilot následovat v jiném dopravním prostředku, ať již letícím, či jedoucím po pevné zemi. Tyto právní aspekty se mohou zdát samozřejmé, ale pro některé oblast využití jsou rozhodně omezujícm faktorem. Kupříkladu ve státní službě, například pro sledování kritické infrastruktury státu, je to faktor podstatně omezující možnosti, které technologie dronů již dnes nabízí. Je tedy třeba vzít v úvahu, že jakýkoli monitoring či sledování pomocí UA, musí být v současné době navrženy tak, aby po celou dobu provozu měl na bezpilotní prostředek jeho pilot neomezený výhled. Topologie pohybu UA by již v současné době byla možná naprogramovat do řídící jednotky v podobě požadované trajektorie letu a navigace za letu by mohla být s únosnou mírou možné odchylky zajištěna pomocí jednotky satelitní navigace, v současnosti buď systému GPS, či GLONASS, v blízké budoucnosti i evropského Galilea. Popřípadě by byla korigována vhodnou vnitřní elektronickou inerciální jednotkou. Proti tomu stojí obava legislativců z možnosti kolize, či jiné mimořádné události. Protože v případě jakékoliv poruchy by následoval v lepším případě automatický sestup dronu v kruzích, v horším neřízený pád. V obou případech by to končilo pravděpodobným dynamickým nárazem do neznámého místa, což by mohlo mít fatální následky. Nabízí se i možnost automatického záchranného systému, který by při ztrátě kontaktu operátora s UA přerušil let a bezpilotní prostředek by se následně snesl na aktivovaném padáku k zemi. I v tomto případě by však mohl dojít k nebezpečným a havarijním situacím. Protože i pomalu snášející se UA o vyšší hmotnosti, může například pro rychle jedoucí automobil představovat smrtelnou hrozbu nejen samotným nárazem, ale i způsobením nebezpečného úleku jeho řidiči, vedoucímu k následné kolizi. Zde tedy před konstruktéry i legislativci zbývá ještě několik nevyřešených a možná i dosud nevyřčených otázek.

*Druhy použití dronů*

Ještě před deseti lety byly pojmy jako dron, či bezpilotní prostředek známy pouze úzké skupině odborníků a zasvěcenců. Dnes neuplyne dne, aby se o použití dronů, ať už ve vojenské, či civilní oblasti média nezmínila. Jejich použití je stále širší a cena provozu stále nižší, u nejmenších typů je oproti pilotovaným letadlům v podstatě zlomková. Bezpilotních prostředků je dnes efektivně využíváno ve více oblastech.

- Letecké snímkování
- Monitorování důležitých infrastruktur
- Monitorování životního prostředí
- Zemědělství – sledování kvality hnojení, osevu, řízení
- Sledování meteorologických jevů – například sledování tornád.
- Vyhledávání a záchrana.
- 3D mapování povrchu – kupříkladu švýcarská firma Pix4D vytváří 3D mapy získané fotografováním povrchu drony.

## Možnosti využití UA v národním hospodářství

Možnost využít dronů ve státní službě pro monitoring důležitých bodů zájmu se s prudkým rozvojem miniaturizace snímací a přenosové techniky dostává stále více do popředí. Současné mini drony velikosti modelu letadla a hmotnosti v jednotkách kil, jsou schopny efektivně provádět velmi kvalitní letecké snímkování se souběžným natáčením videozáznamu širokoúhlým objektivem a to po dobu letu trvajícího několik hodin. Data a TV obraz mohou drony buď uchovávat ve flash paměti, nebo přenášet pomocí radiového signálu přímo k operátorovi (příjemci). Je samozřejmě nepochybné, že čím vyšší bude vyžadována kvalita pořízeného záznamu, tím větší bude datový tok a s ním stoupne i potřeba lepší a dražší technologie. Ale již dnes můžeme v některých oblastech smysluplně uvažovat o náhradě pilotovaných letadel jejich menší nepilotovanou náhradou. Dvě takové klíčové oblasti jsou bezesporu kritická infrastruktura státu a ochrana před živelnými pohromami.

## Sledovaní kritické infrastruktury státu drony

Kritickou infrastrukturou obvykle rozumíme hospodářsky významné provozně-výrobní provozy, dálková vedení velmi vysokého napětí, vodárny s vodovody, ropovody a plynovody, jakož i mezinárodní letiště a páteřní železniční tratě. Tedy výrobní odvětví a klíčové služby, jejichž selhání by způsobila fatální dopad na bezpečnost či hospodářství státu a zabezpečení základních životních potřeb jeho obyvatelstva.

### *Vytýčení cílů*

Aby mohla být provedena seriózní komparace ekonomicko-provozních nákladů dronů a pilotovaných prostředků, musí být nejdříve vytýčeny monitorované objekty, či subjekty společně s periodou a dobou sledování, jakož i trajektorií letů a vzdáleností, ze kterých mají být sledovány. V současnosti je třeba také vzít v potaz legislativní nutnost přímého očního kontaktu pilota a jím řízeného UA. Toto je z hlediska monitoringu důležitých infrastruktur prozatím velký hendikep, kterým nejsou vojenské UA svázány. Jakkoli si totiž můžeme představit monitoring menších objektů a budov pomocí dronů řízených z jednoho stanoviště s dohledem na celou trajektorii letu, těžko toto můžeme předpokládat například při monitoringu ropovodů, vedení vysokého napětí a jiných dálkových přenosových soustav. A nejde jen o problematiky důležitých infrastruktur. Kupříkladu i hasiči, kteří by chtěli využít dronů kupříkladu pro monitoring lesních požárů, budou za současného stavu legislativy ve většině lokalit odkázáni na pilotované prostředky. Ovšem už zde vyvstává klíčová otázka, nakolik by bylo legislativní uvolnění monitoringu prováděného zcela autonomními drony zásahem do soukromí občanů, žijících v monitorovaných oblastech.

### *Topologie monitorovaného prostoru*

Budeme-li chtít monitorovaný prostor popsat co nejvhodněji jako mapový podklad pro budoucí sledovací algoritmus dronu, musíme zvolit jeho vhodnou definici. V podstatě musíme matematicky popsat tvar terénu a trajektorii pohybu, po které má dron prolétat. Primárním úkolem je tedy vytýčení sledovaných cílů či tras. Následně musí být přesně určena jejich poloha a také směr, odkud mají být sledovány. Definice cílů bude obvykle zadána objednatelem monitoringu. Tvorba letové trajektorie, popřípadě letového plánu, bude pak úkolem provozovatele bezpilotního prostředku. Ovšem obojí je nezbytným předpokladem pro smysluplné provedení monitoringu. Dalším prvkem je četnost a periodicita sledování pro vytvoření potřebného harmonogramu monitoringu. (Ta by mohla být s jistou mírou pravděpodobnosti měněna zadavatelem právě na základě získaných dat.) Na základě všech těchto údajů, a s ohledem na typ monitoringu, lze začít s výběrem vhodného typu bezpilotního prostředku, a s tím vyplyne i potřebný počet obslužného personálu a to až do úrovně člověkohodin. Seriózní kalkulace nákladů je tedy fakticky možná až po výběru konkrétního typu dronu, jeho přizpůsobení požadavkům úkolu a kdy bude známá i případná potřeba subdodávek či vytvoření na míru šitých softwarových aplikací.

### *Logistika a algoritmy monitoringu*

V případě budoucí legislativní možnosti provést monitorovací let autonomně pouze bezpilotním prostředkem, bude nutno naprogramovat autopilota UA tak, aby sám dodržoval příslušnou trajektorii letu a zároveň směřoval sledovací zařízení na subjekty zájmu a do žádoucího směru. Nešlo by tedy o pouhou navigaci mezi bodem vzletu, otočnými body a místem přistání ale o komplexnější algoritmus, kdy by musela být sledovací aparatura orientována v prostoru nezávisle na poloze letícího UA. Takovou technologií již v současnosti běžně disponují vojenské drony a postupně se prosazuje i v dronech komerčních. A to nejen v civilních modifikacích původně vojenských UA, ale i v čistě civilních konstrukcích. Ovšem je zde ono legislativní omezení autonomie civilních UA.

### *Sběr a přenos dat*

Zřejmě nejběžnější současným záznamem dat pomocí bezpilotních prostředků, je letecké snímkování v oblasti viditelného spektra a pořizování videozáznamu.

Ale využívá se snímkování a natáčení v oblastech mimo viditelné spektrum, tedy v UV a IR spektru. Již v současnosti je takové snímkování využíváno v zemědělství, pro kontrolu saturace hnojení, nebo v archeologii jako velmi moderní a efektivní metoda pro vyhledávání dávno zapomenutých sídlišť a nalezišť.

Ovšem IR a UV spektrum jsou společně s termovizí důležitým pomocníkem hasičů při kontrole uhašených požářišť a policie při pátrání po pohřešovaných osobách, záchranných akcích na horách, atd.

### Efektivita využití UA v komparaci s jinými dopravními prostředky

Po vytipování primárních kritérií a výběru vhodného typu bezpilotního prostředku, bude třeba upravit jeho schopnosti a výbavu pro co nejefektivnější plnění zadaného úkolu. Dále bude na základě vyspecifikované dráhy a frekvence sledování stanovit potřebný objem sledovaných a přenášených dat. Dále je nutné určit, v jaké periodě bude dron používán a s jakou provozní spolehlivostí má pracovat. Na těchto kalkulacích by se již podílet zadavatel s možnými provozovateli dronů vytipované velikostní kategorie. A v této fázi je také možné stanovit provozní cenu bezpilotního systému.

Jednoduchý vícerotorový dron, určený pro natáčení běžného leteckého videozáznamu, kupříkladu lokální průmyslové havárie či místní sportovní akce, bude velikostí, doletem a možnostmi funkcí příbuzný RC modelu letadla a obdobná bude i pořizovací cena v jednotkách tisíc korun. Náklady na provoz takového dronu řízeného jedním pilotem budou v řádu stokorun až jednoho tisíce Kč na efektivně využitou hodinu letu. Obdobný záznam pořízený z vrtulníku, kupříkladu z menšího dvoumístného typu Robinson R22, bude v řádu desetinásobku, tedy deset a více tisíc korun za hodinu provedeného letu. Samozřejmě zde odpadá omezení přímé dohlednosti mezi UA a jeho pilotem. Ovšem to nemusí být pro lokální monitoring faktickým omezením. Ovšem kromě bezpilotních prostředků běžných konstrukcí, víceméně srovnatelných svou funkcí a výkony se svými většími pilotovanými protějšky vznikají typy zcela nové, umožňující použití i tam, kde by bylo použití klasického pilotovaného letadla neefektivní, nebezpečné, nebo přímo nemožné. U těchto konstrukcí často není vhodné cenové srovnání s pilotovanými letadly. Kupříkladu jsou v oblasti bezpilotních prostředků úspěšně vyvíjeny typy pohonu, který byl u pilotovaných letadel brzy zastaven, nebo se ani nikdy nevyvíjel. Jsou to kupříkladu multirotorové VTOL drony, nebo malé bezpilotní letouny s mávajícími křídly. Malé multirotorové drony je možno kupříkladu používat v členitých, polouzavřených či uzavřených prostorách. Tedy tam, kam by běžný letoun či vrtulník nemohly. Multirotorová konfigurace s elektronickou stabilizací pak umožňuje dříve stěží myslitelnou stabilitu a bezpečnost letu. Druhou zcela ojedinělou konstrukcí jsou drony s mávajícími křídly. Tito dálkově řízení robotičtí ptáci jsou vyvíjeni nizozemskou firmou Clear Fligt Solutions a imitují živé dravce natolik, že jsou dnes ve zkušebním provozu jako plnohodnotná náhrada dravců pro ochranu letišť před ptáky.

# Fyzická bezpečnost

Cílem kapitoly je iniciovat vývoj metodiky analýzy rizik fyzické bezpečnosti, který by vyústil do standardů fyzické bezpečnosti pro významné lokality energetického systému.

Tento dokument je v pořadí druhým dokumentem, který rozpracovává metodiku analýzy rizik v oblasti fyzické bezpečnosti. V prvních statích jsou popsány klíčové dokumenty, ze kterých metodika analýzy rizik vychází. Jsou to:

- „Proposal for a list of security measures for smart grids"
- „Proposal for a list of security measures for smart grids“

### *Zkratky a pojmy*

- SG - Smart Grid
- SGAM - Smart Grids Architecture Model (Model architektury Smart Grid)
- PLSM - Proposal for a list of security measures for smart grids
- Analýza rizik - analýza rizik zabývající se všemi aspekty bezpečnosti
- Analýza rizik fyzické bezpečnosti - analýza rizik zabývající se pouze problematikou fyzické bezpečnosti
- Hranice analýzy - hranice oddělující působnost analýzy rizik a analýzy fyzické bezpečnosti. Za podmínky, že jsou uplatněna všechna opatření doporučená analýzou fyzické bezpečnosti, platí předpoklad, že je vysoce pravděpodobné až jisté, že za tuto hranici nezíská přístup neoprávněná osoba.
- BIA analýza - Business Impact Analysis (analýza dopadů)
- DER - (distributed electrical resources) - distribuované elektrické zdroje přímo připojené k veřejné distribuční soustavě
- SCADA (supervisory control and data acquisition) – systém, který prostřednictvím přenosu telemetrických dat do nadřazeného systému, a za použití zprávy z nadřazeného řídicího systému k ovládání připojených objektů.
- Smart Grid Reference Architecture - CEN-CENELEC-ETSI Smart Grid Coordination Group - listopad 2012 - (Dále také jen "SGRA")
- Proposal for a list of security measures for smart grids - SMART GRID TASK FORCE 4 EG2 DELIVERABLE - prosinec 2013 -(Dále také jen "PLSM")

### *Analýza fyzické bezpečnosti - východiska*

SMART GRID TASK FORCE EG2 vydala koncem roku 2013 publikaci "Proposal for a list of security measures for smart grids" (dále také jen PLSM), jenž lze použít jako východisko pro analýzu rizik.

PLSM je prvním krokem směřujícím ke standardizaci v oblasti energetické bezpečnosti, protože popisuje základní elementy pro provedení analýzy rizik a přináší návrh sady bezpečnostních opatření ke zvládání rizik.

To, co doposud řešeno není, je metodika provádění analýzy rizik, která by navazovala na dokument PLSM.

### SGAM model

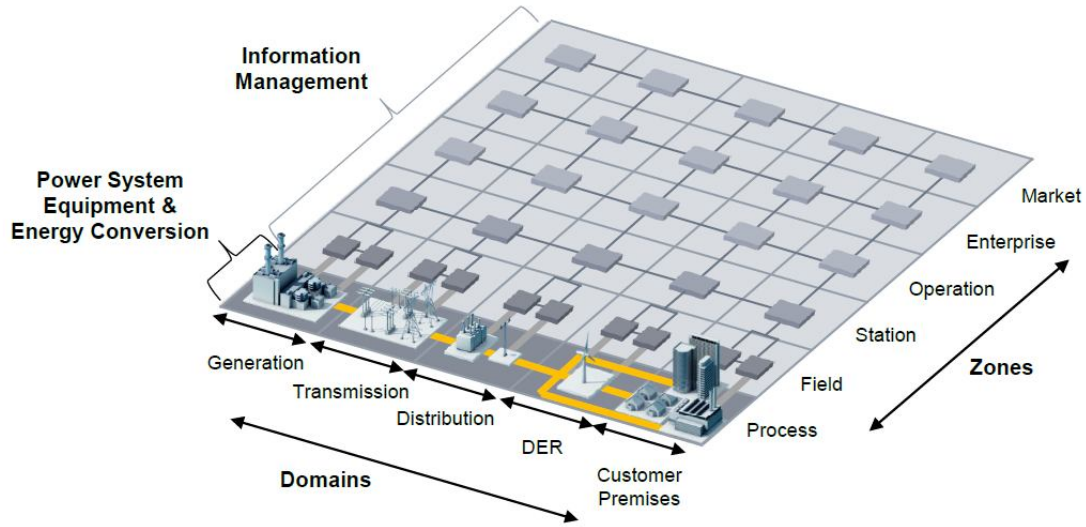
SGAM model presentuje realitu v třírozměrném zobrazení. Základnu tvoří relace Domén a Zón, a vertikálu tvoří vrstvy interoperability.

**Domény** popisují řetězec konverze elektrické energie (infrastrukturu výroby a spotřeby),

**Zóny** popisují hierarchické úrovně řízení energetického systému.

**Vrstvy interoperability** tvoří třetí rozměr modelu, na těchto vrstvách se odehrává vzájemná spolupráce řídících energetických systémů, který byl převzat z dokumentu SGRA.

Základna modelu je znázorněna na následujícím obrázku, který byl převzat z dokumentu SGRA. Pro potřeby analýzy fyzické bezpečnosti jsou významné zejména zóny Process, Field a Station.




*Obrázek 1 Základna modelu "Smart grid"*

#### *Domény SGAM*

Domény SGAM pokrývají celý řetězec vzniku a konverze elektrické energie. Model SAGEM rozlišuje následující domény:

- **Generation** - Reresentuje výrobu elektrické energie ve velkých množstvích, jako jsou fosilní, jaderné a vodní elektrárny, off-shore větrné farmy, rozsáhlé sluneční elektrárny (tj PV, CSP) - typicky zdroje energie připojené přímo k přenosové soustavě.

- **Teransmition** - Reprezentující infrastruktury a organizace, které přenáší elektřinu na dlouhé vzdálenosti.
- **Distribution -** Reprezentující infrastruktury a organizace, které distribuuje elektřinu zákazníkům.
- **DER** – (distributed electrical resources) Presentuje distribuované elektrické zdroje přímo připojené k veřejné distribuční soustavě, které uplatňují v malém měřítku technologie na výrobu energie (typicky v rozmezí od 3 kW do 10.000 kW). Tyto distribuované elektrické zdroje mohou být přímo řízeny operátory distribučních systémů (DSO).
- **Customer premises** – Prostory zákazníka - zahrnují jak koncové uživatele elektřiny, tak i výrobce elektřiny. Prostory zákazníka mohou být průmyslová, obchodní a bytová zařízení (např. chemické továrny, letiště, přístavy, nákupní centra, domy). Také výroba ve formě např. fotovoltaické výroby energie, zařízení na skladování energie, baterie, mikro turbíny, atd.

Právě domény představují fyzická zařízení na výrobu a konverzi elektrické energie – tedy **fyzická zařízení, na která lze uplatnit opatření z oblasti fyzické bezpečnosti**. To je důvod, proč bude koncepce fyzické bezpečnosti navázána na model SAGEM prostřednictvím domén tohoto modelu.

*Zóny SGAM*

Zóny SAGEM představují hierarchické úrovně řízení energetického systému. Model definuje 6 zón:

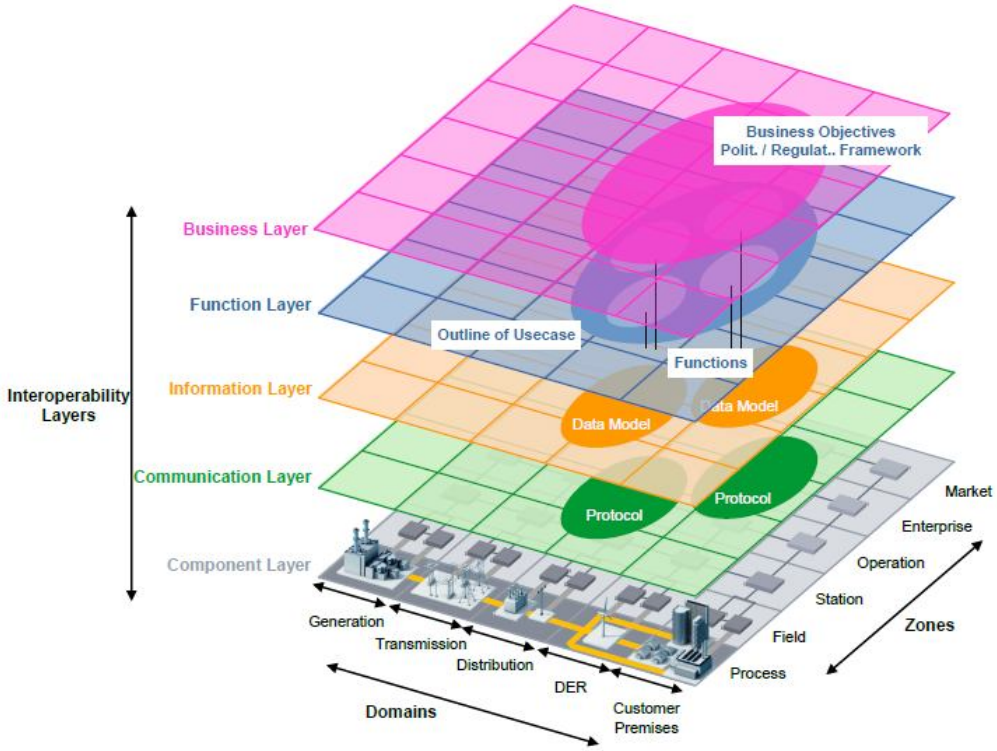
- **Processes** - Zahrnuje fyzikální, chemickou, nebo prostorovou transformaci energie (elektřina, solární, teplo, voda, vítr ...) a fyzická zařízení, která se na ní přímo podílejí. (např. generátory, transformátory, jističe, venkovní vedení, kabely, jhakékoli elektrické zátěže, všechny druhy snímačů a akčních členů, které jsou buďto součástí, nebo jsou přímo vázány na proces, ...). Tato zóna bude především předmětem fyzické bezpečnosti.
- **Field** - Zahrnuje zařízení na ochranu, kontrolu a sledování procesů energetického systému, např. ochranná relé, bay controllery, jakýkoliv druh inteligentních elektronických zařízení, která získávají a používají procesní data z elektrizační soustavy.
- **Station** - Reprezentuje agregaci na úrovni areálu závodu (objektu), např. systémy pro koncentraci dat, funkční agregaci, automatizace trafostanic, místní SCADA systémy, dohled na úrovni závodu apod.
- **Operation** - Hosting pro řízení operací energetického systému v příslušné oolasti, např. Systémy řízení distribuce (DMS), Systémy řízení energie (EMS) v technologiích výroby a přenosových systémů energie, systémy řízení microgridů, Systémy řízení virtuálních elektráren (sloučením několika DER), elektrická zařízení (EV – electric vehicle), flotila systémů řízení nabíjení apod.
- **Enterprise** - Zahrnuje soubor obchodních a organizačních procesů, služeb a infrastruktury pro podniky (nástroje, poskytovatelé služeb, obchodníci s energií ...), např správa majetku, logistika, řízení pracovní síly, školení zaměstnanců, řízení vztahů se zákazníky, fakturace a zprostředkování.

- **Market** - S ohledem na možné tržní operace v oblasti konverze řetězce energie, např obchod s energií, masový trh, maloobchodní trh apod.

Z hlediska fyzické bezpečnosti jsou relevantní zejména první tři zóny, protože ty jsou přímo vázány na fyzická místa spojená s výkonem činností výroby, distribuce a konverze energie.

*Vrstvy interoperability SAGEM*

Třetí rozměr modelu tvoří vrstvy interoperability, na kterých se odehrává vzájemná spolupráce řídících energetických systémů, který byl převzat z dokumentu SGRA.




*Obrázek 2 Úplný "Smart grid" model*

Vrstvy interoperability jsou uvedeny pouze z důvodu úplnosti informací o modelu SGAM. Pro potřeby analýzy fyzické bezpečnosti nemají vrstvy interoperability zásadní význam.

Bližší informace o SGAM modelu jsou uvedeny v publikaci SGRA (Smart Grid Reference Architecture - CEN-CENELEC-ETSI Smart Grid Coordination Group - listopad 2012).

## *Proposal for a list of security measures for smart grids (PLSM)*

Materiál PLSM ve své části identifikuje typická aktiva Smart Grid, následně identifikuje typické hrozby pro Smart Grids, a závěrem definuje 45 opatření rozdělených do 11 domén.

### Aktiva – Hrozby – Opatření

**Aktiva** jsou presentována jako typičtí zástupci aktiv vyskytujících se v SG a jsou uspořádána formou, která je výhodná pro identifikaci aktiv v procesu analýzy rizik.

Dokument se ale nezabývá vlastní metodikou analýzy rizika, proto neposkytuje vodítko, jak přistupovat k aktivům, zejména v oblasti stanovování hodnoty aktiva.

Aktiva PLSM jsou uvedena v příloze „C“.

**Hrozby** jsou definovány jako seznam typických hrozeb a lze konstatovat, že hrozby jsou pokryty komplexně. Z hlediska fyzické bezpečnosti jsou relevantní dvě skupiny hrozeb. Jedná se o skupinu úmyslný fyzický útok a o skupinu přírodní katastrofy.

**Opatření** jsou v dokumentu rozdělena do 11 domén, v rámci těchto domén je definováno 45 opatření (viz. příloha A), kde je uveden přehled názvů všech opatření.

Z hlediska fyzické bezpečnosti je důležitá doména č. 8 Fyzická bezpečnost, která ovšem obsahuje pouze 3 opatření.

Tato doména obsahuje následující opatření:

**31.** Vytvořit a udržovat odpovídající fyzickou bezpečnost zařízení / komponentů / systémů Smart Grid podle kritičnosti, který má být definován vlastníkem majetku.

**32.** Vytvořit a udržovat funkce pro přihlášení a sledování fyzického přístupu k zařízení / komponentům Smart Grid s přihlédnutím ke kritičnosti zařízení.

**33.** Zavést zvláštní dodatečná fyzická ochranná opatření na ochranu zařízení umístěné mimo vlastní pozemky, nebo prostory.

Jak je vidět z výše uvedených popisů opatření, jedná se o vysoce obecnou definici požadavků, které, bez bližší specifikace jsou prakticky těžko uchopitelné.

### Analýza rizik v oblasti fyzické bezpečnosti

Dokument PLSM uvádí vazby mezi hrozbami a opatřeními, které tyto hrozby mají eliminovat.

Z hlediska fyzické bezpečnosti padají v úvahu následující skupiny hrozeb:

- Fyzický útok (úmyslný / záměrný)

- Katastrofy (přírodní, životního prostředí)

Vazby mezi hrozbami a opatřeními jsou uvedeny v následující tabulce.

| **Skupina hrozeb** | **Hrozba** | **Čísla opatření** (viz příloha A) |
|---|---|---|
| Fyzický útok (úmyslný / záměrný) | | 2, 7, 15, 18, 19, 20, 29, 31, 32, 32, 33, 43, 44, 45 |
| | Bombový útok / ohrožení | 18, 19, 21, 31, 32, 33, 43,44, 45 |
| | Podvod | 7, 18, 19, 20, 31, 32, 33, 43,44,45 |
| | Sabotáž | 7, 18, 19, 21, 31, 32, 33, 43,44,45 |
| | Vandalství | 7, 18, 19, 21, 31, 32, 33, 43, 44, 45 |
| | Krádež (zařízení, paměťová média a dokumenty) | 7, 10, 15, 19, 31, 32, 33, 40, 43,44,45 |
| | Únik informací / neoprávněné sdílení | 7, 15, 18, 19, 40, 43,44,45 |
| | Neoprávněný fyzický přístup / Neoprávněný vstup do areálu | 2, 7, 19, 31, 32, 33, 43,44,45 |
| | Nátlak, vydírání nebo korupce | 7, 18, 19 20, 31, 32, 33, 43,44,45 |
| Katastrofy (přírodní, životního prostředí) | | 20, 21,29, 30, 31, 33, 43,44,45 |
| | Katastrofy (přírodní zemětřesení, záplavy, sesuvy půdy, tsunami) | 20, 21,29, 30, 31, 33, 43,44,45 |
| | Katastrofy (životní prostředí - požár, výbuch, únik nebezpečné záření) | totéž jako výše |
| | Požár | totéž jako výše |
| | Povodeň | totéž jako výše |
| | Znečištění, prach, koroze | totéž jako výše |
| | Úder blesku | totéž jako výše |
| | Voda | totéž jako výše |
| | Nepříznivé klimatické podmínky | totéž jako výše |
| | Významné události v životním prostředí | totéž jako výše |

*Tabulka 1 Relace hrozba - opatření*

Souhrn doporučovaných opatření je uveden v následující tabulce, kde jsou shrnuta opatření uveden v tabulce č. 1 jak pro skupinu hrozeb „Fyzický útok“, tak pro skupinu hrozeb „Katastrofy“.

| **Číslo opatření** | **Opatření proti fyzickému útoku** | **Opatření proti přírodním katastrofám** |
|---|---|---|
| 2 | Organizace bezpečnosti informací | |

| | | |
|---|---|---|
| 7 | Dohody se třetími stranami | |
| 15 | Likvidace Smart Grid komponentů / systémů | |
| 18 | Personální prověrky | |
| 19 | Personální změny | |
| 20 | Program rozvoje bezpečnosti a bezpečnostního povědomí | Program rozvoje bezpečnosti a bezpečnostního povědomí |
| 21 | Bezpečnostní školení a certifikace pracovníků | Bezpečnostní školení a certifikace pracovníků |
| 29 | Schopnosti zachování kontinuity provozu | Schopnosti zachování kontinuity provozu |
| 30 | Základní komunikační služby | Základní komunikační služby |
| 31 | Fyzická bezpečnost | Fyzická bezpečnost |
| 32 | Logování a monitorování fyzického přístupu | |
| 33 | Fyzická bezpečnost v prostorách třetích stran | Fyzická bezpečnost v prostorách třetích stran |
| 40 | Manipulace s medii | |
| 43 | Minimální expozice | Minimální expozice |
| 44 | Odolnost | Odolnost |
| 45 | Bezpečné přerušení - Kontinuita provozu | Bezpečné přerušení - Kontinuita provozu |

*Tabulka 2 Souhrn opatření pro vybrané skupiny hrozed*

Opatření uvedená v tabulce č. 2 představují množinu všech opatření, která jsou pro oblast fyzické bezpečnosti doporučována dokumentem PLSM.

### Hodnocení použitelnosti PLSM pro řešení problematiky fyzické bezpečnosti

Dokument PLSM doporučuje vhodná opatření, která jsou použitelná k ochraně funkčnosti a zajištění bezpečného provozu sítě Smart grid.

Svým obsahem PLSM poskytuje jen základní rámec pro provedení analýzy rizik, který ale **není pro provedení analýzy rizik postačující**.

Poskytuje:

- vodítko pro identifikaci aktiv (viz Příloha „C“),
- identifikuje hlavní hrozby (viz Příloha „B“),
- definuje seznam bezpečnostních opatření (viz. Příloha „A“).

Analýza rizik je postavena na stanovení míry rizika za použití kvantifikátorů, jako je číselné, nebo slovní vyjádření intenzity hrozby, stanovení míry zranitelnosti a dopadů působení hrozby.

Takto stanovená (a kvantifikovaná) rizika jsou následně sanována výběrem vhodných opatření (zvládání rizik). Pro výběr opatření je výhodou, když metoda analýzy rizik poskytuje vyjádření účinnosti jednotlivých opatření ke snížení hodnoceného rizika.

Analýza a zvládání rizik by měla poskytnout relevantní informace o opatřeních, která jsou pro hodnocený objekt vhodná. Proto musí být vybrána vhodná metoda analýzy rizik, která by kvantifikovala rizika i vhodnost bezpečnostních opatření pro jejich snížení na akceptovatelnou úroveň.

### *Zajištění fyzické bezpečnosti*

Bezpečnostní opatření uvedení v PLSM se vztahem k fyzické bezpečnosti jsou specifikovány na nejvyšší úrovni obecnosti (viz opatření 31 až 33 ve stati 2.2.1). Z hlediska zajištění fyzické bezpečnosti energetických zařízení (SmartGrid) poskytují sice vodítko k tomu „CO“ má být realizováno, ale neposkytují návod „JAK“ to má být realizováno. Nikde není řešena síla fyzické ochrany, která má být prvkům poskytnuta.

#### Fyzická bezpečnost

V rámci fyzické bezpečnosti se pracuje pouze s hmotnými aktivy, na které lze fyzicky přímo působit.

#### *Zóny ochrany*

V rámci realizace fyzické bezpečnosti lze, jako jedno z bezpečnostních opatření definovat kolem chráněného aktiva (energetického zařízení) směrem k vnějšímu okolí několik zón ochrany.

1. **Zóna vně perimetru** – představuje přilehlý prostor v okolí objektu vně perimetru objektu (za plotem). Tato zóna nemusí být v majetku vlastníka objektu. Smyslem realizace bezpečnostních opatření v této zóně je co nejvčasnější detekce možné hrozby. V této zóně se realizuje fyzická ochrana zejména pozorováním. Obvykle se zde nasazují kamerové systémy, někdy s detekcí pohybu, různé druhy čidel (většinou infra), nebo je tato zóna jen pozorována ostrahou objektu.
2. **Perimetr prostoru** - obvykle je tvořen oplocením, nebo zdí. Perimetr představuje vnější hranici chráněného prostoru – hranici, která zabraňuje volnému přístupu osob do chráněného prostoru. Na perimetr se instalují hlavně detekční prvky, které umožní včasnou indikaci narušení fyzické bezpečnosti.

   Perimetr může být doplněn dalšími bezpečnostními prvky, např. druhým oplocením, které zamezí přístupu zvěře a tím spouštění falešných poplachů. Za perimetr s detekcí směrem k objektu lze instalovat dodatečná zařízení, která mají zbrzdit útočníka na přístupu k chráněnému objektu (obvykle bariéra z žiletkového drátu nebo podobné zařízení). Musí být ale dodrženo pravidlo, instalovat taková zařízení až za detekční prvky na perimetru směrem ke chráněnému objektu, protože smyslem je prodloužit dobu mezi indikací narušení objektu a dobou, kdy se útočník dostane ke chráněnému aktivu, což získá potřebné vteřiny pro zásah.

   U rozsáhlých objektů může být instalováno ještě několik vnitřních perimetrů, které upřesní, o který objekt má útočník „zájem“ a případně jej zase o něco zdrží, na cestě ke chráněnému aktivu.

3. **Perimetr objektu** – je obvykle tvořen obvodovými zdmi, otvory do objektu, což mohou být vstupy do objektu (dveře, brány apod.), okna objektu a provozní otvory (ventilace, kanalizace apod.). Na perimetr objektu se instalují fyzické zábranné prvky (zodolněné dveře, mříže apod.), které mají zadržet, nebo alespoň zdržet případného útočníka. Fyzické zábranné prvky jsou obvykle doplněny detekčními prvky, které mají

zpřesnit informaci o místě vstupu útočníka do objektu. Také se zde instalují prvky fyzického řízení přístupu osob (identifikační zařízení osob, turnikety apod.).

4. **Vnitřní prostory objektu** - pokud je to možné, je vhodné vnitřní prostory objektu rozdělit do zón, kde každá zóna by měla mít definován vlastní bezpečnostní perimetr, který by měl být opatřen detekčními prvky. Ve vnitřních prostorách objektů se instalují čidla prostorové ochrany založené na různých fyzikálních principech např. PIR čidla (passive infrared sensor). Mohou zde být instalovány také prvky automatické aktivní obrany objektu (dodatečné roletové mříže, generátory PUR pěny, generátory zvuku o vysoké intenzitě apod.) Tyto prvky ale musí být instalovány v souladu s právními požadavky (nesmí ohrozit život nebo zdraví útočníka). V neposlední řadě se zde také instalují prvky požární ochrany (detektory požáru a automatické hasicí systémy).
5. **Chráněné místnosti** – místnosti, kde se nachází chráněné aktivum. Ochrana místnosti je obdobná jako ochrana vnitřních prostor objektu, tedy detekční prvky narušení bezpečnosti jak na úrovni plášťové ochrany, tak na úrovni prostorové ochrany. I zde mohou být instalovány prvky automatické aktivní obrany objektu (viz výše), nebo požární ochrany.
6. **Úschovné objekty** – představují poslední zónu ochrany chráněného aktiva. Jsou to různé uzamykatelné skříně, racky, nebo trezory. Úschovné objekty se liší mírou odolnosti v závislosti na významu chráněného aktiva.

*Strategie zásahu*

Budování zón ochrany má jediný účel: detekovat útok a co nejvíce zdržet útočníka před tím, než získá přístup ke chráněnému aktivu. Tento čas je potřebný pro organizaci zásahu, který má eliminovat útok. Bez zajištění zásahu, ztrácí opatření fyzické bezpečnosti podstatnou část své účinnosti, protože je jejich účinek omezen pouze na odstrašení, nebo odrazení útočníka.

Při organizaci zásahu se rozlišují dvě strategie zásahu:

1. **Ochrana před sabotáží** - spočívá v provedení zásahu dříve, než útočník dosáhne chráněného aktiva.
2. **Ochrana před krádeží** - vychází z toho, že se nepředpokládá, že dočasným vyřazením chráněného aktiva z činnosti dojde k velkým škodám, ale chráněné aktivum je natolik cenné, že je potřeba jej chránit před krádeží. V tomto případě se doba na provedení zásahu prodlužuje, protože postačuje provést zásah až v době, když útočník opouští s chráněným aktivem chráněný prostor.

Jednotlivé strategie zdůvodňují smysl zón ochrany, které „získávají čas“ pro zásahový tým, kterému umožňují provést zásah včas v souladu s požadavky té či oné strategie.

*Obecné vztahy v bezpečnostní analýze*

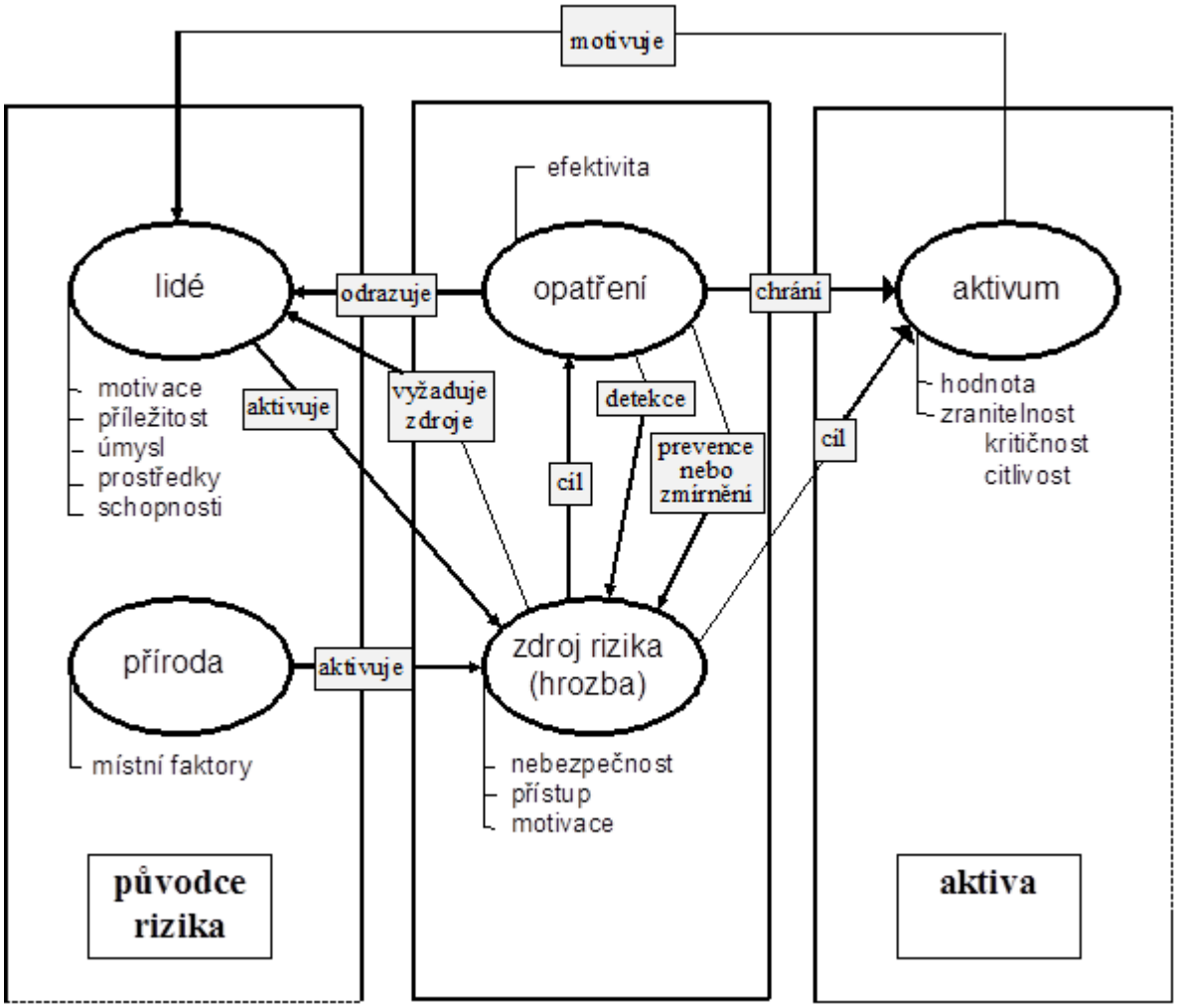
Správné pochopení vztahů v analýze rizik je klíčové pro úspěšné provedení bezpečnostní analýzy. Základní vztahy a souvislosti v bezpečnostní analýze jsou znázorněny na obr. 3.

Mechanismus uplatnění rizika probíhá tak, že Zdroj rizika (hrozba) využije zranitelnosti, případně překoná protiopatření a působí na aktivum, kde způsobí škodu (dopad).

Aktivum (svou hodnotou) motivuje člověka k aktivaci hrozby. Vůči působení hrozby se aktivum vyznačuje určitou zranitelností. Aktivum je zároveň chráněno protiopatřeními před hrozbami.

Opatření chrání aktiva, detekuje hrozby a zmírňuje nebo zcela zabraňuje jejich působení na aktiva. Protiopatření zároveň odrazují od aktivování hrozeb.

Hrozba působí jednak přímo na aktivum, nebo na opatření, s cílem získat přístup k aktivu. Aby mohla hrozba působit, musí být aktivována. Pro svou aktivaci vyžaduje zdroje (vytvoření podmínek pro její působení).



Obrázek 3 Vztahy v analýze rizik

*Velikost rizika*

Různé metody analýza rizik vyjadřují rizika různými způsoby. Pro exaktní práci s rizikem je nutné, aby riziko bylo vyjádřeno numerickou hodnotou. Velikost rizika se obvykle vypočítává jako součin tří veličin:

- **hrozba -** vyjadřuje, s jakou pravděpodobností dojde k úspěšnému ohrožení aktiva danou hrozbou. V rámci fyzické bezpečnosti je důležité brát v úvahu motivační faktor aktiva pro působení hrozby a schopnost útočníka působit ohrožení.
- **zranitelnost aktiva** vůči hodnocené hrozbě, je dána citlivostí aktiva na působení dané hrozby a je snižována instalovanými bezpečnostními opatřeními na ochranu aktiva, které jsou účinné vůči této hrozbě.
- **následek -** velikost škody vzniklé dopadem působení hrozby na aktivum (vyřazení elektrárny, rozvodny, vedení apod.) do velikosti škody je potřeba započítat nejen případnou škodu na aktivu, ale i dopad vyřazení aktiva na stabilitu rozvodné sítě a dopad výpadku v dodávce energie závislým uživatelům.

Součin hrozby a zranitelnosti aktiva představuje pravděpodobnost, že dojde k nepříznivému působení hrozby na aktivum. Pokud se tento součin vynásobí velikostí potenciálně vzniklého následku, je výsledkem hodnota rizika. Je to bezrozměrná hodnota, která poskytuje smysluplnou informaci jedině tehdy, když se srovnává s hodnotami jiných rizik vypočtených toutéž metodou.

Pro srozumitelnější vyjádření lze riziko presentovat formou tzv. „relativního rizika“, což je procentuální vyjádření velikosti rizika v poměru k ostatním rizikům. Největší riziko má hodnotu 100 a všechna ostatní rizika mají svou hodnotu stanovenu v procentuálním poměru k největšímu riziku.

*Management rizika*

Pro stanovení potřebné míry ochrany platí pravidlo, že hodnota prostředků vložených do ochrany musí být úměrná hodnotě chráněného aktiva/aktiv a velikosti rizika, které tato aktiva ohrožuje.

Provedení analýzy rizik identifikuje a kvantifikuje rizika, kterým je energetické zařízení vystaveno. Obecně platí, že rizika se ošetřují v pořadí od významných po méně významná. V rámci fyzické bezpečnosti jsou standardními postupy při ošetření rizika následující možnosti:

- snížení rizika – implementací bezpečnostního opatření, které sníží pravděpodobnost výskytu rizika, nebo jeho následky, popřípadě odstraní zdroj rizika,
- vyhnutí se riziku – pokud riziko způsobuje nějaká zbytná aktivita pak s touto aktivitou nezačínat, nebo v ní nepokračovat,
- sdílet riziko s jinou stranou – typickým příkladem je pojištění rizika,
- uchovat riziko - na základě informované volby akceptovat působení rizika.

V oblasti realizace fyzické bezpečnosti se nejčastěji se budou rizika snižovat implementací bezpečnostních opatření. Při výběru vhodných bezpečnostních opatření k implementaci se zvažuje nejen účinnost bezpečnostního opatření, ale i náklady na jeho realizaci. Bezpečnostní opatření, která jsou již implementována a jsou funkční, představují nulové náklady na implementaci, je ale potřeba zvážit efektivnost takových opatření vzhledem k nákladům na jejich provoz a rizikům, která eliminují.

Metodicky řeší proces managementu rizik standard ČSN ISO 31000 – Management rizik – Principy a směrnice, kde lze najít různé metody řízení rizik.

***Potřeba standardizace***

SmartGrid v ČR je geograficky rozprostřena do stovek objektů a zařízení, která sestávají ze značného množství aktiv. Provádění analýz rizik fyzické bezpečnosti na všechny lokality a všechna aktiva je z hlediska kapacit velmi náročné. Řešením by mohla být kategorizace energetických zařízení.

Přínosem kategorizace by bylo stanovení minimálního standardu fyzické bezpečnosti, který by stanovil minimální rozsah bezpečnostních opatření, který by byl pro každé energetické zařízení v dané kategorii vyžadován. Tak by byla definována a následně zajištěna základní úroveň fyzické ochrany pro každé energetické zařízení spadající do dané kategorie.

Minimální standardy nebrání zavedení dalších bezpečnostních opatření na základě hodnocení rizik lokálním bezpečnostním managementem.

### Kritéria hodnocení energetických zařízení

Při hledání parametrů pro kategorizaci lze vycházet z předpokladů uvedených ve stati 3.1.4. odkud vyplývá, že jak hrozba, tak zranitelnost i následek jsou funkcí určitých vlastností aktiva. Jako parametry by mohly sloužit:

- Následky vyřazení aktiva – energetická vedení, na kterých jsou závislí významní uživatelé, u kterých by výpadek proudu mohl způsobit významné druhotné škody (průmyslové havárie), nebo vedení zásobující velký počet obyvatel, případně vedení, jehož vyřazení by mohlo vést ke kaskádovému efektu v energetické síti. Dalším příkladem mohou být jaderné elektrárny, kde i neúspěšný teroristický útok vzbudí významné obavy u obyvatelstva.
- Motivační faktor aktiva – jsou to vlastnosti energetického zařízení, které motivují útočníka k provedení útoku. Motivační faktor by měl být rozdělen na motivaci ke krádeži a na motivaci k teroristickému útoku. Motivačním faktorem ke krádeži může být např. výskyt a přístupnost barevných kovů v energetickém zařízení pro zloděje kovů. Naopak motivací k teroristickému útoku je možnost vyvolat co největší chaos, proto lze předpokládat, že teroristé budou útočit na páteřní vedení, nebo na významné objekty (např. jaderná zařízení).
- Významná citlivost aktiva – energetické zařízení, které je významně citlivé na určité hrozby, např. energetické vedení vedoucí níže, než okolní terén (úzkým údolím, nebo pod mostem), kde je snadný přístup pro způsobení black-outu.

Výše uvedené parametry mohou sloužit jako příklad, podle kterého by se mohla hodnotit energetická zařízení. Význam parametrů je uveden jejich pořadím.

### Kategorizace energetických zařízení

Kategorizací energetických zařízení se tato zařízení rozdělí do kategorií, ve kterých budou zařazena energetická zařízení s obdobnými bezpečnostními vlastnostmi.

Kategorizaci lze realizovat tak, že se vybere vhodný vzorek energetických zařízení, která by byla hodnocena podle parametrů uvedených v předchozí stati. Na základě výsledků hodnocení by měla být stanovena kritéria, podle kterých se stanoví kategorie, do kterých se budou energetická zařízení zařazovat.

### Minimální standardy fyzické bezpečnosti

Smyslem minimálních bezpečnostních standardů je pro každou kategorii energetických zařízení definovat množinu opatření fyzické bezpečnosti, která má být u každého energetického zařízení implementována.

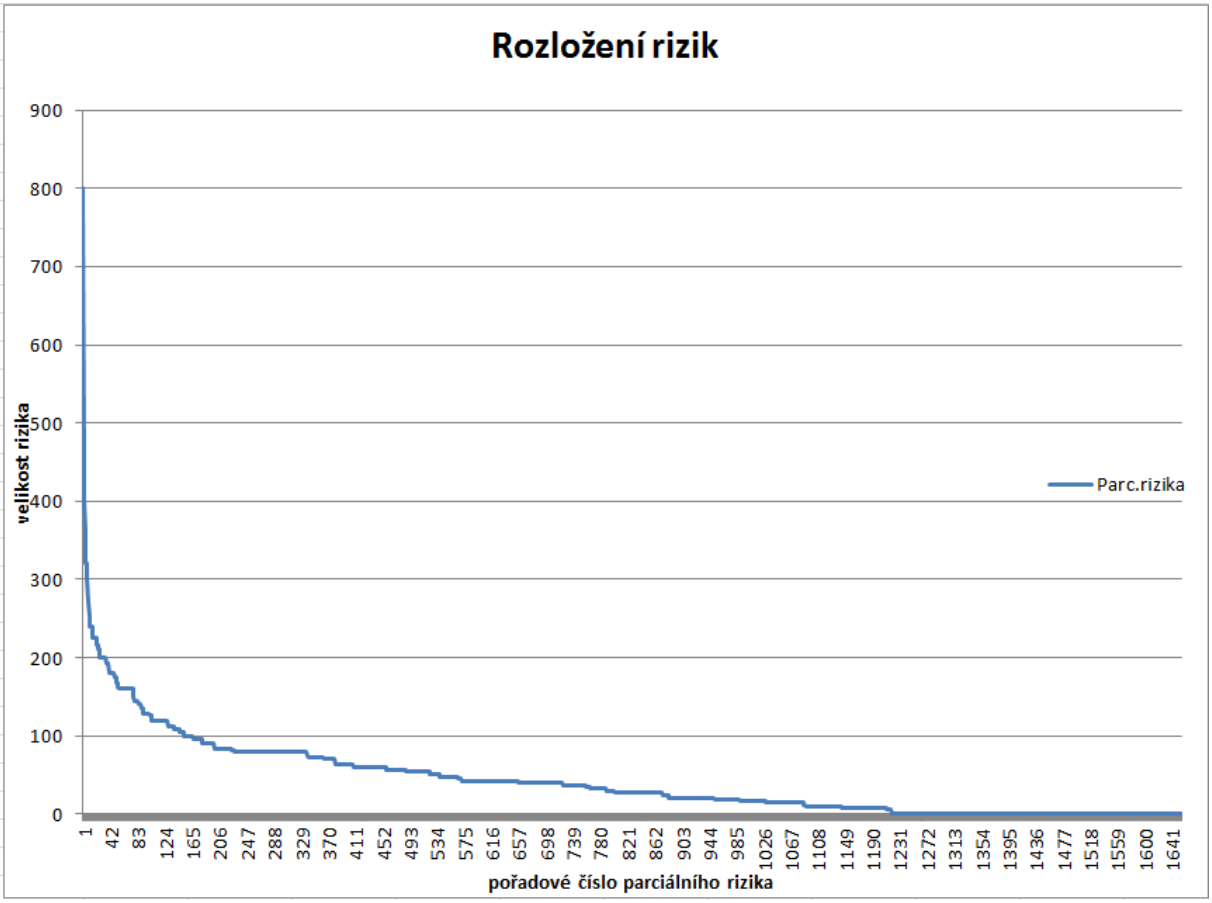
Požadavky minimálních standardů pro jednotlivé kategorie se odvodí z provedení analýzy rizik u vzorku několika energetických zařízení z každé kategorie. Realizací analýzy rizik vznikne pro každý vzorek sada identifikovaných rizik.

*Příklad možné aplikace analýzy rizik*

Autor provedl množství analýz rizik dle metodiky standardu ISO/IEC 27001 Systém řízení bezpečnosti informací (ISMS) v jehož rámci se hodnotí také fyzická bezpečnost. Při seřazení identifikovaných rizik (parciálních rizik, která jsou stanovena hodnocením působení každé hrozby vůči každému aktivu) podle jejich velikosti od největšího k nejmenšímu, dají takto seřazená rizika charakteristické rozložení. Příklad je uveden na obrázku č. 4. kde je zobrazeno rozložení rizik z reálné analýzy rizik u jedné organizace.

Lze předpokládat, že obdobné rozložení rizik bude i v případě analýzy fyzické bezpečnosti, jen pravděpodobně nebude identifikován tak vysoký počet rizik. Z rozložení rizik na obrázku je patrné, že od největšího rizika (hodnota 800) dochází k prudkému poklesu velikosti rizika až k 206-tému riziku na úroveň 1/10 největšího rizika (na hodnotu „80“), kde se prudký pokles rizika zastavuje a dochází jen k pozvolnému poklesu. Je zřejmé, že prvních 206 rizik představuje nejvýznamnější rizika hodnocené organizace.

Protože cílem provádění analýzy bude vytvoření minimálních standardů, má smysl ošetřit pouze nejvýznamnější rizika, o kterých lze předpokládat, že u všech energetických zařízení dané kategorie budou podobná.




*Obrázek 4 Typické rozložení rizik*

*Sada bezpečnostních opatření*

Při ošetření rizika lze využít možnosti uvedené ve stati 3.1.5. Problematický může být výběr sady opatření, ze které se budou vhodná opatření vybírat.

Pokud nebude nalezen vhodný dokument, ze kterého by bylo možné sadu bezpečnostních opatření fyzické bezpečnosti převzít, bude nezbytné takovou sadu sestavit. I při řešení tohoto problému se lze inspirovat postupem, jakým vznikala sada bezpečnostních opatření ISMS. Tato sada byla sestavena tak, že byla provedena identifikace všech použitých bezpečnostních opatření u největších společností Velké Británie. Tato opatření byla následně uspořádána a sestavena do logického systému.

Obdobně lze postupovat i při sestavení sady bezpečnostních opatření fyzické bezpečnosti pro energetickou platformu, využitím identifikace všech aplikovaných bezpečnostních opatření u významných provozovatelů energetických zařízení v ČR i v Evropě a jejich následné uspořádání do logického systému.

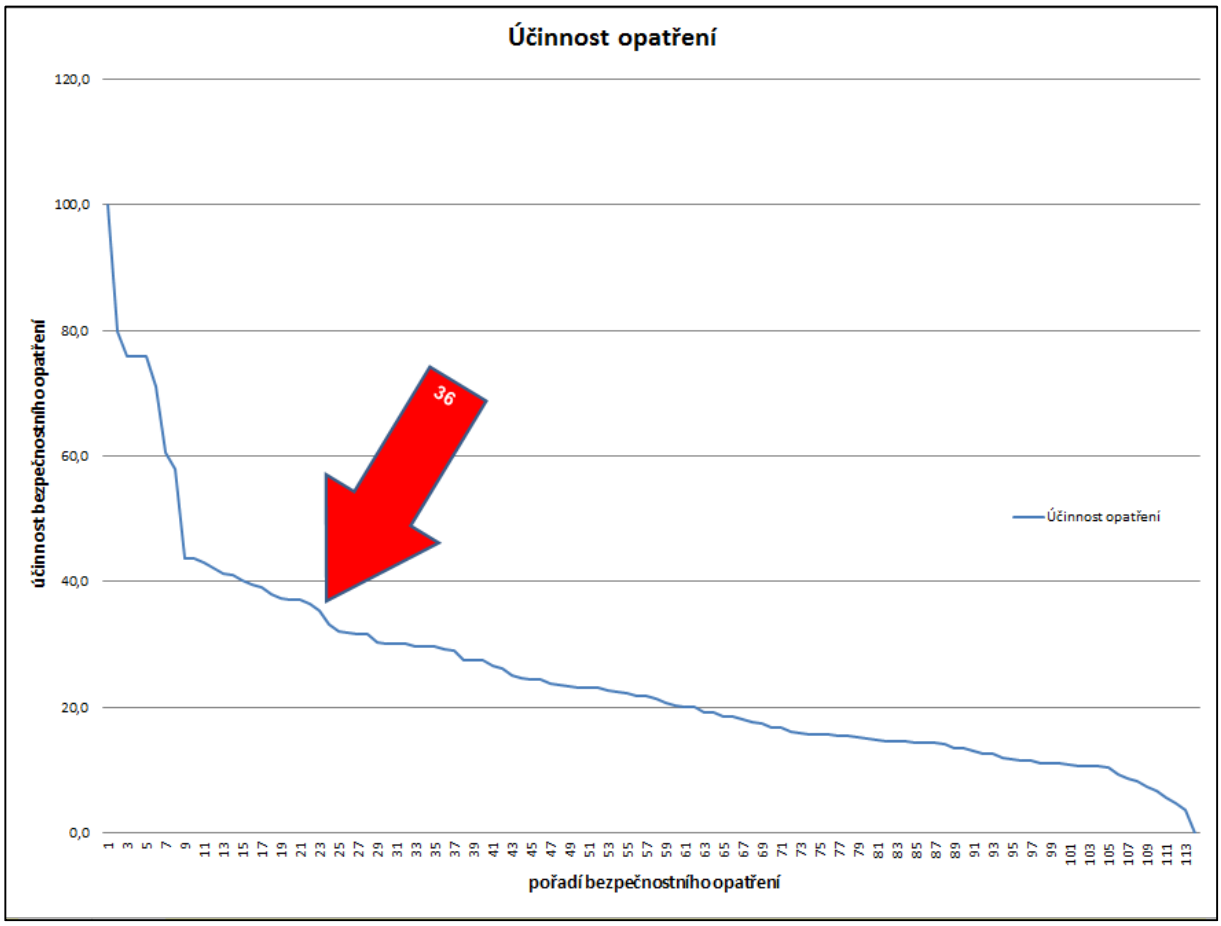
*Stanovení účinnosti bezpečnostních opatření*

Dalším krokem při tvorbě minimálních bezpečnostních standardů bude nutnost stanovit účinnost jednotlivých opatření ze sady bezpečnostních opatření k eliminaci jednotlivých rizik.

Pokud se vychází z parametrů, ze kterých se vypočítá velikost rizika (viz. stať 3.1.4), pak je nejvhodnější vztáhnout účinnost bezpečnostního opatření ke schopnosti snížit hrozbu.

Stanovením koeficientu, který bude vyjadřovat míru snížení hrozby, od úplné eliminace hrozby po naprostou neúčinnost, pak bude možné vypočítat efektivitu jednotlivých opatření vůči každému identifikovanému riziku. Součet všech účinností jednotlivých opatření vůči všem rizikům pak vyjádří celkovou účinnost každého opatření v rámci analyzovaného energetického zařízení.

Stejně jako ve stati 4.3.1. bude zde použit příklad praktické aplikace zvládání rizik v rámci řešení dle standardu ISMS u stejné organizace. Na grafu na obrázku č. 5 je znázorněna presentace vypočtených účinností opatření sady ISMS převedených na stupnice od 1 do 100. Sada opatření ISMS čítá 114 opatření. Z grafu je zřejmé, že největší účinnost má prvních 22 opatření s účinností v hodnotách od 100 do 36 (hodnota na grafu je označena červenou šipkou).




*Obrázek 5 Rozložení účinnosti bezpečnostních opatření*

### *sestavení minimálních standardů*

V rámci řešení zvládání rizik fyzické bezpečnosti energetického zařízení by nejúčinnější opatření ze sady bezpečnostních opatření k eliminaci rizik byli kandidáti do minimálního standardu fyzické bezpečnosti pro energetické zařízení dané kategorie.

Finální stanovení sady bezpečnostních opatření k eliminaci rizik pro minimální standard fyzické bezpečnosti pro energetické zařízení dané kategorie musí být provedeno na základě vyhodnocení analýz celého vzorku energetických zařízení.

Tímto způsobem by bylo možné sestavit minimální standardy pro fyzickou bezpečnost pro jednotlivé kategorie energetických zařízení.

### Standard NERC CIP-014-1 Fyzická bezpečnost

Příkladem odlišného přístupu k zajištění jednotné úrovně fyzické bezpečnosti je standard NERC (North American Electric Reliability Corporation) je standard CIP (Critical Infrastructure Protection) CIP-014-1, který úspěšně prošel finálním hlasováním a v současnosti je připravován administrativní proces k jeho vydání.

Standard se týká všech zařízení připojených na síť s napětím vyšším, než 200kV a stanovuje 6 požadavků:

1. Úvodní analýzu dopadů provedou vlastníci dotčených sítí, přičemž analýza rizik se má týkat všech zařízení, jejichž nefunkčnost nebo poškození by mohlo vést k rozsáhlé nestabilitě, nekontrolovanému odpojení, nebo kaskádovému efektu v rámci propojení sítí.
2. Provést verifikaci analýzy provedené dle bodu 1 nezávislou autoritou.
3. Primárním řídícím střediskům pro řízení přenosu oznamují ve stanovených intervalech podřízená střediska, že plní požadavky 4 až 6.
4. Provést hodnocení rizik a zranitelností fyzického útoku vůči všem dotčeným přenosovým zařízením.
5. Vytvořit, implementovat a dokumentovat plány fyzické bezpečnosti pro všechny dotčené přenosové stanice. Plány fyzické bezpečnosti popisují bezpečnostní opatření ke snížení rizik identifikovaných v předchozím bodu.
6. Provést verifikaci analýzy rizik provedené dle bodu 4 a plánů fyzické bezpečnosti provedené dle bodu 5 nezávislou autoritou.

Problémem aplikace tohoto standardu na podmínky ČR by mohlo být přezkoumávání analýz, nezávislými autoritami. Proto bude vhodné sledovat zkušenosti s implementací tohoto standardu do praxe a následně vyhodnotit případnou použitelnost zásad z tohoto standardu v podmínkách ČR.

***Závěr***

Jelikož energetická soustava funguje jako vzájemně propojený systém energetických soustav jednotlivých států, přičemž se tyto soustavy vzájemně ovlivňují, je nezbytné minimalizovat výskyt všech nežádoucích událostí.

Problematika fyzické bezpečnosti se stává za podmínek vrůstajících teroristických aktivit stále naléhavější, proto identifikace významných prvků energetické infrastruktury a řešení problematiky fyzické bezpečnosti těchto prvků nabývá na důležitosti.

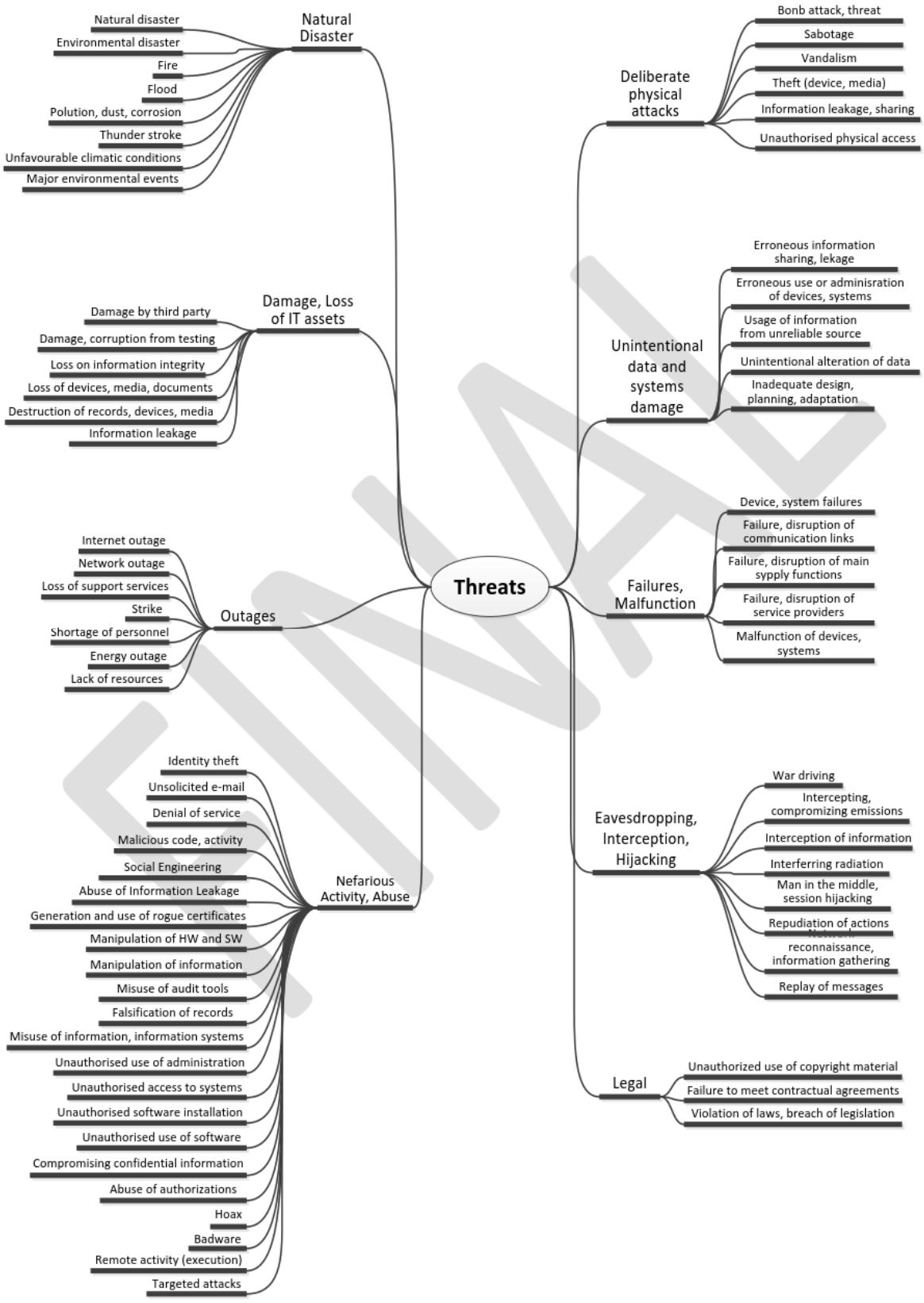
Pro dosažení záruk konzistentního ochrany všech bezpečnostně významných prvků energetické infrastruktury se jeví vývoj a následná aplikace minimálních standardů fyzické bezpečnosti jako použitelný způsob rychlého dosažení definované úrovně fyzické bezpečnosti.

# Seznam opatření PLSM

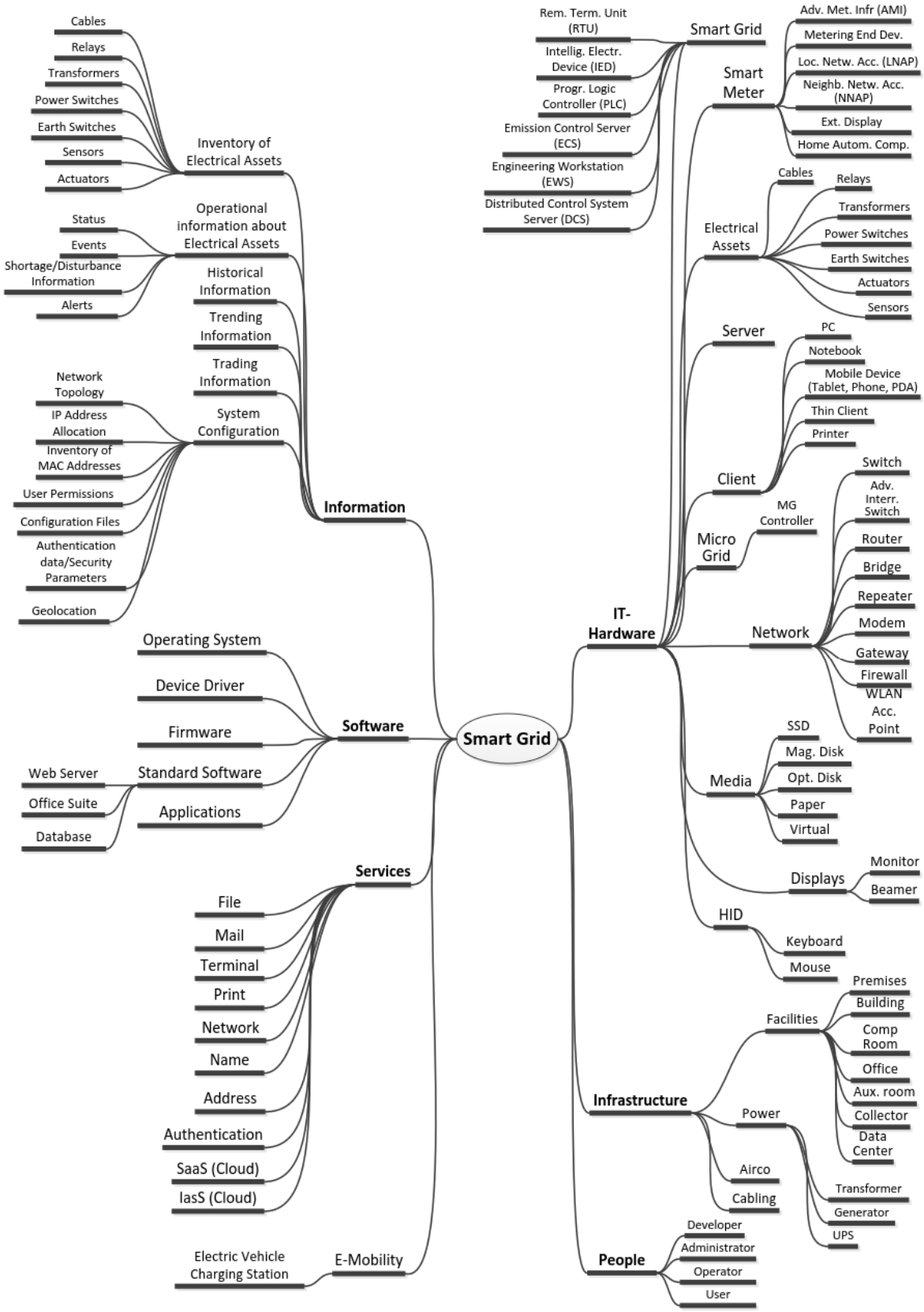
| **Doména opatření** | **Opatření PLSM** | **Číslo opatření** |
|---|---|---|
| Řízení bezpečnosti a řízení rizik | Bezpečnostní politiky informací | 1 |
| | Organizace bezpečnosti informací | 2 |
| | Postupy bezpečnosti informací | 3 |
| | Rámec pro řízení rizik | 4 |
| | Hodnocení rizik | 5 |
| | Plán zvládání rizik | 6 |
| Management třetích stran | Dohody se třetími stranami | 7 |
| | Sledování služeb třetích stran a ověřování řešení podle předem stanovených akceptačních kritérií | 8 |
| Bezpečnost procesů životního cyklu komponentů a operační procedury smart gridu | Analýza a specifikace bezpečnostních požadavků | 9 |
| | Soupis (inventarizační) Smart Grid komponentů / systémů | 10 |
| | Bezpečné řízení konfigurace smart grid komponentů / systémů | 11 |
| | Bezpečná konfigurační dokumentace | 12 |
| | Údržba Smart Grid komponentů / systémů | 13 |
| | Aktualizace software / firmware smart grid komponentů / systémů | 14 |
| | Likvidace Smart Grid komponentů / systémů | 15 |
| | Řízení změn | 16 |
| | Testování bezpečnosti mart grid komponentů / systémů | 17 |
| Personální bezpečnost, povědomí a vzdělávání | Personální prověrky | 18 |
| | Personální změny | 19 |
| | Program rozvoje bezpečnosti a bezpečnostního povědomí | 20 |
| | Bezpečnostní školení a certifikace pracovníků | 21 |
| Reakce na incident a sdílení znalostí a informací | Schopnosti reakce na incidenty | 22 |
| | Posouzení zranitelností | 23 |
| | Ošetření zranitelsnotí | 24 |
| | Kontakt s úřady a bezpečnostními zájmovými skupinami | 25 |

| Doména opatření | Opatření PLSM | Číslo opatření |
|---|---|---|
| Schopnosti audita a odpovědnost | Schopnosti provádět auditní činnosti | 26 |
| | Monitorování informačních systémů smart gridu | 27 |
| | Ochrana auditních informací | 28 |
| Schopnost zachování kontinuity provozu | Schopnosti zachování kontinuity provozu | 29 |
| | Základní komunikační služby | 30 |
| Fyzická bezpečnost | Fyzická bezpečnost | 31 |
| | Logování a monitorování fyzického přístupu | 32 |
| | Fyzická bezpečnost v prostorách třetích stran | 33 |
| Bezpečnost informačních systémů | Klasifikace / politika zveřejňování | 34 |
| | Bezpečnost dat | 35 |
| | Account management | 36 |
| | Řízení logického přístupu | 37 |
| | Bezpečný vzdálený přístup | 38 |
| | Informační bezpečnost v informačních systémech | 39 |
| | Manipulace s medii | 40 |
| Síťová bezpečnost | Funkční a bezpečné oddělení sítí | 41 |
| | Bezpečná síťová komunikace | 42 |
| Odolné a robustní návrh kritických základních funkcí a infrastruktury | Minimální expozice | 43 |
| | Odolnost | 44 |
| | Bezpečné přerušení - Kontinuita provozu | 45 |

## *Hrozby dle PLSM*



## *Aktiva dle PLSM*



# Shrnující studie legislativní etapy

## Legislativní dimenze řešení problémů v oblasti ochrany kritické infrastruktury před kybernetickými bezpečnostními hrozbami

### *Pojem legislativního řešení kybernetické bezpečnosti*

Legislativní řešení kybernetické bezpečnosti nemá v platném právu žádnou prakticky srovnatelnou paralelu. Lze sice pro partikulární otázky používat nejrůznější analogie s bezpečnostními řešeními v oborech s dominantní technologickou komponentou (typicky např. v oborech stavebnictví, protipožární ochrany, dopravy, apod.), právní fenomén kybernetické bezpečnosti se však jako takový ničemu ve své podstatě nepodobá[6].

Prvním důvodem originality kybernetické bezpečnosti je skutečnost, že hodnocení bezpečnostních aktiv má až na výjimky obvykle akcesorickou povahu. Systémy a sítě, jejichž zabezpečení je předmětem právní úpravy, totiž zpravidla nemají hodnotu per se, ale v závislosti na to, čemu v konečném důsledku slouží. Bezpečnostní hodnota určitého systému nebo sítě je tedy přímo závislá na tom, pro jakou funkcionalitu tento systém poskytuje informační servis. S trochou nadsázky tedy lze prohlásit, že tentýž router může sloužit jako součást informační infrastruktury internetové kavárny i atomové elektrárny, přičemž jeho bezpečnostní hodnota není dána jeho cenou, ale způsobem jeho užití[7].

Výjimkou ze shora uvedeného jsou systémy a sítě, jejichž smyslem a účelem je působit jako součást národní informační a komunikační infrastruktury. Typicky např. tzv. páteřní sítě neodvozují svoji důležitost od hodnoty funkcionalit, k nimž byly pořízeny, neboť jejich funkcí je udržovat v chodu informační síť jako takovou – v jejich případě tedy není nutno hodnotit, jakému primárnímu účelu slouží, neboť jejich důležitost je zpravidla dána faktory jako je kapacita, zastupitelnost apod.

Druhým významným faktorem odlišujícím legislativní řešení kybernetické bezpečnosti od ostatních oborů platného práva je její procesní orientace. Zatímco právní úprava krizového řízení resp. úprava bezpečnosti kritických funkcionalit státu je tradičně postavena na objektovém principu, je kybernetickou bezpečnost nutno primárně vnímat jako ochranu informačních procesů. Tomu pak musí odpovídat celá regulatorní logika i fungování příslušných orgánů veřejné moci, neboť primárním smyslem a účelem není ochrana existence nebo funkčnosti konkrétně definovaného objektu, ale zajištění bezproblémové existence informačních transakcí. Výsledné řešení přitom samozřejmě nemůže být vzhledem k objektům dohromady tvořícím naši informační a komunikační infrastrukturu absolutně indiferentní – objekt však má být předmětem regulatorního zájmu až v důsledku jeho konkrétní důležitosti pro kritický informační proces[8].

[6] Srov. Grant, J. Will There Be Cybersecurity Legislation? Journal of National Security Law and Policy, roč. 4, str. 104. Další důvody zvláštního charakteru kybernetické bezpečnosti přidává Paul Rosenzweig v textu Rosenzweig, P. Making Good Cybersecurity Law and Policy: How Can We Get Tasty Sausage?, Journal of Law and Policy for the Information Society, roč. 8, číslo 2, str. 390.

[7] Srov. např. Shane, P. M. Cybersecurity Policy as if "OrdinaryCitizens" Mattered: The Case for Public Participation in Cyber Policy Making, Journal of Law and Policy for the Information Society, roč. 8, číslo 2, str. 435.

[8] Srov. např. Lin, H. Thoughts on Threat Assessment in Cyberspace, Journal of Law and Policy for the Information Society, roč. 8, číslo 2, str. 338.

Třetím specifickým rysem právní úpravy kybernetické bezpečnosti je právní jev, který je doktrínou popisován jako fenomén definičních autorit. Veškeré lidské jednání totiž v prostředí informačních sítí neprobíhá bezprostředně, ale je zprostředkováváno službami informační společnosti. Člověk ani právnická osoba tedy nemůže v prostředí informačních sítí činit nic bez toho, aby se na jeho jednání fakticky nepodílela hned celá řada poskytovatelů služeb informační společnosti. Označení definiční autority si tyto subjekt vysloužily z toho důvodu, že mají faktickou možnost definovat formou kódu (tzv. definiční normy) technické parametry jednání svých uživatelů. Nejedná se přitom o normu právní, neboť poskytovatelé služeb informační společnosti nedisponují právotvornou kompetencí (jde povětšinou o soukromé subjekty) – přesto jde nepochybně o pravidlo, které má na jednání uživatelů zásadní vliv[9]. Definiční charakter těchto technických resp. faktických pravidel je pak od právních norem odlišuje i co do jejich fungování. Jde sice o pravidla vytvořená člověkem a zaměřená k regulaci lidského chování, nemají charakter povinnostní, ale zároveň se jedná o kauzální normy přímo determinující na technické úrovni výsledek lidského jednání. Byť tedy jsou to člověkem vytvořené normy zaměřené k regulaci lidského chování, jejich technický charakter jim dává prakticky povahu kauzálního přírodního zákona.

Z právního hlediska jde o extrémně zajímavý jev mající zásadní dopady především do problematiky odpovědnosti za protiprávní jednání. Především z toho důvodu, že poskytovatelé služeb informační společnosti jsou v problematických případech jedinými subjekty, které lze reálně nalézt, proti nimž lze uplatnit právní postih a které jsou technicky schopny problematickou situaci efektivně řešit, vznikla celá relativně samostatná teorie spoluodpovědnosti těchto poskytovatelů za protiprávní jednání jejich uživatelů[10]. Dokonce lze konstatovat i dříve nevídaný obecný trend přesouvat vymáhání subjektivních práv od jejich skutečných rušitelů (tj. od individuálních uživatelů) právě k poskytovatelům služeb, jejichž prostřednictvím k porušování těchto práv dochází, respektive která protiprávní jednání technicky zprostředkovávají[11].

V oblasti kybernetické bezpečnosti se fenomén definičních autorit rovněž projevuje zásadním způsobem, a to samotnou osobní působností příslušných právních předpisů. Povinnosti plynoucí z potřeby chránit kritické informační funkcionality státu resp. národní informační a komunikační infrastrukturu tedy nejsou v tomto případě vůbec ukládány koncovým uživatelům, ale směřují právě na poskytovatele služeb (otázce osobní působnosti české právní úpravy se věnujeme dále)[12]. V tomto směru je možno vidět i další podstatný rozdíl mezi právní úpravou krizového řízení a kybernetickou bezpečností, neboť v případě krizového řízení může právní úprava bezprostředně dopadat na libovolné fyzické či právnické osoby. Rozsah osobní působnosti právní úpravy kybernetické bezpečnosti naproti tomu nepočítá s dopadem na nikoho jiného, než jsou právě poskytovatelé služeb - v případě české právní úpravy jde konkrétně (pomineme-li orgány veřejné moci) o poskytovatele služeb elektronických komunikací[13].

[9] K pojmu a jeho právním důsledkům viz např. Polčák, R. Internet a proměny práva, Praha: Auditorium, 2012, str. 137.
[10] Viz např. monografii Husovec, M. Zodpovednosť na internete podľa českého a slovenského práva, Praha: CZ.NIC, ke stažení on-line na adrese http://knihy.nic.cz/files/nic/edice/Zodpovednost_web_FINAL.pdf.
[11] Důsledkem tohoto trendu jsou i extrémní právní konstrukce, jako např „třikrát a dost“ v zákoně HADOPI – srov. např. working paper Dejean, S., Pénard, T., Suire, R. Une première évaluation des effets de la loi Hadopi sur les pratiques des Internautes français, Rennes: CREM, ke stažení on-line na adrese http://www.01net.com/genere/article/fichiersAttaches/300415066.pdf.
[12] Srov. Berejka, M. A Case for Government Promoted Multi-Stakeholderism, Journal on Telecommunications and High-Tech Law, roč. 10, str. 9.
[13] Viz § 3 písm. a) zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti).

Posledním základním rysem právní úpravy kybernetické bezpečnosti, který z ní činí specifický regulatorní fenomén, je značná míra konvergence soukromého a veřejného zájmu. Bývá obvyklé, že v případě zájmu na ochraně tzv. nedistributivních práv je výsledná právní úprava konfliktní se soukromým zájmem resp. s distributivními právy osob. Proporcionalita resp. vzájemné vyvážení soukromého a veřejného zájmu je v takových případech nezřídka otázkou právní a politické alchymie. Pokud však má právní úprava nedistributivního práva jako v případě českého zákona o kybernetické bezpečnosti pouze základní charakter, je hodnotově konzistentní s tím, co lze označit za tvrdé jádro ústavy[14], a navíc má vzhledem k distributivním právům jen minimální rozsah, dochází k výjimečně nekonfliktní situaci[15].

Teoreticky vzato nejde o nic zvláštního, neboť nedistributivní práva nemají autonomní charakter a z podstaty ani nejsou vzhledem k právům distributivním v opozici. Bezpečnost nebo ochrana životního prostředí totiž jako práva nefungují bez dalšího, ale vždy je jejich obecný i zvláštní výskyt v důsledku motivován ochranou některého ze základních práv distributivních.

V případě kybernetické bezpečnosti tedy nelze bez dalšího hovořit o bezpečnosti národní informační a komunikační infrastruktury jako o ultimátní teleologii zákonné úpravy, neboť skutečným smyslem a účelem resp. kýženým účinkem zákona je v tomto případě zabezpečení možnosti člověka žít plnohodnotný soukromý život[16]. Komponentami práva na soukromý život přitom nejsou jen ochrana soukromí, ale též možnost přístupu k energiím, zdrojům či základním životním službám, přičemž za základní funkcionalitu moderní společnosti považujeme též fungující služby informační společnosti, jejich prostřednictvím člověk realizuje podstatnou část své sociální existence.

Jestliže tedy můžeme konstatovat, že naše právní úprava kybernetické bezpečnosti není zásadně konfliktní ve vztahu k distributivním právům, je to dáno především skutečností, že omezení distributivních práv, která reálně přináší, jsou v porovnání s důležitostí chráněných zájmů jen nepatrná. Nejzávažnějším zásahem do distributivních práv tak je v tomto případě zásah do práva vlastnického, přičemž povinným subjektům může vzniknout povinnost investovat své prostředky do zabezpečení vlastní informační a komunikační infrastruktury. Jak vyplynulo z jednání vedoucích k přijetí zákona o kybernetické bezpečnosti, jsou tyto investice již standardně povinnými subjekty realizovány – nikoli sice z důvodu jejich zájmu na zajištění národní kybernetické bezpečnosti, ale z čistě zištného zájmu na ochraně vlastních systémů před kybernetickými bezpečnostními incidenty. Ve většině případů tedy bude nutno ze strany povinných subjektů investovat pouze do komponent zajišťujících komunikaci s národním nebo vládním CERT – ani tyto investice však nebudou pro povinné subjekty ztrátové, neboť v jejich důsledku budou moci těžit z účasti na kolektivním systému ochrany.

[14] K pojmu distributivních resp. nedistributivních práv a tvrdého jádra (materiálního ohniska) ústavy viz Holländer, P. Filosofie práva, 2. Vydání, Plzeň: Aleš Čeněk, 2012.

[15] Viz Powell, B. Is Cybersecurity a Public Good? Evidence From the Financial Services Industry, Journal of Law, Economics and Policy, roč. 1, číslo 2, str. 497.

[16] Pojem informačního sebeurčení jako kategorie soukromého života je též dominantním motivem věcného záměru i důvodové zprávy zákona č. 181/2014.

Před výkladem k jednotlivým institutům je nutno vyjádřit se ke třem populárním mýtům vztahujícím se k právu kybernetické bezpečnosti. První z nich týká se smyslu a účelu specifické legislativy a je založen na předpokladu, že právní předpis upravující práva a povinnosti k zajištění národní kybernetické bezpečnosti má ve svém textu obsahovat pro jednotlivé zainteresované subjekty komplexní návod na to, jak se správně chovat respektive důkladný popis toho, co je zakázáno. Zvláštní zákon upravující oblast národní kybernetické bezpečnosti však nemá a ani nemůže sloužit jako kuchařka – namísto toho má pouze v minimální formě upravit specifické povinnosti povinným subjektům a dále pak založit kompetence institucím, do jejichž působnosti tato oblast spadá. Je přitom třeba vycházet nikoli z předpokladu, že všem zainteresovaným je třeba zákonem detailně a nekompromisně sdělit, co mají nebo nemají dělat, ale že:

- právo není jen zákon – konkrétní obsah zákonných povinností nebývá nutně specifikován pouze zákonem, ale může být též např. otázkou judikatury či aplikace obecných či zvláštních právních principů. Z toho mj. plyne i skutečnost, že zákon může zůstat relativně rigidní, ale obsah platného práva se může v čase výrazně měnit[17],
- soukromým subjektům mají být zákonem stanoveny pouze konkrétní příkazy nebo zákazy – dovolené jednání není třeba vymezovat, neboť tyto subjekty mohou činit vše, co jim zákon nezakazuje[18],
- orgánům veřejné moci má zákon vymezit působnost, stanovit povinnosti a možnosti autoritativního jednání (orgány veřejné moci mohou totiž oproti subjektům soukromého práva dělat jen to, co jim zákon výslovně ukládá nebo umožňuje[19]),
- není vhodné ani potřebné upravovat to, co upravují jiné právní předpisy nebo mezinárodní smlouvy resp. zakládat povinnosti, které jsou již založené jinými částmi našeho právního řádu. Z toho plyne též obecná nutnost strukturovat a formulovat zákon tak, aby do systému platného práva nevnášel redundantní nebo nekoherentní prvky[20],
- předmětem zákona je právní povinnost a normativními modalitami jsou příkaz, zákaz a dovolení. Co z nějakého důvodu není možné nebo účelné definovat jako právní povinnost prostřednictvím některé z těchto modalit, nemá v psaném právu co pohledávat. Typickým příkladem jsou technické standardy nemající charakter právních povinností a

[17] Výmluvně to ilustruje Gustav Radbruch v článku Zákonné neprávo a nadzákonné právo původně publikovaným jako Radbruch, G. Gesetzliches Unrecht und übergesetzliches Recht, Süddeutsche Juristenzeitung, roč. 1946, str. 105–108.
[18] Viz čl. 2 odst. 3 Listiny základních práv a svobod.
[19] Viz čl. 2 odst. 2 Listiny základních práv a svobod.
[20] V tomto případě jde o komponenty označované právní teorií jako tzv. materiální náležitosti právotvorby normativního typu. K náležitostem i technice české právotvorby viz např. Šín Z.: Tvorba práva. Praha: C. H. Beck, 2003.

- zákon nesmí odporovat Ústavnímu pořádku České republiky – žádná zákonem založená právní povinnost nesmí vybočovat z rámce proporcionality základních práv člověka a nedistributivních práv státu[21].

Z právě uvedeného mimo jiné vyplývá, že právní úprava kybernetické bezpečnosti České republiky není ani zdaleka tvořena jen zákonem o kybernetické bezpečnosti. Povinnosti při ochraně informační a komunikační infrastruktury totiž kromě něj zakládá i řada dalších součástí českého právního řádu. Následující výklad je tedy zaměřen na instituty, které se z hlediska zajištění kybernetické bezpečnosti jeví jako nejdůležitější z pohledu povinných subjektů. Konkrétně se budeme věnovat otázkám

- bezpečnostních opatření
- protiopatření
- odpovědnosti za nedbalost a prevenčních povinností
- disciplinární odpovědnosti a disciplinárních povinností

## Bezpečnostní opatření

Bezpečnostní opatření jsou základním kamenem zákona o kybernetické bezpečnosti a z operačního hlediska i jeho zdaleka nejdůležitější součástí[22]. Primárním účelem zákona totiž není řešení jednotlivých kybernetických bezpečnostních incidentů ale vytvoření prostředí, v němž jsou kritická informační a komunikační infrastruktura státu a další zájmové informační systémy a sítě preventivně chráněny tak, že pro ně žádná kybernetická bezpečnostní událost nepředstavuje bezpečnostní riziko.

Zákon sám zavádí povinným subjektům pouze základní povinnost mít bezpečnostní opatření v taxativně vymezených kategoriích, přičemž technické podrobnosti upraví prováděcí předpis (tj. vyhláška Národního bezpečnostního úřadu[23]). Je postaven na dokumentačním modelu, tj. ukládá povinným subjektům povinnost především dokumentovat jednotlivé typy bezpečnostních opatření a následně pak dává právo Národnímu bezpečnostnímu úřadu kontrolovat, zda je dokumentace souladná nejen s konkrétními požadavky zákona a prováděcího předpisu, ale samozřejmě též s aktuální skutečností.

Smyslem bezpečnostních opatření je primárně vytvoření takových preventivních mechanismů, které povinným subjektům umožní vyrovnávat se autonomně k kybernetickými bezpečnostními událostmi (ať už jde o prevenci jejich samotného vzniku nebo o nástroje a mechanismy k jejich následnému pokrytí)[24]. Subsidiárně jsou pak bezpečnostní opatření formulována tak, aby jejich zavedení umožnilo

[21] Proporcionalita je metodo poměřování právních principů, přičemž charakter právních principů mají i všechna ústavně zaručená základní práva. K používání této metody v českém právním prostředí viz Holländer, P. Filosofie práva, 2. Vydání, Plzeň: Aleš Čeněk, 2012.
[22] Zákon je v § 4 odst. 1 vymezuje jako „souhrn úkonů, jejichž cílem je zajištění bezpečnosti informací v informačních systémech a dostupnosti a spolehlivosti služeb a sítí elektronických komunikací v kybernetickém prostoru“.
[23] Viz vyhlášku č. 316/2014 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti (vyhláška o kybernetické bezpečnosti).
[24] Za tímto účelem dělí zákon bezpečnostní opatření na organizační a technická a ty pak dále specifikuje v ust. § 5 odst. 2 a 3.

efektivní fungování kybernetických bezpečnostních struktur na úrovni státu, tj. především národního a vládního dohledového pracoviště.

Systematickým problémem bezpečnostních opatření, kterému jsme se věnovali již ve studii na téma principů a perspektiv kybernetické bezpečnosti, je skutečnost, že jsou formulována jako technický a organizační standard, aniž by však zákon předpokládal existenci oficiálních certifikačních nebo jiných a priori procedur použitelných k verifikaci jejich kvality. Povinné subjekty tedy budou investovat do akvizic nebo úprav příslušných bezpečnostních řešení, aniž by měly možnost a priori ověřit, zda to, čím se snaží plnit zákonné požadavky skutečně je nebo není v souladu se zákonem resp. s prováděcím předpisem.

Vedle nejistoty v otázce compliance může být tato situace hodnocena ze strany povinných subjektů jako problematická i z důvodu nemožnosti zapojení oficiální verifikace do procesu externí akvizice resp. outsourcingu bezpečnostních opatření. Typicky tedy může dojít k situaci, kdy si povinný subjekt nebude moci až do případné kontroly ze strany Národního bezpečnostního úřadu být stoprocentně jist, zda řešení, které pořídil od externího dodavatele nebo které průběžně outsourcuje u poskytovatele služby je souladné se zákonnými požadavky[25].

Jako ideální ošetření této situace jeví se být verifikace formou nezávislého expertního posouzení provedeného důvěryhodným a odborně způsobilým externím subjektem. Skutečnost, že zákon je přísně technologicky neutrální[26] a dává ve všech směrech relativně velkou volnost povinným subjektům v otázce konkrétní formy realizace bezpečnostních opatření, povede zřejmě k vytvoření velkého množství individualizovaných bezpečnostních řešení. Tuto skutečnost zákon nejen předpokládá, ale z důvodové zprávy lze vyčíst, že ji považuje za žádoucí, neboť individualizace je v tomto případě vhodným prostředkem technické a ekonomické efektivity.

Lze též očekávat, že povinné subjekty téhož typu provozující informační systémy nebo sítě srovnatelných technických parametrů budou hledat podobná řešení a můžeme předvídat přirozenou unifikaci nejen na úrovni technologických dodávek nebo služeb, ale i požadavků na a priori zákonnou compliance. Typicky v oboru energetiky bude zřejmě docházet k typově podobným realizacím bezpečnostních opatření prováděným jako součást rovněž vzájemně se podobajících organizačních a právních projektů. Bude tedy pak, jak uvedeno ve dřívější studii k principům a perspektivám kybernetické bezpečnosti, vhodné, podaří-li se na úrovni profesního sdružení nebo podobné organizační platformy vytvořit procedury, které pomohou povinným subjektům verifikovat kvalitu jejich bezpečnostních opatření, to navíc při zohlednění jejich oborových specifik.

Pokud bude tato procedura dostatečně odborně důvěryhodná, může její existence usnadnit výkon kontroly a dozoru i samotnému Národnímu bezpečnostnímu úřadu – zatímco totiž standardní postup při kontrolách bezpečnostních opatření musí být založen na aktivním ověřování komplexní jejich souladnosti se zákonnými požadavky, může být nezávisle certifikovaný systém kontrolován jako a priori souladný s tím, že kontrola se může konkrétně zaměřit už jen na jeho potenciálně problémové aspekty.

[25] Srov. např. režim certifikace v § 46 a násl. zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů.

[26] Důvodová zpráva zmiňuje tento princip dokonce na prvním místě – viz důvodová zpráva k návrhu zákona o kybernetické bezpečnosti, str. 63 a násl.

## Protiopatření

Protiopatřeními pro potřeby této studie souhrnně nazýváme to, co zákon označuje jako „opatření“ a dělí dle typu na varování, reaktivní opatření a ochranná opatření. Všechny typy protiopatření mají povahu vrchnostenské činnosti Národního bezpečnostního úřadu, přičemž varování má charakter informativní a zbývající dvě opatření mají formu závazných individuálních právních aktů resp. opatření obecné povahy.

Institut varování se může zdát na první pohled zbytečný, neboť jeho užití nepřináší bezprostřední imperativ ani riziko přímé sankce[27]. Jeho charakter však vystihuje typický efekt zákona o kybernetické bezpečnosti v otázkách odpovědnosti za kybernetické bezpečnostní incidenty. Zákon totiž ani u imperativních institutů nepřináší žádné přímé drakonické sankce, ale zavádí přímo nebo nepřímo nové typy právních povinností, jejichž neplnění může mít za následek vznik povinnosti nahradit škodu vzniklou v jeho důsledku. Povinný subjekt tedy nemůže kalkulovat právní riziko plynoucí z nově založených zákonných povinností pouze ve vztahu k možné pokutě (ta je co do své výše spíše symbolická), ale rovněž vzhledem k velmi neurčitému potenciálu škod, k nimž může dojít v důsledku zaviněného[28] i nezaviněného[29] kybernetického bezpečnostního incidentu.

V případě varování tedy Národní bezpečnostní úřad sice provádí pouze adresnou osvětu ohledně konkrétních bezpečnostních rizik, ta ale ve svém důsledku vede k prokazatelné informovanosti povinných subjektů. Zprostředkovaně tím přináší povinným subjektům možnost založení povinnosti nahradit škodu způsobenou též v důsledku toho, že na základě varování nepřijmou přiměřená opatření k zabránění vzniku kybernetických bezpečnostních incidentů nebo zmírnění jejich následků[30].

V typickém případě tedy bude Národní bezpečnostní úřad formou varování informovat o konkrétním bezpečnostním riziku (např. o tzv. bezpečnostní díře) – jestliže povinné subjekty nebudou na základě této informace za vynaložení přiměřeného úsilí na takto identifikované riziko reagovat (např. instalací záplat) a v důsledku toho dojde ke škodě u třetích osob, mohou třetím osobám povinné subjekty přímo odpovídat z titulu nesplnění tzv. prevenční povinnosti. Je-li pak v této situaci způsobena škoda samotnému povinnému subjektu, může být shora popsaný nedostatek reakce na varování též důvodem pro pojišťovnu, aby odmítla nebo výrazně snížila hodnotu pojistného plnění.

Z hlediska povinných subjektů tedy přináší i na první pohled bezzubý institut varování nový typ právního rizika, které je a priori jen velmi těžko ohodnotitelné – čím větší je přitom povinný subjekt a čím více spravuje systémů spadajících pod rozsah zákona o kybernetické bezpečnosti, tím je toto riziko závažnější, a to co do své potenciální hodnoty i do míry nepředvídatelnosti svého výskytu. Dokonce lze s trochou nadsázky konstatovat, že s rostoucí velikostí můžeme sledovat u povinných subjektů klesající míru zájmu o přímé sankce zákona o kybernetické bezpečnosti (tj. o pokuty) a

[27] Viz § 12 ve spojení s § 25 zákona č. 181/2014 Sb.

[28] Odpovědnost je v tomto případě založena na základě obecných ust. § 2910 a násl. zákona č. 89/2012 Sb., občanský zákoník.

[29] V úvahu zde u podnikatelských subjektů připadá povinnost nahradit škodu způsobenou provozní činností na základě § 2924 zákona č. 89/2012 Sb.: „Kdo provozuje závod nebo jiné zařízení sloužící k výdělečné činnosti, nahradí škodu vzniklou z provozu, ať již byla způsobena vlastní provozní činností, věcí při ní použitou nebo vlivem činnosti na okolí. Povinnosti se zprostí, prokáže-li, že vynaložil veškerou péči, kterou lze rozumně požadovat, aby ke škodě nedošlo.“

[30] K tomu srov. § 2901 zákona č. 89/2012 Sb.: „Vyžadují-li to okolnosti případu nebo zvyklosti soukromého života, má povinnost zakročit na ochranu jiného každý, kdo vytvořil nebezpečnou situaci nebo kdo nad ní má kontrolu, anebo odůvodňuje-li to povaha poměru mezi osobami. Stejnou povinnost má ten, kdo může podle svých možností a schopností snadno odvrátit újmu, o níž ví nebo musí vědět, že hrozící závažností zjevně převyšuje, co je třeba k zákroku vynaložit.“

naopak rostoucí zájmovost nepřímých sankcí ve formě právě popsaného potenciálu povinností k náhradě škody resp. limitace pojistného plnění[31].

Další dva typy protiopatření již disponují v porovnání s varováním též přímou možností autoritativního vynucení. Zákon definuje jejich věcný rozsah velmi široce - prakticky jde jakákoli opatření „k řešení kybernetického bezpečnostního

incidentu anebo k zabezpečení informačních systémů nebo sítí a služeb elektronických komunikací před kybernetickým bezpečnostním incidentem[32]“. V tomto směru ale nelze na rozdíl od některých bulvárních názorů uvažovat o tom, že by takto široce definovaná věcná působnost příslušných správních rozhodnutí nebo opatření obecné povahy dávala Národnímu bezpečnostnímu úřadu do rukou nějaký totalitní nástroj ke kontrole národní informační a komunikační infrastruktury. Vedle konkrétního omezení smyslem a účelem protiopatření (resp. reaktivních nebo ochranných opatření) je v tomto případě Národní bezpečnostní úřad omezen působností zákona a dále pak obecnými principy správního práva, z nichž nejdůležitějšími jsou zřejmě principy dobré správy[33] a zákaz svévole.

V rovině ústavního práva pak je Národní bezpečnostní úřad omezen především judikatorní doktrínou tzv. omezeného testu proporcionality[34]. Jedná se o ústavněprávní metodu, k jejíž aplikaci jsou povinny orgány veřejné moci vždy, pokud svojí činností zasahují do autonomie povinných subjektů a která jim, zjednodušeně řečeno, přikazuje použít takových prostředků, které při splnění svého účelu znamenají pro povinné subjekty minimální zásah do jejich práv. Pokud je tedy více možností, jak dosáhnout kýženého cílového stavu, tj. v tomto případě jak zmírnit dopady hrozícího nebo probíhajícího kybernetického bezpečnostního incidentu, resp. jak na základě zkušeností lépe zabezpečit příslušné systémy nebo sítě, má Národní bezpečnostní úřad implicitní povinnost vybrat pro příslušné reaktivní nebo ochranné opatření takovou alternativu, která bude povinné subjekty nejméně zatěžovat na jejich právech.

Imperativní protiopatření zákon dělí z hlediska jejich účelu na reaktivní a ochranná. První jmenovaný typ uplatní se v případech hrozícího nebo probíhajícího konkrétního kybernetického bezpečnostního incidentu, tj. bezpečnostní hrozby, která je konkrétně identifikována a je nutno na ni odpovídajícím způsobem reagovat. Tomu odpovídá i procesní charakteristika reaktivních protiopatření zahrnující ve správním právu spíše výjimečné instituty okamžité vykonatelnosti a absence odkladného účinku řádného opravného prostředku (v tomto případě rozkladu)[35].

Okamžitost a bezprostřednost imperativního účinku reaktivních protiopatření odpovídá jejich charakteru jakožto bezpečnostních nástrojů výkonné moci. Přestože bylo nutno z hlediska procesní formy dostát požadavkům správního práva na dokonalý proces autoritativní aplikace, je zřejmé, že v tomto případě nejde o klasickou exekutivní aplikaci práva, ale spíše o konkrétní vrchnostenský zásah vedoucí k pokrytí okamžité bezpečnostní hrozby. Připodobnit jej lze namísto jiných procesů, na jejichž konci stojí vykonatelné správní rozhodnutí (resp. opatření obecné povahy), spíše k okamžité akci bezpečnostní složky výkonné moci, tj. např. k zásahu policie nebo integrovaného záchranného

[31] K nim ještě přistupují jen těžko vyčíslitelné náklady spojené s případnou kontrolou a realizací adresně uložených opatření k nápravě ve smyslu § 24 zákona č. 181/2014 Sb.
[32] Viz § 13 odst. 1 zákona č. 181/2014 Sb.
[33] K pojmu viz např. Košičiarová, S. Princípy dobrej verejnej správy a Rada Európy, Bratislava: Iura Edition, 2012, 556 s.
[34] Jako omezený test proporcionality označuje se výstupní část standardního testu proporcionality, která spočívá v hodnocení míry zásahu do zájmu chráněného právním principem. Platí přitom, že zásah do práv osoby nesmí být větší, než je vzhledem k okolnostem pragmaticky nutné – srov. Holländer, P. Filosofie práva, 2. Vydání, Plzeň: Aleš Čeněk, 2012.
[35] Srov. § 15 zákona č. 181/2014 Sb.

systému[36]. V tomto případě však z podstaty věci plyne, že Národní bezpečnostní úřad nemá možnost provést takový zásah autonomně - k tomu viz shora konstatovaný specificky rys kybernetické bezpečnosti spočívající ve zprostředkovanosti veškerých aktivit službami informační společnosti. Exekutivní reakce k zajištění národní kybernetické bezpečnosti tedy v tomto případě nemůže mít povahu přímé akce bezpečnostní složky státu (v tomto případě Národního bezpečnostního úřadu), ale pouze vrchnostenského imperativu vedoucího ke konkrétní akci subjektu, o jehož informační systém nebo síť se jedná. Nemaje ve správním právu jiného použitelného institutu, sáhl tedy v tomto případě právotvůrce logicky po institutu správního rozhodnutí resp. opatření obecné povahy.

Ochranná opatření mají naproti tomu svou náturou blíže ke klasickému správnímu rozhodování resp. k vrchnostenské podzákonné normotvorbě, neboť jde o imperativy, jejichž implementace, lidově řečeno, až tak nehoří. Jejich podkladem jsou rovněž konkrétní kybernetické bezpečnostní incidenty, ale jejich smyslem a účelem není bezprostřední reakce, nýbrž zvýšení úrovně bezpečnosti příslušných informačních systémů a sítí[37]. Především v případech, kdy jsou ochranná opatření vydávána formou opatření obecné povahy neurčitému okruhu adresátů je lze vlastně z funkčního hlediska považovat za doplněk podzákonného předpisu konkretizujícího obsah bezpečnostních opatření.

### Odpovědnost za nedbalost a prevenční povinnosti

Přestože sám zákon o kybernetické bezpečnosti se tomuto typu odpovědnosti z pochopitelných důvodů vůbec nevěnuje, představuje pro povinné subjekty shora konstatovaná možnost odpovědnosti za vědomou či nevědomou nedbalost resp. za nesplnění prevenční povinnosti zřejmě nejsilnější právní motivační faktor k zavádění bezpečnostních opatření.

Odpovědnost v tomto případě znamená, jak bylo uvedeno shora, nejen potencialitu povinnosti nahradit škodu způsobenou třetím osobám v důsledku nedbalosti nebo opomenutí preventivního zásahu, ale též srovnatelně důležité riziko krácení nebo ztráty nároku na pojistné plnění u škod na vlastním majetku[38] resp. na vlastní činnosti nebo i riziko subsidiární sankce za nesplnění povinnosti specificky regulovaného odvětví (např. v oblasti energetiky)[39].

K právě uvedeným typům odpovědnostních důsledků lze ještě připočíst riziko prodlení v případech, kdy kybernetický bezpečnostní incident způsobí neschopnost povinného subjektu plnit jiné právní povinnosti. Typicky může například dojít k situaci, kdy má povinný subjekt povinnost dodávat svým odběratelům zboží nebo služby a v důsledku kybernetického bezpečnostního incidentu toho není po nějakou dobu schopen. Za předpokladu, že kybernetický bezpečnostní incident vedl k takovým důsledkům kvůli neschopnosti povinného subjektu splnit si zákonnou povinnost vyplývající ze zákona

[36] Nabízí se zde například srovnání s pravomocemi policie při zajišťování bezpečnosti chráněných prostorů, objektů a osob ve smyslu ust. § 48 odst. 4 zákona č. 273/2008 Sb., o Policii české republiky, ve znění pozdějších předpisů.
[37] Srov. § 14 zákona č. 181/2014 Sb.
[38] K tomu viz zejm. ust. § 2800 odst. 2 zákona č. 89/2012 Sb.: „Mělo-li porušení povinnosti pojistníka, pojištěného nebo jiné osoby, která má na pojistné plnění právo, podstatný vliv na vznik pojistné události, její průběh, na zvětšení rozsahu jejích následků nebo na zjištění či určení výše pojistného plnění, má pojistitel právo snížit pojistné plnění úměrně k tomu, jaký vliv mělo toto porušení na rozsah pojistitelovy povinnosti plnit."
[39] Vedle pokut či opatření k nápravě může jít též o nebezpečí odnětí licence nebo jiného povolení k výkonu specifické činnosti – tuto možnost dává národním regulátorům úprava např. v oblasti energetiky nebo elektronických komunikací – srov. zákon č. 458/2000 Sb., o podmínkách podnikání a o výkonu státní správy v energetických odvětvích a o změně některých zákonů (energetický zákon), ve znění pozdějších předpisů) nebo zákon č. 127/2005 Sb, o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích), ve znění pozdějších předpisů.

o kybernetické bezpečnosti, nebude se povinný subjekt moci bránit poukazem na tento incident proti nárokům třetím osob z vadného resp. pozdního plnění.

To samozřejmě neznamená, že by povinné subjekty měly důvod obávat se toho, že budou odpovídat za veškeré škody způsobené třetím osobám kybernetickými bezpečnostními incidenty, na nichž se bude nějakým způsobem podílet jejich nedostatečně zabezpečená informační a komunikační infrastruktura. Ani v případě, byla-li by škoda třetím osobám skutečně způsobena v důsledku zanedbání specifických povinností plynoucích ze zákona o kybernetické bezpečnosti (resp. z jeho imperativních institutů), nejednalo by se ze strany povinného subjektu zřejmě o povinnost výlučnou – tam, kde byla např. v důsledku nedbalosti povinného subjektu zneužita jeho infrastruktura k provedení kybernetického útoku, zkoumal by soud u povinného subjektu míru jeho zavinění resp. míru toho, jak se nedbalá realizace opatření k zajištění kybernetické bezpečnosti podílela na celkovém škodním dopadu příslušného kybernetického bezpečnostního incidentu[40].

Za připomenutí stojí především typologie nedbalostního zavinění sestávající vedle hrubé (tj. vědomé) nedbalosti též z nedbalosti nevědomé (tj. lehké)[41]. Za zaviněné porušení právní povinnosti se tak považují nejen situace, kdy má povinný subjekt prokazatelně k dispozici informace o hrozícím nebezpečí a vlastní liknavostí nezabrání škodlivému následku, ale také případy, kdy povinný subjekt sice těmito informacemi objektivně nedisponuje, ale opatřit si je měl a mohl. Ve vztahu ke shora zmíněnému institutu varování to mimo jiné znamená, že ze strany povinného subjektu nebude možno namítat například nefunkčnost povinně sdělované kontaktní adresy nebo interní komunikační problémy v rámci organizace, kvůli kterým se informace o varování vydaném Národním bezpečnostním úřadem nedostane na správné místo.

Nedbalost nebo nesplnění prevenční povinnosti každopádně nemusí mít, jak bylo naznačeno výše, důsledky pouze soukromoprávní. Řada povinných subjektů působí v odvětví, která mají specifickou a často i poměrně rigorózní správní regulaci – příkladem může být energetika, elektronické komunikace, tzv. jiné utility (odpadové hospodářství, distribuce vody apod.), zdravotnictví nebo potravinářství. Ve většině z těchto odvětví mají povinné subjekty nejen povinnosti vztahující se bezprostředně k příslušnému typu činnosti, ale též související povinnosti, z nichž podstatná část se může přímo nebo nepřímo týkat provozu vnitřních informačních systémů nebo komunikačních sítí. Pokud v takovém případě dojde k narušení regulované činnosti povinného subjektu v důsledku kybernetického bezpečnostního incidentu, který povinný subjekt nedokázal zvládnout v důsledku nedbalosti nebo porušení prevenční povinnosti, může to pro něj znamenal vedle shora uvedených odpovědnostních rizik též možnost postihu dle specifických pravidel příslušného regulovaného odvětví. Není pak v tomto směru žádným tajemstvím, že např. pro subjekty v oboru energetiky může být takový subsidiární sankční postih dle energetického zákona nepoměrně citelnější, než primární sankce plynoucí ze zákona o kybernetické bezpečnosti.

Všechna shora uvedená právní rizika jsou v porovnání s imperativními a sankčními mechanismy zákona o kybernetické bezpečnosti pro povinné subjekty nejen mnohem závažnější, ale také co do svého důsledku mnohem méně předvídatelná. Zatímco lze vcelku snadno odhadnout, jaká výše pokuty hrozí při neprovedení reaktivního protiopatření, jen těžko se dá z pohledu povinného subjektu

[40] V tomto případě je specifický charakter kybernetických bezpečnostních incidentů společně s charakterem účasti způsobené nedůslednou ochranou vlastního systému možno obecně považovat a okolnosti hodné zvláštního zřetele a je tedy důvod předpokládat, že povinnost nahradit škodu bude v tomto případě specifikována dle míra zavinění resp. dle míry účasti – k tomu viz § 2915 odst. 2, první věta zákona č. 89/2012 Sb.: Jsou-li pro to důvody zvláštního zřetele hodné, může soud rozhodnout, že škůdce nahradí škodu podle své účasti na škodlivém následku; nelze-li účast přesně určit, přihlédne se k míře pravděpodobnosti."

[41] Viz např. Knapp, V. Některé úvahy o odpovědnosti v občanském právu. Stát a právo I. roč. 1956, str. 66.

odhadovat, jaký dopad může mít tatáž situace z pohledu soukromoprávní odpovědnosti vůči poškozeným třetím osobám, jak velká vymahatelná škoda může vzniknout zákazníkům nebo jak bude reagovat regulátor příslušného specifického odvětví (např. Energetický regulační úřad, Český telekomunikační úřad apod.)

Velká míra této subsidiární právní rizikovosti ve spojení s absencí oficiálních compliance procedur vytváří na povinné subjekty tlak projevující se v důsledku jednak chvályhodnou vůlí investovat do bezpečnostních opatření, to dokonce často i vysoko nad rámec zákonných požadavků. Kromě toho však může tato nejistota vést k tomu, že se povinné subjekty budou za každou cenu snažit o únik z osobního rozsahu zákona nebo se budou pokoušet o různé ohýbání jeho pravidel. Zabránit tomuto efektu by kromě nezávislých certifikačních procedur, které jsme rozebrali v závěru studie k principům a perspektivám kybernetické bezpečnosti, mohla též osvětová činnost Národního bezpečnostního úřadu realizovaná ve spolupráci s odvětvovými regulátory nebo rozšíření nabídky pojistných či zajišťovacích finančních produktů. Svou nezastupitelnou roli pak budou jistě hrát i odvětvové organizace, které mohou vedle zprostředkování komunikace mezi povinnými subjekty a Národním bezpečnostním úřadem působit i v rovině vzdělávací, koordinační nebo poradenské.

### Disciplinární odpovědnost a disciplinární povinnosti

Shora diskutovaná bezpečnostní opatření mají vést k tomu, že povinné subjekty budou mít systematicky řešenu kybernetickou bezpečnost tak, aby kybernetické bezpečnostní incidenty buďto nevznikaly nebo aby jejich výskyt neznamenal bezpečnostní riziko. Nástroje, s nimiž bezpečnostní opatření počítají lze z pohledu platného práva rozdělit do následujících základních skupin:

- Technické prvky (specifický software a hardware vč. detekčních systémů, reportovacích nástrojů, autentizačních či kryptografických nástrojů, technika k zajištění fyzické bezpečnosti apod.)
- Analytické prvky a dokumentace (typicky analýza informačních aktiv, topografie sítí, analýza rizik apod.)
- Interní předpisy (organizační opatření, školící plány, krizové plány, interní instrukce pro vybrané skupiny zaměstnanců, interní pravidla pro nákup a outsourcing ICT apod.)
- Lidské zdroje (specificky vyčleněný personál k zajištění realizace bezpečnostních opatření nebo personál zajišťující výjimečně ad hoc určité činnosti v oblasti kybernetické bezpečnosti)

Poslední dvě uvedené kategorie týkají se vztahu povinného subjektu a jeho pracovníků, ať už jde o zaměstnance nebo obdobně působící externisty. Běžné fungování specificky vyčleněného personálu nebo pracovníků, jimž mohou být úkoly v oblasti kybernetické bezpečnosti ukládány ad hoc, jsou pro existenci a efektivitu bezpečnostních opatření kriticky důležité. Sebelépe postavený a vybavený bezpečnostní systém totiž není k ničemu, pokud není adekvátně obsluhován resp. pokud jeho fungování brání faktická bezpečnostní rizika představovaná vlastními pracovníky povinných subjektů.

Z právního hlediska jde především o otázku povinností, které pracovníkům povinných subjektů ukládá zákon resp. povinností, které na základě zákona svým pracovníkům ukládají povinné subjekty formou interních instrukcí nebo běžné řídící činnosti v rámci korporátní hierarchie[42]. V tomto směru je předně nutno rozlišovat mezi pracovníky, jejichž pracovní náplň souvisí s tvorbou nebo realizací bezpečnostních opatření a pracovníky, jimž jsou pouze na základě bezpečnostních opatření ukládány konkrétní povinnosti s tím, že jejich běžná pracovní náplň s kybernetickou bezpečností jinak nesouvisí.

Bezpečnostní personál nebo pracovníky, u nichž alespoň část běžné pracovní agendy představuje kybernetická bezpečnost lze logicky zatížit nejen větším množstvím pracovních povinností oblasti kybernetické bezpečnosti, ale lze od nich požadovat i vyšší míru odborné erudice a schopnosti plnit specifické požadavky interních bezpečnostních předpisů. Bezpečnostnímu technikovi, správci sítě nebo systémovému administrátorovi tak lze nejen uložit řadu specifických pracovních povinností, jejichž předmětem může být zabezpečení příslušné informační a komunikační infrastruktury, ale tyto povinnosti lze na úrovni interních předpisů nebo individuálních řídících aktů (tj. v rámci běžného podnikového řízení) formulovat i s vysokou mírou odbornosti a spoléhat přitom na adekvátní předvědění příslušných adresátů.

U profesí, jejichž pracovní náplň netvoří kybernetická bezpečnost, je naproti tomu v případě definice povinností týkajících se bezpečnosti informačních systémů a sítí nutno postupovat tak, aby interní instrukce nebo jiné akty řízení byly obecně srozumitelné a aby byly z pohledu běžného pracovníka technicky proveditelné. Z toho plyne, že například instrukce typu „uživatel je povinen měnit své přístupové heslo minimálně jednou týdně, heslo musí mít min. 15 znaků, z nichž min. 7 znaků musí být speciální znaky ASCII“ je vadná hned ze dvou důvodů. Jednak není možno rozumně požadovat po běžném uživateli, aby si každý týden zapamatoval nové patnáctiznakové heslo a navíc nelze předpokládat, že bude poučen v tom smyslu, co to jsou speciální znaky ASCII. Takto formulovaná interní instrukce tedy, byť její přečtení příslušný zaměstnanec potvrdí třeba podpisem vlastní krví, nikdy nepovede k právně vynutitelnému závazku.

Z právě uvedeného plyne, že problém disciplinární odpovědnosti zaměstnanců vzhledem k bezpečnostním opatřením zaváděným u povinných subjektů mandatorně na základě zákona o kybernetické bezpečnosti spočívá primárně ve způsobu, kterým budou různým kategoriím pracovníků ukládány příslušné bezpečnostní povinnosti. Neexistuje přitom žádná konkrétní judikatura, o kterou by bylo možno se opřít, to i přes skutečnost, že typově podobná situace jako v případě kybernetické bezpečnosti objevuje se dlouhodobě například v oblasti protipožární ochrany nebo bezpečnosti práce. Případy, jejichž autoritativní řešení máme k dispozici jako vodítko, týkají se spíše frapantních porušení interních předpisů nebo jiných řídících aktů a neposkytují tím pádem adekvátní návod pro diskutabilní či hraniční případy. Ještě žádného zaměstnavatele tak doposud nenapadlo například žalovat o náhradu škody zaměstnance, který, byť byl proškolen v použití hasicího přístroje, vzal raději před požárem v odpadkovém koši nohy na ramena.

Problematika závaznosti respektive míry závaznosti interních instrukcí na úseku kybernetické bezpečnosti každopádně představuje zajímavé a vysoce žádoucí zadání, jehož řešením se česká právní

[42] Rozdíl mezi interní instrukcí a aktem řízení spočívá v tom, že zatímco interní instrukce je určena neurčitému okruhu pracovníků splňujících určitou podmínku (např. pracovníkům v určité funkci), je akt řízení adresován, tj. určen konkrétnímu člověku. K povaze interní instrukce viz např. Galvas, M. a kol. Pracovní právo. Brno: Masarykova univerzita, 2012, str. 50 nebo Vysokajová, M. Zákoník práce - komentář. Praha : Wolters Kluwer, 2012, str. 623.

věda již intenzivně zabývá[43] – přestože by ale měly být základní doktrinální poznatky k těmto otázkám k dispozici v řádu měsíců či jednotek let, budou povinné subjekty vystaveny právní nejistotě až do doby, kdy bude k dispozici adekvátní judikatura vyšších soudů.

Na tomto místě je nutno připomenout, že právě uvedené se týká pouze specifických bezpečnostních povinností, jejichž existence je podmíněna zvláštní autoritativní informací prokazatelně sdělenou zaměstnanci. Zaměstnavatel však samozřejmě nemusí zaměstnanci formou interních instrukcí nebo jiných řídících aktů sdělovat všechny možné požadavky na bezpečné fungování informačních systémů a sítí. Každé pracovní pozici totiž odpovídá implicitně předpokládaná odborná výbava zaměstnance, s níž zaměstnavatel může počítat a kterou nemusí ani zvlášť ověřovat. Pracovní pozice, u níž se předpokládá znalost práce s osobním počítačem, tedy implicitně předpokládá, že bude zaměstnanec bez dalšího chápat například zákaz psaní přístupových hesel na žluté lístečky a jejich lepení na okraj monitoru (podobně není nutno kancelářské síly školit například v tom, že nemají strkat kancelářské sponky do elektrických zásuvek nebo v pracovní době skákat z oken). Analogicky pak bude zřejmě možno ze strany zaměstnavatele i bez nutnosti přijímat interní instrukce předpokládat, že systémový administrátor je obeznámen se skutečností, že nesmí používat triviální heslo nebo že se má při každém odchodu od počítače odhlásit ze své virtuální identity. Ani v těchto otázkách však nemáme k dispozici žádnou použitelnou judikaturu a vyjma evidentních případů lze spíše předpokládat, že soudy nebudou příliš respektovat presumpci nedbalostního zavinění a budou spíše v případě sporu požadovat po zaměstnavateli důkaz skutečnosti, že zaměstnanec příslušné bezpečnostní pravidlo znát mohl a hlavně, že jej vzhledem ke svému pracovnímu zařazení znát měl[44].

[43] Viz např. aktuálně řešený projekt GAMU MUNI/M/1052/2013, Experimentální výzkum chování uživatelů ICT v oblasti bezpečnosti perspektivou sociálních věd, práva a informatiky.

[44] K tomu ještě přistupuje podstatný rozdíl mezi interní instrukcí a právním předpisem nebo vrchnostenským aktem spočívající v tom, že interní instrukce se nemůže spoléhat na presumpci správnosti resp. presumpci platnosti – srov. Bělina, M. a kol. Pracovní právo. 5. dopl. a podstat. přeprac. vyd., Praha : C.H.Beck,
2012, str. 66.

## *Perspektivy dalšího vývoje práva kybernetické bezpečnosti*

Shora provedená analýza má, jak bylo na několika místech zvlášť zdůrazněno, pouze doktrinální charakter a bez specifické judikatury nelze konstatovat konkrétní tvar jednotlivých institutů aktuálně tvořících českého právo kybernetické bezpečnosti. I v případě právních nástrojů, které již máme v našem právu k dispozici, totiž není jasno v tom, jaké formy může mít jejich aktuální aplikace. Diskutovat za této situace možnosti dalšího vývoje našeho práva kybernetické bezpečnosti je tedy podobno věštění z kávové sedliny.

Následující výklad je zaměřen především na možnosti dalšího vývoje české legislativy, přičemž vychází kromě shora diskutovaného současného stavu též z tendencí patrných v zahraničních právních řádech. České právo má v této souvislosti určitou výhodu spočívající v tom, že máme přístup k dobrým i špatným zkušenostem s různými typy legislativních nástrojů ze států, pro které kybernetická bezpečnost představovala a představuje v porovnání s naší situací daleko naléhavější problém. Můžeme se tedy díky spojeneckým svazkům a tradičním přátelským vazbám poučit ze zkušeností realizovaných v podobném právním prostředí, tj. v situaci standardního demokratického právního státu, ve státech, které kvůli své velikosti nebo zahraničněpolitické aktivitě staly se terčem závažných kybernetických útoků dříve a ve větší míře, než je tomu u nás.

Skutečnost, že v případě USA, Spojeného království nebo například Izraele jde o země fungující na jiných právně-kulturních základech, v tomto případě nebrání vzájemnému srovnání a využití příslušných zkušeností a dalších právních poznatků. Technika fungování právních mechanismů příslušné právní kultury totiž vzhledem k nastavení právních nástrojů pro zajištění národní kybernetické bezpečnosti totiž není nikterak podstatná - hlavní roli při posuzování použitelnosti určitého přístupu, nástroje nebo institutu hraje zde spíše příbuznost hodnotových základů příslušných právních kultur, jimiž jsou v případě českém i v případě právě jmenovaných zemí shodně priorita práv člověka a základní principy demokratického právního státu.

Příkladem takové zkušenosti, která nám ušetřila čas a nemalé zdroje finanční, personální i politické, je původní záměr severoamerické vlády koncipovat národní úpravu kybernetické bezpečnosti na bázi identifikace útočníka[45]. Jedná se o jeden ze dvou způsobů, jak strategicky nastavit právní instituty chránící veřejný zájem na fungování kritické informační a komunikační infrastruktury, který však je vysoce problematický vzhledem k proporcionalitě práv uživatelů služeb informační společnosti (v USA není sice zakotveno právo na ochranu osobních údajů a ochrana soukromí má poněkud jiný charakter než v Evropě, ale právo na anonymní vystupování v prostředí informačních sítí je i tak extrémně silné díky prvnímu dodatku americké ústavy). Politická neprůchodnost tohoto přístupu posloužila nám za vodítko při stanovení základní strategie české resp. evropské právní úpravy kybernetické bezpečnosti, která je namísto zmíněného modelu postavena na strategické prioritě ochrany prostředí[46] s tím, že identifikace a postih útočníka je ponechán na režimu běžného fungování trestního práva resp. na standardní působnosti orgánů činných v trestním řízení.

[45] Srov. Sales, S. A. Regulating Cyber-Security, Northwestern University Law Review, roč. 107, číslo 4, str. 1503.
[46] K tomu viz např. věcný záměr zákona o kybernetické bezpečnosti nebo průvodní dokumentaci k návrhu směrnice o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informací v Unii, COM/2013/048 final - 2013/0027 (COD).

## Zákonná typologie uživatelů vybraných systémů a sítí

Z právě uvedeného plyne, že individuální odpovědnost koncového uživatele, ať je jím útočník nebo i jen subjekt, jehož systém se z nějakého důvodu podílí na kybernetickém bezpečnostním incidentu, představuje politicky velmi citlivou otázku. Předpokladem uplatnění individuální odpovědnosti uživatele, ať už má jít o odpovědnost soukromoprávní nebo trestní, je totiž jeho ztotožnění. To přitom vyžaduje použití takových mechanismů, které mohou obecně ohrozit shora zmíněnou anonymitu (jako nutnou komponentu práva na svobodu projevu) a mohou být především kontradiktorní s kategorickými požadavky výjimečně rigorózně nastavené evropské ochrany soukromí a osobních údajů.

Právě ochrana soukromí, osobních údajů, svobody projevu či obecně vzato práva na informační sebeurčení jsou důvodem toho, že se zřejmě v dohledné době nesetkáme s ničím takovým, jako „internetový řidičský průkaz." Na druhé straně však je možno uvažovat o proporcionální ochraně vitálních zájmů na fungování kritických součástí informační a komunikační infrastruktury prostřednictvím specifické individuální odpovědnosti lidí, kteří na profesionální bázi s kriticky důležitými informačními systémy nebo sítěmi pracují.

Jednou z možností legislativního řešení je maďarský model definice stupňů bezpečnostní důležitosti informačních systémů a sítí a založení práva pracovat s těmito systémy pouze uživatelům s určitým stupněm znalostní certifikace[47]. Nemusí přitom jít pouze o povinnost pro správce příslušného systému nebo sítě spočívající v nutnosti proškolit své zaměstnance používající příslušné systémy nebo sítě respektive najmout si pro jejich obsluhu odborně náležitě vybavený personál. Zprostředkovaně může jít též o vytvoření specifických povinností na straně samotného uživatele založených předpisy na úseku kybernetické bezpečnosti, zakládajících správní odpovědnost za přestupky nebo jiné správní delikty spočívající v neodborném přístupu ke kriticky důležitým systémům nebo sítím a odstupňované adekvátně k bezpečnostní klasifikaci těchto systémů nebo sítí.

Je docela pravděpodobné, že potřebu takové úpravy pocítí v první řadě především správci kritické informační a komunikační infrastruktury poté, co konstatují nutnost až příliš sofistikované tvorby interních instrukcí tak, aby bylo v případě problému na straně uživatele nebo operátora kriticky důležitého systému nebo sítě možno regresně vyvodit alespoň disciplinární odpovědnost na základě institutů diskutovaných v předchozí kapitole. Problémem interních instrukcí totiž je, jak bylo výše zdůrazněno, že jejich závaznost či praktická vynutitelnost není jen otázkou jejich bezrospornosti se zákonem, ale též jejich srozumitelnosti a formy komunikace. Byť to může znít poněkud problematicky, je proto pro zaměstnavatele nepoměrně jednodušší, pokud se může spolehnout na zákonnou nebo podzákonnou definici konkrétních bezpečnostních povinností svých zaměstnanců, než pokud by takovou definici měl sám vytvářet a implementovat. Individuální správní odpovědnost je navíc sama o sobě silným motivačním faktorem, který může pro příslušné zaměstnance představovat ještě pádnější důvod k obeznámení se s bezpečnostními pravidly a k jejich dodržování, než je tomu v případě disciplinární odpovědnosti nebo omezené odpovědnosti za škodu způsobenou zaměstnavateli.

[47] Srov. maďarský zákon o elektronické informační bezpečnosti ústředních a místních správních orgánů ze dne 15. dubna 2013 – ke stažení v anglické verzi on-line na adrese http://www.nbf.hu/anyagok/Act%20L%20of%202013%20on%20the%20Electronic%20Information%20Security%20of%20Central%20and%20Local%20Government%20Agencies.docx.

Ve vazbě k výše uvedenému je možno uvažovat též o zákonem založené povinnosti pro správce vybraných typů vysoce bezpečnostně exponovaných informačních systémů a sítí vyčlenit resp. zaměstnat pracovníka přímo odpovědného za plnění požadavků zákona o kybernetické bezpečnosti. Podobně, jako je tomu v agendě ochrany utajovaných informací[48] nebo v některých členských státech v agendě ochrany osobních údajů[49], mohl by tento zaměstnanec mít v organizační struktuře příslušného správce ze zákona dané specifické postavení a jeho disciplinární odpovědnost by mohla být rozdělena mezi zaměstnavatele a národního regulátora (tj. v našem případě zřejmě Národní bezpečnostní úřad).

### Omezená odpovědnost běžných uživatelů

Nejen z politických důvodů je zřejmě nereálné předpokládat, že by právní úprava kybernetické bezpečnosti v dohledné době specificky založila objektivní odpovědnost koncových uživatelů nebo zavedla nějaký zvláštní mechanismus jejich identifikace. Přes všechny více či méně argumentované požadavky na to, aby uživatelé odpovídali za bezpečné fungování svých systémů bez ohledu na své zavinění, je totiž třeba v první řadě zohlednit skutečnost, že i relativně jednoduché technologie určené k běžnému použití v domácnostech (typicky např. mobilní telefony, domácí wifi routery apod.) jsou z podstaty extrémně technicky složité. Běžný uživatel tedy nejenže nechápe (resp. nemusí chápat) ani základní principy jejich fungování, ale nelze po něm požadovat ani to, aby se zvlášť věnoval jejich zabezpečení proti možnému zneužití. Jestliže tedy prostý spotřebitel např. neprovede instalaci bezpečnostní záplaty a v důsledku toho je jeho systém zneužit k útoku typu DDoS, není v dohledné době možno uvažovat o tom, že by za takový útok měl nést spoluodpovědnost.

Z hlediska proporcionality dotčených práv nesrovnatelně schůdnějším řešením by byla regulace spotřebitelské dostupnosti informačních a komunikačních technologií v závislosti na míře jejich bezpečnosti. Lze tedy uvažovat o tom, že budou pro určité typy informačních a komunikačních technologií zavedeny mandatorní požadavky na jejich kvalitu, které zahrnou i nutnou jejich bezpečnostní výbavu. Podobně, jako je tomu pravidlem v síťových odvětvích, tj. např. v energetice, telekomunikacích nebo v dopravě, může i v oblasti kybernetické bezpečnosti vzniknout katalog požadavků na shodu, který zahrne nejnutnější bezpečnostní prvky a bez jejichž dodržení nebude možno příslušnou technologii spotřebitelsky šířit na tuzemském trhu. I v tomto případě by šlo zprostředkovaně o zatížení koncového uživatele – nikoli sice přímými povinnostmi či odpovědností, ale nutností zaplatit příslušné zabezpečení včetně jeho administrativních externalit v konečné ceně produktu nebo služby. Takové řešení je však stále z hlediska ochrany práv nesrovnatelně schůdnější, než shora diskutovaná objektivní odpovědnost.

Velmi zajímavou možnost řešení individuální odpovědnosti uživatele přinesl doposud výjimečný případ, který řešily americké soudy. Šlo v něm, stručně řečeno, o infekci využívající bezpečnostní díru v systémech společnosti Microsoft, která umožňovala skryté využití napadených systémů jako součástí botnetu pro útoky typu DDoS. Spol. Microsoft se v tomto případě odhodlala k právně originálnímu

[48] Srov. § 71 zákona č. 412/2005 Sb.

[49] Povinnost zřídit u větších subjektů tuto funkci se plánuje k celoevropskému zavedení v připravované nové úpravě evropské ochrany osobních údajů – k tomu viz dokumentaci k návrhu nařízení o ochraně fyzických osob v souvislosti se zpracováváním osobních údajů a o volném pohybu těchto údajů (obecné nařízení o ochraně údajů) - COM(2012) 11 final, 2012/0011 (COD).

řešení, když zažalovala organizátory botnetu a v návrhu rozhodnutí též de facto navrhla postihnout i uživatele, kteří své systémy nezabezpečili bezpečnostní záplatou[50].

Pro právní řády z právní kultury common law je totiž typické, že umožňují uplatnit civilní postih i proti osobám, které sice nejsou určeny jménem a adresou, ale jejichž specifikace je dostatečně přesná na to, aby bylo možno podle příslušného znaku konkrétní subjekt v důsledku identifikovat. Žalovaný tedy v tomto případě může být určen konkrétním znakem bez toho, aby žalobce znal jeho přesnou identitu. V důsledku to pak znamená, že žalovaný ani nemusí vědět o tom, že je žalován (přestože je mu doručováno za známý e-mail).

Plán založit nepřímou odpovědnost koncových uživatelů jeví se být sice ve světle shora uvedených argumentů jako prostá marnost. V tomto případě se však spol. Microsoft podařilo velmi inovativním způsobem vyřešit rovnováhu mezi deliktem a jeho odpovědnostním důsledkem. Žalobní petit totiž nezněl na náhradu škody nebo jiné plnění, ale „pouze" na povinnost uživatele strpět dálkový zásah do svého systému, kterým Microsoft přesměruje za účelem vyšetření celého incidentu případný útok na své vlastní servery. Tento nárok byl díky tomu shledán proporcionálním k deliktu a následně přiznán. Microsoft tedy mohl nepozorovaně zasáhnout do infikovaných systémů a díky přesměrování jejich komunikace nejen zabránit škodám, které by botnet mohl způsobit, ale též získat cenná data k vyšetření celého incidentu.

Tento případ není pro českou právní praxi inspirativní do té míry, že by bylo snad možno uvažovat o podobném řešení v našich podmínkách. Naše procesní právo totiž nedovoluje žalovat na základě identifikačního znaku, nelze-li podle něj přímo v řízení ztotožnit konkrétní subjekt. I pro naše právní prostředí je však zajímavá úvaha soudu ohledně toho, že i běžný uživatel má určitou míru povinnosti vědět o potřebě zabezpečení svého vlastního systému a že tuto povinnost lze uvést do souvislosti s adekvátním typem odpovědnostního následku, tj. nikoli např. hradit škodu ale „pouze" strpět dálkový zásah do svého systému.

Prostředkem, který by bylo možno využít namísto shora popsaného řešení, mohlo by se stát opatření obecné povahy. To totiž umožnuje identifikovat své adresáty na základě obecných znaků a uložit jim určitou povinnost. Je pak možno svěřit konkrétnímu úřadu (v našem případě by zřejmě šlo o Národní bezpečnostní úřad nebo Český telekomunikační úřad) kompetenci vydávat za přesně stanovených okolností tato opatření a ukládat jimi i běžným (nic netušícím) uživatelům podobné povinnosti strpět zásah do jejich systémů, jako se stalo ve shora zmíněném případě.

### Specifická úprava outsourcingu

Jádrem aktuální zákonné úpravy i podzákonných prováděcích předpisů v oblasti kybernetické bezpečnosti jsou bezpečnostní opatření. Požadavky na standard zabezpečení informační a komunikační infrastruktury spravované povinnými subjekty jsou zákonem stanoveny velmi obecně a prováděcí předpisy pak provádějí jen takovou míru jejich konkretizace, která nezasahuje do principu technologické neutrality a umožňuje povinným subjektům velkou míru autonomie při volbě konkrétních řešení. Tento model jeví se jako vhodný hned ze dvou důvodů – předně je povinný subjekt tím nejvíce povolaným, pokud jde o detailní technické znalosti příslušného informačního systému nebo sítě a má tedy nejlepší možnost posoudit, jaká konkrétní bezpečnostní řešení nejlépe

[50] Viz rozhodnutí ve věci 3:13-CV-00319-GCM okresního soudu pro Western District of Notrh Carolina, Charlotte Division, ke stažení on-line na adrese http://botnetlegalnotice.com/citadel/files/Order_Granting_Def_Jdgmt_PI.pdf.

splní zákonné požadavky. Vedle toho je velmi pravděpodobné, že relativní otevřenost standardních požadavků povede společně s jistotou investic k motivaci dodavatelů různých bezpečnostních řešení k investicím do vývoje. To může přinést vítaný impuls k dalším inovacím v oboru ICT bezpečnosti.

Relativně velká míra autonomie u povinných subjektů ohledně způsobu plnění zákonných požadavků však na druhé straně vyvolává i nejistotu ohledně řešení typických případů, kdy správce nerealizuje jednotlivá bezpečnostní opatření sám nebo alespoň ve vlastní režii, ale provádí jejich komplexní outsourcing. Především u středně velkých a menších povinných subjektů lze kromě vzájemné koordinace jejich aktivit při akvizicích bezpečnostních řešení očekávat i společné postupy při komplexním řešení bezpečnostních opatření včetně jejich fungování v reálném čase. Lze si tedy například představit, že místní utility typu vodáren nebo tepláren vytvoří společný podnik, který bude jim bude společně zajišťovat realizaci a fungování bezpečnostních opatření např. i včetně provozu lokálního CERT, reportování incidentů, spolupráce s Národním bezpečnostním úřadem apod.

Zákon a podzákonné předpisy sice možnost outsourcingu bezpečnostních opatření nevylučují a v konkrétních částech s ní přímo počítají – pravidla pro externí dodavatele bezpečnostních řešení však se omezují pouze na obecné povinnosti mít dokumentovány a kontrolovány vztahy s externími dodavateli. Vzhledem k tomu, že zákon o kybernetické bezpečnosti stojí na výlučné odpovědnosti správce příslušného informačního systému nebo sítě, není v jeho současné struktuře obsažena speciální úprava postavení dodavatele nebo provozovatele bezpečnostních opatření. Je tedy plně na správci, jak si vztahy s externími subjekty vyřeší a jak bude ve vztahu k nim zajišťovat například plnění povinností vyplývajících z kontrolních pravomocí Národního bezpečnostního úřadu nebo regresní nároky v případě deliktní odpovědnosti.

Zatímco volnost ve smyslu konkrétní formy bezpečnostních opatření jeví se jako vhodná a není důvod předpokládat v brzké budoucnosti nějaké zásadní změny, je otázku totální volnosti povinných subjektů ohledně outsourcingu bezpečnostních opatření možno považovat za místo, kde bude zákonná úprava průběžně doplňována na základě praktických zkušeností. Nejde pouze o možnost založení přímých pravomocí Národního bezpečnostního úřadu vůči subjektům poskytujícím bezpečnostní řešení jako službu, ale například i o možnost správní regulace činnosti takových subjektů (nabízí se například varianta speciální vázané živnosti). Především ve vztahu k informačním systémům veřejného sektoru spadajících pod rozsah zákona o kybernetické bezpečnosti (tj. k informačním systémům veřejné správy a dalším informační systémům provozovaným veřejnoprávními korporacemi, které budou spadat pod rozsah kritické informační infrastruktury nebo významných systémů) lze očekávat podrobnější úpravu požadavků na outsourcing, která by měla odstranit standardní bezpečnostní nešvary vyskytující se v procesech zadávání veřejných zakázek na ICT.

Vedle konkrétnější úpravy zákonných a podzákonných parametrů outsourcingu bezpečnostních opatření lze očekávat i nepoměrně rychlejší vývoj smluvních nástrojů a alternativních forem řešení obchodních sporů, a to především u soukromoprávních povinných subjektů. Dokonce ještě před platností (nikoli až účinností) zákona o kybernetické bezpečnosti byly některé velké korporace včetně energetických společností nuceny zahrnovat do outsourcingových smluv klauzule zakládající pro dodavatele resp. poskytovatele služby specifické povinnosti v návaznosti na zákonné požadavky. Konstrukce těchto klauzulí, kontrola příslušných plnění v reálném čase (může totiž jít o mnohaleté smlouvy) nebo mechanismy řešení vzájemných sporů představují oblast smluvního ICT práva, která sice u nás není úplně zanedbána, bude však zřejmě ještě procházet velkým rozvojem. Namísto legislativní asistence však je v tomto směru spíše nutno očekávat, že si budou muset soukromoprávní povinné subjekty, zjednodušeně řečeno, pomoci samy – přispět ke zdárnému vývoji smluvních nástrojů, procedur výběru dodavatelů nebo procedur řešení dodavatelských sporů mohou kromě

organizací typu Hospodářské komory především oborové asociace. Kvalitně fungující vztahy s dodavateli bezpečnostních opatření totiž nepředstavují otázku vzájemné konkurence mezi subjekty působícími na týchž trzích a přímo se tak nabízí vzájemná bezkonfliktní spolupráce a koncentrace zdrojů k zajištění efektivně fungujících právních řešení.

### *Další vývojové perspektivy práva kybernetické bezpečnosti*

K právě uvedenému lze spekulativně připojit i další oblasti, jejichž vývoj jsme předpověděli ve studii věnované principům a perspektivám kybernetické bezpečnosti ČR. Na první místě se bude zřejmě jednat o postupnou národní i mezinárodní konkretizaci pojmu informační suverenity státu, jakož i o právní kvalifikaci různých typů jednání souhrnně označovaných jako aktivní obrana před kybernetickými bezpečnostními incidenty. Primárním těžištěm obou problémů bude zřejmě mezinárodní právo veřejné a výstupy můžeme očekávat především z jeho doktríny. Přestože ideálním řešením by v tomto směru byla mezinárodní úmluva, nedá se vzhledem ke zcela rozdílným pohledům na věc a zcela odlišným zájmům jednotlivých národních vlád očekávat, že by k přípravě takové úmluvy mohlo v dohledné době dojít. Příliš pravděpodobný není ani vznik judikatury Mezinárodního soudního dvora, neboť státy, které by toho byly schopny, nemají, stručně řečeno, k přednesení aktuálně se vyskytujících konfliktních situací tomuto fóru prakticky žádnou motivaci. Namísto toho je spíše důvod očekávat další rozvoj vzájemné spolupráce na základě existujících obecných spojeneckých svazků, z nich nejvýznamnější a doposud nejproduktivnější je spolupráce v rámci NATO[51].

Nesrovnatelně jednodušší situace je co do základních hodnot a zájmů v rámci Evropské unie. Díky tomu lze v brzké době očekávat finalizaci směrnice o kybernetické bezpečnosti (resp. směrnice o síťové a informační bezpečnosti) a další rozvoj stávajících evropských bezpečnostních struktur, zejm. ENISA a CERT-EU. Poslední vývoj návrhu cit. směrnice směruje sice spíše k obecnějšímu rozsahu a nižšímu standardu povinností členských států – podobně jako v případě českého zákona o kybernetické bezpečnosti je však i v tomto případě zřejmě vhodné přistoupit k fixaci určitého právně bezproblémového a politicky akceptovatelného řešení a to pak dále rozvíjet institucionální a legislativní aktivitou na základě praktických zkušeností.

V českém právním prostředí můžeme nad rámec toho, co bylo diskutováno v předchozích podkapitolách, očekávat především konkretizaci spolupráce vládního a národního CERT, jakož i konkretizaci spolupráce Národního bezpečnostního úřadu s ostatními orgány veřejné moci, do jejichž zájmu spadá oblast národní kybernetické bezpečnosti (vedle bezpečnostních služeb jde především o Policii ČR, Armádu ČR a ústřední orgány státní správy mající jurisdikci nad kritickými či významnými informačními systémy a sítěmi)[52]. Podobně lze očekávat též rozvoj spolupráce mezi Národním bezpečnostním úřadem a soukromoprávními korporacemi, profesními sdruženími a akademickou sférou – ta může mít charakter neformálních aktivit, memorand, činnosti expertních skupin apod. a může řešit problémy, které z nějakého důvodu není možno nebo vhodno pokrýt veřejnoprávními aktivitami (typicky např. otázky certifikace, vzdělávání, podpory inovací apod.)

[51] Z doktrinálního hlediska nejvýznamnější výstupem této spolupráce je činnost centra excelence CCD CoE v estonském Talinu, jejíž manuál se stal všeobecně uznávaným standardem doktríny mezinárodního práva veřejného pro kybernetickou bezpečnost. Manuál je on-line ke stažení ze http://issuu.com/nato_ccd_coe/docs/tallinnmanual.

[52] Národní bezpečnostní úřad již v tomto směru publikoval několik podpůrných dokumentů jako např. blokové schéma zákona o kybernetické bezpečnosti nebo pomůcky k určení prvku kritické informační infrastruktury a významných systémů – dokumenty jsou ke stažení on-line na adresách: www.govcert.cz.

Jako nanejvýš vhodná jeví se v tomto směru být tendence zahrnovat kybernetickou bezpečnost mezi aktuální politické priority – to umožní podporovat shora uvedené činnosti v rámci standardních forem spolupráce mezi soukromým, akademickým a veřejným sektorem typu podpory vědeckých nebo rozvojových projektů, exportu, investic, rozvoje občanské společnosti aj.

# Celkové shrnutí kapitol

Svým zaměřením na legislativní kontext problematiky energetické a kybernetické bezpečnosti čtvrtá etapa efektivně uzavřela mapování dané oblasti v rámci ČR. Kromě identifikace klíčových norem se nevyhnutelně dotkla také institucionální dimenze řešení české a potažmo i evropské bezpečnosti v oblasti ochrany kritické infrastruktury. V tomto kontextu se jako klíčové jeví strategicky promýšlet vztahy mezi jednotlivými institucemi státní správy, které se více či méně danou problematikou zabývají, ale také vztahy se soukromoprávními aktéry, kteří v mnoha ohledech do zajišťování fungování a ochrany kritické infrastruktury zasahují. Z této perspektivy analýza legislativních aspektů odhalila zásadní téma, které reflektuje relevanci TPEB jako public-private-partnership projektu.

Klíčovou rolí PPP platformy tak nemá být pouze stimulace výzkumných, vývojových a inovačních projektů, ale také snaha o zefektivnění komunikace mezi soukromými a veřejnými institucemi. Tato skutečnost navíc vyplynula také z několika veřejných akcí, které byly v kontextu projektu či mimo něj uspořádány. Zmíněná spolupráce má formální rozměr definovaný platnými právními úpravami, ale také neformální rozměr, který může odpovídat různým formátům expertních setkání.

Výše zmíněné téma by mělo doplnit veřejné a strategické diskuze týkající se efektivnější přípravy na výzvy ohrožující kritickou (informační) infrastrukturu. Zajištění bezpečnosti a odolnosti společnosti není pouze věcí technologické vyspělosti a nastavení krizových procesů, ale závislé také na schopnosti administrativy a v neposlední řadě i politické sféry alespoň absorbovat částečně rozeznat potenciální rozsah problémů a možnosti jejich řešení.

# Další aktivity a výstupy IV. etapy

## Projekt Resilience 2015: Dynamické hodnocení odolnosti souvztažných subsystémů kritické infrastruktury

Předmětem projektu je pokročilý výzkum kritické infrastruktury se zaměřením na dynamické hodnocení souvztažnosti evropsky významných sektorů (energetiky, dopravy a informačních a komunikačních technologií) a jejich prvků, popis synergického efektu selhání těchto prvků a sektorů a jeho vlivu na predikování dopadů a stanovení dynamického hodnocení odolnosti kritické infrastruktury. Praktická část projektu je zaměřena na tvorbu systému určování prvků pozemní dopravní kritické infrastruktury, klíčových prvků kritické infrastruktury odvětví elektroenergetiky a klíčových prvků kritické informační infrastruktury.

Základním způsobem komplexního zkoumání vazeb a dopadů v rámci kritické infrastruktury je systémový přístup tzn., že k dané problematice je nutné přistupovat jako k systému systémů, tedy k systému s vysokou mírou komplexity. To znamená, že kritická infrastruktura jako komplexní systém tvořený základními subsystémy (tj. sektory, odvětvími a prvky), které mají mezi sebou specifické typy vazeb od jednoduchých (vliv a závislost) až po složité (vzájemná závislost).

Počáteční výzkum dopadů kritické infrastruktury byl v Evropě veden formou tzv. sektorového přístupu, který nahlíží na jednotlivé sektory kritické infrastruktury jako na samostatné celky. Tento způsob výzkumu jednotlivých subsystémů je realizován hloubkově a ohraničeně bez respektování mezisektorových vazeb ovlivňujících chování celého systému. Postupem času byly zjištěny značně limitované možnosti tohoto přístupu, a proto od roku 2013 začíná Evropská unie po vzoru USA a Kanady prosazovat tzv. systémový přístup spočívající v mezisektorovém hodnocení založeném na zkoumání vzájemných vazeb jednotlivých sektorů kritické infrastruktury. Na základě toho je nutné konstatovat, že ambicí výzkumného záměru je tudíž systémový přístup. Zmiňované systémové řešení bude v rámci realizace projektu aplikováno progresivním přístupem „bottom-up“, který je založen na hodnocení kritické infrastruktury od nejnižší úrovně (obec) směrem nahoru a v současné době je již realizován v některých vyspělých zemích (např. Švýcarsko či Nizozemsko).

Stanovení souvztažnosti vybraných sektorů kritické infrastruktury umožní identifkovat a stanovit faktory, které mají zásadní vliv na zajištění minimální dostupnosti funkcí v rámci specifikovaných subsystémů kritické infrastruktury. Na základě určení statických a dynamických atributů bude posléze možné analyzovat a modelovat vliv vzájemných závislostí (interdependencies) s cílem zvýšení dostupnosti a odolnosti dodávky vybraných funkcí. Tyto poznatky budou znalostním základem pro výzkum vlivu a dopadů synergického jevu a domino efektu na dynamické hodnocení souvztažnosti a odolnosti (resilience) kritické infrastruktury.

Na základě formulace znalostního základu synergického efektu a jeho vlivu na dynamické hodnocení souvztažnosti, dopadů a následně i odolnosti a dostupnosti vybraných funkcí bude z pohledu dynamického hodnocení definován koeficient souvztažnosti vyjadřující závislost (fyzickou, územní, informační, logickou a společenskou) a vazby mezi jednotlivými subsystémy kritické infrastruktury. Tato část řešení bude vycházet a rozšiřovat problematiku a proces statického hodnocení odolnosti kritické infrastruktury podle certifikované metodiky „Metodika hodnocení odolnosti vybraných prvků a systému prvků kritické infrastruktury“ (dále metodika). Pro tyto účely bude také využit i výstup projektu „Karta souvztažnosti vybraných subsystémů kritické infrastruktury“.

Vymezení atributů dynamického hodnocení úrovně synergického efektu bude také vnímáno i z pohledu dynamického hodnocení dalšího atributu metodiky, a to koeficientu rizikovosti vyjadřujícího pravděpodobnost dopadu hrozby na funkčnost kritické infrastruktury, což je možné vnímat i z perspektivy hodnocení zranitelnosti kritické infrastruktury. Pravděpodobnost dopadu hrozby je třeba pro účely dynamického modelování kvantifikovat. K tomu budou pro hrozby stanoveny vhodné ukazatele pravděpodobnosti jejich výskytu a následků. K těmto ukazatelům bude vztahován rozsah jejich možných hodnot a souvisejících nejistot.

V dalším průběhu řešení projektu budou stanoveny dynamické atributy pro hodnocení robustnosti, a to z pohledu strukturální robustnosti, vyjadřující schopnost kritické infrastruktury ustát působení negativních vlivů ve vztahu k jeho struktuře, systémovým a technologickým vlastnostem a z pohledu robustnosti zabezpečení, která vyjadřuje stav a úroveň bezpečnostních opatření zajišťujících efektivní minimalizaci působení rizik. Pro koeficient strukturální odolnosti budou popsány dynamické atributy ve vztahu k typu topologické struktury kritické infrastruktury, její složitosti, počtu klíčových technologií, flexibilitě, možnosti redundance a dalších ukazatelů. Koeficient robustnosti zabezpečení bude následně dynamicky hodnocen z pohledu vybraných aspektů bezpečnosti a zabezpečení, a to i v kontextu měnících se vah (významnosti) těchto aspektů. Dalším významným aspektem výzkumu dynamického hodnocení odolnosti souvztažných subsystému kritické infrastruktury je koeficient připravenosti, který zohledňuje schopnost reakce, odezvy a obnovy funkce kritické infrastruktury.

Naplnění všech skutečností následně umožní dynamické hodnocení odolnosti kritické infrastruktury v rámci vymezeného území, jehož výstupem bude stanovení relevantních dopadů na společnost, jejich analýza a kvantifikace v čase. Dalším přínosem bude objektivní výběr preventivných opatření k minimalizaci dopadu hrozeb pro zvolené oblasti kritické infrastruktury, a to v oblasti bezpečnosti (safety), v oblasti zabezpečení (security) a oblasti připravenosti (preparedness).

Na základě dynamického hodnocení a modelování odolnosti kritické infrastruktury prostřednictvím vhodné informační podpory bude následně upraven postup určování a seznam prvků pozemní (silniční a železniční)dopravní kritické infrastruktury. Výhodou dynamického hodnocení odolnosti bude v této souvislosti v závislosti na čase i možná detekce těch negativních faktorů, které mají zásadní vliv na funkčnost kritické infrastruktury na

vymezeném území. Výstupy z projektu budou základem pro optimalizaci plánovacího procesu ve vztahu k postupům a opatřením při řešení vybraných krizových situací a tím i plány krizové připravenosti subjektů kritické infrastruktury. Současně bude projekt základem pro vytvoření a zavedení systémů, které umožní hodnotit v čase úroveň souvztažnosti a tím i integrální odolnosti. Tím se významně rozšíří a doplní aktuální stav poznání a možností statického hodnocení odolnosti ve prospěch dynamického hodnocení odolnosti kritické infrastruktury v čase.

TPEB se do projektu zapojí v rámci několika WP, přičemž klíčovým pro její projektovou aktivitu bude balíček zabývající se výzkumem a vývojem systému určování klíčových prvků kritické infrastruktury odvětví elektroenergetiky v kontextu jejích souvztažnosti, domino a synergickému efektu. Specificky do tohoto portfolio náleží:

- Výzkum vybraných atributů pro dynamické hodnocení odolnosti
- Výzkum významných vazeb na vybrané souvztažné subsystémy
- Výzkum systému predikce a včasného varování selhání dodávky funkce a realizaci bezpečnostních opatření z pohledu elektroenergetiky
- Návrh bezpečnostních opatření situačního a technického charakteru

## Compliance table

Projektový tým soustředící se na oblast kybernetické bezpečnosti se ve spojitosti s kybernetickým zákonem, který vstoupil v platnost 1.1.2015, zabýval možností vytvořit analytický compliance test, který by infrastrukturním společnostem umožnil zjistit, jsou-li jejich bezpečnostní opatření a mechanismy v souladu s požadavky nového zákona. Tento nástroj TPEB vyvíjí ve spolupráci s Národním bezpečnostním úřadem, který je gestorem kybernetického zákona.

## Konference Energy & Cyber Security in EU

Konferenci zahájil a přivítal přítomné účastníky Ing. Milan Urban, předseda správní rady TPEB ČR, místopředseda Hospodářského výboru PSP ČR a dále vystoupil JUDr. Richard Hlavatý, předseda výkonného výboru TPEB ČR.

Moderátorem zahraničního panelu konference byl pan Ing. Václav Klučka, poslanec a člen Výboru pro bezpečnost Poslanecké sněmovny Parlamentu ČR. Domácí panel moderoval Doc. JUDr. Radim Polčák, Ph.D. – vedoucí ústavu práva a technologií Právnické fakulty Masarykovy Univerzity Brno.

Konference se konala za účasti zahraničních a tuzemských odborníků. V prvním bloku přednášek, který byl věnován zahraničním hostům, Přednášel pan Dr. Alois Sieber – poradce EK pro bezpečnost; bývalý ředitel bezpečnostního výzkumu v DG Joint Research Centre ISPRA (SRN) Věda a výzkum v EU, realizace programů v členských státech EU, dále se formou conference call zúčastnila paní Maaike van Tuyll – Head of Unit for Analysis of Natural, Technological and Security Threats; Ministerstvo bezpečnosti a spravedlnosti Nizozemska ; Národní koordinátor pro bezpečnost a boj s terorismem(Nl.) Business as (un) usual – Resilience of Critical Infrastructure a pan Dr. Alessandro Lazari – ERNCIP ( DG JRC ISPRA ) Evropská referenční sít ochrany kritické infrastruktury (It.) Directiva 114 na ochranu kritické infrastruktury (KI). Významným hostem byl pan Severin Loffler – Director Legal & Corporate Affairs v regionu střední a východní Evropy, Microsoft Corporation Security for the data in the cloud (Bezpečnost pro data v cloudu).

Druhý blok programu byl věnován panelové diskuzi, ve které vystoupili přední tuzemští odborníci. Doc. JUDr. Radim Polčák, Ph.D. – vedoucí ústavu práva a technologií Právnické fakulty Masarykovy Univerzity Brno tématem jeho přednášky bylo : Zkušenost s komplexním právním a organizačním řešením kybernetické bezpečnosti na úrovni státu a EU. Dále vystoupil pan Ing. Zbyněk Boldiš, člen představenstva ČEPS a.s. , který přednesl přednášku na téma aktivity a zkušenosti ČEPS v oblasti ochrany KI spolu s videoprezentací. Dále vystoupil pan JUDr. Juraj Szabó, Ph.D. – ředitel útvaru právního a Corporate Compliance, ČEZ, a.s., jeho přednáška byla věnována tématu : Zkušenosti ČEZ s ochranou KI. Dalším významným přednášejícím byl na Ing. Jaroslav Šmíd – náměstek ředitele NBÚ, který se zabýval tématem : Stav implementace kybernetického zákona z pohledu NBU, novelizace vládního nařízení o kritické infrastruktuře. Následovalo vystoupení pana Kpt.Mgr.Lukáše Pidhaniuka – Ministerstvo vnitra Generální ředitelství HZS ČR, oddělení civilní nouzové připravenosti , které se zabývalo tématem Evropská politika ochrany kritické infrastruktury a její dopad na Českou republiku.

Na závěr vystoupil pan Ing. Jiří Polák – výkonný ředitel, Czech Association CIO (CACIO), s přednáškou na téma Strategický rozvoj energetického segmentu v ČR a EU

Konference se zúčastnili poslanci z výborů hospodářského, branného a bezpečnostního a zahraničního. Rovněž se jí zúčastnili zástupci ČEZ a.s, ČEPS a.s.; Pražské plynárenské a.s., Generálního ředitelství Záchranného hasičského sboru ČR; Ministerstva vnitra ČR, Ministerstva průmyslu a obchodu ČR, Úřadu pro normalizaci metrologii a zkušebnictví, Ministerstva obrany ČR, Úřadu pro obrannou standardizaci, katalogizaci a státní ověřování jakosti a řada dalších.

## Zvané účasti na domácích a zahraničních akcích

- Dne 22. 10. 2014 se konala konference Cyber Security 2014, kterou pořádalo vydavatelství IDG Czech Republic a.s. ve spolupráci se společností Microsoft CZ. Akce se konala v rámci Evropského měsíce kybernetické bezpečnosti. TPEB ČR se této konference zúčastnila jako odborný garant a JUDR. Richard Hlavatý zde přednesl

přednášku na téma **Ochrana kritické infrastruktury v oblasti energetiky**. Součástí této prezentace bylo seznámení s aktivitami TPEB ČR v rámci projektu Energetická a kybernetická bezpečnost ČR. Konference byla zaměřená na kybernetickou bezpečnost a byla určena IT profesionálům pracujícím ve firemním sektoru, státní správě nebo samosprávě, specialistům z oblasti finančnictví, průmyslu a všem, kteří chtějí získat rozšířenou představu o aktuálních bezpečnostních problémech a rizicích v IT spolu s možnostmi efektivní cesty ke snížení těchto rizik. V příloze naleznete prezentaci TPEB ČR a odkaz na program této zajímavé akce.

- Dne 16. září 2014 se konalo společné mezinárodní bezpečnostní cvičení DRILL 2014, které proběhlo v blízkosti státních hranic nedaleko Hory sv. Šebestiána. Na tomto cvičení spolupracovalo více než 200 profesionálů z České republiky a z Německé spolkové republiky. Společně se podíleli na náročné realizaci stavby náhradního přeshraničního elektrického vedení, které spojuje sítě společností ČEPS a 50Hertz. Cvičení DRILL 2014 simulovalo extrémní situaci, kdy může dojít k selhání některé technické části elektrické sítě, například k pádu stožáru. Dle scénáře způsobí extrémní kalamitní počasí sérii mimořádných situací v elektroenergetických přenosových soustavách v celé řadě zemí Evropy, včetně Česka a Německa. Dojde k výpadku vedení zvlášť vysokého napětí mezi transformovnami Hradec u Kadaně a Röhrsdorf. Zprovoznění mezinárodního propojení se v dané situaci rázem stává strategickou prioritou. Obě společnosti začnou okamžitě stavět náhradní přenosovou trasu pro přeshraniční vedení. Pokud stavbu komplikují další faktory jako požár v okolí nebo nepřístupné cesty, neobejdou se společnosti ČEPS a 50Hertz bez pomoci záchranných složek a armády obou zemí. Krizovou situaci, kterou scénář cvičení připravil, řešili desítky odborníků z energetických společností ČEPS a 50Hertz. JUDr. Richard Hlavatý se této mimořádné akce aktivně zúčastnil a v rámci své přednášky seznámil účastníky akce s **aktivitami TPEB ČR, včetně probíhajících aktivit projektu Energetická a kybernetická bezpečnost**.

- V návaznosti na konferenci Aegis, která se konala v Aténách dne 16. května 2014, Konsorcium Archimedes uspořádalo závěrečnou konferenci dne 4. prosince 2014 v Bruselu. Cílem této konference bylo prezentovat výsledky v oblasti řízení inovací pro koncové uživatele a operátory a jejich doporučení pro zlepšení zapojení koncových uživatelů a provozovatelů do výzkumného procesu EU a podporovat zavádění těchto výsledků. Smyslem a cílem 10 interaktivních kulatých stolů bylo získat zpětnou vazbu v různých tématech souvisejících se zabezpečením, a to zejména:
    - Bezpečnost civilního letectví
    - (CBRN) Ohrožení chemickými, biologickými, radiologickými a jadernými zbraněmi,
    - Cyber-zločin / cyber-terorismus,
    - Vnější rozměr bezpečnosti,
    - Inteligentní sledování hranice
    - Civilní ochrana / krizového řízení,
    - Řízení inovací,
    - Robotika v oblasti bezpečnosti,
    - Ochrana kritické infrastruktury,
    - Urban Security

Závěrečná konference byla také příležitostí představit iniciativu Archimedes. Tedy konsorcia, které bude strukturovaně propojené na národní organizace z různých evropských zemí, které se zabývají bezpečnostními otázkami, s Aliancí pro evropský růst a inovace pro bezpečnost AEGIS. Za TPEB ČR byl na konferenci pozván JUDr. Richard Hlavatý. Ve svém vystoupení představil poslední aktivity platformy, zejména **projekt Energetická a kybernetická bezpečnost ČR** a reagoval na některé předložené návrhy projektu Aegis.

Dr. Hlavatý uvedl, že projekt v předložené podobě užší spolupráce mezi vybranými organizacemi v EU, nejen odráží vývoj v oblasti bezpečnosti, ale nabízí velmi pragmatické řešení na podporu růstu konkurenceschopnosti EU, resp. jednotlivých členských států v této specifické oblasti. JUDr. Richard Hlavatý rovněž uvedl, že je potřeba do tohoto procesu aktivně přivést i „nové“ členské země střední a východní Evropy. TPEB má v plánu zapojit se do dalšího fungování evropské platformy Archimedes a tuto spolupráci převést do projektů pro program H2020.

# Závěr

Projekt Energetická a kybernetická bezpečnost úspěšně prošel všemi čtyřmi etapami, ve kterých řešitelský tým dokázal identifikovat klíčové problémy a potřeby ve všech čtyřech technologických sektorech. V první etapě se podařilo aktualizovat strategickou a výzkumnou agendu a upřesnit směřování projektu ve vztahu k dalším etapám, které se zabývaly standardizací, projektovou aplikací a legislativou. Kromě identifikace projektových a výzkumných témat, která byla následně využita ve třetí etapě, první etapa kontextualizovala celou problematiku s vývojem evropských iniciativ v této oblasti. V této souvislosti bylo zdůrazněno, že i na evropské úrovni lze vysledovat poměrně značnou dynamiku v oblasti ochrany kritické infrastruktury, která bude nadále do značné míry ovlivňovat situaci v ČR.

Druhá etapa projektu se zabývala problematikou standardů, jejichž formování a aplikace představuje významnou problematiku, a to jak z hlediska bezpečnosti, tak i navázaných příležitostí v oblastech výzkumu, vývoje, inovací a stejně tak i samotného byznysu. Procesy standardizace navíc z definice představují interdisciplinární aktivity, což vedlo TPEB i k expanzi její odborné báze. Jako velmi zásadní a do budoucna významné téma se objevila problematika vztahu mezi právní regulací a standardy, kterou lze vnímat z mnoha perspektiv, a která je různým způsobem ošetřována v jiných technologických odvětvích.

Ve třetí etapě činnost řešitelského týmu vyústila v účast hned v několika projektových konsorciích, která usilují o podporu v rámci programu Horizont2020 a zároveň ve stimulaci a formulaci dalších projektových žádostí. V rámci procesu přípravy projektů byly reflektovány závěry z prvních dvou etap týkající se významu evropského kontextu a standardizačních procesů. Ve většině projektů byl vytvořen prostor pro aktivity odborníků z ÚNMZ a UROSKSOJ. Zároveň došlo k zásadní expanzi institucí spolupracujících s TPEB, a to jak z akademické a výzkumné, tak i firemní oblasti.

Čtvrtá etapa uzavírající projekt se soustředila na legislativu, nicméně jako nečekaně silné téma se objevila související problematika rámce institucionální spolupráce při zvyšování společenské resilience v této oblasti. Ve čtvrté etapě zároveň pokračovaly projektové aktivity představující jeden z primárních cílů strategické a výzkumné agendy, které přestavují cestu k dlouhodobé udržitelnosti fungování TPEB.