Univerzita Hradec Králové
Filozofická fakulta
Katedra politologie

Analýza veřejné politiky a kybernetická bezpečnost v zemích Latinské Ameriky

Diplomová práce

Autor: Bc. Barbora Švábová
Studijní program: N6701 Politologie
Studijní obor: 6701T022 Politologie-latinskoamerická studia
Forma studia: Prezenční

Vedoucí práce: Mgr. Karel Kouba M.A., Ph.D.

Hradec Králové, 2020

Univerzita Hradec Králové
Filozofická fakulta

Zadání diplomové práce

Autor: **Barbora Švábová**

Studium: F17NP0053

Studijní program: N6701 Politologie

Studijní obor: Politologie - latinskoamerická studia

Název diplomové práce: **Analýza veřejné politiky a kybernetická bezpečnost v zemích Latinské Ameriky**

Název diplomové práce AJ: Analysis of public policy and cybersecurity in Latin America

Cíl, metody, literatura, předpoklady:

Informační technologie se staly nedílou součástí moderního světa. Zatímco závislost dnešní společnosti na digitální infrastruktuře roste, samotné technologie se stávají stále méně bezpečnými. Státy proto musí vytvářet nové národní bezpečnostní strategie, aby jejich prostřednictvím reagovaly na neustále se zvyšující kybernetické hrozby. Implementace nových pravidel, zákonů a opatření je hlavním cílem každé z politik. Mají za úkol společnost ochránit a podpořit hospodářskou a sociální prosperitu. Jejich pravidelné hodnocení je důležitou součástí analýzy národní bezpečnosti, proto aby byly schopny reagovat na nově vzniklá ohrožení. Diplomová práce je zaměřená na analýzu úspěšnosti nově zavedených strategií a z nich vycházejících opatření národních politik v latinskoamerických státech. Analytická část práce bude provedena na případových studiích Mexika, Chile a Kolumbie. Ve všech vybraných státech existují aktivní programy na ochranu kybernetického prostoru. Zkoumané země se inspirují strategiemi ostatních světových politik. Cílem práce je zjistit, jak jsou zavedené strategie funkční ve sledovaných zemích a jak jsou schopny ovlivnit jejich národní bezpečnost. Postupem bude výzkum oficiálních vládních dokmentů, věnujících se zavedeným strategiím.

1. VESELÝ, Arnošt a NEKOLA, Martin (eds.). 2007. Analýza veřejných politik. Praha: Sociologické nakladatelství. 2. POTŮČEK, Martin a kol. 2006. Veřejná politika. Praha: SLON. 3. McKinsey&Company. 2018. Perspectiva de ciberseguridad en México. México. 4. KOVÁŘOVÁ, Pavla. 2010. Role bezpečnosti v rámci informační gramotnosti. ProInflow: Časopis pro informační vědy. 5. Comité Interministerial sobre Ciberseguridad. 2017. Política Nacional de Ciberseguridad. Chile. 7. HRŮZA, Petr. 2012. Kybernetická bezpečnost. Brno: Univerzita obrany, Fakulta ekonomiky a managementu. 8. JIRÁSEK, Petr, NOVÁK, Luděk, POŽÁR, Josef. 2012. Výkladov slovník kybernetické bezpečnosti. Policejní akademia ČR v Praze a Česká pobočka AFCEA 9. International Telecommunication Union. 2018. Guide to Developing a National Cybersecurity Strategy. ITU. 10. International Telecommunication Union. 2018. Global Cybersecurity Index (GCI). ITU.

Garantující pracoviště: Katedra politologie, Filozofická fakulta

Vedoucí práce: Mgr. Karel Kouba, Ph.D., M.A.

Datum zadání závěrečné práce: 29.4.2019

Prohlášení

Prohlašuji, že jsem tuto diplomovou práci vypracovala (pod vedením vedoucího diplomové práce) samostatně a uvedla jsem všechny použité prameny a literaturu.

V Hradci Králové dne

Anotace

Švábová, B. (2020). Analýza veřejné politiky a kybernetická bezpečnost v zemích Latinské Ameriky. Hradec Králové: Filozofická fakulta Univerzity Hradec Králové, 87 s.

Informační technologie se staly nedílnou součástí moderního světa. Zatímco závislost dnešní společnosti na digitální infrastruktuře roste, samotné technologie se stávají stále méně bezpečnými. Státy proto musí vytvářet nové národní bezpečnostní strategie, aby jejich prostřednictvím reagovaly na neustále se zvyšující kybernetické hrozby. Implementace nových pravidel, zákonů a opatření je hlavním cílem každé z politik. Mají za úkol společnost ochránit a podpořit hospodářskou a sociální prosperitu. Jejich pravidelné hodnocení je důležitou součástí analýzy národní bezpečnosti, proto aby byly schopny reagovat na nově vzniklá ohrožení. Diplomová práce je zaměřená na analýzu úspěšnosti nově zavedených strategií a z nich vycházejících opatření národních politik v latinskoamerických státech. Analytická část práce bude provedena na případových studiích Mexika, Chile a Kolumbie. Ve všech vybraných státech existují aktivní programy na ochranu kybernetického prostoru. Zkoumané země se inspirují strategiemi ostatních světových politik. Cílem práce je zjistit, jak jsou zavedené strategie funkční ve sledovaných zemích a jak jsou schopny ovlivnit jejich národní bezpečnost. Postupem bude výzkum oficiálních vládních dokumentů, věnujících se zavedeným strategiím.

Klíčová slova: kybernetická bezpečnost, veřejná politika, latinská amerika, technologie

Annotation

Švábová, B. (2020). Analysis of public policy and cyber security in countries of Latin America. Hradec Králové: Faculty of Arts, University of Hradec Králové, 87 pp. Diploma Dissertation Thesis.

Information technology has become an integral part of the modern world. While the dependence of today's society on the digital infrastructure is increasing, technology itself is becoming less and less secure. States must therefore develop new national security strategies to respond to ever-increasing cyber threats. The implementation of new rules, laws and measures is the main objective of each policy. Their mission is to protect society and promote economic and social prosperity. Their regular assessment is an important part of national security analysis in order to be able to respond to emerging threats. The thesis is focused on the analysis of the success of the newly introduced strategies and the resulting national policy measures in Latin American states. The analytical part of the thesis will be performed on case studies of Mexico, Chile and Colombia. There are active programs to protect cyberspace in all selected countries. The countries surveyed are inspired by the strategies of other world policies. The aim of this work is to find out how the established strategies are functional in the countries under review and how they are able to influence their national security. The procedure will be research of official government documents dealing with established strategies.

Keywords: cybersecurity, public policy, latin america, technology

Obsah

Seznam použitých zkratek

AMECI	Asociación Mexicana de Ciberseguridad
ANSI	Agencia Nacional de Seguridad de la Información
CCOC	Centro Cibernético Political
CCIT	Cámara Colombiana de Informática y Telecomunicaciones
CCPS	La Comisión de Prevención del Delito y Justicia Penal
CEG	El Grupo de Expertos Gubernamentales
CEPAL	Comisión Económica para América Latina y el Caribe
CERT	Computer Energy Response Team
CICS	Comité Interministerial sobre Ciberseguridad
CICTE	El Comité Interoamericano contra el Terrorismo
CIDGE	Comisión Intersecretarial para el Desarrollo del Gobierno Económico
CSI	Coordinación de Seguridad de la Información
CSIRT	Computer Security Incident Response
eLAC	Agenda Digital para América Latina y el Caribe
EU	Evropská unie
FIRST	Forum of Incident Response and Security Team
GCA	Global Cybersecurity Area
GCI	Global Cybersecurity Index
IGF	Internet Governance Forum
INACAP	Universidad Tecnológica de Chile
ISACA	Sistemas de Información de Auditoría y Control
ITESO	Ingeniería en Seguridad Informática y Redes
ITU	International Telecommunication Union
MINDEF	Ministerio de Defensa Nacional
MISP	Ministerio del Interior y Seguridad Política
MINTIC	Ministerio de Tecnologías de la Información y las Comunicaciones

NCSI	National Cybersecurity Index
NCSC	Národní centrum kybernetické bezpečnosti
OAS	Organizace amerických států
OCDE	Organización para la Cooperación y Desarrollo Económico
ORBA	Observatoio Regional de Banda Ancha
OSN	Organizace Spojených národů
PDI	Polícia de Investigaciones de Chile
PNCS	Política Nacional de Ciberseguridad
SSPC	Secretaría de Seguridad y Protección Ciudadana
WSIS	World Summit of the Information Society

Úvod

Informační technologie se staly důležitou součástí moderního světa. Dnešní společnost je neodlučitelně spjata s užíváním technologií všeho druhu v každodenním životě a její závislost na digitální infrastruktuře neustále roste. Ochrana kybernetického prostoru je velice důležitou otázkou nejen pro společnost a firmy, ale hlavně pro politiku daných států. Proto je tato práce zaměřena na popis implementace strategií kybernetické bezpečnosti ve veřejné politice vybraných států Chile, Kolumbie a Mexika, z čehož vyplývá i hlavní cíl práce, kterým je evaluace úspěšnosti aktuálně zavedených strategií kybernetické bezpečnosti pomocí SWOT analýzy.

I když moderní technologie podporují hospodářskou a sociální prosperitu, bezpečnost států je stále více v ohrožení. S rozvojem technologie a jejího uživatelského rozhraní čelí dnes kybernetický prostor nebezpečí zneužití, které se země snaží zmírňovat nejrůznějšími druhy národních strategií, které mají za úkol proti těmto ohrožením a útokům bojovat, případně (u rozvinutějších strategií) sloužit jako prevence.

V posledních letech se vyvinula široká mezinárodní diskuse o kybernetické bezpečnosti, která odráží potřebu národů reagovat na znepokojující trendy a posiluje stabilitu a bezpečnost globálních kybernetických zdrojů. Národní strategie kybernetické bezpečnosti jednotlivých zemí závisí hlavně na jejich cílech a celkové připravenosti v tomto oboru. Z mezinárodního hlediska tedy není možné určit jednoznačný popis tohoto procesu, nicméně by se mělo jednat o program a iniciativy, jejichž prostřednictvím země chrání svou národní kybernetickou infrastrukturu a zvyšuje tak svou bezpečnost a odolnost. (ITU, 2018)

Vyhodnocování kybernetických útoků a jejich posuzování z právního, ale také politického hlediska je nutné provádět na bázi mezinárodní integrace. Boj s kybernetickou kriminalitou je mnohdy ztížen její nemateriální podstatou. Činy jsou geograficky velmi rozsáhlé a útočníci mnohdy ani nemusí pocházet či žít v

dané zemi, kterou ohrožují. To souvisí hlavně s anonymitou pachatelů, prostředím bez přesně definovaných geografických hranic a časově nestálými digitálními stopami. (Hromada, 2015, s. 78)

V praxi vytváření strategií funguje skrze mezinárodní fóra a konference, kde jsou přejaty již osvědčené strategie partnerských zemí a použity v zemích, které dosud tyto možnosti nevyužívaly. Zde nastupuje důležitost evaluace těchto strategií: ty jsou po určitém čase hodnoceny, aby bylo jasné, jaké změny musí být v konkrétních případech daných zemí použity. Jak bylo již v této práci uvedeno, každá země si tvoří strategie tak, aby odpovídaly nárokům dané politiky.

Hlavním cílem této diplomové práce je zhodnotit nejaktuálnější verze národních strategií kybernetické bezpečnosti z pohledu zadaných indikátorů u zemí Kolumbie, Mexika a Chile. Práce se zabývá nejen popisem implementace samotné národní strategie do veřejné politiky, ale poskytuje také ucelený pohled na jednotlivé části veřejné politiky, které bylo nutno aktualizovat, vytvořit či změnit. Cíl práce vyplývá z její analytické části, kterou hodnotím skrze získané informace s ohledem na předem stanovené cíle jednotlivých strategií.

Veřejná politika je politika, která směřuje k naplnění cílů, které jsou chápány (resp. deklarovány) jako cíle celé společnosti, tedy směřuje uspokojení „společenských“ potřeb. (Malý & Pavlík, 2004, s. 5) V práci se zabývám danou problematikou z pohledu politického, institucionálního, ale také legislativního. Zkoumám spolupráci na mezinárodní úrovni a vývoj kybernetické bezpečnosti v latinskoamerických státech, který přispívá k posílení bezpečnosti v digitálním světě. Závěrečná evaluace bude probíhat skrze hodnocení jednotlivých indikátorů, které byly zkoumány v práci, a následné zhodnocení situace s přihlédnutím k předem stanoveným cílům v originálních textech jednotlivých strategií.

Jak už bylo zmíněno výše, práce je rozdělena na jednotlivé indikátory kybernetické bezpečnosti, díky kterým bude možné přehledněji a jednodušeji zkoumat úspěšnost implementovaných národních strategií ve sledovaných zemích

a následně je hodnotit. Indikátory se věnují hlavně rozvoji dané politiky věnující se problematice kybernetické bezpečnosti, vzdělávání a obecnému povědomí o této problematice, což je z hlediska budoucího rozvoje bezpečnosti a jejího zlepšování důležitou součástí implementace, a také zapojení státu do mezinárodního dění okolo kybernetické bezpečnosti.

V této práci se zabývám zkoumáním a hodnocením kybernetické bezpečnosti v následujících třech latinskoamerických zemích: Mexiku, Chile a Kolumbii. Země byly vybrány jako zástupci latinskoamerického regionu tak, aby jejich výběr geograficky zahrnoval jak část Severní, tak také Jižní Ameriky. Kromě toho, že státy již dlouhodobě využívají určitou formu národní strategie pro kybernetickou bezpečnost, což byl hlavní důvod pro jejich výběr, jsou také ekonomicky velmi rozvinutými státy v tomto regionu. Společně jsou Mexiko, Chile a Kolumbie státy, které figurují na seznamu kybernetických útoku v červených číslech. Čím vyšší je užívání technologie v daném státu, tím vyšší je také nebezpečí, které s sebou tyto technologie přináší.

Hlavní indikátory kybernetické bezpečnosti

U každé z vybraných zemí sleduji, zda splňují (a na jaké úrovni) níže určené indikátory. Výběr indikátorů vznikl na základě nejčastěji zmiňovaných odvětví, ale také cílů v jednotlivých oficiálních textech národních strategií a také v rozdělení evaluace *National Cybersecurity Index*. Indikátory byly vybrány tak, aby pokryly veškerou hlavní problematiku, která při vytváření a implementaci politiky a cílů strategie vznikala, a to s ohledem na konečné hodnocení, které je zároveň cílem celé diplomové práce.

Indikátor č. 1: rozvoj politiky státu v rámci kyberbezpečnosti

Zkoumám, „nakolik mají ústřední vládní subjekty (ministerstvo nebo jednotlivci) specializovaného úředníka nebo jednotku odpovědnou za rozvoj národní politiky kybernetické bezpečnosti.“ (NCSI, 2019) Cílem tohoto indikátoru

je určit a definovat nejnovější národní strategii, která byla vytvořena ve veřejné politice daného státu, popsat taktéž jeho historii a předchůdce, případně jiné legislativní zdroje, ze kterých tato strategie vznikla. Dále je důležitou součástí této části popis institucionálních a legislativních změn, které společně s národní strategií vznikly v politice sledovaného státu a způsob, jakým budou její další fungování ovlivňovat.

V rámci opatření kybernetické bezpečnosti byly v zemích zavedeny nové odbory, ministerstva a příslušná nová pracovní místa, která se touto problematikou aktivně zabývají. Jak tvrdí Petr Hrůza ve své knize o kybernetické bezpečnosti: „zajištění kybernetické bezpečnosti státu je jednou z klíčových aktivit každého státu.“ (Hrůza, 2012, s. 65). Proto je potřebné, aby každý stát, věnující se problematice kybernetické bezpečnosti, také dostatečně hleděl na informovanost o tomto tématu. Vláda by tedy měla počítat s výborem, radou či pracovní skupinou apod., která je schopná koordinovat politiku kybernetické bezpečnosti státu nejen na národní, ale především na mezinárodní úrovni. Výsledkem těchto opatření je vládou schválená a vypracovaná národní strategie, která je použita na vnitrostátní úrovni, či další dokumenty, které jsou schopny takto zajišťovat bezpečnost ve státě.

Je důležité si uvědomit, že telekomunikační sítě a otevírání systému představují problémy s počítačovou bezpečností, které je aktuálně velmi obtížné kontrolovat, a mohou mít kritické důsledky a dopady na fungování a organizaci států. Úspěch ekonomiky státu závisí na schopnosti řídit bezpečnost informací, procesů, systémů a infrastruktury. Odpovědnost za realizaci digitální bezpečnosti totiž leží zcela v rukou státu. Zejména pro definici vhodného právního rámce je jeho zainteresování velmi důležité. Mimo jiné se nejedná pouze o povzbuzení výzkumu a vývoje v oblasti bezpečnosti, ale také o podporu kultury a zavedení dodržování minimálních bezpečnostních norem a zároveň posílení boje proti kybernetickému zločinu. (ITU, 2007, s. 15)

V případě, že jsou ve vnitrostátní politice již takto implementovány jednotlivé orgány a složky, mají za úkol vytvořit specializovanou analýzu situace v oblasti kybernetických hrozeb. Tyto analýzy pak snadněji dokáží v budoucnosti rozpoznávat, co lze považovat za kybernetickou hrozbu, jak se s ní vypořádat a případně, jak hrozbám předcházet a jaké bezpečnostní prvky implementovat do veřejné politiky státu, aby se tomuto druhu ohrožení v budoucnosti předcházelo. Tyto analýzy jsou zveřejňovány nejméně jednou ročně. (NCSI, 2019) Publikované dokumenty jsou na národní, ale také na mezinárodní úrovni (k hlavním patří například dokumenty firmy *Symantec*). Každá ze zemí s již implementovanou a funkční strategií o kybernetické bezpečnosti ve svém týmu aktivně zaměstnává také odborníky z IT, kteří jsou schopni s problematikou efektivněji pracovat.

Indikátor č. 2: vzdělávání a profesní rozvoj v kyberbezpečnosti

Jak již bylo zmíněno na začátku této práce, kybernetické prostředí bylo implementováno do obyčejného života každé společnosti. Užívání technologií se zvýšilo po celém světě, tomuto trendu se samozřejmě nevyhnula ani oblast Latinské Ameriky. Pro lepší obranu kybernetického prostoru je pro každou politiku důležité vložit otázku její bezpečnosti také do osnov vzdělávání na minimálně základním nebo středním stupni. Za úspěšný lze považovat stát, který do svých školních osnov zapojil alespoň jeden program zaměřující se na otázku kybernetické bezpečnosti, či zda je povědomí o těchto hrozbách implementováno také do vzdělávání jednotlivých institucí a firem.

Cílem této kapitoly bude nastínit hlavní body, školy, instituce a profesionální vzdělávání, které se zabývá rozšiřováním povědomí o kybernetické bezpečnosti v dané zemi. Tato část je důležitá hlavně z pohledu implementované politiky, neboť zaujímá vždy jedno z hlavních míst v cílech daných národních strategií jednotlivých států.

Indikátor č. 3: podíl na mezinárodní úrovni v kyberbezpečnosti

O zajištění bezpečnosti se stát nemusí starat pouze v rámci vnitřní politiky, ale také za pomoci mezinárodních složek. Aktuálně existuje několik mezinárodních uskupení, která se otázce kybernetické bezpečnosti naplno věnují. Tato problematika je také jedním z cílů a plánů mezinárodních organizací jako je OSN, EU nebo v případě Latinské Ameriky důležitá OAS (*Organizace amerických států*). Vláda by na této úrovni měla být zastoupena v mezinárodních organizacích a také spolupracovat v rámci těchto problémů.

Cílem této kapitoly je obecný popis mezinárodní aktivity, kterou státy v rámci národní strategie kybernetické bezpečnosti podnikají. Mnohdy je totiž mezinárodní pomoc právě tím jediným, čím státy tuto strategii tvoří a mezinárodní společenství je schopno poradit na jaké úrovni, a jakým způsobem, by pro danou zemi byla tato strategie nejúčinnější a nejadekvátnější. Zapojení se do mezinárodních fór, konferencí a možnost být hostitelskou zemí akcí spojených s kybernetickou bezpečnosti, také dodává zemím větší podporu, znalosti a prestiž.

V rámci *Organizace amerických států* (OAS) byla rozvinuta agenda na podporu kybernetické bezpečnosti členských států. Spolupracuje s celou řadou národních a regionálních subjektů z veřejného i soukromého sektoru v oblasti politiky a technických otázek. Snaží se tímto vybudovat a posílit kapacitu kybernetické bezpečnosti v členských státech prostřednictvím technické pomoci a školení, jednání politiků, cvičení krizového řízení a výměny osvědčených postupů týkajících se informačních a komunikačních technologií. (OAS, 2019)

Jednou z hlavních organizací rozhodující o kybernetické bezpečnosti na mezinárodní úrovni, a zároveň důležitá pro latinskoamerický region, je *International Telecommunication Union* (ITU), která zajišťuje *Global Cybersecurity Index* (GCI), který má za úkol, mimo jiné, měření závazků členských států této unie vůči kybernetické bezpečnosti.

Dalším určovacím bodem k měření úspěšnosti boje s kybernetickou bezpečností je pro mezinárodní politiku státu také její aktivní zapojení do

hostování konferencí a summitů věnujících se danému tématu nebo financování a finanční příspěvky k mezinárodnímu boji s globální kybernetickou hrozbou. (NCSI, 2019)

Na mezinárodní úrovni samozřejmě přetrvává tradice globálních fór a diskusí, které mají za úkol neustále zlepšovat úroveň ochrany kybernetického prostoru v zemích, které již aktivně využívají tohoto sektoru.

Struktura práce, zdroje a metodologie

Práce je rozdělena na teoretickou a analytickou část a bude zakončena závěrečným hodnocením. První zmíněná část – teoretická – obsahuje popis jednotlivých pojmů, se kterými se čtenář bude v průběhu práce setkávat, a slouží k lepší orientaci a pochopení druhé části práce. Popisuji z teoretického hlediska vytváření veřejné politiky, implementaci národních strategií, problematiku kybernetické bezpečnosti, problematiku jejího hodnocení, a hlavně popis hlavních bodů, kterými se strategie zaobírají. Všechny tyto odborné a teoretické popisy jsou čerpány z příslušné literatury odpovídající zadanému tématu.

Druhá, tedy analytická část, se zabývá sledováním detailních případů Mexika, Kolumbie a Chile pomocí SWOT analýzy, která je důkladněji popsána v teoretické části. U každé z jednotlivých zemí jsou sledovány indikátory určené blíže v úvodu práce, podle kterých jsou sestavována zkoumání národních strategií kybernetické bezpečnosti. Veškeré zkoumání a následné hodnocení bude prováděno na základě pečlivého studia oficiálních zdrojů a legislativních dokumentů, tak jako vnitrostátních a mezinárodních dokumentů. Analytická část obsahuje také popis veškerých mezinárodních organizací a spoluprací, které jsou pro pochopení následného hodnocení důležitým informačním přínosem.

V závěru práce jsou porovnávány a zhodnoceny aktuální stavy národních strategií kybernetické bezpečnosti zkoumaných zemí, vzhledem k jejich předem stanoveným cílům. Je zde vysvětleno, jakou část z předem určených indikátorů země splňují a dodržují, a na jaké úrovni. Následně bude na tomto základě každá

strategie hodnocena pomocí *interim hodnocení*. Tímto způsobem bude docíleno aktuálnosti práce a jejích výsledků.

Při hodnocení aktuálního stavu národní strategie kybernetické bezpečnosti je důležité uvědomit si hlavně dané cíle, které jednotlivé země zvolily. Podle nich lze zhodnotit, zda implementovaná politika v rámci dané kybernetické bezpečnosti míří správným a předem stanoveným cílem. Z jednotlivých cílů těchto zemí byly sestaveny indikátory použité v rámci popisů jednotlivých strategií a to tak, aby odrazily všeobecné hledisko cílů daných strategií, tedy položek na seznamu cílů, které se u každé země nejčastěji opakovaly. Z těchto indikátorů bylo dále hodnoceno, jak úspěšná je aktuální politika dané země v otázce kybernetické bezpečnosti a zda je možné něco zlepšit.

Jako zdroje slouží mimo jiné jednotlivé legislativní spisy Mexika, Kolumbie a Chile oficiálně vytvořené k tématu kybernetické bezpečnosti a implementované do politiky jednotlivých zemí. Důležitým zdrojem jsou především jednotlivé národní strategie kybernetické bezpečnosti: *Estrategia Nacional de Ciberseguridad* v Mexiku, *Política Nacional de Ciberseguridad* v Chile a *Política Nacional de Seguridad Digital* v Kolumbii. Tyto dokumenty jsou stěžejním zdrojem pro analytickou část práce, díky kterým jsem schopna vytvořit základní rámec všech indikátorů a dále díky nim rozvíjet jejich obsah.

Důležitým zdrojem informací jsou hlavně internetové stránky jednotlivých ministerstev, organizací a uskupení, které popisují u nastavených indikátorů v analytické části práce. Tyto zdroje poslouží k lepšímu pochopení a také k celkové představě o provedených změnách na základě nově vytvořených národních strategií. Dále jsou to dokumenty mezinárodních a vnitrostátních organizací zapojených do podpory kybernetické bezpečnosti, jako např. *Convenio de Budapest*, *An evaluation Framework for National Cyber Security Strategies* od European Union *Agency for Network and Information Security, Cybersecurity Report* od OSA, *Guide to developing a national cybersecurity strategy* od ITU, aj.

Téma kybernetického prostoru a jeho bezpečí je na úrovni mezinárodních publikací velmi často diskutováno a jeho důležitost v čase stoupá. Jedná se o jedno z novějších témat, které řeší tuto problematiku v zásadě pomocí tří částí: jak funguje kybernetická bezpečnost, proč na ní tak záleží a co můžeme udělat pro její zlepšování. Také v České republice je spousta autorů věnujících se kybernetickému prostoru, kriminalitě s ním související nebo jeho bezpečnosti. Shrnutí informací o tom co je kybernetická bezpečnost, jak se před ní lze chránit a kdo ji vytváří a jaké má podoby, sepisuje ve své publikaci *Kybernetická bezpečnost* Petr Hrůza (2012). Martin Hromada s dalšími autory se zabývají teorií a praxí kybernetické bezpečnosti v knize *Kybernetická bezpečnost: teorie a praxe*. Důležitým pomocníkem zejména pro laickou veřejnost je v české literatuře také *Výkladový slovník kybernetické bezpečnosti* obsahující seznam hesel a jejich popisu věnujících se danému tématu.

Pro teoretickou část diplomové práce čerpám z těchto výše zmíněných knih, které napomáhají vytvořit celkový koncept a popisy jednotlivých termínů, které budou dále rozebírány a v praxi použity v analytické části práce. Teoretická část je postavena tak, aby měl čtenář dokonalý přehled o všech dále se objevujících termínech a byla zajištěna celistvost práce.

Při vypracovávání této diplomové práce byla využita kvalitativní metoda tedy „analytické postupy, které nepoužívají statistické techniky, pracují pouze s jedním nebo několika případy a pro teoretické usuzování využívají kontextuální znalosti analyzovaných případů“. (Kouba, 2011, s. 2) Z předem nasbíraných dat o daných strategiích v oboru kybernetické bezpečnosti analyzuji veřejně politický problém a následně hodnotím formu řešení tohoto problému. Práce byla zapracována na základě komparativní případové studie, která „zkoumá dva nebo několik případů a provádí jejich srovnávací analýzu“. (Drulák, 2008a, s. 62) Komparativní studie neslouží pouze k srovnání, ale také provádí pozorování existující v různých případech. (Drulák, 2008b, s. 62) Hodnocení veřejné politiky

má za úkol dopomoci k vyhodnocení použité strategie tak, aby hodnotící věděl, na jaké úrovni se strategie nachází. V opačném případě dopomáhá k vyhodnocení chyb v dané strategii a veřejné politice. V této chvíli je možné z tohoto hodnocení vytvořit novou a lepší strategii. Podle Veselého (2007) by každá veřejná politika měla být monitorována a vyhodnocována již v průběhu své implementace.

Účinnost implementované politiky a strategie pro udržení kybernetické bezpečnosti má několik důležitých částí, podle kterých je možné jejich úspěšnost kontrolovat. Jednou z důležitých součástí je hlavně ochrana digitálních služeb, tj. jak je právně zajištěna kybernetická bezpečnost nejen ve vnitrostátní politice, ale také v organizacích, firmách a veřejném sektoru, a jaké pravomoci a orgány má příslušný stát k dispozici pro řešení jakékoli kybernetické hrozby. Další částí je ochrana základních služeb před kybernetickou hrozbou. To zahrnuje připravenost jednotlivých orgánů, veřejných služeb a také podnikatelského sektoru proti kybernetickým útokům a hrozbám, jejich přístup k problematice kybernetické bezpečnosti na legislativní úrovni (audity, školení, dokumentace, dohlížení, řízení rizik atd.). Další možností, jak sledovat kybernetickou bezpečnost a její plnění, je otázka elektronické identifikace, která je teď stále více implementována do řízení jednotlivých států. Zde se jedná hlavně o to, jak je s informace nakládáno a jakým způsobem je elektronická identifikace chráněna, včetně elektronických podpisů, zadávání důvěryhodných informací na internet, atd. Poslední složkou v oblasti kybernetického a internetového světa, který je při měření brán v úvahu, je samozřejmě také ochrana osobních dat. (NCSI, 2019)

1. Kybernetická bezpečnost jako součást veřejné politiky

Veřejná politika je součástí hospodářské politiky a jako takovou ji lze definovat jako soubor nástrojů, které využívají tvůrci veřejné politiky k dosažení předem definovaných cílů. Obecně lze tuto politiku vnímat ve dvojím smyslu, jednak ve smyslu teoretické disciplíny, která ale není předmětem této diplomové práce, a jednak z pohledu praktického přístupu tvůrců hospodářské politiky k ekonomice své země. V tomto pojetí se nejedná o samoúčelnou politiku, nýbrž o záměrnou, praktickou činnost státu (Kliková & Kotlán, 2012, s. 9) Cílem každého státu je vytvořit a udržovat strategii, která zabezpečuje kybernetickou bezpečnost. Na základě této strategie je třeba stanovit a přidělit role a odpovědnosti již fungujícím veřejným orgánům. Těm přispívají k poznání aktuálního stavu kybernetické bezpečnosti hlavně informace o stávajících národních programech, mezinárodní iniciativy, projekty v soukromém sektoru, stav IT v zemi či její kybernetické vzdělání a rozvojové programy. Pro rozvojové země je navíc nezbytné iniciovat spolupráci s rozvojovými partnery, aby se tímto způsobem rozvinula technická koordinace a pomoc, společně s investicemi. V procesu tvorby veřejné politiky lze najít možnost explicitní formulace politiky, nejčastěji v podobě písemného dokumentu, případně ústního prohlášení – veřejně politické dokumenty (dále jen VPD). (Veselý, 2007, s. 49) Následně je potřeba provést analýzu silných a slabých stránek, čímž je možné dopomoci k silnější strategii kybernetické bezpečnosti v zemi. (ITU, 2007, s. 14) Kepner a Tregoe (1981) definují problém jako „odchylku od očekávaného standardu fungování“. Na důležitost zapojení kybernetické bezpečnosti do veřejných politik států poukazuje ve své stati také Vladimír Bízik (2016), který tvrdí, že:

> […] Až přibližně v poslední dekádě tedy můžeme jasně sledovat trendy, které přivedly kyberbezpečnost do popředí pozornosti tvůrců politiky kupříkladu i do té míry, že je to dnes již téma, s nímž politici vstupují do kampaní […]. Některé státy (nutno zvlášť podtrhnout Estonsko) definují kyberbezpečnost jako dominantní prvek své velké strategie a přijímají za tímto účelem veškerá dostupná opatření. […]. (Bízik, 2016, s. 1)

1.1. Stanovení cílů

Chceme-li veřejnou politiku, která se týká určitého tématu, který zatím nebyl do politiky implementován či více specifikován, je potřeba se zamyslet nad stanovením cílů, které by bylo možné implementovat a později také zhodnotit. Podle Malého (2006) takové cíle představují "očekávané stavy, kterých chce rozhodovací subjekt dosáhnout". (Malý, 2006a, s. 2) Cílem a výsledkem takto vytvořené analýzy je možné problém ještě více specifikovat a upřesnit, což je důležité pro jeho pozdější evaluaci. (Malý, 2006b, s. 2) V případě tvorby národních strategií kybernetické bezpečnosti si takovéto cíle stanovuje každá země v rámci tvoření tohoto dokumentu. Z těch je možné také vyvozovat ještě lepší hodnocení.

> Stanovení vize, cílů a priorit umožňuje vládám zvážit kybernetickou bezpečnost globálně v celém svém národním digitálním ekosystému, nikoli v daném sektoru, cíli nebo v reakci na konkrétní riziko, tj. umožňuje jim být strategickými. (ITU, 2018, s. 13)

2. Objekt a prostředí kybernetiky

Kyberprostor je metaforou vyjádření virtuálního (nefyzického) prostředí vytvořeného propojením počítačových systémů v síti. V kybernetickém prostoru probíhá vzájemné působení mezi subjekty stejně jako v reálném světě, ovšem bez nutnosti fyzické aktivity. Tento prostor ale nezná hranic, není tedy pouze otázkou teritoriální, ale je nutné jej řešit z pohledu mezinárodního společenství. (Hrůza, 2012, s. 27) Autoři zabývající se kyberkriminalitou tvrdí, že „řešitel případů kybernetické kriminality musí počítat s fakty, které nejsou zvyklostí ve fyzickém prostředí." (Hromada, 2015a, s. 79) Nejčastěji jsou to „[…] neviditelné a v čase nestálé digitální stopy, velká a převážně nezvratná anonymita pachatelů […], prostředí bez přesně definovaných geografických hranic, častá nedostupnost některých důkazních materiálů, obtížně vyčíslitelné škody a podobně." (Hromada,

2015b, s. 79) RAND Corporation na druhé straně líčí kyberprostor jako druh ekosystému, který je vytvářen ze skupin jednotlivců a organizací, která souvisí s výměnou, uchováváním nebo tvarováním informací prostřednictvím digitálních počítačových sítí. (RAND Coproration, 2016, s. 5) Janoušek (2006) vysvětluje ve svém článku kyberprostor jako „svět virtuální reality, v němž se odehrávají různé reálné věci – např. telefonické hovory, mailová komunikace, apod." (Janoušek, 2006, s. 60) Nejeden autor se v pokusu o přesně vyjádření kybernetického prostoru zabývá také jeho historií. Carlini (2016, s. 3) přikládá rozmach fenoménu jménem „kyberprostor" značnému nárůstu uživatelů internetu, který, jak poznamenává „v roce 1993 čítal 14 milionů uživatelů a v červnu roku 2014 2900 milionů uživatelů". V pojetí kyberprostoru je důležité si uvědomit jeho rozsah. Kyberprostor neznamená pouze internet. Podle definice amerického Ministerstva obrany je „[kyberprostor] globální doména v informačním prostředí, skládající se ze síťové infrastruktury vzájemně závislých informačních technologií, které zahrnují internet, telekomunikační sítě, informační systémy a integrované řadiče a procesory spolu s jejich uživateli a operátory". (Department of Defense, 2010) Důležitou součástí kybernetického prostoru je také způsob, jakým se v něm jeho aktéři „pohybují". Ještě v roce 2015 se četnost užívání internetu pohybovala okolo 40 % světové populace. Aktuálně v roce 2019 jej využívá více než 53 % populace. (ITU, 2019) Tento rapidní nárůst je důkazem toho, jak rychle postupuje nejen technologie a její užívání, ale jak velká je nutnost zlepšování obrany tohoto systému. Jak poukazuje Olmedo (2018, s. 181) ve své analýze, „je důležité si uvědomit, že […] uživatelé s vyšším vzděláním mají tendenci využívat více služeb […] online, zatímco uživatelé s nižším vzděláním mají tendenci internet více využívat pro komunikační účely." Zde take vzniká velký prostor pro kybernetické útoky a napadání kybernetického prostoru.

3. Kybernetický útok a kybernetická kriminalita

Kybernetická útok je činnost, při které je záměrem útočníka získat, modifikovat nebo zničit data (informace), negativně ovlivnit nebo převzít kontrolu

nad prvky infrastruktury systému kybernetického prostoru. (Hrůza, 2012b, s. 27) Absolutní prevence útoků není zjistitelná, proto typická ochrana (hlavně před aktivní formou útoku) je založena na detekci útoků a na následné obnově činnosti. Velmi důležité je vzít si poučení ze zjištěných skutečností a dále je uplatnit při vylepšování ochran, ať již preventivních či aktivních. (Hanáček & Staudek, 2000, s. 15) Puime Maroto (2009) ve své stati zase poukazuje na nástroje a postupy pro provádění síťových útoků, které kyberprostor nabízí. Tyto útoky mohou být podle něj organizovány a také prováděny na dálku, navíc umožňují útočníkům skrýt jejich identity či umístění. V kyberprostoru totiž národní hranice ztrácejí svůj význam. *Organizace pro hospodářskou spolupráci* a rozvoj definuje kybernetický útok jako „jakékoli nezákonné, neetické nebo neoprávněné jednání, které zahrnuje automatizované zpracování dat nebo přenos dat.“ (OECD, 2019) Podle Marie de Lourdes se takovýto typ kriminality zahrnoval zpočátku do typických činností tradičního kriminálního charakteru, avšak používání nových technik vytvořilo také nové možnosti pro zneužití užívání počítačů, které přinesly další regulace zákona. (Delgado Granados, 2014) Peréz ve svém článku definuje tzv. počítačovou kriminalitu jako „veškerý nezákonný nebo neautorizovaný úkon, který zabraňuje zpracování dat v počítačovém systému“. (Peréz Peréz, 2014, s. 2) Hlavně v Latinské Americe nastává jeden důležitý problém, který zmiňuje ve své analýze také Olmedo (2018). Tvrdí, že země Latinské Ameriky přistupují ke kybernetickým útokům až ve chvíli, kdy je tyto útoky reálně oslabí. V této chvíli jsou schopny se jejich řešení a problematice začít věnovat. (Olmedo, 2018) Této problematice se mimo jiné věnuje také publikace C*iberseguridad ¿Estamos preparados en América Latina y el Caribe?*, která je shrnutím článků odborníků, kteří se na problematiku kyberprostoru a kybernetické bezpečnosti zaměřili právě v latinskoamerickém regionu. (OAS, 2016)

4. Kybernetická bezpečnost

Ještě než si definujeme samotnou kybernetickou bezpečnost, je potřeba se zaměřit na obecný pojem bezpečnosti. I v tomto ohledu si lze tento pojem vyložit v několika směrech. V kontextu vojensko-politickém jí definuje ve své knize Barry Buzan (2005) jako „synonymum pro přežití čili zachování existence“. Další pohled, tentokráte na bezpečnost kritické infrasturktury, která je nedílnou součástí také tématu kybernetické bezpečnosti, podává ve své práci Dana Procházková. Ta tvrdí, že „bezpečnost každého systému [je] chápána jako soubor opatření, kterými se zajišťuje bezpečná infrastruktura, která se může udržitelně rozvíjet […]“. (Procházková, 2008, s. 2) Jan Eichner (2009) ve své knize *Mezinárodní bezpečnost v době globalizace* poukazuje taktéž na těžké určení jednotné definice bezpečnosti. Sám ale tvrdí, že „pozitivní vymezení bezpečnosti se vždy váže k určitému předmětu, k věci, člověku, obci, státu nebo bezpečnostnímu společenství, a také k vyznávaným a sdíleným hodnotám“. Dále vymezuje bezpečnostní úsilí každého ze států, které podle něj obsahují tři hlavní cíle: eliminaci možných hrozeb, zajištění vnitřního pořádku a soudržnosti a zajištění spravedlnosti a bezpečnosti občanů. (Eichner, 2009, s. 13) Taktéž jednoznačná definice kybernetické bezpečnosti je velmi komplikovaná. Mezinárodní telekomunikační unie ji popisuje ve své publikaci *Guía para la elaboración de una estrategia nacional de ciberseguridad*, jako „popis nástrojů, politik, pokynů, přístupů k řízení rizik, akcí, školení, osvědčených postupů, ujištění a technologií, které lze použít k ochraně dostupnosti, integrity a důvěrnosti majetku v připojených infrastrukturách týkajících se vlády, soukromých organizací a občanů. Tato aktivita zahrnuje připojená počítačová zařízení, personál, infrastrukturu, aplikace, služby, telekomunikační systémy a data v kybernetickém prostředí“. (ITU, 2018, s. 13) Podle tvrzení Hromady (2015) „[…] představuje připravenost služby či systému před potenciálním útokem a jeho následky, spolu s plánováním obnovy funkčnosti při narušení.“

Jednotlivé rozličné definice kybernetické bezpečnosti se mohou v mírných odchylkách lišit, podle toho, které z nich dá autor daného dokumentu přednost. Například mexická *Estrategia Nacional de Ciberseguridad* (2017) ji vysvětluje takto: „kybernetická bezpečnost je soubor akcí, které organizace a jednotlivci přijali ke zmírnění rizik, jimž čelí v kybernetickém prostoru, s cílem snížit pravděpodobnost, že budou vystaveni kybernetickému útoku“. Rizikem vyspělé informační společnosti je nebezpečí vytvoření závislosti na informačních a komunikačních systémech. Stát, který má vysokou úroveň informatizace svého řízení, je výrazně zranitelnější než stát, který má slabou úroveň informatizace. Nejmodernější státy jsou výrazně snadněji paralyzovatelné na úrovni digitálního zpracování a výměny informací. (Hrůza, 2012a, s. 65)

5. Národní strategie kybernetické bezpečnosti

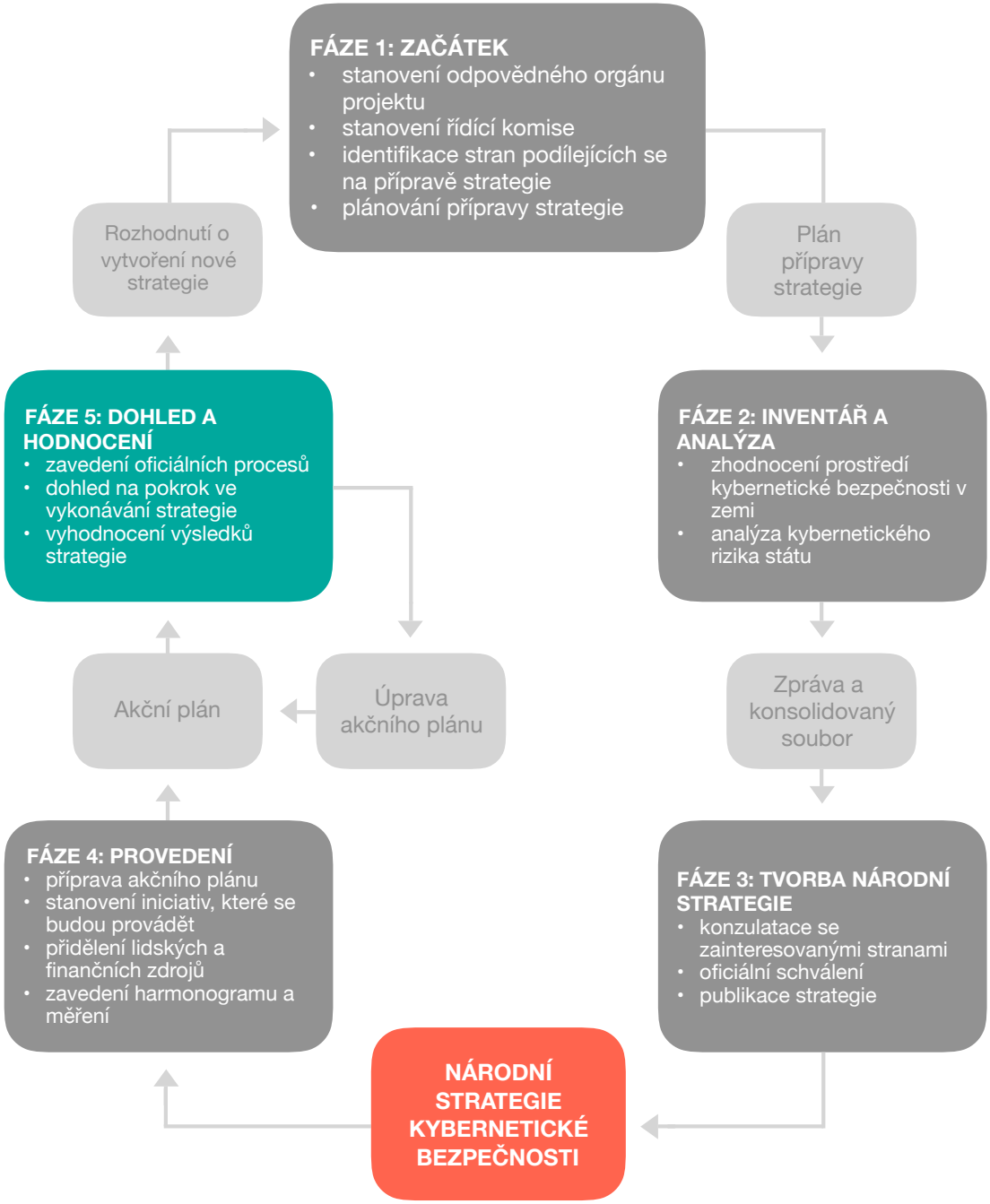
Navrhování strategie je dalším krokem po úspěšné analýze. Země by měly o této strategii uvažovat jako o popisu kroků, programech a iniciativách, kterými se zavazují chránit svou národní kybernetickou infrastrukturu a tímto procesem zvýší její bezpečnost a odolnost. V roce 2015 počítalo se strategií kybernetické bezpečnosti více než 40 zemí světa a některé z nich dokonce pracují již na její druhé či třetí verzi. Vytvářením jejich podkladů se zabývají specializované pracovní skupiny. Strategie musí fungovat na úrovni jasného stanovení cíle, vize a rozsahu, kterého má být dosaženo ve specifických lhůtách. Je potřeba brát v potaz také jejich dopad na společnost, hospodářství a infrastrukturu v závislosti na potřebných zdrojích. Ke správnému vytvoření strategie napomáhá již dříve vytvořená analýza, ze které jsou čerpány stěžejní informace. Nově vzniklý dokument identifikuje subjekty odpovědné za řízení, provádění a hodnocení strategie. (ITU, 2018, s. 23) Podle Espinozy (2015) národní strategie kybernetické bezpečnosti, která je schopna eliminovat nebo snižovat kybernetické útoky, musí mít pět klíčových os:

- vymezení pevného právního rámce,
- šíření informací a akulturace obyvatelstva o tématech kybernetické bezpečnosti a ochrany údajů,
- školení pracovníků v předmětu,
- společná práce mezi vládou a soukromým sektorem,
- posílení kybernetické ochrany.

Schéma na této stránce popisuje koloběh tvorby národní strategie kybernetické bezpečnosti podle příručky *Guía para la elaboración de una estrategia nacional de ciberseguridad*, kterou vydala v roce 2018 Mezinárodní telekomunikační unie. Schéma začíná ***fázi 1***, která je naprostým začátkem tvoření

národních strategií. Na tomto začátku se vláda zaměřuje na procesy, termíny a identifikaci hlavních stran, které by se měly podílet na rozvoji strategie. ***Fázi 2*** je posouzení situace, ve které se země nachází v oblasti kybernetické bezpečnosti. Cílem je získat informace pro účely vypracování a rozvoje národní strategie. Ve ***3. fázi*** již dochází k vypracování finálního textu za účasti hlavních představitelů veřejného sektoru, soukromého sektoru a občanské společnosti. Výsledek vyplývá z veřejných konzultací a pracovních skupin. Výsledkem je národní strategie kybernetické bezpečnosti platná pro danou zemi. ***4. realizační fáze*** je nejdůležitější, jak udává zdroj. Je založena na akčním plánu, který řídí plánované činnosti. ***5. fáze*** je stěžejní hlavně pro budoucnost národní strategie a vytvoření strategie nové. Příslušný orgán by měl navrhnout oficiální postup pro její sledování a hodnocení. Vláda zhodotí příslušný orgán a rozhodne, zda strategie zůstává s ohledem na vývoj rizik relevantní, zda reaguje i nadále na vládní cíle a jaké úpravy jsou pro další její verzi nezbytné. (ITU, 2018, s. 17-18)

Schéma č. 1: Koloběh života národní strategie kybernetické bezpečnosti

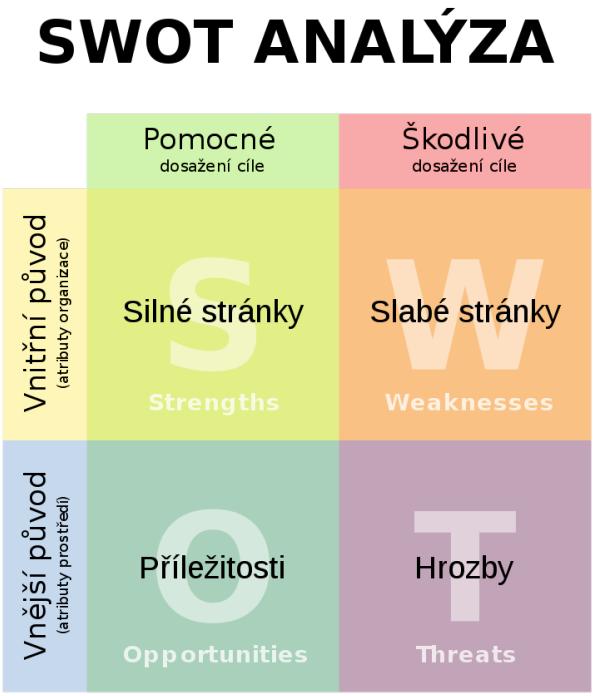


5.1. Hodnocení strategií

Důležitou složkou, hned po tvorbě veřejné politiky, je její monitoring a následné hodnocení. Každá veřejná politika by měla být v průběhu své implementace monitorována a vyhodnocována tak, aby mohlo být rozhodnuto o jejím dalším pokračování, případných úpravách nebo ukončení. (Veselý, 2007) Hodnocení neboli evaluace nastává až po samotné implementaci politiky a je tak poslední fází celého cyklu. Možnost hodnocení využita v této diplomové práci je tzv. ***in media res hodnocení*** neboli ***interim hodnocení***, které je hodnocením průběžným. Provádí se již v průběhu implementace politiky a jeho výsledky slouží k ex-post hodnocení. Toto hodnocení zohledňuje hlavně proces implementace, snaží se stanovit budoucí výsledky veřejné politiky a nebo pracuje s informace ex-ante hodnocení. Interim hodnocení je však také velmi výhodné pro určení směru, kterým se politika ještě ve fázi implementace může vydat a za pochodu je schopna změnit některé části programu veřejné politiky. (Potůček & Pavlík, 2015, s. 132) Orgány by taktéž později měly navrhnout formální proces monitorování a hodnocení dané strategie. Ve fázi monitorování by vláda měla zajistit, aby byla strategie prováděna v souladu s akčním plánem. Ve fázi hodnocení by vláda a její příslušný orgán měly posoudit, zda je strategie stále relevantní ve světle měnícího se rizikového prostředí a zda stále odráží cíle vlády, případně, jaké úpravy jsou nezbytné. (ITU, 2018, s. 2)

5.2. SWOT analýza

K analýze jednotlivých strategií kybernetické bezpečnosti byla určena SWOT[1] analýza. Tato analýza je nejvhodnější pro analyzování jednotlivých prvků národních strategií kybernetické bezpečnosti.



Obrázek č. 1: SWOT matice (zdroj: wikipedia. org)

SWOT analýza je zobrazována pomocí výše přiložené matice, kde lze pozorovat základní vazby mezi jednotlivými prvky. Na základě výsledků je možné upravovat a postupně konkretizovat strategická rozhodnutí, obecné cíle či záměry, formulace konkrétních cílů či úkoly pro jejich naplnění. Postup realizace SWOT analýzy je pouze orientační. Metoda nemá pevný metodologický rámec a je možné si navržený postup využití upravit dle potřeb. (Grasseová, 2006, s. 50)

[1] SWOT je zkratka z anglického originálu, kde **S** = Strengths (Silné stránky), **W** = Weaknesses (Slabé stránky), **O** = Opportunities (Příležitosti), **T** = Threats (Hrozby). (Grasseová & Dubec & Řehák, 2012)

5.3. Institucionální vymezení

K zajištění lepší kybernetické bezpečnosti nestačí pouze vytvoření její agendy, plánů a dokumentů. Zároveň musí každá ze zemí toto téma rozvíjet také po jeho institucionální stránce. Důležitostí institucionálního rámce je, aby se s kybernetickou bezpečností nezacházelo nekoordinovaným způsobem. Institucionální aktéři zodpovědní za tuto záležitost vykonávají změnu a novelu zákona, rovněž je důležité také vytvoření poradní rady pro multisektorovou integraci. (CICS, 2017, s. 25)

5.3.1. Dohled na bezpečnost kybernetického prostoru

Zajištění dohledu a dodržování povinností v jednotlivých státech, které byly uloženy určeným subjektům na základě daného zákona zajišťují zvláštní skupiny vlády zvané CERT (*Computer Emergency Response Team*), někdy také CSIRT (*Computer Security Incident Response Team*), společně s týmy NCSC (*Národní centrum kybernetické bezpečnosti*). (Hromada, 2015, s. 19; Kropáčová, 2013a) Lze je definovat jako „tým, který je ve svém jasně definovaném poli působnosti zodpovědný za řešení bezpečnostních incidentů. Z pohledu uživatelů nebo jiných týmů, tedy místo, na které se mohou obrátit se zjištěným bezpečnostním incidentem nebo i jen podezřením.“ (Kropáčová, 2013b) CERT týmy se rozdělují na národní a vládní. Národní CERT funguje pouze jako metodická podpora subjektů, které o ochranu projeví zájem. Oproti vládnímu mají výhodu, že jakožto soukromý subjekt mohou v nepředvídatelných situacích reagovat operativně a činit vše, co jim není zákonem zakázáno a je tak schopen vytvořit nová řešení či technické postupy. Naproti tomu vládní CERT zajišťuje uplatňování právní moci daného státu a podléhá naprosto jejím zákonům. (Hromada, 2015, s. 19) V praxi tedy lze říci, že každá větší organizace, poskytovatel připojení či služeb takovýto bezpečnostní tým poskytuje, či má k dispozici. CERT/CSIRT, naproti běžným bezpečnostním týmům, je aktivně zapojen do světové bezpečnostní infrastruktury, sdílení informací a stanovení

formálních postupů. (Kropáčová, 2013) Všechny tyto skupiny jsou pod dohledem a záštitou organizace ***FIRST*** (*Forum of Incident Response and Security Teams*), která je přední globální organizací starající se o incidenty bezpečnosti a jejich ochranu. Členství jednotlivých světových organizací pro boj s kyberterorismem a bezpečností v kybernetice je díky této mezinárodní skupině schopno reagovat ještě rychleji a přesněji, také se inspirovat na mezinárodní úrovni, jelikož umožňují přístup k těmto informacím. (FIRST, 2019)

5.4. Mezinárodní aktéři kybernetické bezpečnosti

Jedním z hlavních aktérů, kteří rozhodují o kybernetické bezpečnosti na mezinárodní úrovni je *International Telecommunication Union* (dále jen ITU), která publikuje tzv. *Global Cybersecurity Index* (dále jen GCI), což je dokument vytvořený k měření závazků členských států této unie vůči kybernetické bezpečnosti. GCI je součástí *Global Cybersecurity Agenda* (dále jen GCA), která od roku 2007 odráží pět hlavních pilířů, které lépe formují spolupráci mezinárodních strategií kybernetické bezpečnosti jednotlivých členů unie a pomáhají budování současné i budoucí iniciativy v otázce kybernetické bezpečnosti. Hlavních pět pilířů formuje základní stanoviska pro tvorbu jednotlivých národních strategií, mezi nimi jsou: právní opatření, technická opatření, kapacitní opatření a spolupráce. (ITU, 2018, s. 4) Dalším mezinárodním ustanovením je *Úmluva o počítačové kriminalitě (Convenio de Budapest)*, jež byla podepsána na *109. zasedání Výboru ministrů rady Evropy* v Budapešti v roce 2001. Jedná se o základní mezinárodní dohodu týkající se tématu kybernetické bezpečnosti a určování sankcí kybernetickým zločinům. V současné době Úmluvu podepsalo 63 států. Cílem úmluvy je vytvoření mezinárodního právního rámce, který by byl co nejúčinněji schopen bojovat proti počítačové kriminalitě prostřednictvím adekvátního postihu pachatelů, stanovení nezbytných vnitrostátních vyšetřovacích pravomocí pro zajišťování důkazů v elektronické formě a vyšetřování počítačové kriminality. Důležité je také zavedení pohotového

a efektivního režimu mezinárodní spolupráce ve vztahu k trestným činům souvisejícím s informačními technologiemi. (CONPES 3854, 2016, s. 26; Senát ČR, 2013, s. 1; Council of Europe, 2018) Během shromáždění ministrů v roce 2016 se, pod záštitou *Organizace pro hospodářskou spolupráci a rozvoj* (OCDE), zúčastněné země dohodly na spolupráci v digitální ekonomice, jakožto také na spolupráci v otázce kybernetické bezpečnosti. (CNSP, 2017, s. 10)

5.5. Regionální aktéři kybernetické bezpečnosti

V rámci kybernetické bezpečnosti se legislativa a institucionalizace s ní spojená objevila také v latinskoamerickém regionu, kde se tomuto tématu v poslední době přikládá stále větší význam. Pod dohledem *Organizace amerických států* (OAS) byl vytvořen *El Comité Interamericano contra el Terrorismo* (dále jen CICTE). Ten má pod dohledem komplexní meziamerickou strategii boje proti hrozbám kybernetických útoků, která byla schválena v roce 2004 s názvem *Estrategia Interamericana Integral para Combatir las Amenazas*. Mezi hlavní cíle sekretariátu patří zřízení národních skupin pro výstrahy, monitorování a prevenci, které jsou v každé zemi známé také jako týmy CSIRT/CERT. (OAS, 2003, s. 4) Další důležitou regionální organizací pro podporu kybernetické bezpečnosti vede *Comisión Económica para América Latina y el Caribe* (dále jen CEPAL), je *Observatorio Regional de Banda Ancha* (ORBA). Vznikla na základě požadavků zemí regionu: Argentiny, Brazílie, Kolumbie, Bolívie, Chile, Kostariky, Ekvádoru, Mexika, Paraguaye, Peru a Uruguaye. Jejím cílem je být zdrojem relevantních a včasných informací, které pomohou zemím regionu zpracovat a sledovat veřejné politiky univerzalizace širokopásmového připojení. (CEPAL, 2019) Jedním z výsledků je tzv. *Agenda digital para América Latina y el Caribe* (eLAC). (CNSP, 2017a, s. 11) Jedním z důležitých dokumentů na poli sledování kybernetické bezpečnosti v latinskoamerickém regionu je dokument *Ciberseguridad ¿Estamos preparados en América Latina y el Caribe?*, jež za podpory OAS a Oxfordské univerzity vznikl v roce 2016. Dokument opět, jako již mnoho předešlých,

poukazuje na míru implementace kybernetické bezpečnosti do politiky jednotlivých zemí. (CNSP, 2017b, s. 11)

6. Legislativní vymezení kybernetické bezpečnosti

Zavedenými opatřeními kybernetické bezpečnosti je možné snižovat rizika kyberkriminality. Kybernetický prostor totiž nemá žádné jasně vyhraněné geografické hranice, ani fyzické důkazní materiály, které by spáchaný zločin prokázaly. Proto nejen jeho vymezení, ale také kvalitní ochrana před útoky jsou aktuálně velmi diskutovaným tématem. Základem je ujasnit si právní hlediska a opatření. Tato opatření pověřují stát, aby zavedl základní mechanismy, jejichž prostřednictvím bude probíhat vyšetřování, stíhání a uvalování sankcí na trestné činy s kybernetickou bezpečností spojené. Legislativa by měla být schopna stanovit základ pro chování, postupy a vymezení trestných činů v tomto odvětví bezpečnosti. (ITU, 2018, s. 3) Každá země si vytváří vlastní legislativní rámec, pokud možno, v souladu s mezinárodními stanovami, ale plně přizpůsobený dané situaci a problémům. Podle Jirovského (2007) „[…] některé státy nemají v této oblasti zákony žádné nebo se existující zákony výrazně liší v jednotlivých jurisdikcích. Činnost, která je v jedné zemi trestná, nemusí být v druhé zemi vůbec zahrnuta do legislativy nebo může být legální.“ O to je důležitější vytváření strategií, jejich hodnocení a změn, aby bylo tímto způsobem možno měnit právní hlediska států v závislosti na vyskytujících se problémech.

7. Vzdělávání a profesní rozvoj v kyberbezpečnosti

Ochrana kybernetického prostoru je systematickým poskytováním relevantních informací o rizicích, která se v něm vyskytují, jak pro společnost, tak také pro jednotlivce. Vzdělávací přístup ke kybernetické bezpečnosti začíná zvyšováním informovanosti žáků školního věku o rizicích spojených s používáním internetu, přičemž jsou brány v úvahu také další aktéři, jako například

rodiče, specializované agentury či samotný telekomunikační sektor. (Peña Cayón & García Segura, 2014, s. 8) Šíření kultury o kybernetické bezpečnosti a přístupu k ní, kontrole počítačového rizika a jeho trestného původu je povinností každé země. Strategická vize těchto problémů se stala nezbytností, jak pro organizace, tak pro státy. Je však také nutné vzdělávat, informovat a školit o technologiích zpracování informací, a to nejen v oblasti bezpečnostních opatření. Povědomí o bezpečnostních problémech by podle ITU nemělo být omezeno pouze na podporu určité kultury zabezpečení, ale musí existovat i kultura v užívání počítačů. (ITU, 2007a, s. 97) Proto je nezbytné poskytnout zúčastněným stranám potřebné prostředky pro možnost naučit se řídit technologická, provozní a informační rizika, která mohou být velkou hrozbou při užívání nových technologií. Virtuální rozměr internetu může skrývat - zejména pro populaci mladých lidí dostatečně nevzdělaných v daném tématu - potenciální poškození v podobě kybernetických útoků, které mohou velmi poškodit jednotlivé organizace (jako jsou podnikání, administrativa nebo daná komunita). Nejzávažnější škody obvykle pocházejí z naprosté nedbalosti nekompetentních osob nebo špatné implementace technologií, chybného řízení, apod. (ITU, 2007b, s. 97)

8. Chile

Následující kapitola se zabývá popisem aktuální situace v oblasti kybernetické bezpečnosti v Chile. Jedná se tedy o vývoj národní strategie kybernetické bezpečnosti, její hlavní institucionální, legislativní, regionální a mezinárodní představitele a hlavní body, kterými se aktuálně národní strategie zabývá.

8.1. Indikátor č. 1: rozvoj politiky státu v rámci kyberbezpečnosti

8.1.1. Política Nacional de Ciberseguridad

Aktuální verze chilské národní strategie pro kybernetickou politiku funguje aktivně od roku 2017. I přesto byly její základy budovány již o dva roky dříve. V dokumentu *Bases para una Política de Ciberseguridad* z roku 2015 bylo hlavním cílem připravit proces rozhodování veřejné politiky v rámci kybernetické bezpečnosti, která doposud v Chile chyběla. Lze tedy říci, že tento dokument byl základním kamenem pro národní strategii a jeho části v ní dodnes můžeme naleznout. Je však důležité zaměřit se na společného autora obou dokumentů, kterým je v roce 2015 založené *Comité Interministerial sobre Ciberseguridad* (dále jen CICS), jež je ústředním vládním subjektem specializovaným v odpovědnosti za rozvoj národní politiky kyberbezpečnosti. (CICS, 2017, s. 32; Barrios Achavar, 2018, s. 2; Ministerio de Defensa Nacional a Ministerio del Interior y Seguridad Pública, 2015, s. 3) Národní chilská strategie je součástí tzv. ***Agenda Digital 2020***, která se již od roku 2015 zabývá rozvojem technologií potřebných k sjednocení a přísunu většího počtu možností v technologickém pokroku. (CICS, 2017, s. 14; Agenda Digital 2020, 2015) V dubnu roku 2017 pod vedením ex-prezidentky Michelle Bachelet oficiálně vznikla *Política Nacional de Ciberseguridad 2017-2022* (dále jen PNCS), která je aktuálně platným právním dokumentem o politice týkající se kybernetické bezpečnosti ve státě Chile. (Barrios Achavar, 2018, s. 2; CICS, 2017, s. 14) Hlavní rozvoj jednotlivých částí

národní strategie proběhl v první etapě, a to mezi léty 2017-2018. V tomto období bylo hlavním úkolem stanovit rozvinutí pojmu kybernetická bezpečnost ve vládním a veřejném sektoru. Cíle strategie jsou aktuálně naplánovány až do roku 2022, kdy chilská vláda počítá s již fungující infrastrukturou a velkým zdrojem informací, který zajistí rychlé zotavení z kybernetických incidentů. Jedním z hlavních dílčích úkolů politiky je také vytvoření modelu prevence, monitoringu a řízení rizik, který bude sloužit jako základ pro technická opatření v kyberprostoru na národní úrovni, a která budou v rámci neustálého zlepšování aktualizována.

Důležitou součástí ochrany kybernetického prostoru je v rámci veřejné politiky také ***Política Nacional de Ciberdefensa***, která specifikuje a definuje kapacity na ochranu sítí a kybernetického prostoru, které mohou v případě nouze spolupracovat a zabezpečit ho. (CICS, 2017, s. 14; MINDEF, 2019) Dále také ***Política nacional para el ciberespacio***, což je jeden z hlavních identifikátorů globální spolupráce v odvětví kybernetické bezpečnosti, jež je důležitou součástí politiky každého státu, která se rozhodne tuto problematiku začít řešit. (CICS, 2017, s. 14)

Dalším krokem k zlepšení úrovně kybernetické bezpečnosti v zemi je, podle dokumentu PNCS, vytvoření standardizovaných mechanismů pro hlášení a správu incidentů. Zároveň se dokument vyjadřuje o ochraně informační infrastruktury vlády a státu, která musí mít základní úroveň opatření v oblasti kybernetické bezpečnosti podle předem stanovených norem. (CICS, 2017, s 18)

8.2. Institucionální hledisko kybernetické bezpečnosti

8.2.1. Vládní instituce

Jednou z možností, jak docílit předem daných cílů, které si politika stanoví při implementaci jakéhokoli zákona, či v tomto případě národní strategie, je silné institucionální zázemí. V tomto případě, stejně jako u mnohých dalších, se Chile inspirovalo na mezinárodní úrovni od ostatních států. Příprava a dobré využití

všech institucí v tomto smyslu dává politice mnohem větší kontrolu nad diskutovaným problémem. Silnou institucionální složku mimo jiné zajišťuje skupina *CSIRT (Equipo de Respuesta ante Incidentes de Seguridad Informática)*, která na vládní úrovni zasahuje přímo do politiky státu převážně v technické rovině. Skupina má za úkol průběžný monitoring vládních institucí, které mohou být svým propojením s kyberentickým světem náchylní k porušení bezpečnosti. Taktéž se stará o kontaktní místo pro hlášení incidentů v oblasti kyberbezpečnosti a následně provádí jejich analýzu, odhaduje možná rizika a potenciální útoky či ztráty. Hlavním úkolem však zůstává neodkladné vyřešení jakýchkoli útoků a narušení bezpečnosti obyvatelstva v rámci kybernetické bezpečnosti. CSIRT je v Chile aktivní od roku 2013. (CSIRT, 2019)

V rámci koordinace a komunikace na úrovni politické, Chile stále počítá s přítomnost *Comité Interministerial sobre Ciberseguridad*. Komise se stará o aktéry, akce, plány a programy národní politky kybernetické bezpečnosti, které jsou probírány na měsíčních zasedáních. Jejich cílem je navržení správného opatření při vzniku jakýchkoli nedostatků v dané veřejné politice. V neposlední řade se CICS stará o navrhování legislativních změn, které by odpovídaly předem stanoveným opatřením. (CICS, 2017, s. 25)

Další vládní instituce už spadají pod jednotlivá ministerstva, které se zabývají určitou částí, která je pro celkovou kybernetickou bezpečnost důležitá. O zavádění veřejné politiky se stará především *Ministerio del Interior y Seguridad Pública* (MISP), které také pomáhá s vývojem kybernetických strategií a v otázce kyberbezpečnosti je ministerstvem nejpovolanějším.

V rámci vládních institucí nelze opominout také speciální oddělení na chilské policii, která se v rámci boje proti kybernetickým hrozbám rozhodla sestavit skupinu policistů, schopnou pracovat s rostoucí počítačovou kriminalitou. Speciálně školení policisté z *Policía de Investigaciones de Chile* v rámci *Brigadas Investigadoras del Cibercrimen* řeší případy spojené s hackerstvím, sexuálním obtěžováním na internetu, zpronevěřením kreditních karet online, apod. Brigády

slouží také jako kontaktní místo, na které mohou obyvatelé Chile nahlásit jakýkoli incident spojený s kybernetickou kriminalitou. (PDI, 2019)

8.2.2.Soukromé a akademické instituce

Mimo vládou kontrolované instituce má Chile k dispozici také tzv. Skupiny FIRST, které jsou institucemi převážně soukromými či akademickými. V Chile nalezneme celkem 3 skupiny FIRST z čehož dvě jsou soukromé společnosti fungující nejen v Chile, ale také celém latinskoamerickém regionu (*NeoSecure* a *Novared*). Poslední skupinou je akademická *CLCERT*, která kromě monitorování a analyzování kybernetických útoků, generuje znalosti potřebné k zajištění těchto systémů. Zajímavostí je, že skupina vznikla již dávno před jakýmkoli náznakem funkční strategie kybernetické bezpečnosti v zemi (a funguje již od roku 2001). Neocenitelná je hlavně svým působením ve veřejné politice. Tomuto sektoru aktivně radí při vývoji politik v oblasti bezpečnosti počítačových systémů a také při vzniku veřejných vyhlášek. Odborníci z *Universidad de Chile* se díky tomu dostávají na důležité mezinárodní konference odborníků, což je pro rozvoj této oblasti v zemi velmi důležité. (FIRST, 2019; NeoSecure, 2017; Novared, 2017; CLCERT, 2019)

8.3. Legislativní hledisko kybernetické bezpečnosti

Z legislativního hlediska muselo Chile přistoupit k několika zcela novým zákonům. Veškeří poskytovatelé digitálních služeb v zemi musí s implementací těchto zákonů počítat i ve svém podnikání a dodržovat tak předem stanovenou normu bezpečnosti. Na základě *Convenio de Budapest*, ke kterému se Chile přidalo v roce 2017, byla aktualizována trestní sazba obsažená v *Ley 19.223*, která stanovuje pravidlo pro počítačové trestné činy. Nové formy kriminality a nedávné kybernetické útoky, které se v Chile odehrály a zasáhly také veřejnost, si vyžádaly aktualizovaný katalog počítačových zločinů a prostředky pro rozvoj trestního vyšetřování týkajícího se tohoto tématu. (CICS, 2019; CSIRT, 2019) V rámci

kybernetické bezpečnosti jsou významné hlavně odpovídající *Ley 20.453*, který zakotvuje zásadu neutrality sítě pro spotřebitele a uživatele internetu a regulují opatření pro správu sítě, které je země schopna poskytnout. Dále pak *Ley 20.478*, který popisuje zotavení a kontinuitu veřejného telekomunikačního systému v kritických a nouzových podmínkách. Tento zákon byl uveden v platnost po zemětřesení, které zasáhlo Chile v roce 2010 a jeho hlavním cílem je umožnit kontinuitu fungování telekomunikací a dostupnost informací obsažených v kyberprostoru v zemi. Z iniciativy *Ministerio de Defensa Nacional* v rámci zabezpečení kybernetického prostoru Chile vzešla *Ley 20.424*, která nařizuje proces vytváření obranné politiky v otázkách kyberprostoru a plánování národní obrany v této oblasti. (CICS, 2017, s. 31; Ministerio de Defensa Nacional, 2019) *Decreto 5996* z roku 1999 vytváří vnitřní síť státu (INTRANET) a zajišťuje jeho implementaci, správu a koordinaci. Dalším důležitým legislativním počinem je *Decreto 1299* z roku 2005, jež udává nové normy, které regulují internetovou síť v Chile a stanovuje postupy, požadavky a technologické standardy pro začlenění veřejných institucí do sítě. Ze stejného roku pochází *Decreto 83*, které schvaluje technickou normu pro orgány státní správy týkající se bezpečnosti a důvěrnosti elektronických dokumentů. *Decreto 93* (pocházející z roku 2006) schvaluje technickou normu pro přijímání opatření zaměřených na minimalizaci škodlivých účinků nevyžádaných hromadných elektronických zpráv přijímaných v elektronických schránkách orgánů státní správy a jejich úředníků. A nakonec nejaktuálnější a nejnovější *Decreto 1* z roku 2015, který schvaluje technickou normu pro systémy a webové stránky orgánů státní správy.

8.4. Indikátor č. 2: vzdělávání a profesní rozvoj v kyberbezpečnosti

Vzdělávání v informační gramotnosti a technologiích je důležité z hlediska možnosti bránit se a připravit se na možné hrozby, které z tohoto prostředí plynou. Tato kapitola popisuje veškeré instituce, které se v Chile vzdělávacím a profesním rozvojem v oblasti kybernetické bezpečnosti aktuálně zabývají. Jen v Chile, podle

posledních dostupných měření z roku 2017, užívá internet 85,1 % populace v rozmezí věku 16 a více let. Podle stejné ankety z roku 2017 je pak užívání internetu v rodinách mnohem častější, pokud se v ní objevují děti ve školním věku (5 - 24 let). Na konci roku 2017 mělo přístup k internetu 87,4 % chilské populace. (SUBTEL, 2017) Je tedy očividné, že správné vzdělávání a rozvoj v otázce kybernetické bezpečnosti je v Chile velmi důležitou složkou v boji proti kybernetickým zločinům. V této části práce je forma vzdělávání rozdělena na školní vzdělávání, do kterého spadá veškeré vzdělávání obyvatel ve věku 5-24 let, tedy základní, střední a vysokoškolské. Dalším částí je profesní rozvoj, tedy jakékoli soukromé instituce, které pomáhají rozvíjet povědomí o kybernetické bezpečnosti již v profesní sféře. Poslední součást indikátoru č. 2 jsou kampaně, které taktéž svým působením rozvíjejí povědomí o kyberbezpečnosti v rámci státu.

8.4.1.Školní vzdělávání

Díky opatřením, která by měl stát zajistit již v samotné školní osnově a v rozvoji povědomí o informační gramotnosti jako takové jsou obyvatelé schopni rozpoznat toto nebezpečí, bojovat s ním nebo případně vytvořit libovolnou prevenci, která by je ochránila. Cílem Chile je rozvinutí kultury kybernetické bezpečnosti, která by tyto úkoly zastávala. Povědomí o bezpečnosti se stát snaží zajišťovat hlavně v rámci studia na vysokých školách, jejich zařazení do osnov škol základních a středních v Chile bohužel zatím chybí. (CICS, 2017, s. 21) Na univerzitách vznikají nové a zajímavé obory, které se přímo či nepřímo (skrze IT) věnují problematice kybernetické bezpečnosti a rozšiřují také informační gramotnost. Na úrovni bakalářského studia dnes existuje v Chile obor *Ingeniería de Ciberseguridad*, jejíž absolventi jsou schopni navrhovat, hodnotit, implementovat a monitorovat zásady informační bezpečnosti a zranitelnost informačních systémů. Dále pak dodávat preventivní a nápravná řešení pro posílení informační bezpečnosti. V Chile aktuálně tyto obory lze nalézt na

Universidad Tecnológica de Chile (INACAP) a *AIEP*. (INACAP, 2019; AIEP, 2019; NCSI, 2019) Ve školním prostředí je další z možností také magisterské studium, kde jsou již studenti seznámeni s podrobnějšími koncepty a charakteristikami týkajícími se tohoto odvětví. Naučí se své poznatky aplikovat také v praxi společně s příslušným zaškolením do právních, sociálních, etických a profesních aspektů kyberprostoru. V Chile se magisterskému studiu věnuje *Universidad Adolfo Ibañéz (Magíster en Ciberseguridad)* a *Universidad Mayor (Magíster en Ingeniería de Seguridad de la Información)*. (UAI, 2019; Universidad Mayor, 2019; NCSI, 2019)

8.4.2.Odborné vzdělávání

Proškolení lze získat také od odborníků v oblasti kybernetické bezpečnosti, jako jsou manažeři nebo auditoři. Obyvatelé jsou schopni se sami vzdělávat a rozšiřovat nejen svou informační gramotnost, ale také vlastní prevenci v boji s běžnou kybernetickou hrozbou, která je vzhledem k vysokému počtu Chilanů užívajících internetových služeb, na místě. Hlavními organizacemi, které se v Chile tímto školením zabývají, jsou: *Alianza Chilena de Ciberseguridad, (ISC)² Chile Chapter* a *ISACA*. (Alianza Chilena de Ciberseguridad. 2019; (ISC)² Chile Chapter, 2019; ISACA, 2019; NCSI, 2019)

8.4.3.Kampaně na podporu kybernetické bezpečnosti v Chile

Ministerstvo školství se v Chile zapojuje také do rozvoje povědomí o počítačové gramotnosti a ochraně. K tématu kybernetické bezpečnosti vytvořilo hned několik kampaní. První z nich je ***Internet Segura y Ciudadanía Digital.*** Projekt vznikl v roce 2005 s cílem vést péči o prevenci v digitálním prostředí. Jednou z nich byla iniciativa webové stránky vytvořené k propagaci této kampaně, která dodává nástroje dospělým, aby mohli vzdělávat děti a mladé lidi v digitálním světě a aby základní a střední školy byly schopné z tvořit digitální povědomí občanů, kteří si budou vědomi svých práv a povinností v kyberprostoru.

(Ministerio de Educación, 2019) Druhou vzdělávací kamapaní v Chile je ***Hay palabras que matan*** snažící se zvýšit informovatnost studentů o kyberšikaně. Obsahuje virtuální monitorovací systém, který má za úkol chránit školní komunitu před násilím. (Ministerio de Educación, 2019) Poslední kampaň s názvem ***Me conecto para aprender*** je iniciativa, jejímž cílem je překlenout mezery ve využívání informačních komunikačních technologií a podporovat proces učení prostřednictvím poskytování notebooku (a internetu) každému studentovi 7. ročníku základní školy ve všech veřejných zařízeních v zemi. (Ministerio de Educación, 2019)

8.5. Indikátor č. 3: podíl na mezinárodní úrovni kyberbezpečnosti

Zahraniční politika Chile dodržuje několik zásad řídících její diplomacii a mezinárodní činnost. Kybernetická bezpečnost na mezinárodní úrovni dovoluje budování společných kapacit, přístupů a opatření ve spolupráci s ostatními zeměmi. Diplomatickou prací je možné snížit rizika konfliktů v kyberprostoru na základě neustálé spolupráce agentur, ministerstev a vlád mezinárodní politiky v otázce kybernetické bezpečnosti. V rámci takovéto pomoci bude kybernetická bezpečnosti posílena různými způsoby, jako jsou: pomoc do Chile, či z Chile, výměna informací a zkušeností, provádění a prohloubení mechanismů politického dialogu na toto téma a snaha o transparentnost a opatření na budování důvěry, která upřednostňují multiagenturní přístup k otázkám. (CICS, 2017, s. 22) *Política Nacional de Ciberseguridad* stanovuje v tomto ohledu jasná pravidla, která by měla být zaměřena na podporu digiálního pole jako svobodného, otevřeného a bezpečného prostředí pro všechny uživatele kyberprostoru. Potřeba je také posílení práce země s ohledem na zvláštní výzvy, jak v technických podmínkách, tak také v globální a decentralizované povaze sítě a politických dimenzích charakterizovaných systémem správy Internetu s více zúčastněnými stranami, kde soukromý sektor a občanská společnost zaujímají zvlaštní roli. Stát Chile počítá se zvýšením účasti na globálních příkladech, stejně jako s podporou regionálních a

subregionálních konzultačních procesů v této oblasti, zejména v Latinské Americe, za aktivní účasti dalších zúčastněných stran. (CICS, 2017, s. 22) V dubnu roku 2017 podepsalo Chile *Convenio de Budapest*, jeden z důležitých mezinárodních dokumentů zabývající se mimo jiné kybernetickou bezpečností. Je hlavním a základním dokumentem, jež země podepisují při mezinárodní spolupráci o kybernetické bezpečnosti. Dalším důležitým zapojením do systému kybernetické bezpečnosti a obecně kybernetické kriminality je zastoupení země ve formátu spolupráce na mezinárodní úrovni. Podle oficiálních zdrojů v Chile fungují celkem 3 skupiny FIRST a velmi aktivní je také zvláštní skupina CSIRT. V rámci OSN, tak jako další země latinskoamerického prostoru, je samozřejmě Chile také aktivním členem *Internet Governance Forum* (IGF), *World Summit on the Information Society* (WSIS) nebo *Foro para la Gobernanza de Internet* (FGI). Dále je Chile součástí také *Unión Internacional de Telecomunicaciones* a zapojuje se neustále aktivně na jednotlivých fórech, ať už jako mluvčí, či posluchač. Samozřejmostí je také zapojení Chile do spolupráce k využití potenciálu digitální ekonomiky *Organización para la Cooperación y Desarrollo Económicos* (OCDE). (NCSI, 2019; CSIRT, 2019; FIRST, 2019) Tak jako zapojení v mezinárodní pomoci, je pro Chile důležitá také podpora rozvoje odvětví kybernetické bezpečnosti, která slouží jejím strategickým cílům. Na zlepšení oboru kybernetické bezpečnosti vynakládá země velké úsilí. V chilské ekonomice totiž obor IT zastává přibližně 3-4 %, naproti tomu v zemích *Organizace pro hospodářskou spolupráci a vývoj* je tento sektor zastoupen v průměru až 6 %. Chile tedy vývojem kybernetické bezpečnosti přispěje nejen k lepší obraně státu a jeho politiky, ale také k rozvoji odvětví informačních technologií. (CICS, 2017, s. 23)

9. Mexiko

Následující kapitola se zabývá popisem aktuální situace v oblasti kybernetické bezpečnosti v Mexiku. Jedná se tedy o vývoj národní strategie kybernetické bezpečnosti, její hlavní institucionální, legislativní, regionální a mezinárodní představitele a hlavní body, kterými se aktuálně národní strategie zabývá.

9.1. Indikátor č. 1: rozvoj politiky státu v rámci kyberbezpečnosti

9.1.1. Estrategia Nacional de Ciberseguridad

Potřeba návrhu a vytvoření národní strategie zabývající se tímto tématem vznikl také na popud neustále se zvyšujícího nebezpečí využívání IT technologií v celém státě, které je přímo úměrné s neustále se zvyšujícím rizikem pronikání do zabezpečených zón kyberprostoru u běžných uživatelů. Uživatelské prostředí, které je náchylné na porušení bezpečnosti totiž v Mexiku neustále narůstá a je důležité s těmito výsledky aktivně pracovat a zdokonalovat národní strategii. Proto se vláda republiky rozhodla ve své roli zprostředkovatele strategie zahájit prostor pro dialog a diskusi v rámci spolupráce na fórech a workschopech s názvem *Hacia una Estrategia Nacional de Ciberseguridad*, které se konaly od března do října roku 2017. Přestože v Mexiku do té doby neexistovala ucelená národní strategie kybernetické bezpečnosti, vláda republiky propagovala akce a v této věci byla prováděna cenná cvičení a úsilí občanské společnosti, soukromých organizací, akademických komunit, technických komunit a veřejných institucí v různých pravomocích a řádech vlády. (CIDGE, 2017, s. 3) Tato akce byla prostorem pro různé aktéry společnosti a sdílení jejich myšlenek, obav a návrhů v oblasti kybernetické bezpečnosti, které vyvolaly velkou shodu v potřebách strategie, která by měla plnit daná kritéria. Účastnili se jí experti i reprezentanti z průmyslu, vlády, technických komunit, aj. (Gobierno de México, 2019) Součást dohody byla také koordinace vlády republiky a formulování úsilí různých

subjektů při provádění a sledování strategie pověřena *Comisión Intersecretarial para el Desarrollo del Gobierno Electrońico* (CIDGE) a to skrze specializovaný *Subcomisión de Ciberseguridad.* (CIDGE, 2017, s. 4)

Aktuální verze strategie, která byla přijata roku 2017, byla taktéž vytvořena ve spolupráci s dalšími důležitými dokumenty mexické legislativy jako je *Plan Nacional de Desarrollo 2013-2018, Programa para un Gobierno Cercano y Moderno 2013-2018*, *Programa Nacional para la Seguridad Pública 2014-2018*, *Programa para la Seguridad Nacional 2014-2018***.** Všechny tyto oficiální publikace přispěly k obsahu aktuálního dokumentu. (Gobierno de México, 2013, s. 3*)*. Národní strategie kybernetické bezpečnosti Mexika klade velký důraz hlavně na mezinárodní spolupráci. Společně s tím se také věnuje uchopení tématu na národní úrovni, kde se snaží stanovit strategické cíle a základní osu celého programu. (CIDGE, 2017, s. 7)

9.2. Institucionální hledisko kybernetické bezpečnosti

9.2.1. Vládní instituce

Na vládní úrovni funguje v Mexiku *Subcomisión de Ciberseguridad*, která odpovídá za schvalování a zveřejňování strategie, její sledování, koordinaci a společně s různými jednotkami a subjekty federální policie také za její dodržování. Podporuje programy a interinstitucionální spolupráce v rámci kybernetické bezpečnosti. Hlavním cílem je však podpora a konsolidace využívání informačních a komunikačních technologií ve federální veřejné správě. (CIDGE, 2017, s. 25; Gobierno de México, 2019) V rámci federální policie byla v Mexiku, stejně jako v Chile, založena speciální jednotka. *División científica* je schopná při vyšetřování využít svých vědeckých a technických znalostí a nástrojů, které mnohdy napomáhají nejen předcházení trestných činů, ale také koordinaci, dohledu a provozování vědeckých a technických služeb instituce. (CIDGE, 2017, s. 6; Gobierno de México, 2019) Druhou aktivní policejní složkou je *Policía de Ciberdelincuencia Preventiva*. Jejich hlavním úkolem je monitorování sociálních

sítí a webových stránek, taktéž vedou informativní rozhovory ve školách a institucích s cílem varovat a předcházet nebezpečí a zločinům spáchaným prostřednictvím internetu. Podílejí se na vytváření kultury péče o digitální občanství a 24 hodin denně se starají o kybernetickou bezpečnost mexického obyvatelstva. (Gobierno de la Ciudad de México, 2019) Na vládní úrovni disponuje Mexiko také jednou ze skupin CERT. *CERT-MX* funguje prostřednictvím *Policía Federal* v Mexiku a provádí opatření pro prevenci nezákonného chování prostřednictvím IT. CERT-MX je jediným federálně akreditovaným orgánem pro výměnu informací s národní kybernetickou policií a mezinárodními donucovacími orgány s cílem identifikovat a řešit možné útoky na úkor vládní IT infrastruktury proti občanům, a to prostřednictvím specializovaných nástrojů pro detekci a včasnou reakci útoků v kyberprostoru a neustálého monitorování veřejné internetové sítě. Skupina funguje na bázi mezinárodní sítě a propojení s dalšími podobnými týmy. (Gobierno de México, 2019; CIDGE, 2017, s. 25)

9.2.2.Soukromé a akademické instituce

V oblasti soukromé fungují v Mexiku, stejně jako po celém světě, týmy ze skupiny FIRST. ***Axtel-CSIRT***. Tým je pod záštitou společnosti *Axtel, S.A.B. de C.V.*, která vede nabídku řešení informačních a komunikačních technologií pro obchodní a vládní trhy. (FIRST, 2019; Axtel, 2019) Poměrně nový tým, připojený v únoru roku 2019 k fóru FIRST, je ***CERT DSI Totalsec***. Hlavním cílem skupiny je evaluace bezpečnosti v kyberprostoru, reakce na jakékoli incidenty, které se v tomto prostoru naskytnou, forenzní analýza, oznámení o napadení kybernetické bezpečnosti, konzultace v oboru kybernetické bezpečnosti, aj. (FIRST, 2019; TotalSec, 2019) Další tým nazvaný *CERT-ATTMX* je tvořen firmou *AT&T Mexico*, která je jedním z hlavních telekomunikačních operátorů v zemi. (FIRST, 2019; AT&T, 2019) *IKUSI CSIRT* pomáhá při činnostech zaměřených na reakci při incidentech, které minimalizují dopad i riziko při provozování jejich služeb.

(FIRST, 2019; IKUSI, 2019) Další skupina *Mnemo-CERT* se, kromě prevence a evaluace kybernetické bezpečnosti, zabývá také publikací dokumentů pojednávajících o tomto tématu, které lze stáhnout na jejich oficiálních stránkách. (FIRST, 2019; Mnemo, 2019) Poslední skupinou v soukromém sektoru je *Scitum-CSIRT (či Scitum-CERT),* která vytváří školení a integrace odborníků a stará se o detekce, vyšetřování a reakce na bezpečnostní incidenty. (FIRST, 2019; Scitum, 2019)

V oblasti akademických institucí funguje aktivně v Mexiku tzv. *Coordinación de Seguridad de la Información (CSI)* neboli *UNAM-CERT* na univerzitě v Mexico City. Počítačová komunita zde získává informace, poradenství a bezpečnostní služby, výměnu zkušeností a názorů k dosažení odpovídající bezpečnostní politiky, snížení množství a závažnosti bezpečnostních problémů a šíření kultury počítačové bezpečnosti. (FIRST, 2019; UNAM, 2019)

9.3. Legislativní hledisko kybernetické bezpečnosti

Mexiko aktuálně nedisponuje žádnou nezávislou legislativou pro vyšetřování a zpracování počítačové kriminality, kromě mezinárodně ustanoveného *Convenio de Budapest*. Podle El Economista však vláda v první polovině roku 2019 zavedla jednání ohledně nového zákona o kybernetické bezpečnosti, který by dle všeho měl spadat pod tzv. *Agencia Nacional de Seguridad Informática* (ANSI). (Riquelme, 2019) Za legislativu přibližující se tématu kybernetické bezpečnosti lze považovat např. *Código Penal Federal*, *Ley Federal en contra del Crimen Organizado* a další zákony a státní trestní zákoníky obsahující ustanovení, která postihují a trestají jednání spáchané prostřednictvím a proti používání počítačových systémů, včetně trestných činů, jako jsou: protiprávní přístup do počítačových systémů, modifikace a ničení informací obsažených v počítačových systémech a databázích, zneužívání nebo rušení či ničení informací ve veřejných telekomunikačních sítích, držení a prodej či

distribuce dětské pornografie, propagace a podpora činnosti související se sexuální turistikou na národním území, zločiny proti národní bezpečnosti, které zahrnují špionáž, povstání, terorismus a sabotáž, aj. (Council of Europe, 2019) Stát poskytuje svým občanům, obyvatelům a právnickým osobám jedinečný a trvalý identifikátor, který je běžnou praxí také v jiných zemích světa. V Mexiku je známý jako tzv. *CURP*, tedy jedinečný registrační kód populace, který slouží k individuální registraci všech osob s bydlištěm v Mexiku, státních příslušníků a cizinců, jakožto i Mexičanů s bydlištěm v jiných zemích. (Gobierno de México, 2019; NCSI, 2019)

9.4. Indikátor č. 2: vzdělávání a profesní rozvoj v kyberbezpečnosti

Mexiko přistupuje k ochraně kybernetického prostoru zodpovědně, a proto (podobně jako spousta dalších zemí, které se otázkou kybernetické bezpečnosti začaly zabývat), vytvořilo edukativní programy, které by na různých stupních vzdělání měly o této problematice informovat. V Mexiku využívá, podle nejaktuálnějších měření z roku 2018, internet 74,3 milionů obyvatel ve věku 6 a více let. V tomto věku je to přibližně 68 % obyvatel. Nejvíce uživatelů internetu nalezneme v zemi v rozmezí věku 25 až 34 let. Obyvatelé nad 55 let využívají v poměru k této skupině internet pouze z méně než 5 %. Je tedy jasné, proč je vzdělávání v tomto oboru důležitou součástí nejen národní strategie a dané veřejné politiky. Užívání internetu v Mexiku roste a vzhledem k častému ohrožení je potřeba generace učit, jak správně s těmito složkami zacházet hned od začátku. (INEGI, 2019)

9.4.1. Školní vzdělávání

Na bakalářské úrovni studia je v Mexiku vytvořen program *Ingeniería en Seguridad Informática y Redes (ITESO)* na několika mexických univerzitách. Tento obor má za úkol vyškolit kompetentní absolventy ve vývoji a řešení

technologií, které zvyšují bezpečnost informací, jakož i implementaci a správu komunikačních sítí mezi počítači a technologickými zařízeními, které to umožňují. (Universidad Cuahtemoc, 2019) Na úrovni magisterského studia je v Mexiku rozvinutá *Maestría en Ciberseguridad* na *Universidad La Salle* a *Tec de Monterrey*, která žáky školí a seznamuje se znalostmi, dovednostmi a postoji, které jim umožní navrhovat, řídit, realizovat a hodnotit iniciativy, projekty a strategické plány kybernetické bezpečnosti v souladu s obchodní architekturou a v souladu s cíli jednotlivých organizací. (Universidad La Salle, 2019) Povědomí o kybernetické bezpečnosti zatím v Mexiku chybí na základních a středních školách a jeho rozvinutější a propracovanější verze taktéž na doktorském studiu.

9.4.2.Profesní vzdělávání

Znalosti o tomto tématu je však možné načerpat na úrovni profesní. V zemi existuje profesionální sdružení odborníků, manažerů nebo auditorů v oblasti kybernetické bezpečnosti. Jedním z nich je například sdružení *ISACA* (*Sistemas de Información de Auditoría y Control Association*).Toto celosvětové sdružení profesionálů v IT se v současné době zaměřuje na zabezpečení a správu IT a zároveň poskytuje celosvětově uznávané certifikace. Jednotliví zaměstnanci v oboru kybernetické bezpečnosti či IT mohou zlepšit svou znalostní úroveň a díky ISACA získat také certifikát ke své práci na podporu jejich profesního růstu. (ISACA, 2019) Další společností, která se v Mexiku zabývá poradenstvím, školením a poskytováním služeb a produktů týkajících se bezpečnosti informací a kybernetické bezpečnosti je *AMECI (Asociación Mexicana de Ciberseguridad)*. Hlavní iniciativou této organizace je šíření kultury informační bezpečnosti prostřednictvím sociálních sítí, blogů, video kanálů a konferencí pořádaných v různých institucích, univerzitách, organizacích a společnostech. AMECI se snaží poskytovat tyto informace hlavně ředitelům, manažerům a dalším rozhodovacím funkcím. Dále také techickému personálu zabývajícímu se informačními

technologiemi a bezpečností či komunikací, a samozřejmě zaměstnancům, kteří pracují v rámci těchno společností či organizací. (AMECI, 2019)

9.4.3.Kampaně na podporu kybernetické bezpečnosti v Mexiku

Ciberseguridad México je projekt, který se v Mexiku konal již v letech 2017 a 2018, a aktuálně se čeká také na jeho další ročník na rok 2019. Projekt je pod záštitou *Secretaría de Seguridad y Protección Ciudadana* (SSPC) a v roce 2018 na něm přední představitelé bezpečnosti v Mexiku zdůraznili význam spolupráce mezi občanskou společností a institucemi, aby bylo v mexickém kyberprostoru možné vybudovat společný mír. Tato iniciativa se snaží ovlivnit povědomí o kybernetické bezpečnosti a užívání informačních technologií ve společnosti. Stále více kriminálních případů se totiž odehrává právě v tomto prostředí, což se samozřejmě netýká pouze Mexika. *Ciberseguridad México 2019* bude se svým putovním programem aktivit po celé zemi, a to ve spolupráci s občanskými organizacemi. Informace o kampaních lze vidět také na internetu, např. na oficiálním Twitter účtu SSPC. Kampaň je zaměřena také na školy a seznamování dětí s problematikou informační technologie a hlavně kybernetické bezpečnosti, která je aktuálně v Mexiku velmi diskutovaným tématem. (Alcaldes de México, 2019; El Economista, 2019; Gobierno de México, 2018)

9.5. Indikátor č. 3: podíl na mezinárodní úrovni v kyberbezpečnosti

Mexiko, stejně jako spousta dalších zemí světa, řeší problematiku kybernetické bezpečnosti nejen na národní, ale také na mezinárodní úrovni. V rámci *Organizace spojených národů (OSN)* podporuje *World Summit on Information Society (WSIS)*, který se poprvé konal v Ženevě v roce 2003. Jeho druhá fáze pak byla uskutečněna v roce 2005 v Tunisku. Obou summitů se zúčastnily mezinárodní organizace, vlády, soukromý sektor a také občanská společnost. Diskuse byla vedena směrem k příležitostem nového informačního a

komunikačního prostředí a přístupu k informacím a komunikaci. Mimo vytvoření konečných dokumentů vedl summit také k vytvoření *Internet Governance Forum* (IGF), které se v roce 2016 dokonce konalo v mexickém Jaliscu a *United Nations Group on the Information Society* (UNGIS). (CIDGE, 2017, s. 9; UNESCO, 2017) Dalším významným posunem v mezinárodní spolupráci pro Mexiko bylo vytvoření tzv. *El Grupo de Expertos Gubernamentales (GEG)*, skupiny vládních expertů, která vznikla za účelem analýzy hrozeb a výzev kybernetické bezpečnosti a ke sjednocení doporučení a pokynů týkajících se mírového využívání IT, uplatňování mezinárodního práva v kyberprostoru, opatření pro budování důvěry a stability a posílení národních kapacit týkajících se tohoto tématu. GEG je pod oficiálním vedením OSN s aktuální kolaborací OAS. (Enfoque Noticias, 2019; CIDGE, 2017, s. 9) Pod záštitou OSN se dále Mexiko podílelo na dokumentu *La Comisión de Prevención del Delito y Justicia Penal (CCPCJ)*, ve kterém mezi členy figurují např. Polsko nebo Rusko. Tato komise vypracovala studii o počítačové trestné činnosti, jejímž cílem je posílit výměnu zkušeností a osvědčených postupů k vytvoření příležitosti ke spolupráci a technické pomoci, které umožňují taktickou a operativní podporu státům, jež čelí trestnému využívání IT, včetně internetu. (CIDGE, 2017, s. 9; ONU, 2000, s. 1) V roce 2016 se v mexickém Jaliscu konalo *Foro para la Gobernanza de Internet (FGI)*, jež je mezinárodním prostorem pro dialog o otázkách týkajících se vývoje internetu ve zúčastněných zemích. Snaží se spojit a vytvořit těmto zemím internetový ekosystém, jež by zahrnoval vlády, soukromé sektory a občanské společnosti, tak, jako technické a akademické obce, a to za rovných podmínek a prostřednictvím otevřeného inkluzivního procesu. Fórum pod záštitou OSN funguje již od roku 2006. (Wikipedia, 2019; CIDGE, 2017, s. 10) *Unión Internacional de Telecomunicaciones* (ITU) vytvořila anketu nazvanou *Índice Global de Ciberseguridad*, která má za cíl sledovat závazek vůči kybernetické bezpečnosti u 194 členských států ITU. Podle *Estrategia Nacional de Ciberseguridad* je Mexiko, stejně jako ostatních 76 zemí, identifikováno ve fázi „zrání“, zatímco

pouze 21 zemí se nachází ve fázi „vedoucí“. (Deloitte, 2019; CIDGE, 2017, s. 10) V rámci *Organización para la Cooperación y Desarrollo Económicos (OCDE)* podepsala vláda během jednoho ze zasedání týkajícího se digitální ekonomiky v roce 2016, spolu s dalšími zúčastněnými stranami, spolupráci k využití potenciálu digitální ekonomiky. Mezi hlavními faktory, které toto zasedání vytvořilo, je např. snížení překážek národního elektronického obchodu na mezinárodní úrovni, vypracování globální technické normy pro stabilní a otevřený internet, rozvíjení rozhodovacích pravomocí strategie ochrany soukromí a údajů zdůrazňujících transaprentnost ve veřejném sektoru. (CIDGE, 2017, s. 10; OECD, 2019) Mexiko je také součástí *Convenio de Budapest* nebo-li *Úmluvy o počítačové kriminalitě*, která je jedním z nejdůležitějších dokumentů týkajících se kybernetické bezpečnosti v mezinárodní spolupráci. (Council of Europe, 2019)

10. Kolumbie

Následující kapitola se zabývá popisem aktuální situace v oblasti kybernetické bezpečnosti v Kolumbii. Jedná se tedy o vývoj národní strategie kybernetické bezpečnosti, její hlavní institucionální, legislativní, regionální a mezinárodní představitele a hlavní body, kterými se aktuálně národní strategie zabývá.

10.1. Indikátor č. 1: rozvoj politiky státu v rámci kyberbezpečnosti

10.1.1. Política Nacional de Seguridad Digital

Kolumbijské státní instituce od roku 2007 diskutovaly důležitost vytváření politiky kybernetické bezpečnosti a kybernetické obrany. Za tímto účelem národní vláda, s mezinárodní podporou OAS a prostřednictvím CICTE, uspořádala v roce 2008 workshop zaměřený na zvyšování povědomí o kybernetické bezpečnosti. Výsledkem bylo, že státní instituce požádaly *Ministerio de Defensa Nacional* o převzetí vedení, které by umožnilo prosazování politiky týkající se kybernetické bezpečnosti a také společně s tím vytvoření mechanismů, které by mohly reagovat na incidenty a zločiny postihující celou zemi. Žádost vznikla v důsledku hloubkové analýzy systému národní bezpečnosti, technických možností existujících na ministerstvu obrany a studie o mezinárodním kontextu. (Departamento Nacional de Planeación, 2011, s. 13) Akční plán, který má za úkol realizovat celou politiku týkající se digitální bezpečnosti, se rozhodla kolumbijská vláda realizovat v letech 2016 až 2019 s celkovou investicí 85 070 milionů pesos. Hlavním úkolem národní strategie je vytvoření institucionálního rámce digitální bezpečnosti v zemi. Budou vytvořeny nejvyšší úrovně koordinace a lepší orientace v této oblasti jak ve vládě, tak také v ostatních výkonných subjektech na vnitrostátní úrovni a budou jasně daná sektorová pravidla. Následuje vytvoření podmínek pro řízení rizik digitální bezpečnosti v sociálně-ekonomických činnostech a budování důvěry ve využívání digitálního prostředí prostřednictvím

mechanismů pro aktivní a trvalé zapojení, přizpůsobení právního a regulačního rámce předmětu a školení pro odpovědné chování v digitálním prostředí. Taktéž bude posílena národní obrana a bezpečnost v tomto prostředí na národní a mezinárodní úrovni a budou vytvořeny mechanismy na podporu spolupráce a pomoci v oblasti digitální bezpečnosti na vnistrostátní a samozřejmě také mezinárodní úrovni se strategickým zaměřením. (Departamento Nacional de Planeación, 2016, s. 3) Hlavní vládní strategií pro boj s kybernetickými útoky a ochranou kybernetické bezpečnosti je *Política Nacional de Seguridad Digital*, vedená pod oficiálním názvem CONPES 3854. Tento dokument v sobě zahrnuje veškeré důležité informace, které jsou v digitální kolumbijské politice aktuální. Jedním z předchozích dokumentů, které pomohly formovat aktuální podobu *Política Nacional de Seguridad Digital* je *Lineamientos de Política para Ciberseguridad y Ciberdefensa* (CONPES 3701) z roku 2011. Tento dokument shromažďuje veškeré pokyny ke kybernetické bezpečnosti a kybernetické obraně a je zaměřen na pozdější vypracování národní strategie, která bojuje proti nárůstu počítačových hrozeb. Dalším bodem, který vedl k vytvoření strategického plánu kybernetické bezpečnosti byla skutečnost, že celá tato problematiku byla již v roce 2010 zaimplementovná do národního rozvojového plánu pro roky 2010-2014 s název *Prosperidad para Todos*. Tento plán byl veden *Ministerstvem informačních a komunikačních technologií* a jeho účelem je podporovat masové využívání internetu a udělat zásadní krok k demokratické prosperitě. (Departamento Nacional de Planeación, 2016, s. 3; Departamento Nacional de Planeación, 2011, s. 13)

10.2.Institucionální hledisko kybernetické bezpečnosti

Aktuálně v kolumbijské politice neexistuje na vnitrostátní úrovni mechanismus, který by usnadňoval spolupráci a pomoc mezi více zúčastněnými stranami. Chybí účinná komunikační strategie mezi vládou, soukromým sektorem a univerzitami. Mezinárodní směrnice však tuto komunikaci doporučují a určují v

mezinárodních směrnicích, proto je také důležitou součástí národní strategie. (Departamento Nacional de Planeación, 2016, s. 47)

10.2.1.Vládní instituce

Jednou z vládních institucí je skupina ColCERT, která má za úkol reagovat na mimořádné kybernetické události ve státě. Má hlavní odpovědnost za koordinaci národní kybernetické bezpečnosti a obrany, a to pod záštitou *Ministerio de Defensa Nacional (Mindefensa)*. Jejím hlavním účelem je koordinace nezbytných opatření na ochranu kritické infrastruktury kolumbijského státu před mimořádnými událostmi v oblasti kybernetické bezpečnosti, jež narušují nebo ohrožují národní bezpečnost a ochranu. (colCERT, 2019) Kolumbie je jedna ze zemí, která kybernetickou bezpečnost zohlednila také v armádních institucích. *Comando Conjunto Cibernético (CCOC)* je elitní jednotkou patřící pod *Comando General de las Fuerzas Militares de Colombia*, která má za úkol chránit kybernetickou bezpečnost a starat se o její obranu, a to včetně ochrany národních kybernetických infrastruktur, rozvoje vojenských operací v kyberprostoru na obranu suverenity, nezávislosti, územní celistvosti a ústavního pořádku. Jedná se o vojenské síly, které provádějí vojenské operace zaměřené na tyto hlavní body. Koordinují, plánují, integrují a provádí vojenské operace v kyberprostoru na obranu národních zájmů a národní kybernetické infrastruktury. CCOC radí prezidentovi republiky, ministru obrany a *Consejo de Defensa Nacional* ve vojenských záležitostech, taktéž připravují příslušné primární a sekundární dokumenty týkající se národní bezpečnosti, vykonávají velení sil a strategické vedení vojenských operací, aj. (CCOC, 2019) Stejně jeko předchozí Chile a Mexiko, také Kolumbie má v rámci institucionálním podporu kybernetické bezpečnosti v policejních složkách. *Centro Cibernético Policial (CCP)* pod záštitou *Policía Nacional de Colombia* má na starost kybernetickou bezpečnost na kolumbijském území, poskytuje informace, podporu a ochranu před počítačovými trestnými činy. CCP také rozvíjí prevenci a péči ve vyšetřování a stíhání

počítačových zločinců v zemi a na svých webových stránkách informuje o veškerých potřebných informacích týkajících se kybernetických útoků, ale také bezpečnosti. Spolupracuje s výše uvedenou skupinou colCERT. (Departamento Nacional de Planeación, 2011, s. 25) V rámci IT se Kolumbie rozvíjí díky *Subdirección técnica de seguridad y privacidad de tecnologías de información*. Toto IT oddělení spadající pod *Ministerio de Tecnologías de la Información y las Comunicaciones (MINTIC)* se specializuje na bezpečnost a soukromí a je zodpovědné za vytváření bezpečnostních pokynů a zásad pro státní subjekty. (MINTIC, 2019) Posledním z implementovaných vládních subjektů v rámci nově vznikající politiky kybernetické bezpečnosti je *Comisión Nacional Digital y de Información Estatal*. Účelem této komise je koordinace a lepší orientace výkonu funkcí a veřejné služby související se správou veřejných informací s využitím infrastruktury informačních technologií pro interakci s občany a účinným využíváním informací ve státě Kolumbie. (Departamento Nacional de Planeación, 2016, s. 76)

10.2.2.Soukromé a akademické instituce

Aktuálně disponuje Kolumbie celkem 11 skupinami spadajícími pod fórum FIRST. Jedním z nich je novější ***Cyber Defense Operation Center (C-DOC)***. Toto operační středisko se věnuje odvětví IT a má za úkol digitální ochranu veřejného i soukromého sektoru. Hlavní pobočka se nachází v USA a jedna samozřejmě v Kolumbii. (FIRST, 2019) Další skupinou je ***CSIRT-CC***, která v zemi funguje od roku 2013 v rámci *Cámara Colombiana de Informática y Telecomunicaciones (CCIT)*. Toto kolumbijské koordinační středisko v oblasti incidentů informační bezpečnosti je v přímém kontaktu s bezpečnostními středisky přidružených společností a je schopné koordinovat vyřizování žádostí a stížností v počítačové bezpečnosti. (CSIRT-CC, 2019) ***Equipo de respuesta a incidentes de seguridad informática de la Policía Nacional (CSIRT PONAL)*** nebo také CC-CSIRT je tým *Policía Nacional de Colombia*, který je vytvořen pro

plnění potřeb prevence, pozornosti a vyšetřování událostí a incidentů spojených s počítačovou bezpečností. Tým má za úkol hlavně posilu institucionálního rámce národní strategie kybernetické bezpečnosti a také ochranu před incidenty, které ohrožují důvěrnost, dostupnost a integritu informací. (CSIRT PONAL, 2019) Dalšími skupinami fungujícími na této bázi jsou v Kolumbii: *CSIRT-ETB, CSIRT OLIMPIA, DigiCSIRT, ETEK-CSIRT, ITSSOC-CSIRT, ShieldNow, SOC Team Claro Colombia, SOC-CCOC.*

10.3.Legislativní hledisko kybernetické bezpečnosti

V Kolumbii byly zavedeny či aktualizovány zákony věnující se hlavně ochraně osobních údajů, pornografii, sexuální turistice, atd. Mezi hlavní legislativní nástroje kybernetické bezpečnosti v zemi se stejně jako v ostatních případech, řadí hlavně *Convenio de Budapest*, ke kterému se Kolumbie přidala v roce 2018 a podle něhož byl tvořen a aktualizován zákon *Ley 1928* vypovídající o kybernetické bezpečnosti v zemi. (Departamento Nacional de Planeación, 2011, s. 15; El Congreso de Colombia, 2018) K výše uvedené základní legislativě lze připočítat také *el capítulo 1 del título II de la Constitución*, která se zabývá základními právy na osobní a rodinné soukromí a dobré jméno a povinnost státu je respektovat a přimět je respektu (*artículo 15*) a dále *artículo 20*, kde je každému zaručena svoboda vyjadřovat a šířit své myšlenky a názory, informovat a přijímat pravdivé a nestranné informace a zřizovat hromadné sdělovací prostředky. (Departamento Nacional de Planeación, 2016, s. 20) Co se týče předpisů týkajících se primárně tématu kybernetické bezpečnosti a informační bezpečnosti, Kolumbie v roce 2011 změnila trestní zákon. Aktuálně existuje komplexní a účinná procesní legislativa, která je schopna se zabývat počítačovými trestnými činy a uznává mezinárodní smlouvy vytvořené ve spolupráci s INTERPOLem a EUROPOLem. Kromě toho jsou dané orgány v trestním řízení a soudnictví oprávněny vyšetřovat a řešit případy počítačové trestné činnosti. (Departamento Nacional de Planeación, 2016, s. 21) Z mnoha četných zákonů,

které se v Kolumbii nacházejí a mají spojitost také s kybernetickou bezpečností, je důležité si povšimnout zejména těch signifikantních: *Ley 1273* z roku 2009, který upravil trestní zákon a vytvořil nový chráněný právní statek, který se věnuje ochraně informací a údajů v IT systémech, *Ley 1341* z roku 2009, na jehož základě jsou nejen definovány principy a koncepty informační společnosti a organizací využívajících systémy IT, ale také je vytvořena *Agencia Nacional de Espectro*, která vytváří další potřebná ustanovení. (Departamento Nacional de Planeación, 2016, s. 76) Velmi důležitým krokem vstříc zlepšení kybernetické bezpečnosti v zemi bylo ustanovení *Decreto 2758* z roku 2012, který znamená restrukturalizaci *Ministerio de Defensa Nacional* ve smyslu přiřazení úřadu náměstka ministra k vytváření politik a strategií týkajících se kybernetické bezpečnosti a kybernetické obrany. Kromě toho odpovídá také za ředitelství pro veřejnou bezpečnost a infrastrukturu, funkci implementace politik a programů, které udržují veřejnou bezpečnost a chrání infrastrukturu, a dále sleduje řízení související s kybernetickým rizikem v obranném sektoru a navrhuje strategický plán v oblasti kybernetické bezpečnosti a kybernetické obrany. (Departamento Nacional de Planeación, 2016, s. 76) *MinTIC* v souladu s pokyny uvedenými v dokumentu CONPES 3701 vytvořil *Decreto 0032* z roku 2013 *Comisión Nacional Digital y de Información Estatal*. A nakonec *Decreto 1078* z roku 2015 prostřednictvím kterého je vydána jednotná regulační vyhláška v IT, jejímž cílem je sestavení již existujících regulačních pravidel upravujících toto odvětví. (Departamento Nacional de Planeación, 2016, s. 77)

10.4.Indikátor č. 2: vzdělávání a profesní rozvoj v kyberbezpečnosti

Nutnost implementace povědomí o kybernetické bezpečnosti nejen do veřejné politiky, ale také do edukativních programů je v zemi jedním z dalších rozvíjejících se témat. Problematika vzdělávání v oblasti kybernetické bezpečnosti je jednou z kapitol v *Agenda Estratégica de Innovación: Ciberseguridad*,

dokumentu vytvořeném MinTIC v roce 2014. Kvalitní vzdělání a odborná příprava je zde označena za aktivní entitu a jeden ze základních faktorů kybernetické bezpečnosti. Člověk je podle dokumentu nejslabším článkem zabezpečení při využívání a transformaci informací. To je základním důvodem pro prosazení inovací ve znalostech společnosti, zaměřených na vytváření povědomí, odpovědnosti a povinnosti chránit informace. S ohledem na tuto skutečnost MinTIC v daném dokumentu uvedlo několik inovací, které by se měli v edukačních programech po celé zemi odrazit. Hlavní změnou by mělo být zařazení kybernetické a informační bezpečnosti do akademických osnov na co nejvyšší možné úrovni. Důležitá je také definice, strukturování a implementace následovaná testováním metodických, pedagogických a vzdělávacích schémat a osvědčených postupů v tomto odvětví, a to nejen pro školy, ale také pro státní subjekty. (MinTIC, 2014, s. 9) Podle měření MinTIC mělo počátkem roku 2018 k internetu přístup celkem 30, 4 milionů obyvatel Kolumbie. Toto číslo se od předchozího roku razantně zvýšilo, stejně, jako počet kybernetických útoků. Na internetu se stejně jako v Mexiku či Chile pohybuje aktuálně stále více dětí a mládeže také v Kolumbii. Je proto potřeb zajistit včasnou a vhodnou přípravu a opatření před kybernetickými útoky. (MinTIC, 2018)

10.4.1.Školní vzdělávání

Na úrovni základního a středoškolského vzdělání se aktuálně nepodařilo v Kolumbii tuto myšlenku uplatnit. Na univerzitním stupni lze nalézt dva obory zabývající se kybernetickou bezpečností na magisterském studiu. *Universidad de los Andes* v hlavním městě poskytuje na svém *Departamento de Ingeniería de Sistemas y Computación* obor nazvaný *Maestría en Seguridad de la Información MESI*. (NCSI, 2019; Universidad de los Andes, 2016)

10.4.2.Profesní vzdělávání

Další možností, jak se seznámit s informacemi o kybernetické bezpečnosti je prostřednictvím společností a organizací vedených odborníky v tomto oboru. V Kolumbii i tento způsob již začal aktivně fungovat: ***ISACA Medellín Chapter*** v Kolumbii vznikla v roce 2014 pod vedením místních profesionálů jako 224. světová pobočka. O rok později byla vytvořena také ***ISACA Bogotá Chapter***, která má sídlo v hlavním městě Bogotá. (NCSI, 2019; ISACA, 2019) ***OWASP Bogotá***, tedy globální neziskové profesní sdružení, které kolem sebe shromažďuje lidi zajímající se o softwarové zabezpečení. (NCSI, 2019; OWASP, 2019) ***HackLab Bogotá***: jedná se o komunitu, která koordinuje týdenní setkání, na kterých je možné diskutovat o různých tématech informační bezpečnosti. Tato komunita nabízí nejen možnost setkání s odborníky v oboru, ale také načerpání nových zkušeností a informací a možnosti dalšího osobního rozvoje v této problematice. (HackLab Bogotá, 2019) Poslední kolumbijskou aternativou pro profesní vzdělávání je ***CSIETE Colombia***, nezisková organizace vytvořená pro výzkum vývoje projektů týkajících se digitální bezpečnosti a počítačové bezpečnosti. (NCSI, 2019; CSIETE, 2019)

10.4.3.Kampaně na podporu kybernetické bezpečnosti v Kolumbii

V rámci výuky dětí a nezletilých žáků v Kolumbii se rozhodla začátkem roku 2018 *Policía Nacional* o uspořádání akce *a clases con ciberseguridad*, která vyhledá a internalizuje optimální využití sociálních sítí pro děti a dorost, jejichž bezpečnost a identita je častým cílem kybernetických zločinů díky špatnému užívání těchto platforem. Akce proběhla pod vedením oddělení Boyacá pro třídy v Duitamě ve škole *La Presentation* s účastí dalších škol: *Santo Tomás de Aquino* a *Colegio Guillermo León Valencia*, *Sogamoso*, *Chiquinquirá* a další školy v oblasti Boyacá, které se těmito otázkami zabývají také ve svých osnovách. (MINDEFENSA, 2018)

10.5.Indikátor č. 3: podíl na mezinárodní úrovni v kyberbezpečnosti

Stejně jako ostatní země zabývající se kybernetickou bezpečností, také Kolumbie je jedním ze signatářů *Convenio de Budapest*, mezinárodního ujednání o problematice kybernetické bezpečnosti, které stanovuje hlavní právní řády týkajícího se tohoto tématu. Kolumbie je taktéž jedním z členů na Asamblea *General de la OEA*, které stanovuje komplexní strategii boje proti hrozbám pro kybernetickou bezpečnost s vícerozměrným a multidisciplinárním přístupem k dosažení kultury kybernetické bezpečnosti. Dále je důležitá také účast v *Comunidad Andina*, která spojuje zájem o vnější bezpečnost a politiku všech andských zemí v dokumentu *Política de seguridad externa común andina*. (Departamento Nacional de Planeación, 2016, s. 22) Mezi dalšími mezinárodními spoluprácemi Kolumbie se nachází například: *Wales summit* v roce 2014, kde bylo umožněno všem státům NATO diskutovat o aktuálních otázkách společných zájmů v oblasti bezpečnosti a plánovat strategické aktivity. (Departamento Nacional de Planeación, 2016, s. 22; Wikipedia, 2019) V roce 2015 byl odsouhlasen dokument *Declaración sobre la protección de infraestructura crítica ante las amenazas emergentes* vytvořený pod vedením CICTE. Jedná se o technickou pomoc, která umožňuje jejím členům připravit seznam kritické infrastruktury a její klasifikaci na základě příslušných aktivit, systémů, sítí a základních funkcí, které umožní to nejlepší hodnocení zranitelností, hrozeb a rizik. (Departamento Nacional de Planeación, 2016, s. 23; OAS, 2015)

11. Hodnotící SWOT analýza

11.1.Chile

Silné stránky	Slabé stránky
• Základ pro národní strategii byl založen již dva roky před uvedením samotné strategie - v roce 2015 • Ještě před uvedením strategie byl založen výbor zabývající se výhradně tématem kybernetické bezpečnosti v zemi • Již před oficiální strategií fungovala také skupina CSIRT na vládní úrovni • Národní strategie má jasně daný program na dobu 5 let • Skupiny FIRST jsou obsaženy ve všech oblastech - skupiny jsou na soukromé, akademické a také vládní bázi • Vláda zajistila speciální policejní složky věnující se pouze kybernetické bezpečnosti • Vláda vytvořila několik nových ustanovení v legislativě, která se týkají výhradně kybernetické bezpečnosti • Aktivně fungující obory věnující se kybernetické bezpečnosti na bakalářském a magisterském studiu • Fungující vzdělávání v oblasti soukromého sektoru • Rozvinuté kampaně na podporu vzdělávání v oblasti kybernetické bezpečnosti • Chile je součástí Convenio de Budapest	• Nesnadná identifikace pachatele, který se může nacházet i mimo daný stát, ve kterém páchá zločin • Strategie fungující po dobu 5 let se může pomaleji přizpůsobovat neustálému posunu v technologii • Skupiny FIRST nejsou v zemi zastoupeny telekomunikačními společnostmi, které by je zaštiťovaly • Chile se musí aktivněji zapojovat do mezinárodního práva, které by celosvětově pokrylo stíhání pachatelů. • Vzdělávání není rozvinuto na úrovni základního a středního vzdělání. • Rozšíření vzdělávacích programů na univerzitách pro pokrytí většího území Chile • Rozšíření vzdělávacích programů a oborů na úrovni doktorského studia na univerzitách • V rámci vzdělávání v soukromém sektoru se postarat o kampaně a velké prezentace pro vzdělávání mnohem větší části populace • Pořádání mezinárodních zasedání a fór na území Chile • Rozvinutější ochrana kybernetické bezpečnosti na vojenské úrovni • Vzdělávání policejních složek

Příležitosti	Hrozby
• Rozvinutí vzdělávání v oboru kybernetické bezpečnosti na národní úrovni • Rozšíření FIRST skupin do více sektorů a zvýšení jejich počtu • Zlepšení mezinárodní komunikace v oblasti kybernetické bezpečnosti	• Neustále se zdokonalující technologie • Rostoucí užívání internetu v domácnostech • Rozvíjející se možnosti napadání kybernetického prostoru • Anonymita pachatelů • Nedostatečné vzdělávání obyvatelstva o správném používání a pohybování se v kybernetickém prostoru

Od roku 2015 do roku 2016 stouplo využívání internetu z 12 819 000 uživatelů na 16 157 000. V roce 2018 se k internetu v Chile připojilo celkem 21 365 000 obyvatel. Stejně tak stoupalo také napadení mobilního a pevného internetu, které dosáhlo v prosinci roku 2018 112,9 napadení na každého 100 obyvatele Chile. (Ministerio de Transportes y Telecomunicaciones, 2019) Tato čísla byla také rozhodujícími pro konečné vyřešení oficiálního dokumentu, který by zaručoval jasně vyhrazenou strategii, jak v případě kybernetické bezpečnosti v Chile postupovat. Koordinaci strategie a přesného plnění jejich plánů se zabývá komise, která byla vytvořena již před samotným uvedením strategie a která dohlíží na její vyhotovení a plnění. Pevné kořeny v politice vznikající již před samotnou strategií jsou velice důležité, jelikož byly schopny zmapovat cíl budoucí politiky a také do hloubky analyzovat problematiku, kterou by se měly cíle této strategie zabývat. Díky tomu bylo jednodušší stanovit cíle politiky kybernetické bezpečnosti v zemi a rozhodnout o jejím plánu. Strategie byla oficiálně naplánována na rozmezí 5 let, tedy od roku 2017 až do roku 2022. Jasně daný časový úsek je velmi vhodný pro efektivnější plnění cílů, nicméně lze nalézt také jisté nevýhody. Časové odvětví 5 let může být velmi rizikové zvláštně v technicky založených tématech, neboť za tuto dobu se může vývoj kybernetického prostoru

a kybernetické bezpečnosti změnit natolik, že aktuální plán nebude schopen reagovat na tyto změny adekvátně.

Jednou z nejsilnějších stránek, kterou politika pro kybernetickou bezpečnost v Chile má, je skupina CSIRT na vládní úrovni. Tato skupina vznikla taktéž několik let před národní strategií a lze říci že velkým dílem přispěla k ochraně kybernetického prostoru ještě před vytvořením samotné politiky zabývající se touto problematikou. Taktéž má Chile silné zastoupení (kromě vládního), také v sektorech soukromých a akademických - pomocí skupin FIRST, které dnes oficiálně fungují na jeho území. Nicméně nesmíme zapomínat na významnou složku kybernetické bezpečnosti, kterou tvoří telekomunikační společnosti. Zde vidím jednu nevýhodu ze strany Chile, a to opomenutí vytvoření skupiny FIRST pod záštitou jedné z takovýchto společností. Telekomunikační společnosti jsou mnohdy schopny rychleji reagovat na porušení kybernetické bezpečnosti a mají také velký přehled o užívání internetu či mobilních zařízení v celém státě. Svými znalostmi by mohly významně přispět do boje s kybernetickou kriminalitou.

Další ze silných stránek v postavení Chile ke kybernetické bezpečnosti je zajištění policejních jednotek, které se zabývají kybernetickými zločiny a přispívají k dodržování legislativy v oblasti kybernetického prostoru v zemi. Do budoucna by však podle mého názoru mělo Chile počítat také s vojenskou ochranou kybernetického prostoru a to z důvodu jejího mezinárodního přesahu. Vláda v závislosti na tomto ohrožení zařadila do své legislativy také několik zcela nových zákonů, které pomáhají při udržování kybernetické bezpečnosti, či uzpůsobili tomuto novému fenoménu také několik stávajících zákonů. I v tomto případě je však národní právo neustále třeba kontrolovat, a to v závislosti na právu mezinárodním, které je schopno pomoci s rozvojem legislativy kybernetické bezpečnosti o mnoho více.

Pozitivním výsledkem národní strategie je také její přesah na akademickou půdu. V Chile dnes aktivně funguje několik univerzitních oborů zabývajících se

výhradně tématem kybernetické bezpečnosti. Vzdělávání v tomto oboru je velmi důležité nejen ve školních lavicích, ale také v soukromém sektoru, pro odborníky či profesionály. Zde vytvořilo Chile několik institucí, které se v rámci tohoto sektoru starají o jeho neustálý rozvoj. Spolupráce s mezinárodními společnostmi jako je ISACA je v tomto směru pouze pozitivním krokem vpřed. Nicméně lze Chile vytknout, že vzdělávací program ještě stále nezařadila do osnov základních a středních škol, které jsou aktuálně nejdůležitějším sektorem, na který je potřeba se zaměřit. Také by bylo vhodné zaměřit se na doktorské studium či vytvoření několika vzdělávacích odborných center rozmístěných do největších měst, aby bylo zajištěno vzdělávání mnohem větší části populace. Hlavní příležitostí, kterou v budoucím rozvoji boje proti kybernetickým útokům a k posílení kybernetické bezpečnosti u Chile vidím, je především rozvinutí vzdělávání v oboru kybernetické bezpečnosti na národní úrovni. To znamená, postarat se o školení „nové generace“, která se bude stále více setkávat s technologiemi již od útlého věku a tím zabraňovat a snižovat možnostem kybernetického napadání jak obyvatel země, tak také celého státu. Doba technologií s sebou přináší rozvinutí také veřejného sektoru, banky již dnes celosvětově fungují na bázi internetového bankovnictví.

S rostoucím zájmem o internet nejen u dospělých, ale také menších uživatelů, se Chile rozhodlo podpořit kampaně šířící „osvětu“ kybernetické bezpečnosti mezi mladšími obyvateli. Chile má k dnešnímu dni ve svém programu zařazeny celkem 3 důležité kampaně, které napomáhají seznamování s kybernetickou bezpečností v rámci státu, což je velmi pozitivní změnou v chování státu před zavedením strategie.

Co se týče mezinárodního chování, Chile podepsalo *Convenio de Budapest*, čímž se oficiálně celosvětově přidalo do skupiny států, které s bojem proti kybernetické kriminalitě započaly taktéž. Tento krok byl strategickým a důležitým, pozvedlo Chile na mezinárodní úrovni mezi státy, které jsou za svou historii s kybernetickou bezpečností již schopny mnohem více poradit ve vedení

institucionálním či legislativním. Stále nicméně chybí větší iniciativa ze strany Chile, která by sama navrhovala lepší a rozvinutější ochranu či pořádala mezinárodní konference a dostala se tak do povědomí zkušenějších vlád. Nelze stále zapomínat, že problematika napadání kybernetického prostoru je z mezinárodního hlediska velmi palčivým problémem, jelikož pachatelé těchto činů nejsou omezováni hranicemi státu. Mezinárodní prostor tvoří další příležitost, ke které by se Chile nemělo otáčet zády a naopak jí podporovat v budoucím vývoji své strategie o kybernetické bezpečnosti.

Pro budoucí ochranu kybernetického prostoru však Chile musí počítat se stálými hrozbami, kterými jsou hlavně neustále se zdokonalující technologie a jejich rostoucí užívání v jednotlivých domácnostech. Bude-li užívání internetu stoupat i v budoucích letech se stejnou rychlostí, tlak na politiku vytvářející strategii bude mnohem vyšší a její koordinace těžší. Chile musí předpokládat s neustále se měnícím kybernetickým prostorem, stejně jako s neustále se zdokonalujícími technologiemi, které v něm dominují. S jejich vytvářením bude stále sofistikovanější také způsob napadání internetového či počítačového prostoru, což bude i nadále značně ztěžovat jakoukoli jeho obranu. Přetrvávající anonymita pachatelů bude velkým problémem zejména pro vypátrání jejich identity a proto je důležité také správné vzdělávání policejních složek a jednotek, které se správným vedením budou schopny alespoň držet krok s neustále se měnícím prostředím. Ruku v ruce s tímto problémem jde i (již tolikrát vzpomínané) vzdělávání obyvatelstva, které tak může významně snižovat hranici napadání internetového prostoru v zemi.

11.2.Mexiko

Silné stránky	Slabé stránky
• Již před oficiální strategií byl vytvořen dokument zabývající se kybernetickou bezpečností a vláda propagovala aktivně toto téma • Národní strategie byla podporována plánem pro rozvoj republiky • Vytvoření komise pro koordinaci strategického plánu • Vytvoření speciální odborné technické policejní skupiny • Vytvoření speciální policejní skupiny pro odhalování kybernetického zločinu • Vytvoření skupiny CERT na federální úrovni • Skupiny FIRST pokrývající soukromý, telekomunikační a také akademický sektor • Aktivně fungující obory věnující se kybernetické bezpečnosti na bakalářském a magisterském studiu • Fungující vzdělávání v oblasti soukromého sektoru • Funkční kampaň na rozvoj povědomí o kybernetické bezpečnosti v zemi • Mexiko je součástí Convenio de Budapest • Zapojení do mezinárodního dění v oblasti kybernetické bezpečnosti • Hostování mezinárodní konference věnující se kybernetickému prostoru	• Nesnadná identifikace pachatele, který se může nacházet i mimo daný stát, ve kterém je páchán zločin • Strategie fungující po dobu 5 let se může pomaleji přizpůsobovat neustálému posunu v technologii • Neexistuje žádná armádní skupina zajišťující dostatečnou ochranu kybernetického prostoru • Aktualizované školení policejních složek • Vzdělávání není rozvinuto na úrovni základního a středního vzdělání • Kampaně pro rozvoj povědomí o kybernetické bezpečnosti jsou jen málo rozvinuté a chybí jejich ucelenost • Chybí rozšíření vzdělávacích programů na univerzitách ve více federacích, aby byla pokryta větší část státu • Rozšíření vzdělávacích programů a oborů na úrovni doktorského studia neexistuje • Větší rozvoj vzdělávání v soukromém sektoru pro mnohem větší prezentaci a vzdělávání profesně zaměřené populace • Rozvinutí legislativy věnující se výhradně otázce kybernetické bezpečnosti • Vytvoření pevnější kultury kybernetické bezpečnosti v zemi pomocí rozšířeného vzdělávání

Příležitosti	**Hrozby**
• Vytvoření nové legislativy věnující se výhradně kybernetické bezpečnosti • Zlepšení vzdělávání v oboru kybernetické bezpečnosti napříč celým státem • Rozšíření vojenské obrany v otázce kybernetické bezpečnosti pro lepší ochranu státu • Zlepšení kampaní o šíření vzdělání v kybernetické bezpečnosti	• Neustále se zdokonalující technolgie • Rostoucí užívání internetu v domácnostech • Rozvíjející se možnost napadání kybernetického prostoru • Anonymita pachatelů • Nedostatečné vzdělávání obyvatelstva o správném užívání a pohybování se v kybernetickém prostoru • Nedostatečná legislativní ochrana bezpečnosti kybernetického prostoru

Mexiko se začalo zabývat kybernetickou bezpečnosti již před oficiálním vydáním strategie a její potřebu naznačilo již v rozvojovém plánu pro rok 2013-2018. Důležitost takovéto strategie vyplynula také z neustále se zvyšujícího užívání internetu v domácnostech po celém Mexiku. V roce 2014 užívalo internet celkem 53 900 000 obyvatel státu. V roce 2017, při oficiálním zakládání strategie to bylo už celkem 79 100 000 obyvatel. Do roku 2018 stouplo užívání až na 82 700 000 připojení. (Asociación de Internet, 2019) Takto masivně roustoucí užívání internetu bylo jedním z hlavních impulsů pro vytvoření strategie kybernetické bezpečnosti. *Estrategia Nacional de Ciberseguridad* oficiálně vznikla v roce 2017 a byla podporována četnými vládními programy, které se již před jejím vznikem staraly o mapování problematiky kybernetické bezpečnosti ve státě. Důležitým bodem v propagaci a tvoření strategie byla také nově vytvořená komise zabývající se výhradně tématikou kybernetické bezpečnosti. Nicméně i přes tato opatření a jisté základy je rychle se měnící technologický pokrok velkým ohrožením jakékoli strategie a nesnadná identifikace pachatele tento problém pouze prohlubuje. Strategie, která je naplánována na určitou dobu, v tomto případě na rozmezí 5 let, tak nemusí být adekvátně přizpůsobila neustálým změnám.

Mexiko se věnovalo především rozvoji policejních skupin, což lze považovat za silnou stránku fungující strategie. Policejní složky jsou v tomto případě rozděleny na vědeckou divizi a policii zabývající se kybernetickou kriminalitou. Hlavní výhodou je nepřetíženost jednotlivých složek a jasné rozdělení prací. Velkou výhodou je hlavně věděcká divize, která je schopna vyšetřovat kybernetickou kriminalitu na technologické a vědecké úrovni, což velmi pozitivně působí na neustále se měnící prostředí. Nicméně tím je také potřebné, aby Mexiko poskytovalo svým zaměstnancům adekvátní a aktualizované vzdělávání v tomto oboru a aby boj s kybernetickým zločinem byl ještě účinnější. V případě ochranného systému funguje v Mexiku také skupina CERT na federální úrovni a několik skupin FIRST, které jsou schopny pokrýt jak telekomunikační, tak také soukromý a akademický sektor. Navíc má Mexiko také skupiny, které spolupracují se samotnou policií. Organizace policejních složek a jejich spolupráce je v Mexiku velmi silnou stránkou. Jedna z FIRST skupin spolupracuje aktivně také s přední univerzitou UNAM.

I přesto, že je institucionální ochrana kybernetického prostoru silnějším článkem mexické národní strategie, velmi slabou stránkou je hlavně její legislativní stránka, o jejíž změně již proběhlo v letošním roce několik jednání. Mexiko prakticky nemá k dispozici jakoukoli legislativu zabývající se výhradně problematikou kybernetické bezpečnosti. Je sice součástí mezinárodního *Convenio de Budapest*, avšak v rámci národní legislativy tuto problematiku prozatím nezapojilo do legislativy. To lze považovat za velmi slabou stránku veškerého přístupu ke kybernetické bezpečnosti v zemi a také příležitostí do budoucna.

Vzdělávání v Mexiku věnující se problematice kybernetické bezpečnosti je zavedeno na bakalářském a magisterském studiu. Nicméně, podíváme-li se na rozhlohu Mexika, je jasné, že velkou příležitostí pro vládu je v budoucnu rozšířit tyto obory také na jiné technologické školy v zemi a zajistit tak rovnoměrné možnosti ke studiu těchto oborů. Kybernetické vzdělávání je důležitou součástí

ochrany kybernetického prostoru při neustále se zvětšujícím využívání internetu, a to hlavě u nezletilých či mladých obyvatel, kteří si důsledky svých činů nemusí správně uvědomovat. V Mexiku prozatím informovanost na základních a středních školách chybí, a kybernetická gramotnost není zavedena v osnovách školy. To považuji za jednu z hlavních chyb a slabých stránek strategie, která si za hlavní cíl dává mimo jiné vytvoření kultury kybernetické bezpečnosti. Vzdělávání již od základního vzdělání je důležitou součástí budování povědomí o kybernetické bezpečnosti. V sektoru soukromém a profesionálním zaštiťuje vzdělávání několik organizací, jednou z nich je také mezinárodní ISACA, která například pomáhá již rozvoji vzdělávání také v Chile. Propojení národního a mezinárodního vzdělávání je v tomto ohledu velmi pozitivním krokem vpřed a Mexiku jistě přinese nové a lepší výsledky ve sféře profesionálů. Ačkoli v zemi funguje také jedna vzdělávací kampaň, mělo by se dbát na jejich rozšíření do budoucna, zvlášť u tak velkého státu jako je Mexiko. Mnohdy není možné dostat vzdělávání do všech koutů republiky, a je proto potřeba zavést systém kampaní či školení, které by povědomí o kybernetické bezpečnosti zaštítily po celé zemi. To vidím jako jednu z hlavních příležitostí pro budoucnost Mexika v kybernetické bezpečnosti.

Velmi silnou stránkou na mezinárodní úrovni je aktivní zapojování Mexika a také jeho výhodná geografická poloha. Mexiko dokonce hostilo mezinárodní fórum kybernetické bezpečnosti a v budoucnu se již jedná o dalších akcích podobného rázu. Pro stát je tento postoj velmi důležitý, neboť v rámci kybernetické bezpečnosti není možné aktivně bojovat proti zločinu bez mezinárodní pomoci. V rámci mezinárodních vztahů a zapojování se, je Mexiko na velmi dobrém bodě a bude-li pokračovat takto i v dalších letech, můžeme říci, že své mezinárodní postavení si jistě udrží.

Neustále se měnící kybernetický prostor, obtížná identifikace pachatele či zlepšující se ohrožování a kybernetické útoky jsou jen jedny z mála problémů, se

kterými bude muset počítat nejen aktuální, ale také budoucí národní strategie kybernetické bezpečnosti, stejně jako vláda Mexika.

11.3.Kolumbie

Silné stránky	Slabé stránky
• Problematika kybernetické bezpečnosti byla zahrnuta do akčního plánu mezi léty 2010 až 2014, ale aktivně o ní vláda mluvila již od roku 2007 • Základy pro strategii vznikly již v dokumentu z roku 2011 • ColCERT skupiny na vládní úrovni • Aktivní vojenské skupiny řešící kybernetické útoky • Speciální policejní jednotky zabývající se kybernetickou bezpečností • IT skupina kontrolující kybernetickou bezpečnost na vládní úrovni • Speciální komise zabývající se kybernetickou bezpečností v zemi • FIRST týmy zaměřující se na soukromý, policejní a telekomunikační sektor • Legislativa vytvořená speciálně na problematiku kybernetické bezpečnosti • Kolumbie je součástí Convenio de Budapest • Aktivně fungující obory zabývající se kybernetickou bezpečností na magisterském studiu • Fungující vzdělávání v oblasti soukromého sektoru • Aktivní zapojování do mezinárodního dění věnujícího se kybernetické bezpečnosti států • Aktivní zapojování do regionálního dění věnujícího se kybernetické bezpečnosti	• Nesnadná indentifikace pachatele, který se může nacházet i mimo daný stát, ve kterém páchá kybernetický útok • Strategie je naplánována na určitou dobu a nemusí být dostatečně flexibilní neustálému technologickému postupu • Skupiny FIRST nejsou zastoupeny v akademickém sektoru • Vzdělávání není rozvinuto na úrovni základního a středního vzdělání • Vzdělávání není rozvinuto na úrovni bakalářského studia • Rozšíření vzdělávacích programů na univerzitách pro pokrytí většího území Kolumbie • Rozšíření vzdělávacích programů a oborů na úrovni doktorského studia na univerzitách • V rámci vzdělávání rozšíření působnosti a četnosti kampaní a velkých prezentací na soukromé a akademické úrovni • Pořádání mezinárodních zasedání a fór na území Kolumbie

Příležitosti	**Hrozby**
• Rozvinutí vzdělávání v oboru kybernetické bezpečnosti na národní úrovni • Rozšíření FIRST skupin na akademický sektor • Zlepšení kampaní o šíření vzdělání v kybernetické bezpečnosti • Vhodné vzdělávání obranných složek	• Neustále se zdokonalující technologie • Rostoucí užívání internetu v domácnostech • Rozvíjející se možnosti napadání kybernetického prostoru • Anonymita pachatelů • Nedostatečné vzělávání obyvatelstva o správném používání a pohybování se v kybernetickém prostoru

Problematiku kybernetické bezpečnosti se Kolumbie rozhodla řešit již velmi brzy. Zájem o toto téma projevila vláda v roce 2007, kdy proběhly diskuze o vzniku politiky kybernetické bezpečnosti a obrany. Několik následujících workshopů a jednání rozhodlo o zahrnutí tohoto cíle do akčního plánu již pro rok 2010-2014. Dokument z roku 2011 pomohl formovat pozdější přesné znění národní strategie z roku 2017. Tuto přípravu tedy lze považovat za silnou stránku, protože strategie měla dobře promyšlené základy. Neustálý rozvoj užívání internetu samozřejmě neminul ani Kolumbii. V roce 2018 bylo naměřeno, že internet v zemi užívá více než 30 000 000 obyvatel. (MinTIC, 2019) Dalším z pozitivních rysů je vytvoření skupiny CERT na vládní úrovni, která se stará o bezpečnost kybernetického systému. Navíc má Kolumbie taktéž zajištěnou bezpečnost v sektoru vojenském, který zajišťuje *Comando Conjunto Cibernético*, tedy zvláštní vojenské jednotky školené pro boj s kybernetickou kriminalitou. Součástí strategie je také zavedení speciálních policejních jednotek. I přes tyto výhody je však potřeba poskytovat policejním složkám neustále aktualizovaná školení a informace o kybernetické kriminalitě, aby byly schopny včas a přesně reagovat. Nejistota identifikace pachatelů je i v tomto případě palčivým problémem a neustálý rozvoj technologií a možností, jak kybernetický prostor napadnout. I v tomto případě, přes dlouhodobý základ a sledování prostoru

kybernetické bezpečnosti, nemusí strategie vždy reagovat včas na neustále se rozvíjející hrozby. Jednou ze silných stránek kolumbijské strategie je také zavedení zvláštních IT jednotek starajících se o technologickou stránku kybernetické bezpečnosti. Vzhledem k výše zmíněným problémům a hrozbám je tento krok pozitivním pro lepší budoucnost udržení strategie i v budoucích letech.

Kolumbijské FIRST týmy jsou silné na vládní úrovni, zahrnují však také sektor telekomunikační a policejní. Kolumbie má četný seznam FIRST týmů, nicméně jednou z jejich slabin je absence zastoupení tohoto typu týmů také v akademické sféře, tedy na jedné z kolumbijských univerzit. Pokrytí i tohoto odvětví může být do budoucna velkou příležitostí pro kolumbijskou strategii a pozitivně se odrazí nejen v ochraně kybernetického prostoru, ale také ve vzdělávání v daném oboru.

Přestože jedním z hlavních cílů národní strategie kybernetické bezpečnosti v Kolumbii byl také správný rozvoj vzdělávání v tomto oboru, můžeme vidět značné slabé stránky v plnění tohoto programu. Kolumbie sice disponuje dvěma magisterskými obory věnujícími se kybernetické bezpečnosti, na akademické úrovni je to však jediné vzdělání, kterého se obyvatelům Kolumbie v rámci této problematiky dostane. Velkou nevýhodou je nerozvinutí jakýchkoli školských programů na úrovni základního a středního studia a také na úrovni bakalářského studia. Vzhledem k velikosti geografického území, kterým Kolumbie disponuje, měla by více dbát o vzdělávací program, který přinese povědomí o využívání internetu, ale hlavně o bezpečnosti při úkonech, které jeho uživatelé denně provádějí. Vzhledem k vysokému, a neustále rostoucímu číslu uživatelů internetu v zemi, je toto téma velkou příležitosti a jeho ignorování zároveň velkou hrozbou. V rámci soukromého a profesionálního vzdělávání je Kolumbie o mnoho napřed, než v rámci vzdělávání akademického či školního. O soukromé vzdělání se v Kolumbii starají mezinárodní společnosti, které taktéž působí například v Mexiku (ISACA), což je velkou výhodou při hodnocení a nastavování nových podmínek kybernetické bezpečnosti v zemi. Další velkou příležitost v tématu vzdělávání lze

vidět hlavně u kampaní na podporu kybernetické bezpečnosti. Kolumbie aktuálně disponuje jednou kampaní pořádanou státní policií. Nicméně dosah této kampaně není dostatečný pro pokrytí větší oblasti a větší části obyvatelstva, je tedy do budoucna velkou otázkou, zda by Kolumbie i v tomto směru neměla přistoupit k inovaci a zlepšení tohoto sektoru.

Na poli mezinárodního dění je Kolumbie jako stát v rámci kybernetické bezpečnosti aktivní. Kromě podpisu *Convenio de Budapest*, který je důležitým legislativním dokumentem, zavedla ještě další legislativní opatření v rámci národní bezpečnosti, které se týkají výhradně kybernetické bezpečnosti a ochrany kybernetického prostoru v zemi. Spolupracuje taktéž s několika důležitými mezinárodními skupinami a stará se o rozvoj důležitých mezinárodních dokumentů. Kolumbii by velmi prospěla možnost uspořádání mezinárodního fóra či jednání o kybernetické bezpečnosti na jejím území. Aktivně se zapojuje také do regionálního dění v rámci tohoto tématu.

12. Závěr

V závěru budou zhodnoceny jednotlivé indikátory a jejich úspěšnost podle předem analyzovaných oddílů v jednotlivých zemích. V této kapitole jsou porovnány jednotlivé země a účinnost jejich národních strategií, navrženy vhodné změny do budoucna či sektory, ve kterých by se země mohly v rámci boje s kybernetickým zločinem zlepšit.

12.1. Indikátor č. 1: Rozvoj politiky státu v rámci kyberbezpečnosti

V rámci rozvoje politiky kybernetické bezpečnosti se rozhodly všechny tři sledované země v této diplomové práci publikovat národní strategii kybernetické bezpečnosti na určité časové období. Všechny měly pevné základy, které mapovaly prostředí pro návrh národní strategie již před jejím samotným vznikem. Vznik strategií byl taktéž u všech tří zemí zařazen do akčních plánů za dané období. Mexiko a Chile svou národní strategii oficiálně spustily v roce 2017 s plánovaným funkčním obdobím na 5 let. Kolumbie problematiku kybernetické bezpečnosti řešila již v roce 2007, oficiálně svou strategii vydala v roce 2016 s funkčním obdobím na 4 roky. Lze se tedy shodnout, že nástup a tvoření strategií měly podobný vývoj ve všech sledovaných zemích. Každé strategii předcházelo její zařazení do akčního plánu či dokument, který zaštiťoval hlavní body rozvinuté v budoucím oficiálním dokumentu.

Co se týče institucionálního hlediska kybernetické bezpečnosti, zde již jisté odchylky a různosti v chování každé ze sledovaných zemí pozorovat lze. Každá z nich má CSIRT/CERT skupinu na vládní úrovni, která se stará o bezpečnost kybernetického prostoru v dané zemi. Nicméně jsou zde také jistá ohrožení, která platí napříč celým tímto prostorem a nezáleží, na jakou zemi se aktuálně soustředíme. Nesnadná identifikace pachatele, který může zaútočit na systém a kybernetickou obranu jakékoli země bez určení jeho přesného umístění. To je problém, který řeší všechny vlády světa v otázce kybernetické bezpečnosti.

Taktéž je jednou z hlavních hrozeb napříč celým světem zdokonalování technologií a možností v narušování kybernetického prostoru, kterým bohužel nelze nijak zabránit pomocí jakýchkoli prostředků. Díky neustálému růstu užívání internetu v jednotlivých domácnostech po celém světě, je jejich napadání mnohem jednodušší, než před několika málo lety. Jednotlivé země tak zdokonalují také jednotky pro ochranu tohoto prostoru. Nejen pomocí FIRST skupin, které Chile, Mexiko a Kolumbie úspěšně zařadili do svých strategií. Jedná se také o ochranu policejních složek a jednotek. V Chile i Mexiku dnes fungují policejní složky specializované přesně na kybernetickou bezpečnost, Kolumbie má navíc výhodu v tom, že ochranu kybernetického prostoru zařadila také mezi vojenské útvary a proto je schopna ještě lépe celý prostor ochránit.

Ruku v ruce jde také legislativní stránka této problematiky. Ochrana prostoru musí být zajištěna také pomocí právních ustanovení. V této oblasti je jednou z nejtěžších věcí neustále se přizpůsobovat novým trendům a možnostem napadení, aby byla legislativa schopna adekvátně soudit a vyhodnocovat útoky. V této části nejvýrazněji zaostává legislativa Mexika, která se sice na nové legislativní zákony týkající se kybernetické bezpečnosti chystá, nicméně oproti Chile a Kolumbii v této problematice prozatím není dostatečně zabezpečeno.

Co se týče prvního indikátoru lze říci, že Chile stejně jako Kolumbie si vedou velice dobře, a budou-li pokračovat ve stejném tempu a kvalitě, v jaké doposud národní strategii budovali, můžeme počítat s velkým zlepšením nejen v rámci této politiky, ale i v politikách budoucích. V Mexiku stále vidíme jisté mezery, hlavně v legislativě. Nicméně podle posledních zpráv se i v této oblasti již plánuji velké změny.

12.2.Indikátor č. 2: vzdělávání a profesní rozvoj v kyberbezpečnosti

V rámci národní strategie a obecné ochrany kybernetického prostoru je velmi důležité si uvědomit naléhavost vzdělávání. Dnešní i budoucí generace se s tímto pojmem a kybernetickým prostorem budou setkávat mnohem častěji a již od

útlého věku se učí užívání nejrůznějších technologických vymožeností. Je tedy doslova povinností státu ochránit své občany a připravit je vhodným vzděláváním na neustále se zvyšující nebezpečí v oblasti užívání technologií, zejména stále se rozvíjejícího internetu. V rámci Chile, Mexika a Kolumbie lze tuto část shrnout do několika jasných bodů. Ani v jedné ze zemí doposud nefunguje základní a střední vzdělávání, které by se aktivně o šíření těchto informací postaralo. Zde vidím nejen velkou hrozbu, ale také velký potenciál pro zlepšení celkové veřejné politiky v oblasti kybernetické bezpečnosti. Číslo užívání internetu u mladistvých se ve všech třech zemích neustále zvyšuje a je tedy potřeba děti učit zacházet adekvátně se sdílením dat již od útlého věku. Navíc, pokrytí tak velkých území jako je Mexiko, Chile a Kolumbie je další podstatnou stránkou. Vzdělávání by mělo být poskytnuté a dosažitelné rovnoměrně, aby bylo dosaženo co nejširšího předávání informací v rámci celé země. Nestačí proto zařadit bakalářské a magisterské obory do hlavních univerzit v zemi, ale také do univerzit vzdálenějších, které však stále poskytují možnost naplnit kapacity tříd. Všechny tři sledované země by taktéž měly lépe dohlížet na zlepšení úrovně již probíhajících, nebo se postarat o vytvoření nových kampaní pro rozvoj tohoto tématu. Pomocí kampaní pro boj s kybernetickým zločinem by mohly mnohem efektivně podpořit vzdělávání v rámci této problematiky a pokrýt tak rozlohu celého státu, aniž by museli vytvářet nové školní osnovy či obory.

V rámci soukromého vzdělávání si země vedou velmi dobře. Spolupráce s mezinárodními společnostmi je v rámci vzdělání výhodné, jelikož informace a zkušenosti z jiných států mohou mnohem efektněji a rychleji pomoci i ve státech sledovaných.

Ve směru vzdělávání hodnotím všechny tři země jako rovnocenné, minimálně zaostává snad jen Kolumbie, která prozatím na úrovni bakalářského studia nemá k dispozici žádný obor týkající se kybernetické bezpečnosti, jako Mexiko či Chile. Nicméně zde vidím spoustu příležitostí, jak rozvinout a zlepšit ochranu nejen v soukromém, ale také veřejném sektoru země.

12.3.Indikátor č. 3: podíl na mezinárodní úrovni v kyberbezpečnosti

V oblasti mezinárodní mají všechny tři země úspěšně podepsáno *Convenio de Budapest*, což je důležitý legislativní úkon pro mezinárodní pomoc při kybernetické bezpečnosti. Jednou z nejsilnějších zemí v mezinárodní oblasti je samozřejmě Kolumbie, která se jako první začala o kybernetickou bezpečnosti zajímat, i když národní strategii oficiálně přijala až v roce 2016. Ačkoli aktivně spolupracuje na mezinárodní legislativě a také je ve spojení s několika důležitými skupinami v rámci kybernetické bezpečnosti, jistě by ve svém mezinárodním zapojení mohla a měla postoupit ještě dále. Její výhodná pozice a také možnost zapojit další země jižní polokoule, jí dává možnost být v budoucnosti leaderem pro severní část jižních států.

Ačkoli Mexiko zaostávalo v legislativních programech na národní úrovni, na mezinárodním poli se mu prozatím daří velice dobře. Stalo se dokonce hostitelem akce týkající se kybernetické bezpečnosti a nelze také zapomenout na jeho velmi výhodnou geografickou pozici, která mu dovoluje blíže se seznamovat s řešením těchto problémů v USA či Kanadě. Mexiko je v budoucnu jednou z klíčových zemí v latinskoamerickém regionu, jelikož díky němu by bylo možné aktivnější zapojování do mezinárodních jednání či konferencí. Pomoc v těchto sférách je důležitá, hlavně pro problematiku dopadení pachatele, který (jak už bylo řečeno) je nesnadno indentifikovatelný. Také lze tímto způsobem lépe a rychleji rozvíjet jednotlivé národní strategie i u států, které s jejich zkušenostmi zatím nejsou na tak vysoké úrovni.

Mexiko, Kolumbie a Chile jsou velmi aktivní jak v OSN, tak také v zapojování v rámci OAS, která je klíčovým bodem v mezinárodních ustanoveních a jednáních pro tento region. Velký potenciál v mezinárodních vodách neustále vidím v Chile, které by se mohlo v budoucnu více angažovat a v rámci kybernetické bezpečnosti rozvíjet své dovednosti na mezinárodní úrovni. Pro všechny tři země je samozřejmě do budoucna velmi výhodné se těchto společenství a pomoci co nejvíce držet a mít jistotu, že díky těmto spojením se

bude úroveň kybernetické bezpečnosti ve všech sledovaných zemích zvyšovat a zlepšovat, pokud možno rychleji a efektivněji.

Jsem si jistá, že v rámci všech tří zemí jsou neustálá zlepšování velkým přínosem nejen pro ně samotné, ale hlavně pro latinskoamerický region, který se díky svému geografickému postavení může v oblasti kybernetické bezpečnosti pozvednout. Mexiko, které může zkušenosti předávat v sektoru Střední Ameriky a Karibiku. Chile, které jistě ovlivní část „cono sur" a Kolumbie, která může pomoci andským zemím. V rámci hrozby je u všech zemí tou hlavní rozvoj technologií, neustále zdokonalování v napadání kybernetického prostoru a hlavně anonymita útočníků. V tomto směru je důležitá především mezinárodní a regionální pomoc. Příležitosti, které aktuální národní strategie a politika nabízí jsou hlavně rozvoj ochrany prostoru pomocí školených skupin, rozvoj vzdělávání, které by bylo schopno ochránit veřejný prostor a také v rámci ochrany rozvoj opatření pro ochranu samotného státu. Chile, Mexiko a Kolumbie ještě oficiálně nedokončily svou historicky první národní strategii kybernetické bezpečnosti. Nicméně až po konečném hodnocení budou schopni opravdu reagovat na hrozby a možnosti, které, jak doufám, zohlední v dalších verzích svých národních strategií.

Bibliografie

Primární literatura

1. Achavar Barrios, V. (2018). Política Nacional de Ciberseguridad: 2017-2022. *Asesoría Técnica Parlamentaria,* 08/2018, 2-7. Chile: Bilbioteca del Congreso Nacional de Chile. Dostupné z https://www.bcn.cl/obtienearchivo?id=repositorio/10221/26760/1/POLITICA_NACIONAL_DE_CIBER.pdf
2. *CONPES 3854: Política de Seguridad Digital.* (2016). Bogotá: Consejo Nacional de Política, Económica y Social: Departamento Nacional de Planeación. Dostupné z https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854_Adenda1.pdf
3. *Estrategia Nacional de Ciberseguridad*. (2017). Mexiko: Consejo de Seguridad Nacional. Dostupné z https://www.gob.mx/cms/uploads/attachment/file/271884/Estrategia_Nacional_Ciberseguridad.pdf
4. *Guía de ciberseguridad para los países en desarrollo*. (2007). UIT. Dostupné z http://www.itu.int/ITU-D/cyb/publications/2007/cgdc-2007-s.pdf
5. Hrůza, P. & kol. (2025). *Kybernetická bezpečnost II.* Brno: Masarykova univerzita. Dostupné z https://www.researchgate.net/publication/276202307_Kyberneticka_bezpecnost_II
6. Hrůza, P. (2012). *Kybernetická bezpečnost.* Brno: Masarykova univerzita. Dostupné z https://docplayer.cz/13439496-Kyberneticka-bezpecnost.html
7. Jirovský, V. (2007). *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. Praha: Grada Publishing.
8. Veselý, A. & Nekola, M. (2008). *Analýza a tvorba veřejných politik: přístupy, metody a praxe*. Praha: SLON.
9. Potůček, Martin a kol. (2006). *Veřejná politika.* Praha: SLON.
10. Hromada, M a spol. (2015). *Kybernetická bezpečnost: Teorie a praxe*. Praha: Powerprint.
11. Hrůza, P. (2012). Kybernetická bezpečnost. Brno: DUKASE, s. r. o.

Sekundární literatura

1. *2014 Wales summit*. (2019). Wikipedia. Dostupné z https://en.wikipedia.org/wiki/2014_Wales_summit
2. *Acerca de AMECI: Quiénes somos*. (2019). Mexiko: AMECI. Dostupné z https://www.ameci.org/index.php/acerca-de-ameci/quienes-somos
3. *Acerca de la CSI: UNAM-CERT*. (2019). Mexiko: UNAM. Dostupné z https://www.cert.unam.mx/acerca-de-la-csi
4. *Acerca de*. (2019). Kolumbie: colCERT. Dostupné z http://www.colcert.gov.co/?q=acerca-de
5. *Acerca del MinTIC*. (2019). Kolumbie: MinTIC. Dostupné z https://www.mintic.gov.co/portal/inicio/Ministerio/Acerca-del-MinTIC/
6. *Acerca*. (2019). Chile: ISACA. Dostupné z http://www.isaca.org/chapters10/Santiago/Acerca/Pages/Default.aspx
7. *Agenda Digital 2020*. (2015). Chile: Ministerio de Secretaría General de la Presidencia; Ministerio de Economía, Fomento y Turismo; Ministerio de Transporte y Telecomunicaciones. Dostupné z http://www.agendadigital.gob.cl/#/
8. *Agenda Estratégica de Innovación: Ciberseguridad*. (2014). Bogotá: Ministerio de Tecnología de la Información y las Comunicaciones. Dostupné z https://www.mintic.gov.co/portal/604/articles-6120_recurso_2.pdf
9. *Anuncia la SSPC campaña nacional de Ciberseguridad México 2019*. (2019). Mexiko: Alcaldes de México. Dostupné z https://www.alcaldesdemexico.com/notas-principales/anuncia-la-sspc-campana-nacional-de-ciberseguridad-mexico-2019/
10. *Basea para una Política Nacional de Ciberseguridad*. (2015). Chile: Ministerio de Defensa Nacional a Ministerio del Interior y Seguridad Pública. Dostupné z https://www.ciberseguridad.gob.cl/media/2015/12/Documento-Bases-Pol%C3%ADtica-Nacional-sobre-Ciberseguridad.pdf

11. Birkland, T. A. (2016). *An Introduction to the Policy Process: Theories, Concepts, and Models of Public Policy Making*. New York: Routledge.
12. Bízik, V. (2016). *Kyberbezpečnost a veřejná politika*. Praha: Evropské hodnoty z.s. Dostupné z https://www.evropskehodnoty.cz/wp-content/uploads/2016/02/Kyberbezpe%C4%8Dnost1.pdf
13. *Bogotá*. (2019). Kolumbie: OWASP. Dostupné z https://www.owasp.org/index.php/Bogota#OWASP_Bogot.C3.A1.2C_Colombia
14. *Boletín trimestral de las TIC*. (2019). MinTIC. Dostupné z https://colombiatic.mintic.gov.co/679/w3-article-103108.html
Budapešťská úmluva o smlouvě o přepravě zboží po vnitrozemských vodních cestách (CMNI). (2000). Praha: Senát ČR. Dostupné z https://www.senat.cz/xqw/xervlet/pssenat/webNahled?id_doc=27409&id_var=23503
15. Buzan, B. & de wilde, J. & Waever, O. (2005). *Bezpečnost: Nový rámec pro analýzu*. Brno: Centrum strategických studií.
16. *Capítulo Monterrey*. (2019). Mexiko: ISACA. Dostupné z http://www.isaca.org/chapters7/Monterrey/AboutOurChapter/Pages/default.aspx
17. Carlini, A. (2016). *Ciberseguridad: Un nuevo desafío para la comunidad internacional*. Dostupné z http://www.ieee.es/Galerias/fichero/docs_opinion/2016/DIEEEO67-2016_Ciberseguridad_Desafio_ComunidadInt_ACarlini.pdf
18. Cayón Peña, J. & García Segura, L. A. (2014). *La importancia del componente educativo en toda estrategia de Ciberseguridad*. Bogotá: Escuela Superior de Guerra. Dostupné z https://esdeguerevistacientifica.edu.co/index.php/estudios/article/view/9/4
19. *Centro Nacional de Respuesta a Incidentes Cibernéticos de la Policía Federal*. (2019). Mexiko: Gobierno de México. Dostupné z https://www.gob.mx/policiafederal/articulos/centro-nacional-de-respuesta-a-incidentes-ciberneticos-de-la-policia-federal?idiom=es
20. *Ciberseguridad*. (2019). Chile: CICS. Dostupné z https://www.ciberseguridad.gob.cl/el-cics/

21. *Clave Única de Registro de Población: CURP*. (2019). Mexiko: Gobierno de México. Dostupné z https://www.gob.mx/segob/acciones-y-programas/clave-unica-de-registro-de-poblacion-curp
22. *Clcert.cl*. (2019). Chile: Universidad de Chile, 2019. Dostupné z https://www.clcert.cl/
23. *Comisión de Prevención del Delito y Justicia Penal: Informe sobre el noveno período de sesiones*. (2000). New York: ONU. Dostupné z https://www.legal-tools.org/doc/3c061a/pdf/
24. *Comisión Intersecretarial para el Desarrollo del Gobierno Electrónico: ¿Qué hacemos?*. (2019). Mexiko: Gobierno de México. Dostupné z https://www.gob.mx/cidge/que-hacemos
25. *CONPES 3701: Lineamientos de Política para Ciberseguridad y Ciberdefensa.* (2016). Bogotá: Consejo Nacional de Política, Económica y Social: Departamento Nacional de Planeación. Dostupné z https://www.mintic.gov.co/portal/604/articles-3510_documento.pdf
26. *Convenio sobre la Ciberdelincuencia*. (2001). Budapešť: Council of Europe. Dostupné z https://www.oas.org/juridico/english/cyb_pry_convenio.pdf
27. *Council of Europe: Mexico*. (2019). Council of Europe. Dostupné z https://www.coe.int/es/web/octopus/country-wiki/-/asset_publisher/hFPA5fbKjyCJ/content/mexico?inheritRedirect=false&redirect=https://www.coe.int/en/web/octopus/country-wiki?p_p_id%253D101_INSTANCE_hFPA5fbKjyCJ%2526p_p_lifecycle%253D0%2526p_p_state%253Dnormal%2526p_p_mode%253Dview%2526p_p_col_id%253Dcolumn-4%2526p_p_col_count%253D1
28. *Csirt.gob.cl.* (2019). Chile: Ministerio del Interior y Seguridad Pública. Dostupné z https://www.csirt.gob.cl/funciones/
29. *Cumbre Mundial sobre la Sociedad de la Información (CMSI)*. (2017). Mexiko: UNESCO. Dostupné z http://www.unesco.org/new/es/

communication-and-information/resources/multimedia/photo-galleries/world-summit-on-the-information-society-wsis/

30. *Declaración Protección de Infraestructura Crítica ante las Amenazas Emergentes*. (2015). Washington, D.C.: CICTE. Dostupné z http://www.oas.org/en/sms/cicte/documents/sessions/2015/CICTE%20DOC%201%20DECLARACION%20CICTE00955S04.pdf
31. Delgado Granados, M. de Lourdes. (2014). *Delitos Informáticos, Delitos Electrónicos*. Mexiko: Gobierno de México. Dostupné z http://www.ordenjuridico.gob.mx/Congreso/pdf/120.pdf
32. *Department of Defense*. (2010). Dictionary of Military and Associated Terms. Dostupné z https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/dictionary.pdf
33. *División Científica de la Policía Federal*. (2019). Mexiko: Gobierno de México. Dostupné z https://www.gob.mx/policiafederal/articulos/division-cientifica-de-la-policia-federal?idiom=es
34. Duncker, K. (1945). *On problem-solving*. Německo: Praeger.
35. Dunn, W. (1988) Methods of the second type: Coping with the wilderness of conventional policy analysis. *Policy Studies Review*. *7*(4).
36. Dunn, W. (1997). Probing the Boundaries of Ignorance in Policy Analysis. *American Behavioral Scientist,* 40/3, 777-780. Dostupné z https://journals.sagepub.com/doi/abs/10.1177/0002764297040003005?journalCode=absb
37. Dye R., T. (1976). *Policy Analysis: What Governments Do, Why They Do It, and What Difference It Makes*. USA: University of Alabama Press.
38. Eichner, J. (2009). *Mezinárodní bezpečnost v době globalizace*. Praha: Portál.
39. *En Boyacá, lanzamos campaña "A Clases con Ciberseguridad"*. (2019). Kolumbie: Gobierno de Colombia. Dostupné z https://www.policia.gov.co/noticia/boyaca-lanzamos-campana-clases-ciberseguridad

40. Espinosa, E. I. (2015). Hacia una Estrategia Nacional de Ciberseguridad en México. *Revista de Administración Pública,* 9/2015, 1-35. Mexiko: Instituto Nacional de Administración (INAP). Dostupné z https://www.academia.edu/12107238/Towards_a_Cybersecurity_Strategy_in_Mexico
41. *Estudios*. (2018). Mexiko: Asociación de Internet. Dostupné z https://www.asociaciondeinternet.mx/es/estudios
42. *FIRST*. (2019). USA: FIRST.Org. Dostupné z https://www.first.org/
43. *Foro para la Gobernanza de Internet*. (2019). Wikipedia. Dostupné z https://es.wikipedia.org/wiki/Foro_para_la_Gobernanza_de_Internet
44. *Global Cybersecurity Index 2018*. (2018). UIT. Dostupné z https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf
45. Grasseová, M. (2006). Využití SWOT analýzy pro dlouhodobé plánování. *Obrana a strategie*.
46. Grasseová, M. & Dubec, R. & Řehák, D. (2012). *Analýza podniku v rukou manažera*. Brno: BizBooks.
47. *Hacia la Estrategia Nacional de Ciberseguridad*. (2017). Mexiko: Gobierno de México. Dostupné z: https://www.gob.mx/mexicodigital/articulos/hacia-la-estrategia-nacional-de-ciberseguridad?idiom=es
48. *HackLab Bogotá*. (2019). Kolumbie: HackLab. Dostupné z https://www.meetup.com/HackLab-Bogota/
49. Hanáček, P. & Staudek, J (2000). *Bezpečnost informačních systémů: Metodická příručka zabezpečování produktů a systémů budovaných na bázi informačních technologii*. Dostupné z http://media0.vesele.info/files/media0:50f8645ae2040.pdf.upl/uvis_bezpecnost_20000701.pdf
50. *Hay Palabras Que Matan*. (2019). Chile: Ministerio de Educación. Dostupné z: http://www.haypalabrasquematan.cl/
51. *Ikusi CSIRT*. (2019). Mexiko: IKUSI. Dostupné z http://www.csirt.ikusiredes.com/

52. *Índice Global de Ciberseguridad - 2018*. (2019). Chile: Deloitte. Dostupné z https://www2.deloitte.com/cl/es/pages/risk/revista-perspectivas-4ta-edicion/seccion-2/Indice-Global-de-Seguridad-2018.html
53. *Ingeniería en Ciberseguridad*. (2019). Chile: AIEP. Dostupné z https://www.aiep.cl/carrera/ingenieria-en-ciberseguridad/77/
54. *Ingeniería para la Seguridad Informática y Redes*. (2019). Mexiko: Universidad de Cuahtemoc. Dostupné z https://www.ucg.edu.mx/licenciaturas/oferta/ingenierias/24/ingenieria-para-la-seguridad-informatica-y-redes
55. *Internet Segura y Ciudadanía Digital: Quiénes somos*. (2019). Chile: Ministerio de Educación. Dostupné z http://www.internetsegura.cl/quienes-somos/
56. *ISACA Bogotá Chapter*. (2019). Kolumbie: ISCA. Dostupné z https://www.isacabogota.org/nuestro-capitulo/
57. *ISACA Medellín Chapter*. (2019). Kolumbie: ISACA. Dostupné z https://www.isacamedellin.org/nosotros
58. Janoušek, M. (2006). Kyberterorismus: Terorismus informační společnosti. *Obrana a strategie, 2*/2006, 60-66.
59. Kepner, H. & Tregoe, B. (1981). *The New Rational Manager: An Updated Edition for a New World*. USA: Kepner-Tregoe, Inc.
60. Kliková, Ch. & Kotlán, I. a kol. (2012). *Hospodářská politika*. Ostrava: Sokrates.
61. Kropáčová, A. CERT/CSIRT týmy a jejich role. *Root.cz,* 05/2013. Dostupné z https://www.root.cz/clanky/cert-csirt-tymy-a-jejich-role/
62. *La Comisión Nacional de Seguridad inaugura campaña de concientización "Ciberseguridad México 2018*. (2018). Mexiko: Gobierno de México. Dostupné z https://www.gob.mx/segob/prensa/la-comision-nacional-de-seguridad-inaugura-campana-de-concientizacion-ciberseguridad-mexico-2018
63. *Ley 1928 de 2018*. (2018). Kolumbie: El Congreso de Colombia.

64. *Maestría en Ciberseguridad*. (2019). Mexiko: Universidad La Salle. Dostupné z https://lasalle.mx/oferta-educativa/facultades/facultad-de-ingenieria/maestria-en-ciberseguridad/
65. *Maestría en Seguridad de la Información*. (2016). Kolumbie: Universidad de los Andes. Dostupné z https://sistemas.uniandes.edu.co/es/mesi-general/descripcion
66. *Magíster en Ciberseguridad*. (2019). Chile: UAI. Dostupné z https://ncsi.ega.ee/country/cl/
67. *Magíster en Ingeniería de Seguridad de la Información*. (2019). Chile: Universidad Mayor. Dostupné z https://www.umayor.cl/web-postgrados/curso/magister-de-ingenieria-en-seguridad-de-la-informacion-santiago/
68. Malý, I. (2006). *Stanovení cílů veřejných politik*. Brno: Univerzita Masarykova. Dostupné z https://is.muni.cz/el/1456/podzim2008/D_VE/um/107767/Stanoveni_cilu.pdf
69. Malý, I. & Pavlík, M. (2004). *Tvorba a implementace veřejné politiky: Stručný průvodce studiem*. Brno: Masarykova univerzita. Dostupné z https://is.muni.cz/el/1456/jaro2014/BKV_VESP/um/47107911/47108153/DSO_Tvorba_a_implementace_verejne_politiky-VESP.pdf
70. *Me conecto para aprender*. (2019). Chile: Ministerio de Educación. Dostupné z http://meconecto.mineduc.cl/
71. *Mexico City Chapter*. (2019). Mexiko: ISACA. Dostupné z http://www.isaca.org/chapters4/Mexico-City/AboutOurChapter/Pages/default.aspx
72. *Mindefensa CSIRT*. (2019). Kolumbie: Gobierno de Colombia. Dostupné z https://cc-csirt.policia.gov.co/
73. *Ministerio de Defensa Nacional. Ciberdefensa*. *Defensa.cl* [online]. 2019 [cit. 2019-04-20]. Dostupné z: https://www.defensa.cl/temas-de-contenido/ciberdefensa/
74. *Ministerio de Hacienda solicita asistencia técnica del FMI para ciberseguridad en el marco del trabajo del Consejo de Estabilidad Financiera*

(CEF). (2018). Chile: Ministerio de Hacienda. Dostupné z https://www.hacienda.cl/consejo-de-estabilidad-financiera/comunicados-del-consejo/ministerio-de-hacienda-solicita.html

75. *Ministerio del Interior y Seguridad Pública*. (2019). Chile: Ministerio del Interior y Seguridad Pública. Dostupné z https://www.interior.gob.cl/
76. *Mnemo CERT*. (2019). Mexiko: Mnemo. Dostupné z https://cert.mnemo.com/
77. *National Cyber Security Index*. (2019). Chile: NCSI. Dostupné z https://ncsi.ega.ee/country/cl/
78. *NeoSecure*. (2017). Chile: NeoSecure S. A. Dostupné z http://www.neosecure.com/
79. *Nosotros*. (2019). Kolumbie: CSIETE. Dostupné z https://www.csiete.org/nosotros/
80. *Nuestra empresa*. (2018). Mexiko: Axtel. Dostupné z https://www.axtelcorp.mx/nuestra-empresa/
81. *Observatorio Regional de Banda Ancha*. (2016). Naciones Unidas: CEPAL. Dostupné z https://www.cepal.org/es/observatorio-regional-de-banda-ancha
82. Olmedo Izaguirre, J. (2018). *Análisis de los Ciberataques Realizados en América Latina*. Ekvádor: Universidad Internacional de Ecuador.
83. Peréz Peréz, Y. (2014). *Importancia de la ciberseguridad en Colombia*. Kolumbie: Universidad Piloto de Colombia. Dostupné z http://polux.unipiloto.edu.co:8080/00003620.pdf
84. *Plan Nacional de Desarrollo 2013-2018*. (2013). Mexiko: Gobierno de México. Dostupné z https://www.snieg.mx/contenidos/espanol/normatividad/MarcoJuridico/PND_2013-2018.pdf
85. *Policía de Ciberdelincuencia Preventiva*. (2019). Mexiko: Gobierno de México. Dostupné z http://data.ssp.cdmx.gob.mx/ciberdelincuencia.html
86. *Policía de Investigaciones de Chile*. (2019). Chile: Policía de Investigaciones de Chile. Dostupné z https://www.pdichile.cl/instituci%C3%B3n/unidades/cibercrimen

87. Potůček, M. & Pavlík, M. (2105). *Veřejná politika*. Brno: Masarykova univerzita. Dostupné z https://is.muni.cz/el/1456/podzim2015/BKV_VPTP/um/50929760/verejna_politika_sazba.pdf?lang=cs
88. Procházková, D. (2012). *Bezpečnost kritické infrastruktury*. Praha: České vysoké učení technické.
89. Puime Maroto, J. (2009). El Ciberespionaje y la Ciberseguridad. In: Monografías del CESEDEN, *La violencia del siglo XXI. Nuevas dimensiones de la guerra* (s. 45-76). Španělsko: Ministerio de Defensa. Dostupné z https://dialnet.unirioja.es/servlet/libro?codigo=548996
90. *Quienes somos?*. (2019). Kolumbie: CSIRT. Dostupné z http://www.csirt-ccit.org.co/nosotros.html
91. *Quiénes somos*. (2019). Chile: Alianza Chilena de Ciberseguridad. Dostupné z https://alianzaciberseguridad.cl/#somos
92. *Quiénes somos*. (2019). Kolumbie: CCOC. Dostupné z https://www.ccoc.mil.co/quienes_somos_mision_responsabilidad
93. *Quiénes somos*. (2019). Kolumbie: OECD. Dostupné z http://www.oecd.org/acerca/
94. *Quienés somos*. (2019). Mexiko: AT&T. Dostupné z https://www.att.com.mx/quienes-somos.html
95. *RAND Corporation: A Framework for Exploring Cybersecurity Policy Options*. (2016) USA: RAND Coproration.
96. Riquelme, R. (2019). Gobierno federal despliega campaña para crear conciencia en ciberseguridad. *El Economista, 02/2019*. Dostupné z https://www.eleconomista.com.mx/tecnologia/Gobierno-federal-despliega-campana-para-crear-conciencia-en-ciberseguridad-20190228-0096.html
97. Riquelme, R. (2019). Morena propone la creación de una agencia nacional de ciberseguridad. *El Economista*, 4/2019. Dostupné z https://www.eleconomista.com.mx/tecnologia/Morena-propone-la-creacion-de-una-agencia-nacional-de-ciberseguridad-20190402-0044.html

98. Říha, J. (2007). Kritická infrastruktura a riziko mimořádné události. *Urbanismus a územní rozvoj,* 4/2007, 44-50. Dostupné z https://www.uur.cz/images/5-publikacni-cinnost-a-knihovna/casopis/2007/2007-04/08_kriticka.pdf
99. *Scitum-CERT*. (2019). Mexiko: Scitum. Dostupné z https://www.scitum.com.mx/ScitumCert
100. *Sector Telecomunicaciones Cierre 2018*. (2019). Chile: Ministerio de Transportes y Telecomunicaciones. Dostupné z https://www.slideshare.net/subtel_cl/series-estadsticas-cierre-2018
101. *Senado Aprueba Idea de Legislar Proyecto de Ley de Delitos Informáticos*. (2019). Chile: Ciberseguridad. Dostupné z https://www.ciberseguridad.gob.cl/noticias/senado-aprueba-idea-de-legislar-proyecto-de-ley-de-delitos-informaticos/
102. *Statistics*. (2019). ITU. Dostupné z https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx
103. The World Bank. The World Bank in Chile. *Worldbank.org* [online]. 2019 [cit. 2019-10-30]. Dostupné z: https://www.worldbank.org/en/country/chile
104. *Totalsec-Cert*. (2019). Mexiko: Totalsec. Dostupné z https://www.totalsec.com.mx/en/totalsec-cert.php
105. Trejo, R. (2019). México formará parte del grupo de expertos en seguridad del ciberespacio de la ONU. *Enfoque Noticias,* 08/2019. Dostupné z https://www.enfoquenoticias.com.mx/noticias/m-xico-formar-parte-del-grupo-de-expertos-en-seguridad-del-ciberespacio-de-la-onu
106. *Una Estrategia Interamericana Integral de Seguridad Cibernética: Un Enfoque Multidimensional y Multidisciplinario para la Creación de una Cultura de Seguridad Cibernética*. (2003). Ciudad de México: OAS. Dostupné z http://www.oas.org/juridico/english/cyb_pry_estrategia.pdf
107. *Únete a la primera generación de Ingenieros en Ciberseguridad del país*. (2019). Chile: INACAP. Dostupné z http://portales.inacap.cl/admision/

destacados/Ingenier%C3%ADa-en-Ciberseguridad-Conoce-nueva-Carrera-de-la-Universidad-Tecnol%C3%B3gica-de-Chile-INACAP