Acta Informatica Pragensia, 2016, 5(2): 180–191
DOI: 10.18267/j.aip.93
Peer-reviewed paper

Informační rámec kritické infrastruktury

Information Framework of Critical Infrastructure

Stanislava Mildeová[*], Antonín Dvořák[†], Pavel Zahradníček[‡]

Abstrakt

Informační a komunikační technologie jsou odbornou veřejností v souvislosti s problematikou bezpečnosti diskutovány z mnoha pohledů. Autoři chápou informační a komunikační technologie jako potenciál a zároveň hrozbu pro bezpečnostní prostředí. Cílem článku je holisticky analyzovat základní souvislosti mezi infomačním rámcem a funkčností systému kritické infrastruktury spojenou s činností veřejné správy v České republice. Jako modelový případ je diskutována ochrana kritické infrastruktury před toxickými látkami. Turbulentnost bezpečnostního prostředí, transformace konfliktů do hybridních nebo asymetrických forem a, jak je v článku prokázáno, klíčové a průřezové postavení informatiky v těchto procesech činní toto téma velmi aktuální.

Klíčová slova: ICT, informační systémy, kybernetická bezpečnost, kritická infrastruktura, kritická informační infrastruktura, toxické látky, veřejná správa, systémový přístup.

Abstract

Information and communication technologies are in connection with security discussed by professional community from many perspectives. The authors perceive information and communication technologies as potential as well as threat to the security environment. The aim of the article is to holistically analyze the basic connection between the information framework and functionality of the critical infrastructure system involved in the activities of the public administration. As a model case is discussed the protection of critical infrastructure against toxic substances. Turbulence of the security environment, conflict transformation into hybrid or asymmetric forms and, as it is proven in the article, a crucial position of informatics in these processes makes this a very actual topic.

Keywords: ICT, Information systems, Cybersecurity, Critical infrastructure, Critical information infrastructure, Toxic substance, Public administration, Systems approach.

[*] Department of Computer Science and Mathematics, Faculty of Economic Studies, University of Finance and Administration, Estonská 500, 101 00 Prague 10, Czech Republic
✉ mildeova@mail.vsfs.cz

[†] Institute for Sustainable Business, Faculty of International Relations, University of Economics, Prague, W. Churchill Sq. 4, 130 67 Prague 3, Czech Republic
✉ advorak@vse.cz

[‡] Institute of Security, Karel Englis College, Mezírka 775/1, 602 00 Brno, Czech Republic
✉ pavel.zahradnicek@vske.cz

1 Úvod

Současné bezpečnostní prostředí je prostředím nejistoty, vyznačujícím se vyšší mírou nepoznatelnosti a nižší možností kontroly. Dle Horáka et al. (2015) bezpečnostní hrozby, jejich zdroje a nositelé mají jak státní, tak stále více i nestátní a nadnárodní charakter a z toho potom plynoucí asymetrickou povahu. Trendy v globálním prostředí zesilují potenciál těchto rostoucích asymetrických hrozeb a zvyšují možnost jejich šíření z relativně vzdálených oblastí lokálních či regionálních konfliktů a napětí.

Bezpečnostní prostředí je úzce spjato s oborem informatika a staví nová zadání i pro její vývoj. Informace a znalosti jsou fenomény v dnešní společnosti, po právu nazývané jako informační či znalostní. Je tedy jasné, že informační a komunikační technologie jsou potenciálem bezprostředně ovlivňujícím ekonomický růst, jak prokazuje (Hančlová et al., 2015), zároveň jsou hrozbou pro bezpečnostní prostředí. V tomto rámci autoři vidí zkoumanou problematiku.

Zvyšující se závažnost nevojenských hrozeb, do kterých patří i kybernetické útoky, a zhoršující se bezpečnostní situace v oblastech bezprostředně sousedících s členskými státy NATO a EU, kladou rostoucí nároky na schopnost Evropy reagovat a zvýrazňují nedostatky v připravenosti bezpečnostním hrozbám odolat. Bezpečnostní strategie české republiky z roku 2015 zařadila problematiku ochrany kritické infrastruktury mezi závažné specifické hrozby vůči státu (Kolektiv autorů, 2015).

Cílem článku je analyzovat základní souvislosti mezi infomačním rámcem a funkčností systému kritické infrastruktury spojenou s činností veřejné správy České republiky. Vědeckou hypotézou, která bude v článku ověřována, je teze „Informatika je se svými informačními a znalostními nástroji průřezová, ovlivňující synergicky ostatní oblasti kritické infrastruktury“. Jako modelový případ je diskutována ochrana kritické infrastruktury před toxickými látkami, coby aktuální téma. Problematika zneužití vysoce toxických látek byla diskutována např. na zasedání Bezpečnostní rady OSN v únoru 2016 v Ženevě, a to v souvislosti s nekontrolovanou migrací do Evropy.

Zkoumání provedené v článku je založeno na dílčí obsahové analýze a syntéze, dedukci a indukci dříve poznaného. V aplikovaném systémovém přístupu autoři navazují na tvrzení, které uvádí Kný (2015), jež zdůrazňuje nezbytnost holistického řešení a systémového myšlení v problematice bezpečnosti. Hranicí zkoumání je ČR, při současném respektování zahraničních, především evropských kontextů. Článek navazuje na (Dvořák a kol., 2016; Zahradníček, 2015; Zahradníček, 2016), a rozvíjí informační pozadí zde uvedeného výzkumu.

2 Systém kritické infrastruktury státu

2.1 Bezpečnostní prostředí

Bezpečnostní prostředí je vnějším prostředím ovlivňujícím bezpečnostní politiku státu. Lze jím rozumět prostor či soubor podmínek, v němž se realizují a střetávají zájmy státu se zájmy jiných aktérů systému mezinárodních i vnitrostátních vztahů viz (Zahradníček, 2015). Odehrávají se zde procesy, které mají významný vliv na úroveň bezpečnosti státu. Vývoj v tomto prostředí je ze strany referenčního objektu (státu) ovlivnitelný v omezené míře a to v závislosti na jeho potenciálu (Juříček, Rožňák, 2014).

2.2 Kritická infrastruktura

Kritická infrastruktura státu (KI) představuje klíčový systém prvků ve smyslu NV č. 432/2010 Sb. a jeho novele č. 315/2014 Sb., jejichž narušení nebo vyřazení by mělo závažný dopad na bezpečnost státu, zabezpečení základních životních potřeb obyvatel nebo hospodářství státu (SZČR, 2010; NVČR, 2014). S ohledem na velmi vysoký stupeň vzájemného propojení jednotlivých odvětví je kritická infrastruktura ohrožena komplexně a to přírodními, technologickými a asymetrickými hrozbami. Z tohoto vyplývá, že stát v případě kolapsu kritické infrastruktury by nebyl schopen plnit svoje základní funkce vnější ani vnitřní (Zahradníček, 2016).

Dle Směrnice ES/114/2008 a související české legislativy jsou rozhodující funkční oblasti činnosti státu, které vyžadují funkčnost kritické infrastruktury (EUR-Lex, 2009):

- energetika
- vodní hospodářství
- potravinářství a zemědělství
- zdravotnictví
- doprava
- komunikační a informační systémy
- finanční trh a měna
- nouzové služby
- veřejná správa.

2.3 Kritická informační infrastruktura

Součástí Kritické infrastruktury je Kritická informační infrastruktura. Národní centrum kybernetické bezpečnosti jako součást Národního bezpečnostního úřadu stanovilo postup rozhodování rozhodovacím stromem viz Obrázek 1. Zde se informační systém (IS) nebo komunikační systém (KS) stává prvkem tzv. *kritické informační infrastruktury*. Posuzována jsou průřezová kritéria a odvětvová kritéria v oblasti kybernetické bezpečnosti - odvětvová kritéria v rámci odvětví VI. Komunikační a informační systémy (Kritická informační infrastruktura, 2014):

Průřezová kritéria jsou:

a) Více než 250 mrtvých nebo více než 2 500 osob s následnou hospitalizací delší než 24 hodin.

b) Mezní hodnota hospodářské ztráty je větší než 0,5 % HDP.

c) Omezení poskytování nezbytných služeb nebo jiný závažný zásah do každodenního života postihující více než 125 000 osob.

Odvětvová kritéria jsou:

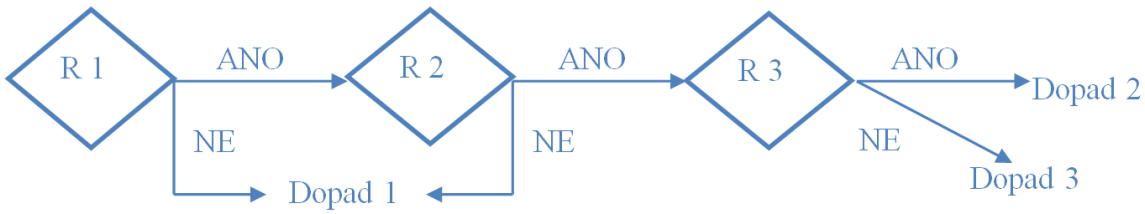
a), b) Ovlivňuje-li IS nebo KS významně nebo zcela činnost určeného prvku KI a zároveň je nahraditelný jen při vynaložení nepřiměřených nákladů nebo v časovém období delším jak 8 hodin.

c) Je-li IS spravovaný orgánem veřejné moci obsahující osobní údaje o více než 300 tis. osobách.

d) Je-li systém komunikačním systémem, který zajišťuje připojení nebo propojení prvku KI s kapacitou garantovaného datového přenosu min. 1 Gbit/s.

e) Odvětvová kritéria pro stanovení prvků kritické infrastruktury v rámci odvětví *Komunikační a informační systémy* se použijí, pokud je ochrana prvku naplňujícího tato kritéria nezbytná pro zajištění kybernetické bezpečnosti. U odvětvových kritérií v rámci odvětví VI. Komunikační a informační systémy jsou předmětem zájmu následující technologické prvky:

- pevné sítě elektronických komunikací
- mobilní sítě elektronických komunikací
- sítí pro:
    - rozhlasové a televizní vysílání
    - pro satelitní komunikaci
    - pro poštovní služby
- informačních systémů.



Rozhodování 1 (R1): Může mít narušení bezpečnosti informací IS nebo KS za následek alespoň jedno z průřezových kritérií?

Rozhodování 2 (R2): Splňuje IS nebo KS alespoň jedno z odvětvových kritérií?

Rozhodování 3 (R3): Jde o organizační složku státu?

Dopad 1: IS nebo KS v tuto chvíli není kritickou informační infrastrukturou. Může však být významným informačním systémem (u orgánů veřejné moci).

Dopad 2: IS nebo KS splňuje podmínky pro zařazení do kritické informační infrastruktury.

Dopad 3: NBÚ navrhne Ministerstvu vnitra zařadit IS nebo KS do seznamu, který bude následně předložen vládě ČR k rozhodnutí.

Obr. 1. *Posuzování prvků kritické informační infrastruktury.*
Zdroj: Autoři na základě (Kritická informační infrastruktura, 2014)

Mimo kritické informační infrastruktury jsou dále vymezeny tzv. *významné informační systémy* (orgánů veřejné moci). Postupuje se dle zákona č. 181/2014 Sb. o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), včetně jeho prováděcích právních předpisů, tj. vyhlášky č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích a vyhlášky č. 316/2014 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti (Národní centrum kybernetické bezpečnosti, 2014).

2.4 Krizové řízení veřejné správy

Veřejnou správou zpravidla rozumíme správu věcí veřejných (Hadrabová, 2008). Veřejná správa se neobejde bez procesu udržování takového prostředí, ve kterém lze efektivně dosahovat společenských cílů. Tento proces je spojen s pojmy "řízení" nebo-li "management". Máme-li na mysli řešení mimořádných nebo krizových situací, pak hovoříme o krizovém řízení (managementu) veřejné správy.

Krizové řízení autoři článku chápou jako souhrn řídících činností věcně příslušných orgánů, zaměřených na analýzu a vyhodnocování bezpečnostních rizik, plánování, organizování, realizaci a kontrolu činností, prováděných v souvislosti s řešením mimořádné nebo krizové situace. Krizový management se stal standardní součástí managerského prostředí. Zpravidla vyžaduje připravené specialisty, tzv. krizové managery.

Krizový management se z hlediska svých funkcí neodlišuje od obecného managementu. Rozdíl je nutné spatřovat v obsahu, který je v případě krizového managementu formován zásadně jiným vnějším i vnitřním prostředím. Jiné jsou pro veřejnou správu zejména cíle, úkoly, postupy, síly a prostředky pro zvládání mimořádných nebo krizových situací. Veřejná správa vykonávaná v případě výše uvedených situací je vázána přísnou legislativou (Antušák, 2009).

Veřejná správa ve své struktuře zahrnuje orgány, které jsou určeny k řešení mimořádných nebo krizových situací. Tyto orgány (krizového řízení) zabezpečují analýzu a vyhodnocení možných ohrožení, plánování, organizování, realizaci a kontrolu činností prováděných v souvislosti s přípravnými opatřeními, řešením krizových stavů nebo ochranou kritické infrastruktury.

Zákon o krizovém řízení č. 240/2000Sb. v hlavě II definuje tyto orgány krizového řízení (SZČR, 2000):

- vládu,
- ministerstva a jiné ústřední orgány,
- Českou národní banku,
- orgány kraje a další orgány s působností na území kraje,
- orgány obce s rozšířenou působností a
- orgány obce.

2.4.1 Charakteristika orgánů s územní působností

Bezpečnostní rady jsou zřízené k přípravě na řešení krizových situací (KS) a jsou poradním orgánem zřizovatele. Na svém jednání projednávají zejména stav připravenosti území a orgánů na řešení krizových situací a k tomu zpracovanou dokumentaci.

Krizové štáby jsou pracovními orgány zřizovatele pro řešení mimořádné nebo krizové situace. Členové krizového štábu v době řešení vzniklé situace připravují předsedovi krizového štábu podklady a návrhy řešení. Efektivitě práce krizových štábů napomáhá využití výpočetní techniky a speciální software pro řešení krizových situací.

Územní správní úřady uvedené v krizovém plánu kraje nebo krizovém plánu ORP zabezpečují krizovou připravenost v oblasti své působnosti a k tomu účelu zpracovávají příslušný Krizový plán.

3 Informační rámec systému kritické infrastruktury

3.1 Toxické látky

Ochrana kritické infrastruktury státu před vysoce toxickými látkami je aktuální a v „Plánech krizové připravenosti subjektů kritické infrastruktury“ by se vždy měla objevit odpovídající varianta ochrany v případě napadení vysoce toxickými látkami. Vysoce toxické látky se podle jejich určení dělí na bojové toxické látky a průmyslové toxické látky. Oba tyto druhy mohou způsobit smrt osob nebo jejich vyřazení z činnosti. Nejsou primárně určeny ke

způsobování ztrát na technice, materiálu a zařízení. Bartlová (2005) dělí toxické látky na 1/ Bojové toxické látky jsou chemické sloučeniny nebo směsi, kterých může být použito v polních podmínkách. 2/ U průmyslových toxických látek je toxický účinek výsledkem interakce živé hmoty a látky.

Vlastnosti bojových toxických látek a průmyslových toxických je potencionálně předurčují i k napadení kritické infrastruktury státu. Jejich rozdílné vlastnosti (fyzikální, chemické, toxikologické) jejich efektivní použití k vyřazení prvků kritické infrastruktury limitují (Balog et al., 2007).

3.2 Kybernetické útoky

Problematika kybernetických útoků, tedy útoků v kyberprostoru, je vzhledem ke své aktuálnosti široce diskutována, v kontextu se standardem ISO 27037 odkažme alespoň na (Veber, Smutny, 2015) a v souvislosti s kybernetickou kriminalitou na zkoumání Požára (2015). V našem zkoumání se soustředíme na problematiku kybernetických útoků spolu s prvky kritické infrastruktury.

Prvky kritické infrastruktury ve smyslu NV č. 432/2010Sb a 315/2014 Sb. mohou být vyřazeny z činnosti v důsledku technologických havárií, selhání obsluhy anebo v důsledku záměrné destruktivní činnosti (SZČR, 2010; NVČR, 2014).

Příčina vyřazení může být jak vnitřní, tak vnější. Vyjdeme-li z faktu, že stávající obsluhy prvků kritické infrastruktury jsou zpravidla dobře vybrány a odborně připraveny a že nemají motiv (politický, ekonomický, sociální, náboženský, atd.) k útoku na kritickou infrastrukturu, pak se logicky nabízí, že případný útok lze očekávat z vnějšího prostředí státu, tedy zahraničí. Hrozba útoku se tak bude zvyšovat se zásadními změnami bezpečnostního prostředí státu.

Na základě EC Directive 114/2008 *kybernetické útoky jsou specifickou hrozbou pro bezpečnost*. Mezi dalšími hrozbami zde uvedenými uveďme: oslabování mechanismu kooperativní bezpečnosti i politických a mezinárodněprávních závazků v oblasti bezpečnosti, nestabilita a regionální konflikty v euroatlantickém prostoru a jeho okolí, terorismus, šíření zbraní hromadného ničení a jejich nosičů, negativní aspekty mezinárodní migrace, extremismus a nárůst interetnického a sociálního napětí, ohrožení funkčnosti kritické infrastruktury, přerušení dodávek surovin nebo energie a pohromy přírodního a antropogenního původu a jiné mimořádné události (EUR-Lex, 2009).

Pokud se týká podstaty ataků, kybernetické ataky směřující k napadení řídících systémů a informačních systémů prvků kritické infrastruktury jsou jedním z typů ataků. Další typy ataků mohou být svojí podstatou fyzické (použití výbušnin, útok pomocí letounů či dronů, atd. na prvky či systémy kritické infrastruktury), na veřejné zdraví (rozšíření vysoce infekčních nemocí) a na výživovou základnu (epifytie, zoofytie).

Proces výběru cíle(ů) v kritické infrastruktuře zahrnuje dle (Zahradníček, 2015):

- výběr vhodných cílů,
- přiřazení vhodného způsobu útoku pro dosažení smrtícího nebo nesmrtícího účinku, určeného před útokem
- vyhodnocení ataku (účinku).

Při výběru cílů se klade důraz na identifikaci objektů (prvků v kritické infrastruktuře), jejichž ztráta je pro stát nepřijatelná nebo které mu poskytují standardní výhody, např. zásobováni pohonnými hmotami. Důraz při určování objektů musí být zaměřen na ty součásti prvku kritické infrastruktury, které jsou pro výsledný, požadovaný efekt klíčové. Nejde jen o efekt

vlastní destrukce, ale i efekt psychologický, celospolečenský, tj. neletální (Zahradníček, 2015).

Abychom přešli do více konkrétní roviny, ilustrujme analýzu cílů pro atak námi zvoleného modelového případu použití vysoce toxických látek. V systému vymezme jako základní prvky rozhodujících funkční oblasti činnosti státu, které vyžadují funkčnost kritické infrastruktury a hledejme jejich vztah k typům cílů, míře vhodnosti pro napadení, převažujícímu účinku. Součástí námi vymezeného systému je specifikace citlivých míst (viz Tabulka 1). Za citlivá místa kritické infrastruktury považujeme ta místa daného systému, jejichž nefunkčnost by měla osudové důsledky.

OBLAST kritické infrastruktury	**CÍL (bodový/plošný)**	**VHODNOST pro napadení toxic. látkami**	**PŘEVAŽUJÍCÍ ÚČINEK (letální/neletální)**	**CITLIVÁ MÍSTA**
Energetika	bodový	malá	letální	dispečinky
Vodní hospodářství	bodový/plošný	malá/střední	letální/neletální	kontaminace nádrží, úpravny, rozvody
Potravinářství a zemědělství	bodový	malá/střední	letální	kontaminace prvotních produktů, nákupní centra
Zdravotnictví	bodový	malá	letální/neletální	velká nemocniční zařízení
Doprava	bodový	střední	letální/ neletální	železniční a letecké řídící stanoviště, metro
Informační a komunikační systémy	bodový	střední	letální	centrální pracoviště operátorů
Finanční trh a měna	bodový	malá	letální	banky, burzovní instituce
Nouzové služby	bodový	malá	letální	operační centra IZS
Veřejná správa	bodový	střední	letální/neletální	Ústřední správní orgány

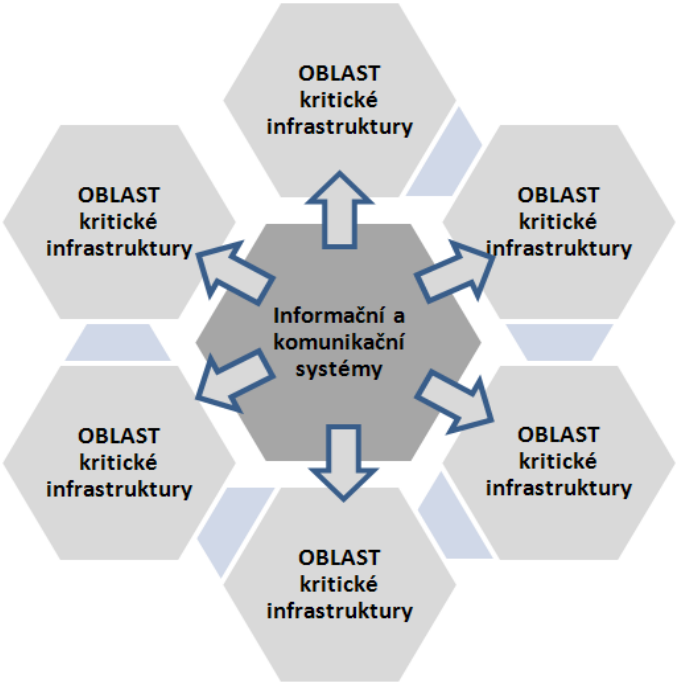
Tab. 1. *Zneužití vysoce toxických látek k napadení kritické infrastruktury. Zdroj: (Dvořák et al., 2016)*

Pokud má dojít k výraznému narušení či dokonce úplnému vyřazení prvku nebo systému kritické infrastruktury, pak útok musí být veden na citlivá místa daného systému a nebo plošně na celý systém. *Do těchto hrozeb patří vyřazení informačních systémů*, dále technologických zařízení s fatálními důsledky jako jsou jaderné elektrárny, popř. i vyřazení či zneschopnění personálu (obyvatelstva).

3.3 Klíčová úloha ICT

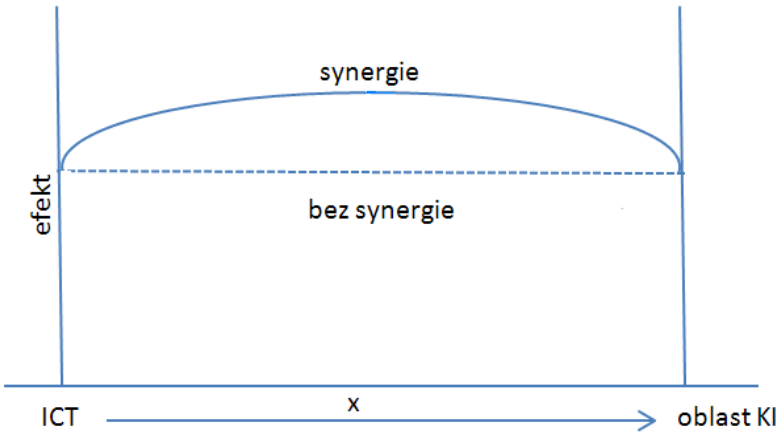
Jestliže v našem zkoumání aplikujeme systémový přístup, je potřeba opustit úhel pohledu typu jedna hrozba, jedna oblast, jeden cíl atd. *Informatika je se svými informačními a znalostními nástroji průřezová, ovlivňující všechny ostatní oblasti* viz Obrázek 2. Současně

platí, že oblasti kritické infrastruktury jsou podsystémy systému celé kritické infrastruktury, kde platí teorie holismu dle (Smuts, 1926), tedy „celek je víc než součet jeho částí“. Dodejme, že i každý prvek kritické infrastruktury lze pokládat za systém – organizační, technický a personální.



Obr. 2. *Postavení ICT v oblastech kritické infrastruktury. Zdroj: Autoři*

Jestliže, jak jsme ukázali v Tabulce 1, napadení informačních a komunikačních systémů je při tradiční analýze lokalizováno pouze v rámci centrálního pracoviště operátorů. Při systémovém pohledu pravděpodobný účinek, tj. *ochromení informační a znalostní podpory nebo havarijní vyřazení systémů bude mít dopady do celého systému ochrany*. Tyto dopady mohu být dalekosáhlé. Je pravděpodobné, že závislost na informačních a komunikačních technologiích při současné jejich dnešní vyspělosti bude v případě takového útoku mít negativní synergické efekty. Rozdíl mezi efektem synergickým a efektem bez synergie je dobře patrná na Obrázek 3.



Obr. 3. *Synergický efekt vztahů ICT a oblastí kritické infrastruktury (KI). Zdroj: Autoři*

Bezpečnost je v odborných kruzích velmi často diskutována v souvislosti s hospodářskými organizacemi a jejich podnikovou informatikou (Helfert et al., 2013). V konsekvencích výkonu veřejné správy jsou *aktivity proti zneužití dat a informací většinou pojímány jako nastavení vhodných technologických podmínek informačních systémů veřejné správy* (Lidinský et al., 2008). *Informační bezpečnost*, zajišťující důvěrnost, integritu a dostupnost informací, *je pouze součástí kybernetické bezpečnosti*.

Pojetí bezpečnosti v námi výše aplikovaném pohledu není v ČR tolik předmětem publikačního zájmu, intenzivněji se jimi zabývá pouze Požár (2015) či Kný (2015). Bohužel nepříznivý posun v bezpečnosti vlivem teroristických útoků a klíčové postavení informatiky v něm nás nutí vidět mnohem více rizik oproti přínosům tak, jak jsme to mohli vidět např. v (Pavlíček et al., 2011) ještě před pár lety. Změna situace a nezbytnost ochrany před systémovými hrozbami se odráží v iniciativách Národního centra kybernetické bezpečnosti, v jejím vymezení prvků *kritické informační infrastruktury* a významných informačních systémů orgánů veřejné moci, jak jsme ukázali v kap. 2.3.

Z pohledu veřejné správy lze na základě výše provedeného zkoumání vyvodit pro ochranu kritické infrastruktury poznání, že mimořádnou pozornost je u krizových plánů třeba věnovat bodům:

- *"Spojení a získávání informací" a*
- *"Informovat nadřízené, podřízené, sousedy a veřejnost".*

Bez tohoto nelze zajistit plnění dalších bodů, jako jsou: promyslet a plánovat varianty řešení krizových jevů, souvisejících s ochranou kritické infrastruktury; být připraven na řešení nejhorší varianty; převzít iniciativu při řešení krizové situace; přijímat opatření proti stupňování a šíření krize; každou krizovou situaci hodnotit z více aspektů; v průběhu krize se zabývat pouze jejím řešením; uznávat zásadu, že krize jsou součástí života a že každou krizi lze řídit. Znamená to také nespoléhat se jednostranně na informační systémy a počítačové sítě.

4 Závěr

Dnešní svět je bez informačních a komunikačních technologií nepředstavitelný a jeho rozvoj bez nich nemyslitelný. Informační a komunikační technologie nejsou ale jen potenciálem růstu, především závislost na nich je zároveň hrozbou pro bezpečnostní prostředí. Z pohledu bezpečnosti je primární fungování kritické infrastruktury.

Článek analyzoval základní souvislosti mezi infomačním rámcem a funkčností systému kritické infrastruktury, zde spojenou zejména s činností veřejné správy. Informační a komunikační systémy byly vymezeny jako jedna z funkčních oblastí činnosti státu, které vyžadují funkčnost kritické infrastruktury. V kontextu s bezpečností byly kybernetické ataky směřující k napadení řídících systémů a informačních systémů prvků kritické infrastruktury identifikovány jako specifická hrozba pro bezpečnost.

Na modelovém případě ochrany kritické infrastruktury před vysoce toxickými látkami byla prokázána nezbytnost systémového přístupu pro holistický pohled na systém ochrany. Snahou bylo zkoumat jevy a procesy komplexně v jejich vnitřních a vnějších souvislostech, vidět celek i jeho části a jejich vztahy při respektování vysokého stupně komplexity problému. Na tomto základě byly informační a komunikační technologie identifikovány jako klíčový prvek a autoři upozornili i na možné synergické efekty při jejich napadení. Vědeckou hypotézu, která byla v článku ověřována a zněla „Informatika je se svými informačními a znalostními nástroji průřezová, ovlivňující synergicky ostatní oblasti kritické infrastruktury", lze považovat za ověřenou.

Závěrečná diskuze vede k tezi pravděpodobného zprostředkovaného dopadu kybernetického útoku do všech dalších oblastí hrozeb. Bezpečnosti informačních a komunikačních systémů musí být proto věnována zvýšená pozornost, ochrana kritické infrastruktury je významným bezpečnostním problémem. Aby byla účinná, je třeba zkoumat všechny druhy potenciálního ohrožení kritické infrastruktury s akcentem na zranitelnost kritické informační infrastruktury a nacházet odpovídající ochranná opatření.

Námi uvedené analýzy, návrhy a komentáře by mohly být základem dalšího zkoumání, komplexního řešení ochrany a kladení si dalších vědeckých hypotéz pro úlohu informačních a komunikačních technologií.

Seznam použité literatury

Antušák, E. (2009). *Krizový management: hrozby - krize - příležitosti*. Praha: Wolters Kluwer ČR.

Balog, K. et al. (2007). *Základy toxikologie*. Ostrava: Kleinwachter.

Bartlová, I. (2005). *Nebezpečné látky*. Ostrava: Kleinwachter.

Dvořák, A., Lisa, A., Mildeová, S., & Zahradníček, P. (2016). Critical Infrastructure Protection: Systems and Information Framework of the Czech Republic. In P. Doucek, G. Chroust, V.C. Oškrdal (Eds.), *Proceedings of the 24th Interdisciplinary Information Management Talks,* (pp. 115-122). Linz: Trauner Verlag.

EUR-Lex. (2009). Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection. Retrieved from http://eur-lex.europa.eu/legal-content/CS/TXT/?uri=uriserv%3Ajl0013

Hadrabová, A. (2008). *Veřejná správa životního prostředí I*. Praha: Oeconomica.

Hančlová, J., Doucek, P., Fischer, J. & Vltavská, K. (2015). Does ICT capital affect economic growth in the EU-15 and EU-12 countries? *Journal of Business Economics and Management*, 16(2), 387-406. DOI: 10.3846/16111699.2012.754375

Helfert, M., Doucek, P. & Maryška, M. (2013). The "Enterprise Architect" – A new Approach to Business Informatics Management. *Quality Innovation Prosperity*, 17(1), 67-87. doi: 10.12776/qip.v17i1.171

Horák, R. et al. (2015). *Zásady ochrany společnosti*. Ostrava: KEY Publishing.

Juříček, L. & Rožňák, P. (2014). *Bezpečnost, hrozby a rizika v 21. století*. Ostrava: KEY Publishing.

Kolektiv autorů. (2015). *Bezpečnostní strategie České republiky 2015*. Praha: Ministerstvo zahraničních věcí České republiky.

Kný, M. (2015). Bezpečnostní management – systémový přístup. *Acta Informatica Pragensia*, 4(3), 326-335. doi: 10.18267/j.aip.79

Kritická informační infrastruktura. (2014). Národní centrum kybernetické bezpečnosti. Retrieved from https://www.govcert.cz/download/kii-vis/container-nodeid-663/2schemakii-cz.pdf

Lidinský, V. et al. (2008). *eGovernment bezpečně*. Praha: Grada Publishing.

Národní centrum kybernetické bezpečnosti. (2014). Legislativa. Retrieved from https://www.govcert.cz/cs/legislativa/legislativa/

NVČR. (2014). Nařízení vlády č. 315 ze dne 8. prosince 2014, kterým se mění nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury. Retrieved from http://docplayer.cz/1290580-315-2014-sb-narizeni-vlady.html

Pavlíček, A., Kačín, R., Sigmund, T. & Hubáček, J. (2011). The Position of ICT Sector in the National Economy of Czech Republic. In P. Doucek, G. Chroust, V.C. Oškrdal (Eds.), *Proceedings of the 19th Interdisciplinary Information Management Talks,* (pp.147-156). Linz: Trauner Verlag.

Požár, J. (2015). Vybrané trendy kybernetické kriminality. *Acta Informatica Pragensia*, 4(3), 336-348. doi: 10.18267/j.aip.80

Smuts, J. (1926). *Holism and Evolution*. New York: Macmillan.

SZČR. (2010). Nařízení vlády č. 432 ze dne 22. prosince 2010 o kritériích pro určení prvku kritické infrastruktury. In *Sbírka zákonů České republiky*, částka 73, p. 3461.

SZČR. (2000). Zákon č. 240 ze dne 28. června 2000 o krizovém řízení a o změně některých zákonů (krizový zákon). In *Sbírka zákonů České republiky*, částka 73, p. 3475.

Veber, J. & Smutny, Z. (2015). Standard ISO 27037:2012 and Collection of Digital Evidence: Experience in the Czech Republic. In *Proceedings of the 14th European Conference on Cyber Warfare and Security,* (pp. 294-299). Reading: ACPI.

Zahradníček, P. (2015) Kritická infrastruktura státu a její ochrana před vysoce toxickými látkami. In *Historie a současnost chemických zbraní – vědecko-odborná konference ke 100. výročí použití chemických zbraní*, (pp. 254-262). Uherské Hradiště: UTB/FLKŘ.

Zahradníček, P. (2016) Aktivní záloha AČR jako součást systému zajištění bezpečnosti regionu. In *Bezpečnost regionů – 9. mezinárodní vědecká konfer*ence, (pp. 356-376). Brno: VŠKE.