FAKULTA POLITICKÝCH VIED A MEDZINÁRODNÝCH VZŤAHOV
UNIVERZITA MATEJA BELA V BANSKEJ BYSTRICI

Karol Fabián, Michaela Melková

VYBRANÉ OTÁZKY KYBERNETICKEJ BEZPEČNOSTI

ISBN 978-80-557-1205-5

2016

BELIANUM

Univerzita Mateja Bela
Fakulta politických vied a medzinárodných vzťahov

VYBRANÉ OTÁZKY KYBERNETICKEJ BEZPEČNOSTI

Karol FABIÁN
Michaela MELKOVÁ

Učebné texty

BELIANUM

2016
Banská Bystrica

Autori:
© doc. Ing. Karol FABIÁN, CSc.
Mgr. Michaela MELKOVÁ

Názov:
Vybrané otázky kybernetickej bezpečnosti

Vydavateľ:
Belianum – Vydavateľstvo Univerzity Mateja Bela v Banskej Bystrici
Fakulta politických vied a medzinárodných vzťahov

Recenzenti:
prof. Ing. Pavel NEČAS, PhD.
JUDr. Miroslav BRVNIŠŤAN, PhD.
PhDr. Peter BÁTOR, PhD.

ISBN 978-80-557-1205-5

PREDSLOV

Ľudská spoločnosť je charakteristická snahou o neustále napredovanie, či už sa jedná o politickú, ekonomickú, sociálnu alebo technologickú oblasť. Avšak v posledných dekádach rokov pozorujeme, že práve technológie a nové inovatívne myšlienky majú obrovský vplyv nie len na samotnú populáciu, ale aj na aktérov medzinárodného systému. Digitálna éra so sebou prináša neopísateľné výhody, možnosť rýchlejšej komunikácie a výmeny informácii, ale na druhej strane nelimitovaná kybernetická sféra vytvára priestor pre vznik nových asymetrických hrozieb. Už nestačí, aby sa štáty i medzinárodné organizácie sústredili pri tvorbe svojich obranných stratégií len na fyzické domény, pretože kybernetický priestor je ohniskom nových a doposiaľ neobjavených bezpečnostných neistôt.

Kybernetická sféra do značnej miery ovplyvnila a zmenila doterajšie chápanie národnej i medzinárodnej bezpečnosti. Zároveň prispela k transformácii postavenia štátov i neštátnych aktérov, pretože vznikli nové skutočnosti, ktoré doposiaľ vo fyzických doménach neexistovali alebo nemali opodstatnenie. Jeden z najvýraznejších faktorov je samotná povaha kybernetického priestoru, ktorý nie je ničím limitovaný a národné hranice štátov v ňom nemajú význam. To znamená, že úspech ovládnutia kybernetickej domény jednou mocnosťou je takmer nulový. Zároveň ani veľkosť teritória a kapacitná prevaha nezohráva v spomínanom priestore skoro žiadnu rolu, pričom malé štáty majú väčšiu pravdepodobnosť úspechu a presadenia svojich národných záujmov a cieľov prostredníctvom využitia kybernetických nástrojov ako vo fyzickej sfére. Zároveň môžeme tvrdiť, že kybernetické útoky sú efektívnejšie, pretože útočníci pôsobia anonymne, preberajú digitálnu podobu a dokážu bez použitia vojenskej sily ohroziť stabilitu, rozvoj, infraštruktúru alebo bezpečnosť štátu či organizácie. Súčasne ovplyvňovanie demokratických volieb v štátoch záujmovými skupinami či mocnosťami prostredníctvom kybernetických aktivít vidíme v priamom prenose.

Hoci sa problematika kybernetickej bezpečnosti v súčasnosti stáva čoraz viac diskutovanou témou v zahraničí aj doma, tak v podmienkach Slovenskej republiky ešte neexistuje ucelená publikácia zameraná na primárne otázky späté s bezpečnosťou štátov v kontexte kybernetického priestoru. Naša práca má preto ambíciu slúžiť ako základná poznatková báza pre verejnosť i akademickú obec a to hlavne

pri štúdiu kybernetickej bezpečnosti v rámci odborov bezpečnostných štúdií, obrany i bezpečnostného manažérstva.

Publikácia pozostáva z ôsmich hlavných kapitol a prílohy. Skúmanie kybernetickej bezpečnosti v sebe zosobňuje potrebu osvojenia si multidisciplinárnych poznatkov z oblasti medzinárodných vzťahov i informačných a komunikačných technológií. Prvá kapitola sa preto zameriava na vymedzenie základných teoretických východísk a zároveň ponúka definície primárnych pojmov využívaných v oblasti informačných technológií. V rámci druhej kapitoly sa zameriavame následne na charakteristiku hlavných kybernetických hrozieb a v tretej kapitole definujeme aktérov kybernetického priestoru, s dôrazom na neštátnych aktérov. Štvrtá kapitola sa venuje analýze vybraných kybernetických incidentov so snahou určiť ich pôvod prostredníctvom definovania záujmov a cieľov možných aktérov. Zároveň vychádza aj zo vzájomných medzinárodných vzťahov a vtedajšieho rozpoloženia medzinárodného systému. Ďalšia kapitola sa zaoberá analýzou najznámejších malvérov vyžitých pri kybernetických incidentoch, definuje ich dopady, porovnáva ich navzájom a aj s konvenčnými i jadrovými zbraňami. Šiesta kapitola vymedzuje aktivity, ktoré podnikajú vybraní aktéri medzinárodného systému na nové výzvy kybernetického priestoru, vrátane Slovenskej republiky. Kapitoly 1 - 6 sú súčasťou čiastočného výskumu dizertačnej práce Michaely Melkovej s názvom Význam kybernetickej bezpečnosti v kontexte národnej a medzinárodnej bezpečnosti.

Praktickými možnosťami obrany a ochrany jednotlivcov, korporácií a štátov v kybernetickom priestore sa zaoberajú ďalšie kapitoly v tejto publikácii vrátane prílohy, ktorých autorom je Karol Fabián. V siedmej kapitole uvádzame konkrétne nástroje a rozoberáme možnosti ochrany pred kybernetickými útokmi. Ukazuje sa, že ochrana jednotlivca aj organizácie pred útokom z vnútra inštitúcie zasluhuje zvýšenú pozornosť, keďže tento typ útoku spôsobuje najväčšie škody. Vo štvorvrstvom modeli kybernetickej bezpečnosti popíšeme jednotlivé komponenty ochrany a ich funkciu. Posledná kapitola sa venuje detailnejšie popisu šifrovania informácií a elektronickému podpisovaniu dokumentov. V súčasnosti tieto funkcie tvoria základnú možnosť ochrany údajov každého používateľa informačnej diaľnice – Internetu.

Koniec každej kapitoly pozostáva z niekoľkých otázok, ktoré slúžia čitateľovi na zopakovanie najdôležitejších poznatkov a na vlastné zhrnutie danej problematiky. Zároveň v prílohe skrípt ponúkame

základné cvičenia pre plné zvládnutie elektronického podpisu s občianskym preukazom, tak ako sú súčasťou predmetu Kybernetická bezpečnosť na FPVaMV UMB. Zvládnutie techniky elektronického podpisu je základným predpokladom informatizácie našej spoločnosti a umožňuje prístup k službám na portáli štátnej správy, portáli finančnej správy a onedlho na portáli ministerstva zdravotníctva.

Nový rozmer kybernetickej bezpečnosti do budúcnosti zrejme zohrá "nová" technológia úschovy informácií vo forme reťazcov blokov, distribuovaných a replikovaných na tisícoch až miliónoch počítačov na Internete, vzájomne previazaných a prípadne aj šifrovaných. Technológiu blockchainu zaviedol v r. 2008 dokonalý matematický aparát, ktorým bola definovaná kryptomena Bitcoin dodnes neznámym autorom Satoshi Nakamotom. Najvýznamnejšie svetové IT firmy sa touto technológiou už intenzívne zaoberajú a prvé produkty a služby už majú v ponuke. Úspešnému hromadnému nasadeniu tejto technológie v bankách a všeobecne v cloudoch najväčších prevádzkovateľov však zatiaľ bráni obrovská výpočtová náročnosť tejto revolučnej technológie úschovy a spracovania informácií. Najmä jej nasadenie do cloudových riešení v budúcnosti podľa autorov dramaticky zvýši kybernetickú bezpečnosť na informačnej diaľnici - Internete a predstavuje novú nádej pre bezpečný kybernetický priestor dnes plný pokročilých hrozieb, ktoré nás už všetkých ohrozujú, alebo ešte len čakajú na vhodný čas úderu.

Dúfame, že predmetná publikácia obohatí čitateľa o nové poznatky, vytvorí mu obraz prepojenosti technologického rozvoja s výkonom politiky i medzinárodnými vzťahmi a otvorí mu nové obzory v oblasti kybernetickej bezpečnosti.

Autori

OBSAH

1 ZÁKLADNÉ TEORETICKÉ VÝCHODISKÁ

Pokiaľ chceme bližšie skúmať problematiku kybernetickej bezpečnosti, tak je potrebné definovať primárne pojmy a terminologický aparát využívaný v tejto oblasti. Aj napriek faktu, že terminológia využívaná na charakterizáciu skutočností odohrávajúcich sa v kybernetickej sfére je súčasťou vládnych vyhlásení či dokumentov medzinárodných organizácií, tak v súčasnosti neexistujú ustálené a spoločné definície špecifikujúce kybernetické javy. Samotná terminológia je v niektorých prípadoch nejednotná, diferencovaná a niekedy sa odborníci v rámci terminologického vymedzenia nevedia zhodnúť vôbec.

1.1 KYBERNETICKÝ PRIESTOR

Na rozdiel od väčšiny počítačovej terminológie, charakteristickej jasnými a štandardnými definíciami, pre pojem kybernetický priestor absentuje jednoznačné a jednotné vymedzenie. Prvý krát použil slovo kybernetický priestor spisovateľ **William Gibson** v roku 1982, ale popularitu získal až v roku 1984, kedy bol spomenutý v rámci publikácie *Neuromancer*. Samotný kybernetický priestor opisuje ako *„konsenzuálne halucinácie, ktoré denne pociťujú miliardy oprávnených operátorov i deti všetkých národov, ktoré sa učia matematické koncepty .. grafická reprezentácia dát abstrahovaných z každého počítača ľudského systému. Nepredstaviteľná komplexnosť. Línie svetla zoradené v nepriestore mysle, zhluky a súhvezdia dát. Ako svetlá mesta, ustupujúce..“* (Gibson, 1986). V súčasnosti sa pojem kybernetický priestor využíva sa na opis virtuálneho sveta tvoreného počítačmi, pričom kreáciou internetu kybernetický priestor expandoval na úroveň globálnej počítačovej siete. Na doplnenie ponúkame niekoľko definícií:

- Podľa výkladového slovníka pre kybernetickú bezpečnosť je kybernetický priestor *„digitálne prostredie umožňujúce vznik, spracovanie a výmenu informácií, tvorené informačnými systémami a službami a sieťami elektronických komunikácií“* (Jirásek - Novák - Požár, 2013, s. 60).
- Medzinárodná organizácia pre štandardizáciu definuje kybernetický priestor v širšom ponímaní ako *„komplexné prostredie, ktoré je výsledkom interakcie ľudí, softvéru a služieb na internete prostredníctvom technologických zariadení a sietí, ku ktorým sú pripojené a ktoré neexistujú vo fyzickej podobe“* (ISO, 2012, s. 2).

- Skupina expertov na kybernetické záležitosti vníma kybernetický priestor ako *„globálnu doménu, tvoriacu súčasť informačného prostredia, ktorého odlišujúci a unikátny charakter je určený použitím elektronického a elektromagnetického spektra na vytváranie, ukladanie, modifikovanie, výmenu a získavanie informácií využitím vzájomne prepojených a previazaných sietí, využívajúcich IKT“* (Kramer et al, 2009, s. 26)

Dlhú dobu ľudstvo využívalo iba dve domény priestoru - zem a more. Rozvojom technológií ľudstvo dokázalo ovládnuť neskôr vzdušný a následne kozmický priestor v priebehu 20. storočia. Približne pred dvoma dekádami k týmto štyrom doménam pribudla aj piata, a síce kybernetická, ktorá bola v rámci varšavského samitu NATO v júli 2016 oficiálne deklarovaná ako piata operačná doména fungovania štátnych a neštátnych aktérov v čase mieru i vojny. Svojou existenciou kybernetický priestor ovplyvňuje medzinárodné právo i legislatívu štátov, a preto má uznanie kybernetickej sféry za ďalšiu operačnú doménu veľký vplyv na kreáciu nových doktrín a spôsoby zabezpečenia národnej a medzinárodnej bezpečnosti.

Kybernetický priestor sa nie vždy musí spájať výhradne s internetom nakoľko môže predstavovať i komunikáciu medzi počítačmi navzájom. V tomto prípade môžeme za kybernetické riziko považovať aj USB kľúč obsahujúci škodlivý vírus a umožňujúci hackerovi stiahnuť duševné vlastníctvo tej ktorej organizácie. Na rozdiel od predošlých sfér (zem, more, vzduch a vesmír) však kybernetická dimenzia funguje prevažne vo virtuálnej rovine. Hoci potrebujeme fyzické zariadenia ako káble, hardvér či iné vybavenie, tak samotný kybernetický svet nedokážeme vidieť ani uchopiť bez pomoci technológie. Unikátnosť kyberpriestoru podľa **Daniela Kuehla** spočíva najmä v 4 aspektoch (Kuehl, 2009):

1. v operatívnosti: využívanie technológií za konkrétnym účelom. Na prvý pohľad sa toto hľadisko neodlišuje od ostatných fyzických domén, rozdiel však spočíva vo využívaní informácií, ktoré sú v digitálnej podobe. Každý deň sa napríklad prostredníctvom kybernetického priestoru na svetovej burze preinvestujú bilióny amerických dolárov. Rovnako, ani tvorcovia stratégií politických kandidátov nemôžu ignorovať kybernetický priestor, pretože správne jeho využitie môže viesť k víťazstvu počas volebného obdobia;

2. v nutnosti použiť elektronické alebo elektromagnetické technológie pre vstup do kybernetického priestoru. Práve tu môžeme vidieť, že fyzické charakteristiky vzájomne odlišujú jednotlivé domény;
3. v špecifickom zámere: vytváranie, ukladanie, modifikovanie, vymieňanie a získavanie informácií s využitím elektronických technológií, čím sme nahradili snahu plaviť sa na moriach alebo obliehať zem. Autor v tomto bode zdôrazňuje enormnú rýchlosť rozširovania kybernetického priestoru a nové spôsoby využívania technológií;
4. prepájanie vzájomne závislých sietí využívaním informačno-komunikačných technológií.

Jadro kybernetického priestoru je tvorené globálnou internetovou sieťou prepájajúcou celý svet. Spomínaná sieť pozostáva zo štyroch základných sfér, pričom fungovanie internetu a ostatných telekomunikačných nástrojov zabezpečujú primárne prvé dve vrstvy (Clark - Choucri, 2012):

- ***fyzické základy internetu*** - počnúc optickými káblami, mobilnými vežami a končiac osobnými počítačmi a servermi.
- ***logistické vrstvy*** - internetové protokoly, World Wide Web (www.), prehliadače, domény, webové stránky a softvéry, ktoré využívajú fyzické základy internetu.
- ***informačná vrstva*** - zakódovaný text, fotky, videá a iný materiál, ktorý je uložený, prenášaný a transformovaný v rámci kybernetického priestoru.
- ***používateľa*** - ľudia a klientela, ktorá formuje samotnú povahu kybernetického priestoru v rámci svojej komunikácie, rozhodovania, vykonávania plánov a práce s informáciami.

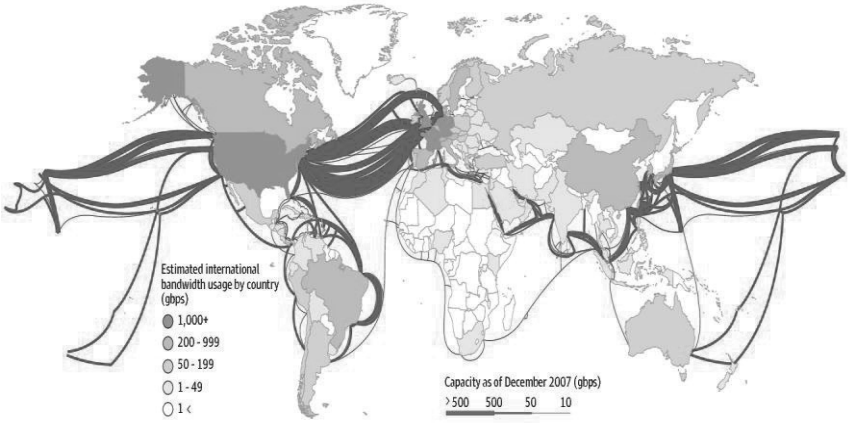
Ako sme už spomínali vyššie, kruciálnym aspektom fungovania internetových sietí je fyzická zložka. Väčšina svetových telekomunikačných nástrojov však nie je poprepájaná satelitmi, ale trans-oceánskymi optickými káblami nachádzajúcimi sa na dne svetových oceánov[1].

Káble slúžia na prepravu elektrickej energie, prenos hlasu a v neposlednom rade prenos dát medzi kontinentmi. Mapu znázorňujúcu optické siete môžete vidieť na Obrázku 1. Najdlhším podmorským systémom káblov je

[1] Veľmi zaujímavou publikáciou v tejto oblasti je dielo autorov Roba Kitchina a Martina Dodgea s názvom Atlas of Cyberspace, ktorý znázorňuje fyzickú štruktúru telekomunikačných sietí na celej mape sveta .

SeaMeWe-3 ťahajúci sa od Nordenu v Nemecku do Geoje v Južnej Kórei, ktorý spája 32 štátov s 39 prístavnými bodmi. Jeho výsledná dlážka je 39 tisíc kilometrov (Obrázok 2).

Obrázok 1: Mapa trans-oceánskych optických káblov.



Zdroj: Guardian, 2008.

Obrázok 2: Systém káblov SeaMeWe-3.

Zdroj: SEA-ME-WE3, 2016.