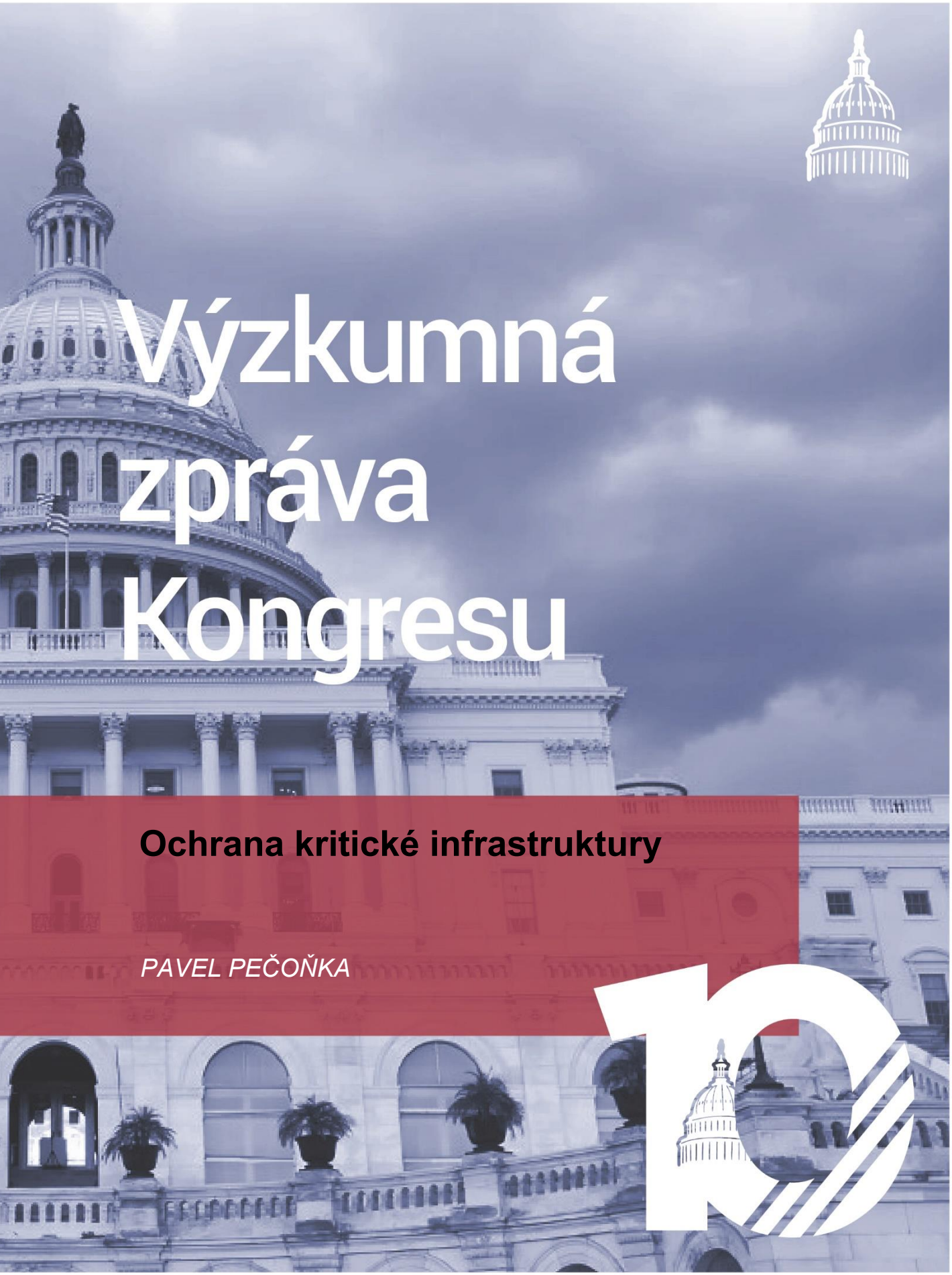

Výzkumná zpráva Kongresu

Ochrana kritické infrastruktury

PAVEL PEČOŇKA

PRO ČESKÝ MODEL AMERICKÉHO KONGRESU 2020

1. Úvod

Účelem tohoto dokumentu je nastínit problematiku ochrany kritické infrastruktury a představit kroky, které federální vláda a Kongres učinily v zájmu zamezení jejího poškození a s tím spojených rizik.

Kritickou infrastrukturu tvoří prvky nebo systémy prvků (stavby, zařízení, prostředky nebo veřejná infrastruktura a jejich provozovatelé), u kterých by narušení jejich funkce mělo závažný dopad na bezpečnost státu, zabezpečení základních životních potřeb obyvatelstva, zdraví osob nebo ekonomiku státu.[1]

Hladké fungování systémů a sítí, které tvoří infrastrukturu společnosti, je často považovány za samozřejmé, avšak narušení pouze jednoho z těchto systémů může mít v ostatních odvětvích hrozivé důsledky.

Typickým příkladem (jehož důsledky jsme již mnohokrát viděli) může být například počítačový virus, který naruší distribuci zemního plynu v regionu. To by mohlo vést k následnému snížení výroby elektrické energie, což zase vede k nucenému vypnutí počítačových systémů a komunikace. Mohlo by dojít k ovlivnění silniční, letecké a železniční dopravy. Tísňové služby mohou být také omezeny.

Celý region může mít poškozenou kritickou infrastrukturu vlivem přírodní katastrofy, nebo útokem na civilní, nebo vojenský cíl.

2. Klasifikace kritické infrastruktury

Federální vláda vyvinula standardizovaný popis kritické infrastruktury, za účelem usnadnění monitorování a přípravy na danou událost.

Vláda požaduje, aby soukromý sektor:

a) Posuzoval zranitelnost vůči fyzickým nebo kybernetickým útokům;

b) vypracoval plány na odstranění významných zranitelných míst;

c) prioritizoval vývoj systémů pro identifikaci a prevenci pokusů o útok.

Dále se od soukromých subjektů očekává, že budou upozorňovat na útoky, pokoušet se omezit a zabraňovat útokům a poté společně s Federální agenturou pro řízení mimořádných událostí (Federal Emergency Management Agency, FEMA) vyhodnocovat konkrétní útoky a situace.

3. Vývoj vládního přístupu ke kritické infrastruktuře

Spojené státy byly jednou z prvních zemí, které se začaly věnovat otázce ochrany kritické infrastruktury. V roce 1996 byla vytvořena Prezidentská komise na ochranu kritické infrastruktury (PCCIP). Ta měla za cíl prověřit rostoucí závislost americké ekonomiky a na kritické infrastruktuře. V říjnu 1997 Komise vyzvala k zajištění bezpečnosti částí klíčové infrastruktury, jako jsou telekomunikace, bankovnictví a finance, doprava a základní vládní

[1] critical infrastructure protection. In: *Wikipedia: the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2001- [cit. 2020-07-19].

služby. Prezident Clinton v květnu 1998 vydal na základě této komise dvě nové směrnice – PDD-62 (boj proti terorismu) a PDD-63, která se věnuje ochraně kritické infrastruktury. Směrnice PDD-63 zahrnovala řešení zranitelnosti kritické infrastruktury ve veřejném i soukromém sektoru. Stanovila cíle, poskytla koncepci a zdroje a zařadila kritickou infrastrukturu mezi národní životní zájmy.

16. října 2001 vydal prezident George W. Bush Vládní nařízení na ochranu kritické infrastruktury. Jeho účelem bylo zabezpečit ochranu informačních systémů pro kritickou infrastrukturu, včetně nouzové komunikační připravenosti a ochrany hmotných zařízení, které informační asystémy podporují. Jako prioritní bylo stanoveno zabezpečení tří vzájemně závislých funkcí: ekonomiky, činnost státu (vlády) a vedení národní obrany.

První definici kritické infrastruktury přinesl tzv. Patriot Act, který stanovil, že *„systémy a zařízení, jak hmotné tak virtuální, které jsou životně důležité pro Spojené státy a zneschopnění, nebo kdyby zničení takových systému nebo zařízení mělo vliv na snížení bezpečnosti, národní ekonomické bezpečnosti, národního veřejného zdraví nebo bezpečnosti nebo jakoukoliv jejich kombinaci.“*

V roce 2002 byla vydána Národní strategie pro vnitřní bezpečnost (The National Strategy for Homeland Security). S předcházet teroristickým útokům na Spojené státy, snížit zranitelnost Ameriky vůči terorismu a minimalizovat škody a zotavit se z útoků, které nastanou.

O rok později vydal Bílý dům Národní strategii fyzické ochrany kritické infrastruktury a klíčových zařízení (The National Strategy for The Physical Protection of Critical Infrastructures and Key Assets) a Národní strategii zabezpečení kybernetického prostoru. (The National Strategy to Secure Cyberspace). Zde došlo k specifikaci kritické infrastruktury z hlediska kybernetiky a fyzickou ochranu klíčových zařízení.

Cílem Národní strategie je dosáhnout jednotnějšího, koordinovaného a vzájemně se doplňujícího systému, který vyžaduje aktivní přístup jak státní administrativy, tak i soukromého sektoru a občanů USA. Formuluje a popisuje zabezpečení kritické infrastruktury v 11 sektorech a ochranu klíčových zařízení v pěti sektorech.

Výše uvedené strategie popisují obecný směr zabezpečení kritické infrastruktury vjednotlivých sektorech. Samotné plánování identifikace a prioritizace zabezpečení jednotlivých prvků má na starosti nařízení prezidenta, tzv. Homeland Security Presidential Directive 7, které slouží jako podklad pro zpracování globálního plánu pro ochranu kritické infrastruktury a na něj navazujících jednotlivých sektorových plánů pro ochranu kritické infrastruktury.[2]

[2] KUBICOVÁ, L. *Bezpečnost a ochrana kritické infrastruktury společnosti v České republice.* Brno: Vysoké učení technické v Brně, Fakulta chemická, 2010. 59 s. Vedoucí bakalářské práce Ing. Otakar Jiří Mika, CSc.

4. Sektory kritické infrastruktury

Níže uvedená tabulka zachycuje přístup federální vlády ke klasifikaci jednotlivých prvků kritické infastruktury.

Federal Government Organization to Protect Critical Infrastructure and Key Assets

President

Secretary of Homeland Security
Federal, state, local, and private sector coordination and integration
Comprehensive national infrastructure protection plan
Mapping threats to vulnerabilities and issuing warnings

Sector	Lead Agency
Agriculture	Department of Agriculture
Food:	
Meat and poultry	Department of Agriculture
All other food products	Department of Health & Human Services
Water	Environmental Protection Agency
Public Health	Department of Health & Human Services
Emergency Services	Department of Homeland Security
Government:	
Continuity of government	Department of Homeland Security
Continuity of operations	All departments and agencies
Defense Industrial Base	Department of Defense
Information and Telecommunications	Department of Homeland Security
Energy	Department of Energy
Transportation	Department of Homeland Security*
Banking and Finance	Department of the Treasury
Chemical Industry and Hazardous Materials	Environmental Protection Agency
Postal and Shipping	Department of Homeland Security
National Monuments and Icons	Department of the Interior

PDD-63 poskytnul mandát k vytvoření národního plánu ochrany infrastruktury (NIPP). Hlavní úkol je komunikace soukromého sektoru, na čemž závisí vysoké procento kritické infrastruktury, a federální vlády. Dále obsahuje granty, které vydává ministerstvo vnitřní bezpečnosti pro soukromé entity v rámci „ochranných opatření“ Patří sem granty na řízení krizových situací, školení v oblasti vodní bezpečnosti, železniční, tranzitní a přístavní

bezpečnost, reakce na metropolitní lékařskou péči, programy prevence terorismu a Iniciativa pro bezpečnost městských oblastí.

5. Národní plán ochrany infrastruktury

National Infrastructure Protection Plan (NIPP) definuje odvětví kritické infrastruktury ve Spojených státech a stanovuje následujících 16 odvětví kritické infrastruktury:

1. Chemikálie
2. Komerční zařízení
3. komunikace
4. Kritická výroba
5. Přehrady
6. Obranná průmyslová základna
7. Pohotovostní služby
8. Energie
9. Finanční služby
10. Potraviny a zemědělství
11. Vládní zařízení
12. Zdravotnictví a veřejné zdraví
13. Informační technologie
14. Jaderné reaktory, materiály a odpady
15. Dopravní systémy
16. Systémy vody a odpadních vod

Oblasti spadající přímo do kompetence Ministerstva vnitřní bezpečnosti pak zahrnují:

a) chemikálie
b) komerční zařízení
c) komunikace
d) kritickou výroba
e) přehrady
f) pohotovostní služby
g) vládní zařízení (společně se správou všeobecných služeb)
h) informační technologie
i) jaderné reaktory, materiály a odpady
j) dopravní systémy (společně s ministerstvem dopravy)

Zbylé sektory kritické infrastruktury pak spadají do gesce zbylých ministerstev a agentur:

Bankovnictví a finance – Zodpovědné je Ministerstvo financí nejenom za stabilitu systému, ale také udržování důvěry veřejnosti skrze Financial Services Information Sharing and Analysis Center (ISAC).

Doprava – Ministerstvo dopravy je zodpovědné za ochranu cest, železnic, vodní a letecké dopravy, včetně regulace a transportu nebezpečného materiálu.

Energetika – Ministerstvo energetiky dohlíží na dodávky elektřiny, zemního plynu, ropy, spolupracuje s Nuclear Regulatory Commission v rámci ochrany jaderných elektráren a jaderného materiálu.

Informace – telekomunikace a informační technologie spadají pod Ministerstvo obchodu.

Federální budovy – ty spadají pod jednotlivé ministerstva a úřady, zajištují chod federální vlády a spolupráci s lokálními orgány k zajištění nezbytných služeb. Vodní systém a další součásti spadají pod EPA

Integrované složky záchranného systému – spadají pod Ministerstvo zdravotnictví a sociálních služeb. Hasičské sbory spadají pod FEMA.

Zemědělství a jídlo – dodávky a bezpečí potravin kontroluje Ministerstvo zemědělství.

Obraná průmyslová základna – Spadá pod Ministerstvo obrany

Pro každý z identifikovaných hlavních sektorů kritické infrastruktury jmenovala federální vláda styčného úředníka pro sektor z určené vedoucí agentury. Rovněž byl identifikován protějšek ze soukromého sektoru.

Kromě toho bylo každé ministerstvo a agentura federální vlády zodpovědné za vývoj vlastního plánu CIP na ochranu své části kritické infrastruktury federální vlády. Federální plány jsou taktéž vzájemně propojeny a tvoří jeden komplexní plán. Tento plán má brát v potaz také vzdělávaní, vyhledávání hrozeb, vývoj a výzkum.

Proces monitoringu hrozeb zahrnuje hodnocení:

a) ochrany – jak je daný sektor chráněn a připraven na hrozby různého rozsahu?
b) zranitelnosti – jak náchylný je sektor k napadení nebo zničení?
c) rizik – jaká je možnost nebo pravděpodobnost napadení nebo zničení prvků kritické infrastruktury?
d) zmírnění hrozeb – existuje potenciál pro snížení nebo zmírnění zranitelnosti sektoru a snížení nebo dokonce odstranění rizika?[3]

[3] CRITICAL INFRASTRUCTURE SECTORS. *CISA.com* [online]. USA: CISA, 2020 [cit. 2020-07-19].

6. Výzvy

a) nové hrozby

S vývojem nových technologií souvisí i nárůst možností a nových hrozeb. Nejprve můžeme hovořit o tzv. vzdálených hrozbách, které umožnila automatizace, robotizace a vývoj umělé inteligence. V otázkách kybernetické bezpečnosti je rozšířený názor, že většinu budoucích kybernetických útoků bude mít na starosti umělá inteligence. Ta by mohla vytvářet velmi pokročilé malwary, které by byly pro člověka téměř nemožné zastavit.

Zatím nejsou tyto útoky nikde zaznamenány, přesto tato hrozba klade důraz na přípravu kritické infrastruktury tímto směrem. Jedno z řešení se nabízí větší decentralizace a možnost diverzifikovat zdroje, aby lépe čelily případným útokům. Taktéž je v zájmu ochrany kritické infrastruktury, rozvíjet pokročilejší možnosti ochrany a využívat i automatizaci k obraně počítačových systému.

b) Větší propojenost světa

Stále více věcí v našem životě je závislé na vzájemné komunikaci, ať už se jedná o mobilní telefon, různá chytrá zařízení, nebo automobily. To dává potenciálním vyzyvatelům daleko širší pole působnosti, jak proniknout do systému kritické infrastruktury, zde je nanejvýš důležité téma výstavba 5G sítí a je v nejvyšším zájmu národní bezpečnosti zajistit jednak neproniknutelnost do tohoto systému, tak i se připravit na větší propojování informačních technologií.

c) Větší důraz na specifika jednotlivých sektorů

Vzhledem k obrovskému záběru kritické infrastruktury i samotnému faktu, že značná část leží v soukromých rukách je potřeba dbát na větší míru flexibility a přizpůsobení jednotlivých části kritické infrastruktury. To klade nároky na větší kooperaci federálních a soukromých složek a větší míry specializace jednotlivých sekcí.

d) Komunikace

V roce 2017 Národní bezpečnostní rada prověřila zabezpečení více než 140 federálních objektů a vyhodnocovala jejich připravenost a ohrožení.

„Podle závěrečné zprávy bezpečnostní rady mají federální úřady i soukromý sektor dostatek zdrojů k ochraně kritické infrastruktury, ale tato ochrana není téměř nijak koordinovaná a špatně využívaná. „Vyzýváme administrativu prezidenta Trumpa, aby využila tohoto varování a podnikla náležitá a rozhodná opatření," uvedla rada.

Konkrétně pak Národní bezpečnostní rada navrhuje vytvořit samostatná bezpečnostní řešení pro sítě zařazené do kritické infrastruktury USA, včetně páteřních optických sítí a také vyhrazení části spektra pro záložní komunikační sítě.[4]

[4] Critical Infrastructure Protection Challenges in 2018. *Lanner-america.com* [online]. 3160A Orlando Drive, Mississauga, ON L4V 1R5, Canada: Lanner, 2018 [cit. 2020-07-19].

Vysokou prioritu by podle rady mělo mít i sdílení informací o veškerých pokusech narušení kritické infrastruktury mezi jednotlivými úřady a Národním sborem poradců pro infrastrukturu. Zpráva rovněž doporučuje, aby vznikl systém, který bude účinně monitorovat chování kritických sítí a vyhodnocovat případné výkyvy.

Federální vláda by podle sboru poradců měla vypsat pobídky na investice do modernizace kritických infrastruktur. Na to vše by měl dohlížet nový operační útvar, který by se skládal z expertů z vládních úřadů a společností z oblastí energetiky, financí a komunikace. Prezidentův poradce pro národní bezpečnost by měl náležitě prostudovat všechna tato doporučení a naplánovat jejich realizaci, dodala Národní bezpečnostní rada.“[5]

7. Možnosti pro zákonodárce

Předchozí kapitoly nastínily problematiku ochrany kritické infrastruktury (včetně klasifikace jednotlivých prvků) a stručně shrnuly přístup federální vlády. Závěr tohoto textu je věnován krátké diskuzi toho, jak se k problematice může postavit Kongres.

Jak naznačeno výše, federální vláda rizika spojená s potenciálními útoky na kritickou infastrukturu vnímá dlouhodobě vážně a podniká aktivní kroky k minimalizaci a prevenci těchto rizik. Navzdory dlouhodobému přístupu se ale stále jedná primárně o prezidentova exekutivní nařízení nebo vnitřní pravidla jednotlivých ministerstev. Nabízí se tedy možnost rozšíření tohoto přístupu na bližší spolupráci se zákonodárnou mocí. Toto by mohlo zahrnovat formalizaci vládních kroků zákonnou předlohou. Zároveň by Kongres mohl využít svého kapitálu k facilitaci a podpoře větší míry spolupráce mezi vládami států a federální vládou.

Kongres by také mohl využít svých zákonodárných pravomocí v jiných oblastech. Jak zmíněno výše, v případech, kdy jsou komponenty klíčové infrastruktury operovány a spravovány soukromými subjekty, požaduje vláda po těchto subjektech určité kroky (především reporting instancí útoků nebo spolupráci s vládními agenturami). Nabízí se nicméně otázka, zda by Kongres neměl ve skutečně odůvodněných případech povinnosti formalizovat nebo dokonce rozšířit. Toto by samozřejmě mohlo vést ke sporům mezi kompetencemi zákonodárné a výkonné moci, nemluvě o možné kolizi s právem na svobodné nakládání se soukromým majetkem – témata, se kterými by se zákonodárci museli příslušným způsobem vypořádat.

Další kapitolou je možnost o hlubší integraci tématu ochrany klíčové infrastruktury s otázkami národní bezpečnosti. Případné útoky na prvky kritické infrastruktury se pochopitelně nemusejí omezovat na domácí aktéry, ale mohou (a pravděpodobně stále častěji také budou) pocházet ze zahraničí. S ohledem na stále fluidnější charakter mezinárodního prostředí je prevence tohoto typu rizika nanejvýš složitá, Kongres nicméně může zvážit preventivní kroky mající za cíl takové potenciální útoky zastrašit a v případě selhání na původce těchto útoků adekvátně reagovat. Toto by se patrně týkalo kriticky důležitých (a také potenciálně hodně zranitelných) oblastí jako je kyberprostor nebo například bezpečnost ve vnějším vesmíru.

[5] POTŮČEK, Jan. Americké úřady nejsou dobře zabezpečeny. USA hrozí kybernetické útoky. *Novinky.cz* [online]. Praha: Seznam.cz, 2017 [cit. 2020-07-19].

8. Zdroje

a. Užitečné odkazy

https://georgewbush-whitehouse.archives.gov/news/releases/2003/12/20031217-5.html

https://www.cisa.gov/2015-sector-specific-plans

https://www.cisa.gov/2015-sector-specific-plans

b. Citace

Critical infrastructure protection. In: *Wikipedia: the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2001- [cit. 2020-07-19]. Dostupné z: https://en.wikipedia.org/wiki/Critical_infrastructure_protection#cite_note-HSPD7bush-2

CRITICAL INFRASTRUCTURE SECTORS. *CISA.com* [online]. USA: CISA, 2020 [cit. 2020-07-19]. Dostupné z: https://www.cisa.gov/critical-infrastructure-sectors

POTŮČEK, Jan. Americké úřady nejsou dobře zabezpečeny. USA hrozí kybernetické útoky. *Novinky.cz* [online]. Praha: Seznam.cz, 2017 [cit. 2020-07-19]. Dostupné z: https://www.novinky.cz/internet-a-pc/bezpecnost/clanek/americke-urady-nejsou-dobre-zabezpeceny-usa-hrozi-kyberneticke-utoky-40044765

KUBICOVÁ, L. *Bezpečnost a ochrana kritické infrastruktury společnosti v České republice.* Brno: Vysoké učení technické v Brně, Fakulta chemická, 2010. 59 s. Vedoucí bakalářské práce Ing. Otakar Jiří Mika, CSc.

Critical Infrastructure Protection Challenges in 2018. *Lanner-america.com* [online]. 3160A Orlando Drive, Mississauga, ON L4V 1R5, Canada: Lanner, 2018 [cit. 2020-07-19]. Dostupné z: https://www.lanner-america.com/blog/critical-infrastructure-protection-challenges-2018/