Bc. Tomáš Petrů

Útoky na produktovody v dnešním světě a možná protiopatření

Anotace

Studie se zabývá útoky na produktovody v dnešním světě, se zaměřením na ropovody a plynovody. Studie se soustředí zejména na typologii možných způsobů narušení fungování produktovodů, kam spadají hrozby terorismu, kybernetických útoků a krádeží z ropovodů. Větší pozornost je věnována regionům, v nichž dochází k největšímu počtu útoků v této oblasti. V studii je řešena také problematika přístupu k ochraně produktovodů a navrhovaná protiopatření. Cílem studie je nejenom analyzovat současnou situace ve vybraných regionech, ale také poukázat na hrozbu útoků na produktovody a jejich možných důsledků pro moderní společnost.

Klíčová slova

Bezpečnostní opatření, krádež, kybernetické hrozby, ochrana produktovodů, produktovody, terorismus, útoky.

Summary

Attacks against Pipelines in the World of Today and Possible Countermeasures

Study is about attacks on pipelines in the world of today, mainly focusing on oil and gas pipelines. Study focuses mainly on the typology of possible ways of disrupting the operation of pipelines, which include threats of terrorism, cyber attacks and theft from pipelines. Greater attention is paid to regions with the highest number of attacks in this area of interest. The study also deals with the issue of approach to pipeline protection and proposed countermeasures. The aim of the study is not only to analyze the current situation in selected regions, but also to point out the threat of attacks on pipelines and their possible consequences for modern society.

Keywords

Attacks, cyber threats, pipelines, pipelines protection, security measures, terrorism, theft.

Úvod

Energie je považována za strategickou otázku hned z několika důvodů. Na jednu stranu může být energie brána za strategickou, neboť patří k jádru způsobu života moderní společnosti a hrála zásadní roli v jejím historickém vývoji. Na straně druhé představuje energie bezpečnostní otázku, jelikož prochází procesem sekuritizace. Strategický rozměr energie se zdá být patrný vzhledem k rostoucí spotřebě fosilních paliv, což současně vytváří závislost na zdrojích energie. Tyto překážky jsou bezesporu výzvou dnešní společnosti i v současnosti. Energie hraje fundamentální roli pro hladké fungování všech ekonomik, zejména pak ekonomik v rozvinutých státech. Moderní státy se spoléhají na energii k realizaci klíčových politických cílů souvisejících s ekonomikou obecně, které jsou přímo nebo nepřímo spojené s téměř každým aspektem společenského života. Zkráceně řečeno, představit si moderní společnost z ekonomického, bezpečnostního, politického a sociálního hlediska by nebylo možné bez značného množství energie, zejména z fosilních paliv.

Dvě hlavní charakteristiky dávají fosilním palivům geopolitický rozměr. Jsou vysoce koncentrované v několika regionech světa a nejsou obnovitelné. Tato situace s sebou nese geopolitické důsledky z několika hledisek. Útoky na produktovody se stávají prostředkem teroristických organizací k dosažení jejich cílů. Cíle se mohou lišit v závislosti na teroristické organizaci nebo na regionu, zpravidla jde ovšem o snahu poškodit ekonomiku daného státu, na jehož území k útokům dochází a v neposlední řadě také o finanční zisk. Útoky na produktovody mají za následek snížení exportu, což činí z regionálních konfliktů globální problém.

Studie je strukturována do pěti hlavních kapitol. První kapitola studie se zaobírá společnostmi provozující produktovody na území České republiky. Hlavní záběr je věnován provozovatelům ropovodů (Družba a IKL[1]) a plynovodů (Gazela a tranzitní plynovody) a také významným ústředně správním úřadům v této oblasti. Druhá kapitola je zaměřena na produktovody na teritoriu České republiky, jmenovitě na ropovody a plynovody. Další část studie se zaobírá typologií možných způsobů narušení fungování produktovodů. Náplní této kapitoly je definování obecných cílů a motivací útoků na liniové stavby a zároveň konkrétní případy útoků ve vybraných regionech a jejich dopady na společnost. Vymezeny jsou zde tři hlavní typy útoků na produktovodní systémy – teroristické útoky, krádeže a kybernetické útoky. Předposlední kapitola se zaobírá incidenty spojenými s produktovody optikou odborníků, do jejichž pracovního oboru spadá také problematika ohrožení produktovodů. Současně jsou náplní této kapitoly projekty, které se zabývají ochranou kritické infrastruktury a jejichž plnění se odehrávalo na území České republiky. Závěrečná kapitola rozebírá formy bezpečnostní ochrany a konkrétní opatření, které lze uplatnit při ochraně liniových staveb a jejich objektů a zařízení.

Co se týče hypotéz, které si tato studie klade za cíl případně verifikovat či falsifikovat, ty jsou následující:

[1] Ingolstadt – Kralupy nad Vltavou – Litvínov.

Hypotéza č. 1: Evropa (zejména prostor členských států Evropské unie) patří mezi regiony, kde jsou incidenty, týkající se produktovodů, zatím relativně málo časté.

Hypotéza č. 2: V souvislosti s technologickým vývojem se stává větší hrozbou spíše kybernetický útok na liniové stavby (produktovody), než snaha o jejich narušení „v terénu“.

V studii je uplatněn zejména deskriptivní přístup. Metoda dotazování probíhala na základě rozhovoru nebo emailové komunikace. Teoretické poznatky, použité pro tuto studii, jsou čerpány z literárních zdrojů, z internetových zdrojů a ze zákona. Cílem studie je verifikovat nebo falsifikovat stanovené hypotézy. Dalším cílem je analyzovat tuto problematiku a zhodnotit aktuální situaci ve vybraných regionech a poukázat na závažnost útoků na produktovody a rostoucí hrozbu energetického terorismu obecně. K cílům studie patří také analýza bezpečnostních opatření v rámci ochrany produktovodů a jejich účinnost, slabé a silné stránky.

1. Hlavní společnosti, provozující produktovody na území České republiky

V této kapitole bude prostor věnován organizacím, které provozují produktovody na území České republiky. Hlavní záběr v této kapitole je zejména na společnosti, které provozují ropovody Družba a IKL a tranzitní plynovody, společně s plynovodem Gazela. Blíže definované je i Ministerstvo průmyslu a obchodu České republiky, neboť zastává významnou roli v oblasti energetiky. Správa státních hmotných rezerv je rovněž zásadním ústředním správním orgánem, a to zejména v oblasti státních hmotných rezerv a hospodářských opatřeních pro krizové stavy. Vymezené jsou i organizace uplatňující se na území České republiky v případě stavu ropné nouze a společnosti podílející se na přepravě a prodeji ropy a zemního plynu.

1.1 Mezinárodní ropovody

Společnost Mezinárodní ropovody (MERO) je vlastníkem a provozovatelem tuzemské části ropovodů Družba a IKL. Společnost zároveň zabezpečuje centrální tankoviště ropy v Nelahozevsi, do kterého oba zmiňované ropovody vstupují. Jsou nejvýznamnější společnosti na našem území v oblasti zajišťování skladování nouzových strategických zásob ropy. Centrální tankoviště ropy Nelahozeves obsahuje celkem 16 ropných nádrží, jejichž celková kapacita dosahuje 1 550 000 m^3.

Společnost vznikla sloučením subjektů MERO IKL, a. s., Kralupy nad Vltavou a PETROTRANS, a. s., Kralupy nad Vltavou, a to 1. ledna 1994. Následkem bylo mimo jiné spojení provozu ropovodu Družba a výstavbu ropovodu IKL do jednoho celku. V prosinci 2012 se MERO Česká republika, a. s. stalo vlastníkem 5% podílu na ropovodu TAL. Ministerstvo financí České republiky je stoprocentním vlastníkem této společnosti.[2]

1.2 České produktovody

Společnost České produktovody, a. s. (ČEPRO) je státní společnost, která zajišťuje zejména skladování, přepravu a prodej ropných produktů na území České republiky. V této oblasti zprostředkovávají také skladovací, přepravní a speciální služby ostatním subjektům. Mezi jejich cíle patří také ochrana zásob státních hmotných rezerv. ČEPRO a. s. je registrovaným distributorem pohonných hmot, přičemž provozují síť vlastních čerpacích stanic, jejichž obchodní název je EuroOil. V současné době vlastní 200 čerpacích stanic v České republice.

Společnost vznikla 1. ledna 1994 v rámci privatizačního projektu bývalého státního podniku Benzina. Tehdejší název společnosti zněl České produktovody a ropovody, a. s. Zakladatelem byl Fond národního majetku České republiky, v současné době je jediným akcionářem Ministerstvo financí České republiky.[3]

[2] Mezinárodní ropovody Česká republika. https://mero.cz/
[3] Produktovodní síť a sklady. České produktovody, a. s.
https://www.ceproas.cz/o-nas/produktovodni-sit-a-sklady

1.3 Národní organizace pro společný postup ve stavu ropné nouze

Národní organizace pro společný postup ve stavu ropné nouze ((National Emergency Sharing Organization; NESO) je organizací, kterou zřizuje každý členský stát Mezinárodní energetické agentury pro společný postup při stavu ropné nouze, kde funguje jako koordinační orgán. V České republice slouží jako poradní orgán předsedy Správy státních hmotných rezerv (SSHR), jehož úkolem je monitorovat sektor dodávek ropy a ropných produktů do České republiky. Dále má za úkol posuzovat a navrhovat opatření v případě hrozící nebo probíhající ropné nouze a zároveň doporučuje opatření k využití nouzových zásob a k omezení spotřeby ropy a ropných produktů.[4]

Mezi další aktivity NESO patří například:

- Koordinace případných přídělů na základě rozhodnutí Mezinárodní energetické agentury.
- Účast na cvičeních týkajících se stavu ropné nouze na základě požadavků a pokynů Mezinárodní energetické agentury.
- Soustavné vyhodnocování a monitorování situace na světovém trhu ropy.
- Soustavné sledování dovozu a vývozu ropy a ropných produktů v České republice.
- Zpracovávání a kontrola dokumentů Správy státních hmotných rezerv, vztahující se k řešení krizových situací, které souvisejí s narušením dodávek ropy a ropných produktů velkého rozsahu, včetně přípravy realizace příslušných regulačních opatření.[5]

1.4 Správa státních hmotných rezerv

Správa státních hmotných rezerv je ústřední správní orgán v oblastech hospodářských opatření pro krizové stavy a státních hmotných rezerv. Správa státních hmotných rezerv byla zřízena kompetenčním zákonem a je upravena především zákonem č. 97/1993 Sb., o působnosti Správy státních hmotných rezerv, ve znění pozdějších předpisů. Poslání Správy státních hmotných rezerv je dále definováno v zákoně č. 189/1999 Sb., o nouzových zásobách ropy, o řešení stavů ropné nouze a o změně některých souvisejících zákonů, ve znění pozdějších předpisů a v zákoně č. 241/2000 Sb., o hospodářských opatření pro krizové stavy a o změně některých souvisejících zákonů, ve znění pozdějších předpisů. V čele Správy státních hmotných rezerv je předseda, který je jmenován i odvoláván Vládou České republiky. Mezi úkoly Správy státních hmotných rezerv patří:

- Vytváření a udržování nouzových zásob ropy a vybraných ropných produktů, a to nejméně na 90 dní průměrného denního čistého dovozu.
- Navrhuje Vládě České republiky opatření týkající se omezení spotřeby ropy a ropných produktů.
- Vede trvale aktualizovaný seznam nouzových zásob.

[4] Zasedání NESO. Správa státních hmotných rezerv. http://www.sshr.cz/aktuality/Stranky/zasedani_neso.aspx
[5] Zasedání NESO. Správa státních hmotných rezerv. http://www.sshr.cz/aktuality/Stranky/zasedani_neso.aspx

- Zastupování České republiky v koordinační skupině pro ropu a ropné produkty, dále ve výborech a skupinách Mezinárodní energetické agentury a v dalších mezinárodních organizacích v oblasti nouzových zásob.
- Předseda Správy státních hmotných rezerv předkládá Vládě České republiky návrh na vyhlášení a odvolání stavu ropné nouze a návrh na použití nouzových zásob.[6]

1.5 Ministerstvo průmyslu a obchodu České republiky

Ministerstvo průmyslu a obchodu České republiky je ústředním správním úřadem pro: energetiku; státní průmyslovou politiku; obchodní politiku; jednotlivá odvětví průmyslu; vnitřní obchod a zahraniční obchod a podporu exportu. Resort spolupracuje s Českou obchodní inspekcí, Českou energetickou inspekcí a Licenčním úřadem.[7] Ministerstvo průmyslu a obchodu České republiky dále:

- Koordinuje zahraničně obchodní politiku České republiky ve vztahu k jednotlivým státům.
- Zabezpečuje sjednávání dvoustranných a mnohostranných obchodních a ekonomických dohod včetně komoditních dohod.
- Realizuje obchodní spolupráci s mezinárodními organizacemi.
- Posuzuje dovoz dumpingových výrobků a přijímá opatření na ochranu proti dovozu těchto výrobků.
- Řídí a vykonává činnosti spojené s uplatňováním licenčního režimu v oblasti hospodářských styků se zahraničím.
- Dohlíží na provádění obchodní inspekce a inspekce v oblasti energetiky, na oblast puncovnictví a zkoušení drahých kovů i na oblast zkoušení zbraní a střeliva.
- Koordinuje přípravu právního rámce a implementace evropského práva v působnosti resortu.[8]

1.6 NET4GAS

Společnost NET4GAS, s. r. o. je výlučným držitelem licence pro distribuci zemního plynu na území České republiky. Jsou výhradním provozovatelem přepravní soustavy zemního plynu, kterou tvoří téměř 3800 km plynovodů v České republice. Z toho 2 455 km tvoří tranzitní plynovody, 1187 km je tvořeno vnitrostátními přepravními plynovody a plynovod Gazela je dlouhý přibližně 170 km).[9] Společnost NET4GAS provozuje plynovody nejenom pro vnitrostátní distribuci, ale i pro mezinárodní tranzitní přepravu zemního plynu. Plynovodní soustava v České republice má celkem 5 kompresních stanic, rozdělených do severní a jižní větve. V severní větvi se kompresní stanice nachází v Kralici nad Oslavou a v Kouřimi, v jižní větvi plynovodu se vyskytuje v Břeclavi, v Hostimi a ve Veselí nad Lužnicí. Zemní plyn je následně distribuován do celkově 96 předávacích stanic, z nichž může být přepravován do

[6] Správa státních hmotných rezerv. http://www.sshr.cz/Stranky/default.aspx
[7] Působnost ministerstva. Ministerstvo průmyslu a obchodu. https://www.mpo.cz/dokument1926.html
[8] Zákon č. 2/1969 Sb., o zřízení ministerstev a jiných ústředních orgánů státní správy České republiky, ve znění pozdějších předpisů (kompetenční zákon).
[9] 40 Let Tranzitu Zemního Plynu Přes Území České republiky. NET4GAS, 2011. https://www.net4gas.cz/files/0tiskove-zpravy/n4g-40_ngta-brozura-web.pdf

podzemních zásobníků nebo přímo k zákazníkům. Společnost NET4GAS se neustále angažuje v integrování evropských trhů s plynem a v hledání nových cest a zdrojů, na které by se mohla napojit česká distribuční soustava zemního plynu.[10]

1.7 Česká plynárenská

Společnost Česká plynárenská, a. s. obchoduje se zemním plynem v České republice a v rámci střední Evropy. Tato společnost vznikla v roce 2007, přičemž již v roce 2009 se stala registrovaným obchodníkem se zemním plynem v rámci České republiky, Německa a Rakouska. Co se týče zabezpečení přeshraniční distribuce, Česká plynárenská má zajištěnou smlouvu se společností NET4GAS, s. r. o. Mezi jejich činnost patří zajištění dodávek zemního plynu a případné uskladnění dle potřeby odběratelů. V České republice je jejich působnost zaměřena zejména na přímé dodávky licencovaným obchodníkům se zemním plynem.[11]

[10] Přepravní Soustava. NET4GAS. https://www.net4gas.cz/cz/prepravni-soustava/
[11] Česká plynárenská. http://www.ceskaplynarenska.cz/

2. Produktovody na teritoriu České republiky

Tato kapitola pojednává o produktovodech na teritoriu České republiky. Jak je již avizováno v úvodu, studie je zaměřena především na ropovody a plynovody, neboť ty patří k nejohroženějším typům produktovodů. Proto jsou v této kapitole detailněji zpracovány ropovody Družba a IKL, jejichž vlastníkem a provozovatelem na území České republiky je společnost Mezinárodní ropovody. Krátce je zde zmíněna historie výstavby obou ropovodů, modernizace Družby, jejich trasa i základní technické parametry. Co se plynovodů na území České republiky týče, jsou zde tranzitní plynovody, které jsou rozdělené do severní a jižní větve a pokrývají značnou část České republiky. Plynovod Gazela je novější projekt, jehož provoz odstartoval v roce 2013. V kapitole je zmíněn také plán na výstavbu nového plynovodu.

2.1 Ropovod Družba

Ropovod Družba představuje stěžejní zásobovací tepnu pro 8 evropských zemí, včetně České republiky. Jedná se o nejdelší ropovod na světě, jehož délka činí více než 5 100 km a který je v provozu více než 50 let. Každý den tímto ropovodem proteče až 2 miliony barelů ropy. Výstavba ropovodu započala v ruské Samaře, kde ropovod začíná a kam se sbíhají také ropovody ze Sibiře či Uralu. V Československu byla zahájena výstavba ropovodu v letech 1961–1972. Družba se po své délce větví, přičemž nejvýznamnějším rozdělením je bezesporu na jižní a severní větev. Jižní větev Družby vede přes Ukrajinu, kde se následně dále větví na dvě další části, z nichž jedna vede přes Maďarsko až do Chorvatská a druhá vede přes Slovensko až do České republiky. Severní větev vede skrze Polsko a končí v Německu. Co se technických údajů týče, délka trasy Družby na území České republiky je celkem 473 km, včetně odboček a zdvojení.[12]

Přepravní kapacita ropovodu Družba je až 9 milionů tun ropy ročně. Na přelomu tisíciletí docházelo k modernizaci Družby na území České republiky, což kladlo důraz na vylepšení prevence závažných havárií a snížení dopadů ropovodu na životní prostředí. Díky této modernizaci je současná technologie komunikačních, řídících a bezpečnostních systémů Družby na úrovni modernějších ropovodů.[13] Na následujícím obrázku je zobrazena trasa ropovodů Družby a IKL na teritoriu České republiky.

[12] MERO Česká republika. https://mero.cz/

[13] Ropovod Družba. Petroleum. http://www.petroleum.cz/doprava/ropovod-druzba.aspx

Ilustrace: Ropovodní síť na teritoriu České republiky. Družba vstupuje do České republiky v oblasti Hodonínska a vede až do Lítvínova, kde ropovod končí. Současně jsou vybudovány dvě odbočky, a to do Pardubic a do Kralup nad Vltavou. Ropovod IKL vede z německého města Vohburg a končí v Centrálním tankovišti Nelahozeves.[14]

2.2 Ropovod IKL

Ropovod IKL (Ingolstadt – Kralupy nad Vltavou – Litvínov) je druhým hlavním zásobovacím zdrojem ropy, dovážené na teritorium České republiky. Projekt se začal realizovat počátkem devadesátých let, přičemž výstavba ropovodu započala v roce 1994. Oficiální zahájení provozu proběhlo 13. března 1996. Zajímavostí je, že varianty původní trasy, vedoucí na území České republiky skrze Litvínov a Kralupy nad Vltavou, nakonec nebyla realizovaná.[15] Projekt byl během let postupně upraven a jeho finální podoba vede z německého města Vohburg do Centrálního tankoviště v Nelahozevsi v České republice. Navzdory značným změnám na trase ropovodu byl původní název ponechán.[16]

Celková délka trasy ropovodu IKL na území České republiky je 168,6 km. Přepravní kapacita činí 11 milionů tun ropy ročně, z čehož vyplývá, že ropovod IKL má větší přepravní kapacitu než ropovod Družba.

[14] Ropovodná Síť České republiky. Mezinárodní ropovody Česká republika. https://mero.cz/images/stranka/pcs.php?obr=https://mero.cz/images/stranka/mapa_oba_big.jpg
[15] Mezinárodní ropovody Česká republika. https://mero.cz/
[16] Ropovod IKL. Petroleum. http://www.petroleum.cz/doprava/ropovod-ikl.aspx

V roce 2008 proběhla výměna řídícího systému, přičemž nový systém SCADA je modernější a zajišťuje bezpečnější provoz ropovodu. Mezi výhody nového systému patří:

- Zrychlení přenosu dat.
- Přidání možnosti dálkové údržby ropovodu.
- Automatický výpočet životnosti potrubí, na základě provozu a zátěže ropovodu.
- Možnost převzetí řízení ropovodu z velícího střediska ve Vohburgu do velícího střediska v Centrálním tankovišti Nelahozeves (tato varianta se dá uplatnit například v případě mimořádné události).[17]

2.3 Plynovod Gazela

Provoz plynovodu Gazela byl zahájen v roce 2013. Gazela začíná v obci Brandov v Krušných horách, která současně slouží jako hraniční předávací stanice na území České republiky. Plynovod posléze vede až do hraniční předávací stanice v obci Weidhaus v Německu. Plynovod Gazela umožňuje distribuci zemního plynu v obou směrech. Co se týče přepravní kapacity, ta dosahuje až 33 miliard m^3 za rok. Celkové délka plynovodu Gazela činí 166 km.[18]

Zajímavostí je, že v roce 2018 společnost NET4GAS oznámila plán na výstavbu nového plynovodu, který by měl vést souběžně s plynovodem Gazela, a jehož délka by měla být přibližně 150 km. Vést by měl zhruba mezi Přimdou na Tachovsku a Kateřinským potokem na Mostecku. Plánovaná výstavba je součástí projektu Capacity4Gas, který by měl do projektu investovat stovky milionů eur. Hlavním důvodem pro výstavbu nového plynovodu je rozšíření mezery mezi poptávkou a nabídkou po zemním plynu v Evropě.[19]

2.4 Tranzitní plynovody

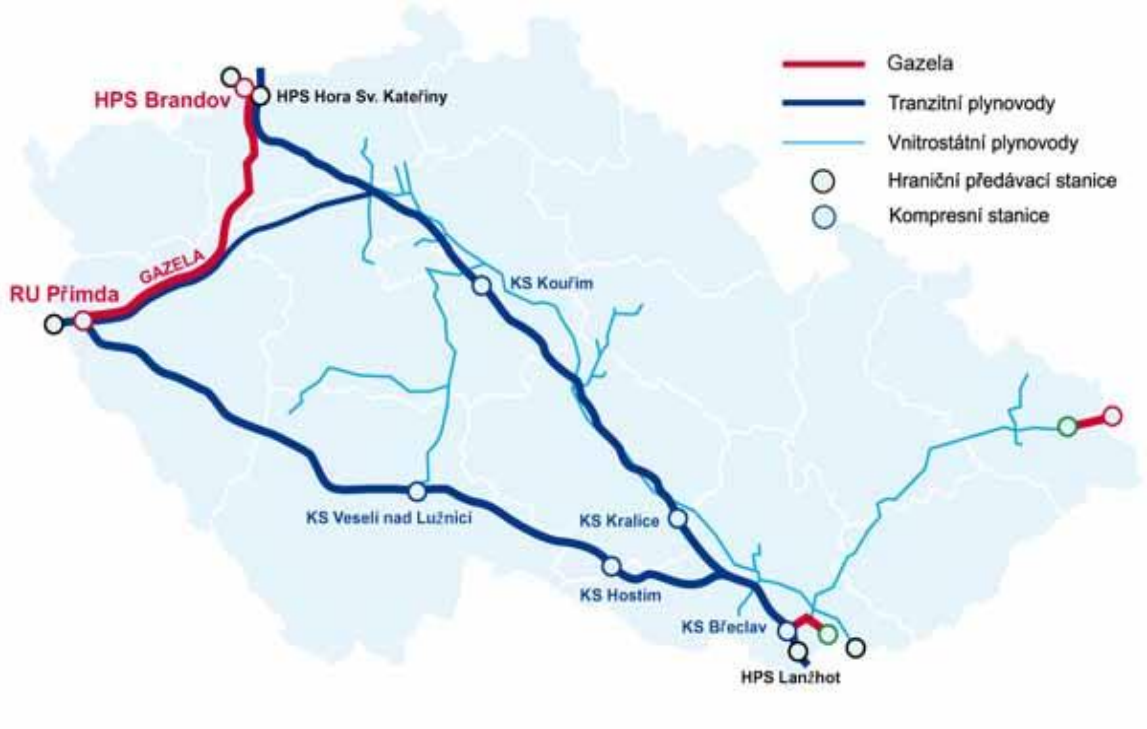
Tranzitní plynovody přepravují zemní plyn na území České republiky již přes 45 let. V roce 1971 byla podepsána mezivládní dohoda o přepravě zemního plynu. Realizace projektu byla v podstatě řečeno dvoufázová. V období od 1975 do 1985 byla uskutečněna výstavba plynovodu v rámci mezivládní dohody o délce 556 km. V období od 1986 do 1999 byla realizována další výstavba o délce 570 km na území Ruské federace a Ukrajiny. Souběžně se zahraniční výstavbou probíhala taktéž stavba na území tehdejšího Československa.

V současné době mají tranzitní plynovody v České republice délku více než 2 400 km.[20]

Přepravní kapacita těchto plynovodů činí až 50 miliard m^3 za rok, přičemž zhruba pětina je určena pro potřeby České republiky a zbytek je určen pro tranzit zemního plynu do západní

[17] Mezinárodní ropovody Česká republika. https://mero.cz/
[18] Přepravní Soustava. NET4GAS. https://www.net4gas.cz/cz/prepravni-soustava/
[19] NET4GAS Plánuje v České republice postavit další plynovod, vést má podél Gazely. O energetice, 5. III. 2018. https://oenergetice.cz/plyn/net4gas-planuje-v-cr-postavit-dalsi-plynovod-vest-ma-podel-gazely/
[20] 40 Let Tranzitu Zemního Plynu Přes Území České republiky. NET4GAS, 2011. https://www.net4gas.cz/files/0tiskove-zpravy/n4g-40_ngta-brozura-web.pdf

Evropy.[21] Na následujícím obrázku je vyznačena plynovodní soustava na území České republiky.



Ilustrace: Plynovodní síť na teritoriu České republiky. Tmavě modrou čárou jsou vyznačeny tranzitní plynovody, které jsou rozdělené do dvou větví a mají celkem 5 kompresních stanic. Červenou barvou je označen plynovod Gazela, jehož provoz byl zahájen v roce 2013. Světle modrá barva značí vnitrostátní plynovody.[22]

[21] 40 Let Tranzitu Zemního Plynu Přes Území České republiky. NET4GAS, 2011. https://www.net4gas.cz/files/0tiskove-zpravy/n4g-40_ngta-brozura-web.pdf
[22] Gazela Zahájila Zkušební Provoz. Petrol, 2013. http://www.petrol.cz/aktuality/archiv/2013/1/gazela-zahajila-zkusebni-provoz-2141.aspx

3 Typologie možných způsobů narušení fungování produktovodů

V této kapitole bude prostor věnován typologii možných způsobů narušení fungování produktovodů. Vymezeny jsou celkově tři zásadní formy ohrožení, které mohou závažným způsobem ohrozit funkčnost produktovodní sítě. Terorismus ve světě je dlouhodobým fenoménem, nicméně strategie některých teroristických organizací se během let změnila. Energetický terorismus patří k významným problémům zejména v regionech severní Afriky, na Blízkém východě a v některých zemích v Jižní Americe. V kapitole je vymezen terorismus na produktovody z obecného hlediska, přičemž je zde uveden také detailnější rozbor situace v Nigérii a v Kolumbii, které se nacházejí na předních příčkách z hlediska teroristických útoků na produktovody. Dále jsou zde rozebrány jednotlivé formy teroristických útoků, využívané při útocích na produktovody a energetický sektor obecně.

Následující část této kapitoly je zaměřena především na krádeže z produktovodů, které představují rovněž závažnou bezpečnostní situaci. Je zde rozebrán rozsah těchto krádeží, u nichž se může jednat o drobné krádeže až po masivní sabotáže, které jsou organizovány koordinovanými ozbrojenými organizacemi a místními kartely. Důraz je kladen také na nebezpečnost krádeží pro civilní obyvatelstvo, neboť při těchto zločinech dochází k vážným ztrátám na lidských životech. Detailnější rozbor situace je uveden na příkladu Mexika, ve kterém je v současné době problematika krádeží z ropovodu velice aktuálním tématem. V této části jsou rovněž uvedené příklady fyzických a technických opatření k ochraně produktovodů a názory, proč v mnohých případech selhávají.

Závěrečná část této kapitoly vymezuje hrozby kybernetických útoků jakožto formu narušení fungování produktovodů. Kybernetické hrozby jsou celosvětově považovány za aktuální fenomén a energetický sektor je považován za jeden z nejohroženějších sektorů. Jsou zde stanoveny obvyklé cíle kybernetických útoků na produktovody a zároveň závažnost možných dopadů, které mohou představovat. Jako příklad jsou v této části uvedené dva případy kybernetických útoků, které se odehrály v roce 2017 v Saudské Arábii a v roce 2018 ve Spojených státech amerických. Nakonec se tato část kapitoly věnuje analýze výsledků studie organizací Ponemon Institute a Siemens, která je zaměřena na připravenost společností na kybernetické hrozby v oblasti produktovodů ve Spojených státech amerických.

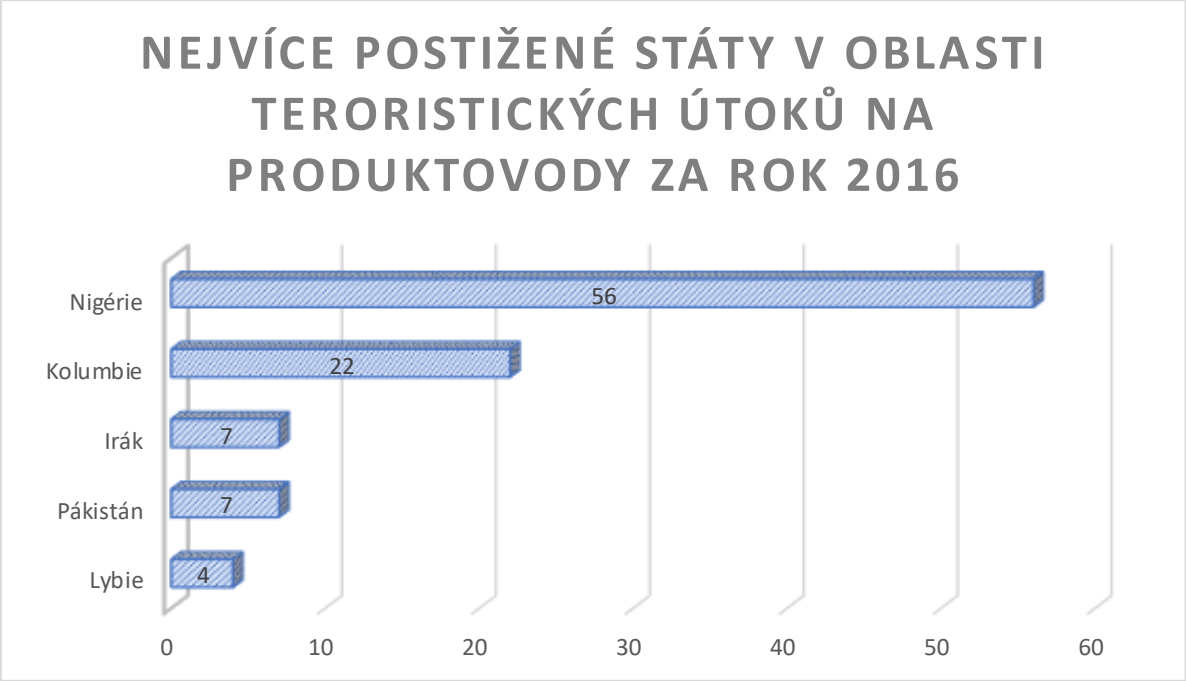
3.1 Terorismus

Ve srovnání s lodní, železniční nebo jinou formou energetické přepravy, potrubní přeprava je nejbezpečnější a nejrychlejší formou přepravy energie (ať už hovoříme o ropě, zemním plynu nebo jiném typu přepravované energie). Je však zranitelnější vůči teroristickým útokům. Produktovody patří k cílům mající vysokou prioritu pro státy, na jejichž území se nachází a patří rovněž mezi měkké cíle. Trendem některých teroristických skupin se v posledních letech stává zaměření na energetický sektor, včetně produktovodů, neboť jejich ohrožení představuje zásadní riziko a škodu nejenom pro státy, na jejichž území se nachází, ale i pro další země. Problém představují také zneužitelné informace, kdy na webových stránkách lze v některých případech nalézt přesné informace o poloze produktovodů.[23]

[23] Kenya's Oil Pipeline and Terrorism. Journal of Defense Resources Management, 2014. http://journal.dresmara.ro/issues/volume5_issue1/03_odhiambo_maito_onkware.pdf

Trendy za posledních deset let naznačují, že ropná a plynárenská infrastruktura patří celosvětově k nejvíce zasaženým sektorům, s téměř 700 útoky v letech 2010-2016. Zdá se, že největší počet útoků se týkal ropovodů a plynovodů nacházejících se v odlehlých oblastech, což má za následek narušení produkce a v některých případech pozastavení vývozu ropy nebo plynu. **Studie společnosti Aon, ve spolupráci se společností Terrorism Tracker**, ukazují, že v roce 2016 došlo celosvětově k celkem 106 teroristickým útokům na ropnou a plynárenskou infrastrukturu. Tento výsledek znamenal nejenom největší počet útoků na tento sektor od roku 2011, ale také nárůst oproti předchozímu roku celkově o 36 %.[24]

K teroristickému útoku na ropný nebo plynárenský průmysl došlo v roce 2016 ve 14 různých zemích. Navzdory globálnímu rozpětí incidentů došlo v Kolumbii a Nigérii k 74 % útoků na zmiňovaný sektor. Jedná se o dvě země závislé na uhlovodících, kde se protíná těžební infrastruktura, odlehlost a ozbrojené konflikty.[25] Na následujícím grafu je zobrazena statistika 5 nejčastěji napadnutých států v oblasti produktovodů. Z grafu vyplývá výrazná převaha incidentů, které se odehrály v Nigérii a v Kolumbii.



Ilustrace: Přehled teroristických útoků na produktovody v roce 2016 na základě dat společnosti Aon. Nigérie zažila jednoznačně největší počet teroristických útoků na produktovody v roce 2016, což úzce souvisí se vznikem militantní skupiny, jejíž aktivity jsou detailněji rozebrány v další části studie. Druhý největší počet teroristických útoků na produktovody se odehrálo v Kolumbii.[26]

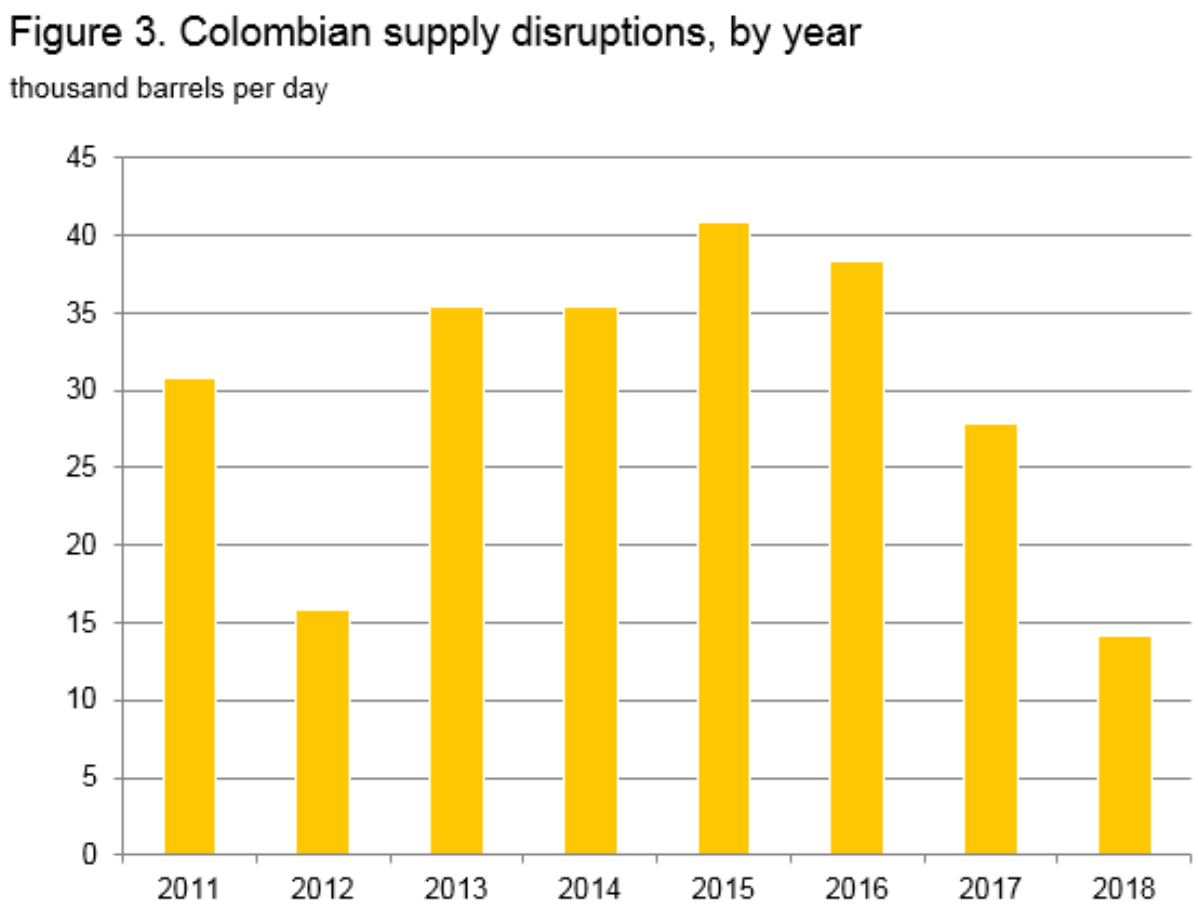
[24] 2017 Risk Maps. Aon Risk Solutions, 2017. https://www.aon.com/germany/publikationen/risk-solutions/2017-risk-maps/risk-map-brochure-2017.pdf
[25] 2017 Risk Maps. Aon Risk Solutions, 2017. https://www.aon.com/germany/publikationen/risk-solutions/2017-risk-maps/risk-map-brochure-2017.pdf
[26] 2017 Risk Maps. Aon Risk Solutions, 2017. https://www.aon.com/germany/publikationen/risk-solutions/2017-risk-maps/risk-map-brochure-2017.pdf

Zranitelnost a poměrně vysoká návratnost za útoky, které zároveň nejsou nákladné či náročné na provedení, vysvětluje, proč jsou v současnosti produktovody tak častým a preferovaným cílem teroristických a jiných ozbrojených organizací. Rozsáhlá plocha a vzdálenost produktovodů z nich činní prvky, které je enormně obtížné bránit. Obzvláště to platí u míst, kde produktovody obklopují hory a džungle, představující výhodné podmínky pro partyzánskou taktiku ozbrojených skupin. Tímto se dá vysvětlit také jeden z důvodů, proč většina těchto útoků, ohrožující energetický sektor, je zaměřena právě na produktovody. Výrobní zařízení a těžební rafinérie jsou typicky lépe chráněné a pro takový útok by bylo zapotřebí vynaložit podstatně více úsilí a prostředků, za dosažením podobného cíle.[27]

Militantní skupiny v Kolumbii jsou aktivní již desetiletí v zaměřování svých útoků na ropnou a plynárenskou infrastrukturu. Přestože došlo během roku 2016 k příměří mezi Kolumbijskou vládou a organizací Revoluční ozbrojené síly Kolumbie (Fuerzas Armadas Revolucionarias de Colombia; FARC), působící v Kolumbii od roku 1954, další militantní skupina Národní osvobozenecká armáda (Ejercito de Liberación Nacional, ELN) zůstává i nadále aktivní.[28]

Podle dat vyplývajících z databáze Terrorism Tracker, pokračuje ELN v zaměřování na energetický sektor. Za rok 2016 jsou odpovědní přinejmenším za 27 útoků na produktovodní sféru v Kolumbii.[29] Následující graf znázorňuje počet narušení dodávek ropy v Kolumbii, v letech 2011 až 2018. Výsledný počet je udáván v tisících barelech ropy za den.

[27] 2017 Risk Maps. Aon Risk Solutions, 2017. https://www.aon.com/germany/publikationen/risk-solutions/2017-risk-maps/risk-map-brochure-2017.pdf
[28] Farc's 'Definitive' Ceasefire Takes Effect in Colombia. BBC, 29. VIII. 2016. https://www.bbc.com/news/world-latin-america-37211085
[29] 2017 Risk Maps. Aon Risk Solutions, 2017. https://www.aon.com/germany/publikationen/risk-solutions/2017-risk-maps/risk-map-brochure-2017.pdf



Ilustrace: Narušení dodávek ropy v Kolumbii v období od 2011 do 2018. Z grafu je patrné, že v Kolumbii dochází ke značným útokům na ropovody, což do značné míry narušuje dodávky ropy. Roky 2012 a 2018 jsou výrazně klidnější než ostatní roky ve stanoveném období. Počet je udáván v tisících barelech ropy za den.[30]

3.1.1 Formy teroristických útoků v energetickém sektoru

Útoky na energetický sektor jsou nejtypičtěji sabotáže, jejichž hlavním cílem je způsobení významných finančních nákladů a narušení služeb. Velmi častou formou jsou také bombové útoky, jejichž dopadem bývá zničení a odstavení částí produktovodů. Útoky v tomto odvětví se řadí mezi nejméně ničivé z hlediska ztrát na lidských životech. Podle Terorrism Tracker došlo za rok 2016 průměrně k méně než 0,5 obětem na útok v energetickém sektoru, včetně útoků na produktovody. Nízký počet úmrtí však nutně neodráží riziko pro pracovníky energetických společností. Kolumbijská policie uvedla, že mezi roky 2001 a 2015 unesly místní partyzáni 219 zaměstnanců ropných společností, za které následně požadovaly výkupné. Ropné společnosti v tomto období vyplatily milióny ozbrojeným skupinám za

[30] Colombian Supply Disruptions, by Year. United States Energy Information Administration, 2019. https://www.eia.gov/beta/international/analysis_includes/countries_long/Colombia/images/Colombia_fig3_bg.png

propuštění zaměstnanců.[31] Teroristický útok na plynárenské zařízení Tigantourine v Amenas v Alžírsku v roce 2013 vedl k úmrtí 40 zdejších pracovníků.[32]

Nejvíce smrtelný teroristický útok v této oblasti se odehrál v Etiopii v roce 2007, kde během útoku Ogadenské fronty národního osvobození (Ogaden National Liberation Front, OLNF) zahynulo přes 70 místních obyvatel a státních příslušníků Čínské lidové republiky.[33] Společnost China Poly Group započala produkci zemního plynu v tomto regionu počátkem roku 2013. Zároveň se ve stejném roce začala podílet na čerpání ropy z ropného pole v Ogadenu. Další čínské společnosti jsou zapojeny do těžby a přepravy ropy v Etiopii, přičemž Peking projevoval velký zájem na stabilizaci tohoto prostoru.[34] K uklidnění situace v regionu došlo v srpnu roku 2018, kdy Etiopie podepsala mírovou dohodu s organizací OLNF. Tato organizace posléze uvedla, že se bude snažit dosahovat svých politických cílů skrze mírové prostředky.[35]

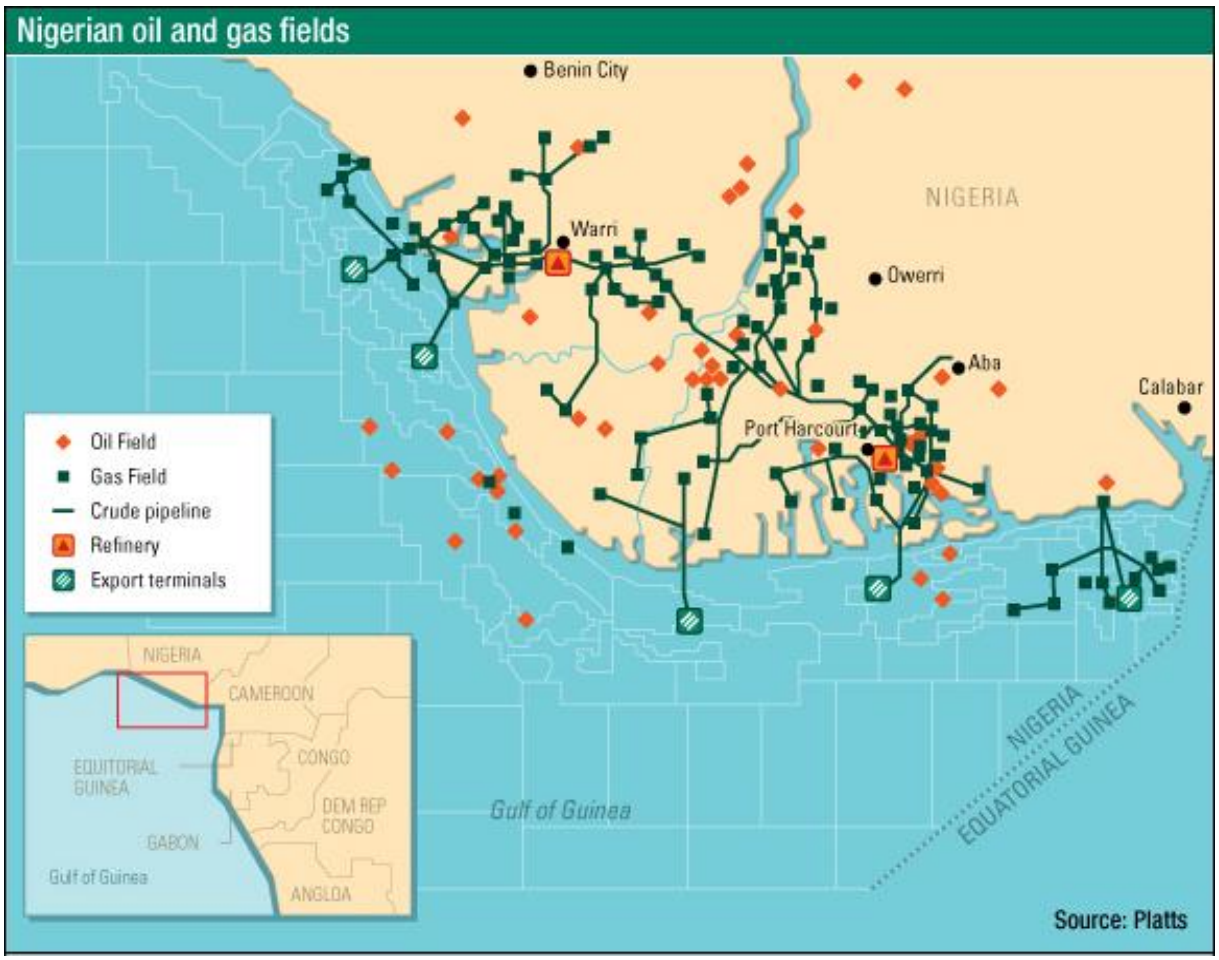
Přestože jsou v dnešním světě častějším cílem produktovody, nelze opomíjet i hrozby týkající se únosů a přímých útoků na výrobní zařízení a těžební rafinérie. V některých případech však může být cílem teroristických organizací také převzetí kontroly nad energetickými zařízeními, které mají významnou strategickou hodnotu. Příkladem mohou být převzetí ropných a plynárenských zařízení v Iráku a Sýrii, způsobené Islámským státem. Takový útok může být velice hodnotný pro financování a celkový růst povstaleckých organizací. Země v konfliktu s rozsáhlou infrastrukturou ropy a zemního plynu, jsou ohrožené vůči této hrozbě. Mezi takové země patří například Sýrie, Irák, Nigérie, Afghánistán a další.[36] V následující podkapitole je blíže rozebrána situace v Nigérii.

3.1.2 Útoky na produktovody v Nigérii

Jako příklad lze uvést Nigérii, kde každoročně dochází k nejvíce útokům na produktovody. V průběhu let se ropné úniky způsobené vandalismem považují za jeden z hlavních problémů Delty Nigeru, regionu, který je nejvýznamnější oblastí z hlediska těžby ropy v Nigérii. Rostoucí případy útoků na místní produktovody, způsobené zejména členy militantních skupin Hnutí za osvobození Delty Nigeru (Movement for the Emancipation of Niger Delta, MEND) a Mstitelé Delty Nigeru (Niger Delta Avengers, NDA), kdy druhá zmiňovaná skupina

[31] 2017 Risk Maps. Aon Risk Solutions, 2017. https://www.aon.com/germany/publikationen/risk-solutions/2017-risk-maps/risk-map-brochure-2017.pdf
[32] CHRISAFIS, Angelique; Julian BORGER, Justin MCCURRY and Terry MACALISTER. Algeria Hostage Crisis: The Full Story of the Kidnapping in the Desert. The Guardian25. I. 2013. https://www.theguardian.com/world/2013/jan/25/in-amenas-timeline-siege-algeria
[33] POWELL, Anita. Ethnic Somali Rebels Kill 74 at Chinese Oilfield in Ethiopia. The Guardian, 25. IV. 2007. https://www.theguardian.com/world/2007/apr/25/ethiopia
[34] SLAV Irina. Ethiopia Inks Peace Deal with Rebels from Gas-Rich Region. Oil Price, 22. X. 2018. https://oilprice.com/Latest-Energy-News/World-News/Ethiopia-Inks-Peace-Deal-With-Rebel-Group-In-Gas-Rich-Region.html
[35] MAASHO, Aaron. Ethiopia Signs Peace Deal with Rebels from Gas-Rich Region. Reuters, 22. X. 2018. https://www.reuters.com/article/us-ethiopia-politics/ethiopia-signs-peace-deal-with-rebels-from-gas-rich-region-idUSKCN1MV0YO?utm_source=applenews
[36] 2017 Risk Maps. Aon Risk Solutions, 2017. https://www.aon.com/germany/publikationen/risk-solutions/2017-risk-maps/risk-map-brochure-2017.pdf

vznikla v únoru roku 2016[37], zásadně ovlivňují zdroje příjmů vládních a ropných společností působících v regionu.

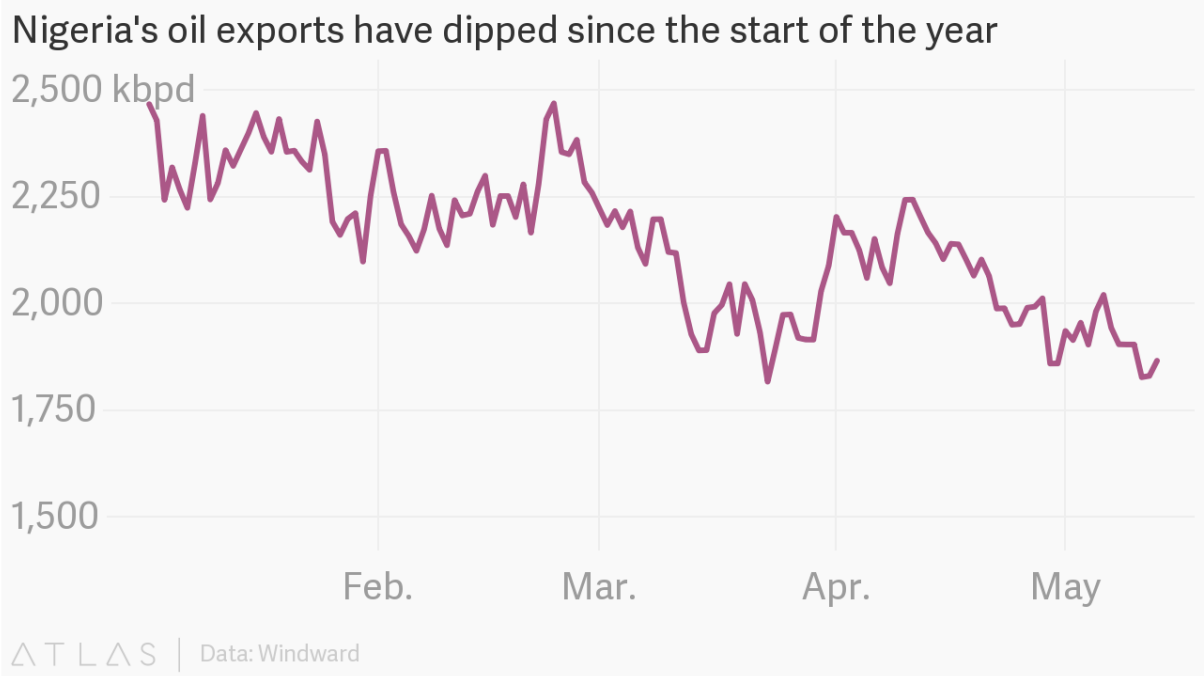


Ilustrace: Nigerijská ropná a plynová pole v regionu Delta Niger. Z obrázku je zjevné, že je tato oblast bohatá na zásoby ropy a zemního plynu. Nachází se zde desítky ropných a plynových polí a celkově dvě rafinérie, a to ve městech Warri a Port Harcourt.[38]

Statistiky naznačují, že Nigérie ztrácí až 300 000 barelů ropy denně (bpd) v důsledku ozbrojených útoků na ropovody, což vede k obrovským finančním ztrátám. Toto mimo jiné vede k významným negativním socioekonomickým a environmentálním problémům v regionu s vážnými důsledky na lidské životy.[39] U tohoto příkladu je rovněž důležité zmínit, že tyto útoky nejsou cílené na obyvatele, ale na poškození nebo zničení infrastruktury. Zejména jsou určeny pro řadu potrubí, které přepravují tisíce galonů ropy na rafinerie na nigerijském pobřeží. To má za následek, že ropa ze zničených produktovodů nebude

[37] HALLMARK, Terry. Oil And Violence In The Niger Delta Isn't Talked About Much, But It Has A Global Impact. Forbes, 13. II. 2017. https://www.forbes.com/sites/uhenergy/2017/02/13/oil-and-violence-in-the-niger-delta-isnt-talked-about-much-but-it-has-a-global-impact/#625ad12b4dc6
[38] S&P Global Platts, 2019. https://www.spglobal.com/platts/en/market-insights/latest-news
[39] TUKUR UMAR, Ahmed. Causes and Consequences of Crude Oil Pipeline Vandalism in the Niger Delta Region of Nigeria: A Confirmatory Factor Analysis Approach. Cogent Economics and Finance, 12. VII. 2017. https://www.cogentoa.com/article/10.1080/23322039.2017.1353199

exportována.[40] Na následujícím grafu je demonstrován značný propad v exportu barelů ropy, který koreluje se vznikem a začátkem působení militantní skupiny NDA.



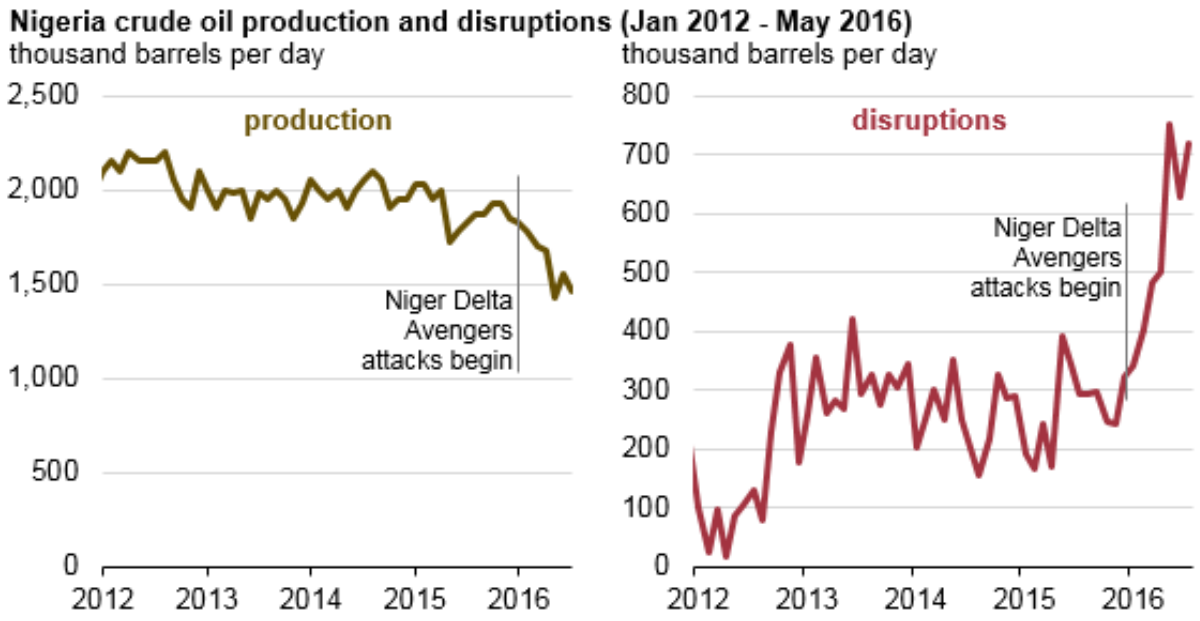
Ilustrace: Vývoz ropy z Nigérie se začátkem roku 2016 podstatně snížil (přehled pro období únor až květen). Graf znázorňuje sestupnou tendenci produkce ropy v tomto období, zejména od března do května 2016.[41]

Data společnosti Terrorism Tracker ukazují, že v první polovině roku 2016 došlo k nejméně 56 teroristickým útokům na ropnou a plynárenskou infrastrukturu v deltě Nigeru, ve srovnání s pouhými dvěma útoky v předchozích dvou letech. Náhlý nárůst útoků způsobil, že produkce ropy v Nigérii klesla o téměř 36 %. V roce 2009 způsobily útoky militantní organizace MEND a dalších ozbrojených skupin pokles výnosů vlády z ropných produktů o přibližně 50%.[42] Nigerijský státní tajemník pro zdroje ropy Ibe Kachigwu konstatoval, že čísla útoků jsou podstatně větší. Dle jeho slov došlo jenom během roku 2016 přes 1 600 zaznamenaným případům vandalismu na produktovodech.

V období od roku 2010 do roku 2015 se jednalo údajně až o 3 000 zaznamenaných případů.[43] Zde je ovšem důležité poznamenat, že data společnosti Terrorism Tracker odkazují na teroristické útoky a nezahrnují tedy sabotáže, krádeže a jiné formy narušení produktovodů.

[40] Terrorist Attacks And Political Violence: How Oil Is Impacted. The One Brief; AON, 2019. https://theonebrief.com/terrorism-political-violence-risk-impact-to-oil-energy-industry/
[41] KAZEEM, Yomi. Nigeria's Oil Exports Have Dipped since the Start of the Year. The Atlas, 2016; 2017. https://www.theatlas.com/charts/BJvELhVE
[42] 2017 Risk Maps. Aon Risk Solutions, 2017. https://www.aon.com/germany/publikationen/risk-solutions/2017-risk-maps/risk-map-brochure-2017.pdf
[43] Nigeria Records 1,600 Pipeline Vandalism Cases. Punch, 18. II. 2016. https://punchng.com/nigeria-records-1600-cases-pipeline-vandalism-kachikwu/

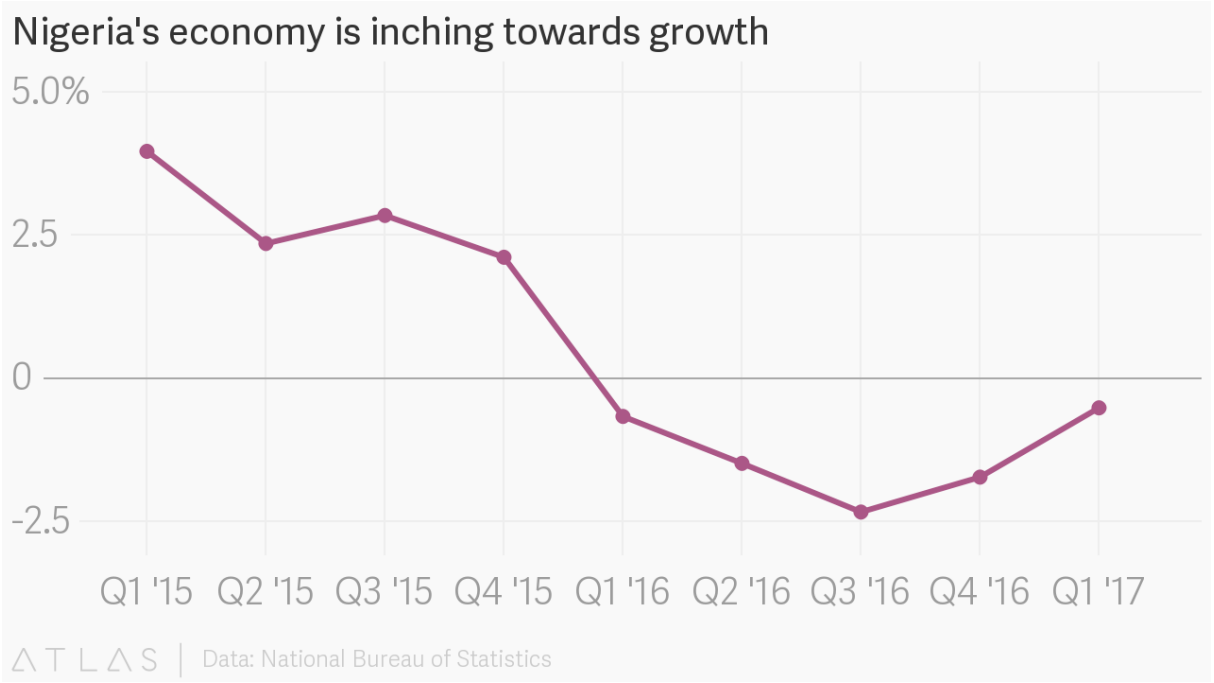
Následující graf zobrazuje pokles produkce ropy a počet narušení produktovodů v období od ledna 2012 do května 2016 v Nigérii.



Ilustrace: Nigerijská produkce ropy a počet narušení ve stanoveném období od ledna 2012 do května 2016. Na levé části grafu je vyznačena produkce ropy v barelech za den. Na pravé straně grafu lze vidět narušení místní produkce ropy v řádu stovek. Důležitým parametrem v obou grafech je bod, který označuje počátek aktivity organizace NDA.[44]

V druhé polovině roku 2016 došlo v Nigérii k zásadnímu posunu, kdy militantní skupina NDA oznámila dočasné příměří a zastavila sabotážní útoky na produktovody.[45] Nicméně příměří bylo krátce porušeno již koncem roku 2016 při útoku NDA na ropovod v Deltě Niger a opětovně se tak stalo i v březnu 2017. Přestože tyto ojedinělé útoky mohou být chápány jako varovný signál, je to znepokojující zpráva pro produkci ropy v Nigérii, která se během měsíců příměří postupně zotavovala a částečně stabilizovala.[46] Jak je patrné z následujícího grafu, po několika kvartálech recese se nigerijská ekonomika během příměří částečně vzrostla.

[44] Nigeria's Crude Oil Production and Disruptions. United States Energy Information Administration, 18. VIII. 2016. https://www.eia.gov/todayinenergy/images/2016.08.18/main.png
[45] KAZEEM, Yomi. Militants Have Finally Declared a Ceasefire in Nigeria's Oil-Rich Delta Region. Quartz Africa, 22. VIII. 2016. https://qz.com/africa/763391/militants-have-finally-declared-a-ceasefire-in-nigerias-oil-rich-delta-region/
[46] PARASKOVA, Tsvetana. Oil Pipeline Attack Breaks Months Of Truce In Nigeria. Oil Price, 23. V. 2017 . https://oilprice.com/Latest-Energy-News/World-News/Oil-Pipeline-Attack-Breaks-Months-Of-Truce-In-Nigeria.html



Ilustrace: Graf demonstruje hybnost Nigerijské ekonomiky ve stanoveném období od prvního kvartálu 2015 do prvního kvartálu 2017. Značný propad je k vidění zejména na konci roku 2015 a na začátku roku 2016. V posledních třech kvartálech sledovaného období dochází k mírnému růstu ekonomiky.[47]

Aktuální situace v Nigérii je pochopitelně daleko složitější a k plnému porozumění probíhajícího konfliktu je zapotřebí detailní rozbor situace v daném regionu. Existují zde neustálé tenze, které momentálně vrcholí během prezidentských voleb v únoru 2019. Organizace NDA zveřejnila oznámení, v němž tvrdí že ochromí ekonomiku dalšími útoky, pokud bude znovuzvolen prezident Muhammadu Buhari. Ten byl o několik dní později skutečně opětovně zvolen do funkce a není úplně zřejmé, do jaké míry bude případný konflikt eskalovat.[48] Počátkem března došlo rovněž k úniku surovin z ropovodu a k následnému požáru, při kterém se pohřešuje více než 50 osob.[49] Z celkového hlediska lze konstatovat, že mezi hlavní faktory ropovodního vandalismu v regionu Delta Niger patří špatný management, špatná správa a právní faktory a zhoršování životního prostředí. Zatímco marginalizace, ačkoli je významná, naznačuje s negativním znamením, že je použita jako prostředek ovlivnění přidělování dotací, rozvojových programů, zvýšení odvodů příjmů a ospravedlnění vandalismu plynovodů.[50]

[47] Nigeria's Economy Is Inching Towards Growth. The Atlas, 2017. https://www.theatlas.com/charts/S1sF-3ZZb
[48] CARSTEN, Paul and Alexis AKWAGYIRAM. Nigeria 'Delta Avengers' Militants Vow to Cripple Economy If Buhari Re-Elected. Reuters, 14. II. 2019. https://www.reuters.com/article/us-nigeria-election-oil/nigeria-delta-avengers-militants-vow-to-cripple-economy-if-buhari-re-elected-idUSKCN1Q31GH
[49] UGURU, Hillary. More Than 50 People Missing After Pipeline Explodes in Nigeria. Bloomberg, 2. III. 2019. https://www.bloomberg.com/news/articles/2019-03-02/urgent-50-plus-people-missing-after-pipeline-explodes-in-nigeria
[50] TUKUR UMAR Ahmed and Moh'd SHAHWAHID HAJJ OTHMAN. Causes and Consequences of Crude Oil Pipeline Vandalism in the Niger Delta Region of Nigeria: A Confirmatory Factor Analysis Approach. Cogent Economics and Finance, 12. VII. 2017. https://www.tandfonline.com/doi/pdf/10.1080/23322039.2017.1353199

3.2 Krádeže z produktovodů

Krádeže produktů z produktovodů se stává hlavní příčinou "selhání" v mnoha potrubích po celém světě. Krádeže se vyskytují především v chudých zemích a odráží sociální problémy a těžkosti. Nejedná se o problém, který lze jednoduše vyřešit technickým vynálezem. Ztráta strategických surovin kvůli poškození potrubí je znepokojující, avšak alarmující jsou také významné ztráty na životech, které jsou v některých případech spojené s těmito krádežemi.[51]

Pokud vezmeme v potaz vrcholnou cenu ropy, během sedmi minut napíchnutí mexického ropovodu může místní kartel vydělat až 90 000 dolarů.

Boj proti této kriminální činnosti je obtížným úkolem také proto, že mnoho z těch, kteří jsou schopni omezit tyto zločiny, z nich zároveň profitují. Mezi země, v nichž je tato hrozba aktuální, patří například Mexiko, Kolumbie, Nigérie, Uganda, Thajsko nebo Turecko. Modality krádeže v těchto geograficky a kontextuálně nesourodých případech se pohybují od nízkých úrovní odběru, sifonování, falšování a pašování až po mimořádně sofistikované námořní operace, zahrnující rozsáhlé sítě zapojených aktérů. Je tedy patrné, že tento fenomén představuje hrozbu nejenom pro místní a regionální prosperitu, ale také pro globální stabilitu a bezpečnost.[52]

Pokud blíže nahlédneme na případ Mexika, tak záměrné sabotáže a krádeže ropy jsou zde aktuálním tématem, které způsobují závažná ekonomická rizika. Napíchnutí ropovodů a krádeže cisteren převážející ropu patří v Mexiku k problémům, vůči nimž místní vláda bojuje již řadu let. V lednu roku 2019 zde došlo ke dvojnásobnému poškození ropovodu, vedoucího ze státu Veracruz do Mexico City, což zapříčinilo dočasné kompletní uzavření ropovodu. Mexická armáda následně objevila 3 kilometry dlouhou hadici, přes kterou pachatelé čerpali palivo ze skladových nádrží v rafinérii Salamanca do utajené skladovací oblasti.[53] Na následujícím obrázku jsou zobrazeny ropovody, rafinérie a ropná a plynná pole v Mexiku.

[51] HOPKINS, Phil. Pipeline Integrity: Some Lessons Learnt. Penspen Integrity, 9. III. 2004. http://www.penspen.com/wp-content/uploads/2014/09/integrity-lessons-learnt.pdf
[52] RALBY, Ian. Downstream Oil Theft. Atlantic Council; Global Energy Center, 6. I. 2017. ISBN 978-1-61977-440-7. https://www.atlanticcouncil.org/images/publications/Downstream_Oil_Theft_web_0327.pdf
[53] BETH SOLOMON, Daina and Marianna PARRAGA. Mexico City Pipeline Hit By 'Sabotage' Amid Crackdown on Fuel Theft. Reuters, 11. I. 2019. https://www.reuters.com/article/us-mexico-oil-theft/mexico-city-pipeline-hit-by-sabotage-amid-crackdown-on-fuel-theft-idUSKCN1P52C3

Ilustrace: Ropná infrastruktura Mexika, včetně vyznačených rafinérií a oblastí (zejména na pobřeží Mexického zálivu), v nichž se těží ropa a zemní plyn. Nachází se zde celkově šest rafinérií, včetně zmiňované rafinérie Salamanca.[54]

Uzavření produktovodu z rafinérie Salamanca v centrálním státě Guanajuato už bylo pod záštitou mexického prezidenta, který nařídil uzavření celkem šest produktovodů, vedoucí napříč Mexikem. Mexický prezident označil toto nařízení jako pokus eliminovat neustálé krádeže z produktovodů.[55] Mexická vláda musela posléze zajistit tisíce policistů a stovky bezpečnostních vozidel, aby mohl být bezpečně přepravován benzín do čerpacích stanic.

Tento počin způsobil v Mexiku značný chaos, jelikož dovážet benzín do čerpacích stanic pouze pomocí cisteren se ukázalo býti značně nákladným a neefektivním procesem. Na benzínových stanicích se tvoří až několika hodinové fronty, což má za následek zvýšenou frustraci obyvatel. Sabotáže tudíž způsobily řetězovou reakci, kvůli níž se značná část země potýká s nedostatkem ropy.[56]

Řešení se navíc nedostavilo ani v oblasti krádeží, neboť ty nadále pokračují v oblastech, kde jsou stále aktivní produktovody. To se stalo osudným téměř 80 lidem 19. ledna 2019, kdy po sabotáži produktovodu severně od Mexico City došlo k masivní explozi. Závažnost výbuchu

[54] Mexico – Downstream Infrastructure Map. United States Energy Information Administration, 2017. https://www.eia.gov/beta/international/analysis.php?iso=MEX
[55] KAHN, Carrie. Theft From Fuel Pipelines Is A Rampant, Deadly Problem In Mexico. National Public Radio, 19. I. 2019. https://www.npr.org/2019/01/19/686835080/theft-from-fuel-pipelines-is-a-rampant-deadly-problem-in-mexico?t=1552302650988
[56] BETH SOLOMON, Daina and Marianna PARRAGA. Mexico City Pipeline Hit By 'Sabotage' Amid Crackdown on Fuel Theft. Reuters, 11. I. 2019. https://www.reuters.com/article/us-mexico-oil-theft/mexico-city-pipeline-hit-by-sabotage-amid-crackdown-on-fuel-theft-idUSKCN1P52C3

byla umocněna tím, že se stovky občanů snažily získat zásoby zdarma, což posléze způsobilo tak vysoké ztráty na životech. Podle oficiálních stanovisek místních úřadů je situace v Mexiku ještě podstatně závažnější. Podle jejich informací kartely a další ozbrojené skupiny způsobily celkem 12 581 nelegálních a nebezpečných vrtů do produktovodů během prvních 10 měsíců roku 2018, což činní průměr 42 za den.[57]

Poškození produktovodů za účelem krádeže může mít obecně několik forem a liší se nejenom provedením, ale i rozsahem poškození a množstvím ztracených surovin. Rozdělení vypadá zhruba takto:

- Místní oportunistické krádeže pro vlastní potřebu, zpravidla v malém měřítku. Tato forma se dá označit jako amatérská, nicméně zároveň obnáší největší riziko následků v podobě ohrožení života.
- Úmyslné poškození produktovodů místními lidmi za účelem uplatnění nároků na náhradu škody. Zde stále můžeme hovořit o relativně malém měřítku.
- Organizovaná krádež místní zločineckou skupinou či organizací. Zde už dochází ke znatelně větším ztrátám a v případě ropy může nakradené množství odpovídat obsahu běžné silniční cisterny.
- Velké krádeže ropy způsobené mezinárodními organizovanými zločinci, které lze provést pomocí trvale namontovaných ventilů na potrubí. V souvislosti s předchozími body se jedná o největší měřítko rozsahu.[58]

Krádeže z produktovodů mohou tedy představovat kritický dopad na ohrožení lidského života. Zde je pro názornost uvedená statistika z let 2000–2006, z níž je patrné, že důsledky krádeží z produktovodů mohou mít alarmující následky na lidské životy. Následující statistické údaje pochází z Nigérie. Zde je počet mrtvých civilistů ve stanoveném období:[59]

- Březen 2000 – více než 50 obyvatel zabito v regionu Abia.
- Červenec 2000 – více než 300 obyvatel zabito ve Warri.
- Červen 2003 – více než 150 obyvatel zabito v regionu Abia.
- Září 2004 – více než 60 obyvatel zabito v Lagosu.
- Prosinec 2004 – více než 20 obyvatel zabito v Lagosu.
- Květen 2006 – více než 150 obyvatel zabito v Lagosu.
- Prosinec 2006 – více než 260 obyvatel zabito v Lagosu.

Co se týče novějších údajů, aktuální informace se nepodařilo dohledat. Počet případů vandalismu měl ovšem v následujících letech spíše vzestupnou tendenci, tudíž se lze domnívat, že docházelo k dalším ztrátám na lidských životech.[60] Jiné země (např. Indonésie,

[57] ELLIOTT, Josh, K. Mexico Pipeline Explosion That Killed 79 is an 'Example' For Fuel Thieves, Officials Say. Global News, 19. I. 2019 . https://globalnews.ca/news/4866684/mexico-pipeline-explosion-fuel/
[58] HOPKINS, Phil. Learning from Pipeline Failures. Penspen Integrity, 2008. http://www.penspen.com/wp-content/uploads/2014/09/learning-from-failures.pdf
[59] HOPKINS, Phil. Learning from Pipeline Failures. Penspen Integrity, 2008. http://www.penspen.com/wp-content/uploads/2014/09/learning-from-failures.pdf
[60] 2011 Draft Annual Statistical Bulletin. Nigerian National Petroleum Corporation, 2011; 2012. https://www.nnpcgroup.com/Portals/0/Monthly%20Performance/2011%20ASB%201st%20edition.pdf

Mexiko, Uganda, Thajsko) mají také závažné problémy s krádežemi z produktovodů. Je evidentní, že krádeže z potrubí jsou pro potrubní průmysl jednou ze stěžejních otázek a měla by se tomu věnovat náležitá pozornost. Problémem může být i určitá sofistikovanost těchto nelegálních krádeží, které jsou v některých případech velmi těžko identifikovatelné. V současnosti existuje mnoho detekčních prvků, třebaže některá řešení obsahují také významné nedostatky.

- Kamerové systémy, detektory pohybu, bariéry a ploty patří nepochybně k nejzákladnějším opatřením, kterými lze chránit produktovody. Zde ovšem vyvstává problém, že tímto způsobem se reálně dají chránit pouze nadzemní části produktovodů. Nelze zároveň předpokládat ani možnost celkového pokrytí nadzemní části produktovodů, jelikož náklady by pravděpodobně byly vysoké, nehledě na možné logistické úskalí. Tento způsob ochrany lze považovat za dostačující v místech, kde je obecně vzato rušno a krádež je tak méně pravděpodobná. Kdežto u odlehlých míst, kde k útokům na produktovody dochází nejčastěji, budou tyto detekční prvky snadno zneškodněné.
- Další možností ochrany vůči krádežím jsou pozemní hlídky. Zde však platí podobný problém, jako u předchozího bodu. Rozmístění pozemních hlídek by logicky muselo být uskutečněno na základě priorit, přičemž stěžejními body by byly především důležité úseky jednotlivých produktovodů. Kvůli enormní délce produktovodů je nemyslitelné, aby bylo možné uhlídat celou plochu. Díky těmto faktorům lze usoudit, že v odlehlých částech produktovodů by tento typ ochrany nebyl prakticky vůbec efektivní. Navíc existuje další riziko, na které je v tomto případě nutné upozornit. Cílené krádeže a sabotáže jsou mnohdy způsobené organizovaným zločinem, ve formě silně ozbrojených skupin. V takovém případě by pozemní hlídce hrozilo extrémní nebezpečí a nelze očekávat, že by každá hlídka byla vycvičena k tomu, aby se za takové situace dokázala účinně bránit.
- Letecký dohled může být do značné míry užitečný, neboť možnosti pokrytí jsou mnohonásobně zvětšeny. Na druhou stranu lze těžko očekávat, že ochrana produktovodů touto formou by byla nepřetržitá. Dále je nutné si uvědomit, že krádeže z produktovodů se mohou provádět ve dne i v noci. Ačkoliv je možné vybavit letecké hlídky noktovizory nebo termovizory, finanční náročnost tohoto opatření okamžitě stoupne.[61]
- Další možností ochrany vůči krádežím jsou online detekční systémy úniku surovin. Tyto systémy jsou nepochybně účinné v odhalování zásadnějších úniků, nicméně nelze předpokládat dostatečnou citlivost online detekčních systémů na identifikaci menších krádeží.
- Fyzický dohled nad pozemními poruchami rovněž představuje zajímavou formu fyzické ochrany, ale podobně jako u pozemních hlídek zde figuruje zásadní logistický problém. Opět je nutností připomenout délku produktovodů a s tím související jev, že vždy bude možné identifikovat odlehlé místo, což je v takovém případě slabý článek celého systému. Navíc existují případy krádeží, kterých bylo dosaženo těžbou pod potrubím, což zabránilo jakémukoliv viditelnému narušení na povrchu.

[61] HOPKINS, Phil. Learning from Pipeline Failures. Penspen Integrity, 2008. http://www.penspen.com/wp-content/uploads/2014/09/learning-from-failures.pdf

- Detektory nárazu zachycují vibrace, způsobené například snahou prokopat se k produktovodům. Zde hraje roli zásadní otázka, a to nakolik citlivé takové detektory skutečně jsou. Vykopávka může být prováděna ručně a s určitou dávkou citlivosti, což může být problematické z hlediska zachycení takového narušení. Samotná krádež může posléze být provedena pouze pomocí ručního vrtáku. Zásadní rozdíl v tomto ohledu vyplývá ze zkušenosti zlodějů. Pokud zloději vědí, že jsou produktovody monitorovány pomocí detektorů nárazu, mohou tato zařízení vyřadit z provozu. V případě organizovaného zločinu se nabízí také možnost vytvoření falešného signálu, sloužící k odvedení pozornosti.
- Kabely s optickými vlákny představují další variantu, jak odhalit krádeže z produktovodů. Kabely s optickými vlákny mohou být umístěny podél produktovodů a jejich účelem je detekce případných narušení. Jedná se bezesporu o zajímavou formu ochrany, nicméně i zde je možné identifikovat slabé stránky takového řešení. Jakmile by byla známa přítomnost kabelů s optickými vlákny, staly by se okamžitým cílem pro vandaly a zloděje. Zde je podstatné upozornit na logický fakt, že pokrýt produktovody kabely s optickými vlákny je nepochybně reálnějším řešením než celoplošná fyzická ochrana.[62]

V současnosti již pochopitelně existují modernější, a především vyspělejší a účinnější metody ochrany produktovodů proti krádežím. Na druhou stranu je důležité si uvědomit, že výše zmíněné formy fyzické a technické ochrany produktovodů jsou v dnešní době stále aktuální a žádné z těchto opatření nepředstavuje stoprocentní ochranu. Ačkoliv technologie ochrany produktovodů se neustále zdokonaluje, finanční stránka věci úměrně stoupá s modernizací bezpečnostních opatření. Faktem zůstává, že země potýkající se s největším počtem krádeží z produktovodů, jsou zároveň státy s nedostatečnou ochranou produktovodní sféry.[63]

3.3 Kybernetické hrozby / útoky

Kybernetické hrozby z obecného hlediska jsou v posledních letech aktuálním fenoménem, kterému je zapotřebí přikládat značnou důležitost. Jedná se o stěžejní problematiku a energetický sektor je bezpochyby oblast, náchylná k možným kybernetickým útokům, jejichž důsledky mohou být zničující pro kritickou infrastrukturu daných zemí. Kybernetickým útokem v energetice se míní situace, kdy se hacker nebo skupina hackerů pokusí získat přístup ke klíčovým informacím či prvkům infrastruktury, mezi které patří například rozvodné soustavy, elektrárny a zejména jejich řídící centra. Cílem kybernetických útoků v energetické oblasti mohou být konkrétní prvky energetické infrastruktury, včetně produktovodů, které se tímto útokem snaží vyřadit z provozu, případně aplikovat škodlivý software, díky němuž je možné získat kontrolu nad objektem. Nelze podceňovat zisk kritických informací a jejich možná zneužitelnost, což může být hlavní příčinou kybernetického útoku.

[62] HOPKINS, Phil. Learning from Pipeline Failures. Penspen Integrity, 2008.
http://www.penspen.com/wp-content/uploads/2014/09/learning-from-failures.pdf
[63] RALBY, Ian. Downstream Oil Theft. Atlantic Council; Global Energy Center, 6. I. 2017.
ISBN 978-1-61977-440-7.
https://www.atlanticcouncil.org/images/publications/Downstream_Oil_Theft_web_0327.pdf

3.3.1 Příklady kybernetických útoků v energetickém sektoru

Jeden z příkladů provedených kybernetických útoků se uskutečnil v srpnu 2017 v Saudské Arábii, kde byla napadena petrochemická elektrárna. Ačkoliv se tato událost přímo netýká napadení produktovodů, slouží jako názornost možné ničivosti kybernetických útoků. Vyšetřovatelé tohoto incidentu věří, že záměrem sofistikovaného útoku nebylo pouze zničení dat nebo přerušení provozu elektrárny, ale měl sabotovat firemní provoz a následně vyvolat explozi. Tento kybernetický útok vytvořil nebezpečný precedent, jelikož hackeři demonstrovali zájem i schopnosti způsobit vážnou fyzickou újmu. Následkem jsou zejména obavy, zda podobný útok nebude replikován i v jiných zemích, jelikož tisíce dalších elektráren používají stejný počítačový systém. Současně zde vyvstávají další možné zranitelné cíle, mezi které bezesporu patří také produktovody.[64]

Podle vyšetřovatelů zabránila explozi chyba v počítačovém kódu útočníka. V počítači na pracovní stanici v elektrárně byl objeven zvláštní soubor, který byl naprogramován k sabotáži systému. Vyšetřování rovněž potvrdilo, že nic nenasvědčuje tomu, že by soubor někdo nahrál do počítače uvnitř elektrárny, tudíž systém byl sabotovaný na dálku.[65]

Organizace FireEye, zabývající se počítačovou bezpečností, uvedla koncem roku 2018, že stopy kybernetického útoku na petrochemickou elektrárnu v Saudské Arábii z roku 2017 vedou do Ruské federace.[66]

Centrální vědecký a výzkumný ústav chemie a mechaniky, se sídlem v Moskvě, je významnou institucí vlády Ruské federace, byl zodpovědný za vznik přinejmenším části malwaru Triton, který byl během útoku použit.[67] Tato informace byla zveřejněna pár měsíců poté, co bezpečnostní experti a britští experti odhalili plný rozsah hackingu na britském území.[68]

Jako další příklad lze uvést případ z dubna loňského roku, kdy ve Spojených státech amerických došlo ke kybernetickému útoku na sdílenou datovou síť čtyř společností (Oneok; Energy Transfer Partners; Eastern Shore Natural Gas; Boardwalk Pipeline Partners), které provozují plynovody. Všechny dotčené společnosti uvedly přerušení komunikačních systémů během útoků a není zřejmé, zda došlo k úniku informací. Kromě spotřebitelských

[64] PERLROTH, Nicole and Clifford KRAUSS. A Cyberattack in Saudi Arabia Had a Deadly Goal. Experts Fear Another Try. The New York Times, 15. III. 2018. https://www.nytimes.com/2018/03/15/technology/saudi-arabia-hacks-cyberattacks.html?module=inline

[65] PERLROTH, Nicole and Clifford KRAUSS. A Cyberattack in Saudi Arabia Had a Deadly Goal. Experts Fear Another Try. The New York Times, 15. III. 2018. https://www.nytimes.com/2018/03/15/technology/saudi-arabia-hacks-cyberattacks.html?module=inline

[66] TRITON Attribution: Russian Government-Owned Lab Most Likely Built Custom Intrusion Tools for TRITON Attackers. FireEye, 23. X. 2018. https://www.fireeye.com/blog/threat-research/2018/10/triton-attribution-russian-government-owned-lab-most-likely-built-tools.html

[67] FIELD, Matthew. Russian Hackers Linked to Attempted Sabotage of Saudi Energy Plant. The Telegraph, 24. X. 2018. https://www.telegraph.co.uk/technology/2018/10/24/russian-hackers-linked-attempted-sabotage-saudi-energy-plant/

[68] Joint United States– United Kingdom Statement on Malicious Cyber Activity Carried Out by Russian Government. National Cyber Security Centre, 15. IV. 2018. https://www.ncsc.gov.uk/news/joint-us-uk-statement-malicious-cyber-activity-carried-out-russian-government

a obchodních dat uchovávají energetické společnosti mnoho informací o svých podnicích, obchodních strategiích a průzkumných a výrobních technologiích.[69]

Podle zdejších kybernetických odborníků útok zdůraznil zranitelnost národního energetického systému vůči kybernetickým hrozbám. Současný trend digitalizace energetických systém představuje nesporné benefity, ale zároveň nevýhody v podobě zvětšené hrozby a dopadů kybernetických útoků.[70] Proniknutí do řídicích systémů produktovodů by mohlo způsobit podstatně větší škodu než narušení dodávek. Rizika zahrnují požáry, rozsáhlé rozlití surovin nebo exploze, přičemž všechna tato rizika vedou k ohrožení lidského života, zdraví, majetku a životního prostředí.[71]

3.3.2 Výzkumná studie Ponemon Institute

Výzkumná studie organizace Ponemon Institute, ve spolupráci se společností Siemens, zveřejnila v únoru 2017 vypracovanou studii týkající se aktuálního stavu kybernetické bezpečnosti Spojených států amerických v oblasti ropného a plynného průmyslu. Celkově se výzkumu zúčastnilo 377 osob, kteří jsou ve svých organizacích zodpovědní za zabezpečování kybernetických rizik. Podle těchto zjištění nedrží zavedená opatření v oblasti kybernetické bezpečnosti krok s růstem digitalizace v provozech ropy a zemního plynu. Pouze 35 % respondentů ohodnotilo úroveň kybernetické ochrany ve své organizaci za vysokou. Většina z ostatních dotázaných účastníků ohodnotila úroveň jejich kybernetické ochrany za střední až nízkou. Celkem 68 % všech respondentů potvrdilo, že v uplynulém roce museli řešit přinejmenším jeden případ ohrožení bezpečnosti, které vedlo k úniku důležitých informací nebo k narušení operačních technologií.[72]

K dalším výsledkům výzkumné studie patří:

- Kybernetické útoky mohou zůstat nezpozorovány (průměrně až 46 % kybernetických útoků není podle respondentů vůbec detekováno).
- Mnohé organizace nemají povědomí o kybernetických rizicích a nejsou připraveny na kybernetické narušení bezpečnosti (jak již bylo zmíněno výše, pouze 35 % dotazovaných ohodnotilo úroveň jejich kybernetické ochrany za vysokou).
- Digitalizace systémů přestavuje benefity i rizika (66 % respondentů se obává, že tato změna učinila jejich organizace zranitelnějšími vůči kybernetickým útokům)

[69] KRAUSS, Clifford. Cyberattack Shows Vulnerability of Gas Pipeline Network. The New York Times, 4. IV. 2018. https://www.nytimes.com/2018/04/04/business/energy-environment/pipeline-cyberattack.html
[70] MUNCASTER, Phil. United States Gas Pipelines Hit by Cyber-Attack. Infosecurity Magazine, 4. IV. 2018. https://www.infosecurity-magazine.com/news/us-gas-pipelines-hit-by-cyberattack/
[71] KRAUSS, Clifford. Cyberattack Shows Vulnerability of Gas Pipeline Network. The New York Times, 4. IV. 2018. https://www.nytimes.com/2018/04/04/business/energy-environment/pipeline-cyberattack.html
[72] The State of Cybersecurity in the Oil & Gas Industry: United States. Siemens. Traverse City: Ponemon Institute, February 2018. https://news.usa.siemens.biz/sites/siemensusa.newshq.businesswire.com/files/press_release/additional/Cyber_readiness_in_Oil__Gas_Final_4.pdf

- Největší zranitelnost organizací vyplývá ze zastaralých systémů kontroly v zařízeních (63 % dotázaných uvádí zastaralost systémů kontroly jako zdroj rizika pro jejich společnost).[73]

Na základě těchto výsledků lze říci, že organizace si ve větší míře uvědomují rizika kybernetických hrozeb, ale úroveň kybernetické ochrany je spíše podprůměrná. Zásadní problém představují útoky, které se nepodaří vůbec detekovat. V takovém případě mohou útočníci získat stěžejní informace, aniž by si toho postižené organizace byly vědomy, což představuje značné riziko. Je patrné, že výzkumná studie poukázala na největší hrozby v této oblasti. Energetický průmysl je zde označen jako druhé nejvíce ohrožené odvětví kybernetickým útokem.

Více lidí v energetickém průmyslu si začíná uvědomovat hrozby, jakými jsou například malware WannaCry, který vypustila Korejská lidově demokratická republika, nebo malware NotPetya a Triton, pocházející z Ruské federace. Je pravděpodobné, že jednotlivé organizace budou muset zvážit postupné přijetí dalších bezpečnostních opatření, aby úspěšně předešly narušení jejich systémů. Jak ukázaly nedávné kybernetické útoky, tradiční firewally již nestačí k ochraně před sofistikovanými státními protivníky a kybernetickými zločinci. Odborníci se mezitím snaží pracovat na kvalitních a efektivních řešeních, a zároveň analyzovat vzájemný vztah mezi kybernetickými útoky a terorismem.[74]

[73] The State of Cybersecurity in the Oil & Gas Industry: United States. Siemens. Traverse City: Ponemon Institute, February 2018. https://news.usa.siemens.biz/sites/siemensusa.newshq.businesswire.com/files/press_release/additional/Cyber_readiness_in_Oil__Gas_Final_4.pdf

[74] HOPE. MCDONALD, Natalie. Are Our Nation's Oil and Gas Pipelines Safe From Cyber-Attack?. Comptia, 24. X. 2018. https://www.comptia.org/about-us/newsroom/blog/comptia-blog/2018/10/24/are-our-nation-s-oil-and-gas-pipelines-safe-from-cyber-attack

4 Téma incidentů souvisejících s produktovody optikou nadnárodního risk managementu a expertní komunity České republiky

V této kapitole bude prostor věnován zejména projektům, které byly realizované na území České republiky v rámci programu Evropské Komise CIPS. Tyto projekty se týkají ochrany kritické infrastruktury a aplikovatelná bezpečnostní opatření. Cílem těchto projektů je preventivní činnost, ale také řešení následků a dopadů možných rizik v oblasti kritické infrastruktury. V další části kapitoly jsou uvedené rozhovory se třemi odborníky z bezpečnostní oblasti, kteří odpovídají na stanovené otázky k problematice útoků na produktovody.

4.1 Projekty realizované v programu Evropské Komise CIPS

Celý název projektu zní „Prevence, připravenost a zvládání následků teroristických útoků a jiných rizik spojených s bezpečností“. Projekt CIPS byl jedním ze dvou programů, který se uskutečnil pod záštitou rámcového projektu „Bezpečnost a ochrana svobod“, na němž se podílely všechny členské státy Evropské Unie. Projekt CIPS byl realizován rozhodnutím Rady 2007/124/ES a probíhal v letech 2007 až 2013. Zapojení do tohoto programu bylo umožněno také veřejným orgánům (ať už vnitrostátním, regionálním nebo místním), ale i univerzitám a jiným soukromým subjektům. Projektu byl v celé jeho délce vyhrazen rozpočet ve výši 126,8 milionů eur.

Program byl zaměřen především na kritickou infrastrukturu, její ochranu a bezpečnostní opatření. Jedním z hlavních bodů byla snaha identifikovat připravenost jednotlivých oblastí energetického sektoru na zvládnutí krizí. Cílem programu byla nejenom preventivní činnost, ale současně i řešení následků teroristických útoků a podobných bezpečnostních rizik a mimořádných událostí.[75] V rámci programu CIPS se následně uskutečnily v České republice projekty PACITA, APENCOT a CIPnES, které jsou následně v studii detailněji rozebrány. Všechny tyto zmiňované projekty se uskutečnily na území České republiky pod záštitou společnosti F.S.C.[76], která poskytuje bezpečnostní poradenství v České a Slovenské republice. Celkové výsledky projektu byly vyhodnoceny jako relevantní pro potřeby ochrany kritické infrastruktury a boje vůči předcházení trestné činnosti. Projekt byl v celém jeho období označen jako přínosný. Jedním z úspěchů programů je také demonstrace reálné potřeby koordinace a mezinárodní spolupráce v oblasti preventivní činnosti a zvládání následků terorismu a jiných bezpečnostních hrozeb. Z výsledků rovněž vyplývá, že program CIPS přispěl k rozvoji politiky ochrany kritické infrastruktury a dosáhl splnění obecně stanovených cílů, zatímco specifické cíle byly splněny ve větší míře také.[77] Nyní následují podkapitoly,

[75] Zpráva o zpětném hodnocení opatření financovaných z programu „Předcházení trestné činnosti a boj proti ní“ (ISEC) a z programu „Prevence, připravenost a zvládání následků teroristických útoků a jiných rizik spojených s bezpečností“ (CIPS) za období 2007–2013. Zpráva komise Evropskému parlamentu, Radě, Evropskému hospodářskému a sociálnímu výboru a Výboru regionů. EUR-Lex. Brusel: Evropská Komise, 12. VI. 2018. COM(2018) 455 final.
https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2018:0455:FIN:CS:PDF

[76] Společnost F. S. C. bezpečnostní poradenství, a. s.

[77] Zpráva o zpětném hodnocení opatření financovaných z programu „Předcházení trestné činnosti a boj proti ní“ (ISEC) a z programu „Prevence, připravenost a zvládání následků teroristických útoků a jiných rizik

v nichž jsou detailněji rozebrány konkrétní projekty, které byly plněny na teritoriu České republiky v rámci programu CIPS.

4.1.1 Projekt PACITA

Celý název projektu zní „Metodika hodnocení fyzické ochrany prvků Kritické infrastruktury proti napadení teroristickým útokem a dalšími formami útoků“. Projekt PACITA byl realizován s finanční podporou Programu prevence, připravenosti a řízení následků teroristických útoků a jiných bezpečnostních rizik, který vyhlásila Evropská komise – Generální ředitelství justice, svobody a bezpečnosti. Délka projektu byla stanovena celkem na 21 měsíců, přičemž projekt odstartoval v lednu roku 2012 a skončil v září roku 2013.[78]

Jako partneři projektu jsou uvedeny:

- Ministerstvo průmyslu a obchodu České republiky.
- Žilinská univerzita v Žilině
- DIRICKX BOHEMIA spol., s. r. o.
- Ministerstvo hospodárstva Slovenskej republiky (vystupuje jako přidružený partner projektu).

Specifickým cílem projektu PACITA bylo vytvoření nástroje pro hodnocení fyzické ochrany objektů kritické infrastruktury proti teroristickým a jiným formám útoků včetně modelování parametrů a ověření účinnosti daných opatření, zda jsou ve shodě se Směrnicí Rady 2008/114/EK. K dalším cílům patřilo posílení a podpora rozvoje dokumentace a metodik v oblasti ochrany kritické infrastruktury, zaměřené zejména na posuzování rizika. Prosazování a podpora rozvoje bezpečnostních norem a výměna zkušeností a znalostí v ochraně osob a kritické infrastruktury patří k dalším cílům, o které tento projekt usiloval. Plánované výsledky projektu zahrnují vytvoření metodiky testování odolnosti pasivních bariér, metodiky ověřování účinnosti systému fyzické ochrany a související penetrační testy a také seznam ochranných opatření.[79]

4.1.2 Projekt CIPnES

Název projektu zní „Ochrana kritické infrastruktury energetiky“. Projekt byl realizován v období od ledna roku 2010 do prosince roku 2011. Jedná se o další z grantových projektů, jehož stěžejním přínosem je využití finančních prostředků Evropské Unie pro zhodnocení aktuálního stavu fyzické ochrany objektů kritické infrastruktury a stanovení návrh standardů fyzické ochrany přenosu a distribuce energie (zejména ropy a zemní plynu).[80]

---

spojených s bezpečností“ (CIPS) za období 2007–2013. Zpráva komise Evropskému parlamentu, Radě, Evropskému hospodářskému a sociálnímu výboru a Výboru regionů. EUR-Lex. Brusel: Evropská Komise, 12. VI. 2018. COM(2018) 455 final.
https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2018:0455:FIN:CS:PDF

[78] PACITA. PACITA. F. S. C., 2013. https://sites.google.com/site/pacitacz/seznam

[79] PACITA. PACITA. F. S. C., 2013. https://sites.google.com/site/pacitacz/seznam

[80] CÍGLER, Jaroslav. Ochrana kritické infrastruktury energetiky (prezentace). F. S. C., 2011.
ŘEHÁK, David; Jaroslav CÍGLER; Pavel NĚMEC a Libor HADÁČEK. Kritická infrastruktura elektroenergetiky: určování, posuzování a ochrana. Ostrava: Sdružení požárního a bezpečnostního inženýrství, 2013.

Projekt CIPnES navazuje na projekt APENCOT a úzce spolu souvisí. Mezi partnery projektu jsou uvedeny:

- Ministerstvo průmyslu a obchodu České republiky.
- Ministerstvo hospodárstva Slovenskej republiky.
- MERO, a. s.
- ČEPRO, a. s.
- ČEPS, a. s.
- RWE Transgas, a. s.

Specifickým cílem projektu je zvýšení úrovně ochrany kritické infrastruktury, podílet se na vytvoření metodiky pro posuzování fyzické ochrany kritické infrastruktury a také přispět k tvorbě protiopatření ve formě bezpečnostních standardů. Dalším zásadním cílem je identifikovat aktuální stav ochrany kritické infrastruktury v energetice a posoudit připravenost systému na rizika teroristického útoku a jiných podobných hrozeb. S tímto souvisí zejména identifikace zranitelných článků v systému a aplikace protiopatření.[81]

4.1.3 Projekt APENCOT

Kompletní název projektu zní „Studie ochrany rozhodujících objektů energetické soustavy před terorismem a návrh bezpečnostních standardů“. Projekt byl realizován od roku 2008 do roku 2010. Přestože byl tento projekt zaměřen především na ochranu elektrizační soustavy jakožto části kritické infrastruktury, některé výchozí poznatky jsou podstatné i pro systém produktovodů. Jednou z řešených problematik projektu bylo vytvoření přehledu rizikových událostí a jejich následná identifikace na základě úrovně hrozby a úrovně zranitelnosti.

Rizikové události jsou rozděleny do čtyř kategorií – obecně rizikové události, a hrozby týkající se elektrické soustavy, zemního plynu a ropy. Mezi partnery projektu patří:

- Ministerstvo průmyslu a obchodu České republiky;
- Ministerstvo vnitra – generální ředitelství Hasičského záchranného sboru České republiky;
- České energetické závody;
- Česká energetická přenosová souprava.[82]

K hlavním cílům projektu APENCOT patří vytvoření metodiky pro hodnocení ochrany objektů a tvorba minimálního standardu fyzické ochrany pro jednotlivé kategorie objektů elektrizační soustavy. Účelem zmiňovaných standardů je předejít násilnému vniknutí do budov a zařízení

ISBN 978-80-7385-126-2.
https://www.researchgate.net/publication/261437766_Kriticka_infrastruktura_elektroenergetiky_urcovani_posuzovani_a_ochrana_Critical_Infrastructure_in_the_Energy_Sector_Identification_Assessment_and_Protection

[81] CÍGLER, Jaroslav. Ochrana kritické infrastruktury energetiky. Konference Parkhotel Praha, 24.-25. II. 2011.

[82] F.S.C. Bezpečnostní poradenstsví. Apencot. In: Studie ochrany rozhodujících objektů energetické soustavy před terorismem a návrh bezpečnostních standardů. Ostrava, 2010; 2011.
https://technologicky-katalog-sluzeb.webnode.cz/products/f-s-c-bezpecnostni-poradenstvi-a-s-/

a zabránit zničení nebo poškození technického vybavení a jiných aktiv. Tyto bezpečnostní standardy uplatňují přesné pokyny a případný subjekt musí přijmout přesně definovaná bezpečnostní opatření. Každý prvek elektrizační soustavy je stěžejní pro bezproblémové fungování celého systému. Některé prvky jsou však zásadnější a podle jejich významu pro bezpečnost daného systému jsou stanovena případná opatření.[83] Kategorie objektů elektrizační soustavy jsou vymezeny do 4 skupin a kategorie prostoru je rovněž vymezena do 4 skupin – kontrolovaný prostor; chráněný prostor; prostor se zvýšenou ochranou a zvlášť chráněný prostor.[84]

[83] Production Management and Engineering Sciences. Proceedings of the International Conference on Engineering Science and Production Management (ESPM 2015), Tatranské Matliare, High Tatras Mountains, Slovak Republic, 16th-17th April 2015. Milan MAJERNÍK; Naqib DANESHJO and Martin BOSÁK eds. London: CRC Press, 2015. ISBN 978-0429225888. https://www.taylorfrancis.com/books/9780429225888

[84] ŘEHÁK, David. Kritická infrastruktura elektroenergetiky: určování, posuzování a ochrana. Ostrava: Sdružení požárního a bezpečnostního inženýrství, 2013. Spektrum. ISBN 978-80-7385-126-2.

4.2 Rozhovory s experty

Následující část této studie je koncipována jako sonda mezi experty v bezpečnostní a energetické oblasti. Cílem výzkumu je identifikace názorů odborníků, kteří se pohybují v oblasti řešené problematiky.

V rámci této studie jsem použil metodu dotazování na základě rozhovoru a emailové komunikace s vybranými odborníky. Mezi respondenty se řadí experti z oblastí:

- Odborník č. 1: oblast terorismu.
- Odborník č. 2: oblast surovinové politiky.
- Odborník č. 3: oblast energetické bezpečnosti.

Průzkum

Otázka č. 1: V čem vidíte hlavní výzvy v oblasti útoků na produktovody?

Odborník č. 1: Zabezpečení energie je základním požadavkem, který v podstatě zajišťuje další rozvoj a potřebnou úroveň lidí. Jde o technologii, zajišťující existenci moderní společnosti jako takové. Z tohoto důvodu jsou produktovody přitažlivé z hlediska útoků, neboť v případě narušení těchto systémů dojde k výraznému omezení potřeb lidí a na tom principu se začínají měnit společenské vztahy. Mění se priority a vzniká určitá forma napětí ve společnosti, což představuje nebezpečnou záležitost z hlediska politického systému. Společnost se jako taková radikalizuje a může dojít k nepředvídatelnému vývoji událostí.

Odborník č. 2: Produktovody jsou podle mého názoru jedním ze zranitelných míst našeho kontinentu. Útoků na produktovody se běžně používá v rámci otevřených válečných konfliktů (např. Irák, Írán), občanských válek (aktuálně např. Nigérie), hlavním cílem je připravit protivníka o zisk z prodeje strategických surovin. V Evropě by se jednalo spíše o cíl postihnout velkou část obyvatelstva např. s cílem vyvolat jejich nespokojenost. Jako hlavní výzvu v Evropě vidím disponovat dostatkem finančních a technických prostředků, aby byla ochrana produktovodů na takové úrovni, že bude riziko potenciálního útoku co nejvíce minimalizováno.

Odborník č. 3: Domnívám se, že hlavní výzvou je celkové zajištění produktovodů. Útoky na tyto systémy převládají zejména v severní Africe a na Blízkém východě. V těchto regionech teroristické organizace usilují o ublížení ekonomice daného státu a snaží se dosáhnout jejich vlastní agendy. Evropa je touto problematikou zatím nepostižena, a tak můžeme pouze predikovat závažnost dopadů, které by případný útok způsobil.

Otázka č. 2: Myslíte si, že cílené útoky na produktovody budou přibývat i v Evropě?

Odborník č. 1: Do určité míry to souvisí s celkovou globální a mezinárodní bezpečností a politickou situací. V současnosti hrají roli i islámští bojovníci, kteří se vrací do Evropy. Může to být také předmětem soutěžení různých států. V tomto případě lze uvést projekty, vedoucí z Ruské federace do Evropy, jejichž existence není v zájmu USA. Tyto tenze mohou teoreticky vyústit i ve fyzické útoky. Z hlediska destabilizace společnosti se jedná o velice účinný cíl. Pokud bude ekonomicky, sociálně i politicky klidná situace, dá se předpokládat, že rizika do určité míry budou stagnovat. V případě narušení rovnovážného stavu je pravděpodobné, že například ropovody se mohou stát cílem útoku a nemusí se jednat pouze o útok fyzický, ale i o útok kybernetický. Zároveň mohou být předmětem politických požadavků a vydírání.

Odborník č. 2: Domnívám se, že v Evropě se budou útoky v budoucnu soustřeďovat hlavně na kybernetické útoky a snahu ochromit fungování kritické infrastruktury. A těch může samozřejmě přibývat. Vzestup či pokles rizika fyzických útoků si netroufám posoudit, podle mého názoru tam jsou dvě tendence, které jdou proti sobě: fyzická ochrana evropských produktovodů je na poměrně dobré úrovni, současně však v rámci organizačně nezvládnuté vlny utečenců se mohou po kontinentu pohybovat i potenciálně nebezpečné osoby.

Odborník č. 3: Doposud k útokům na produktovody v Evropě prakticky nedocházelo a je těžké odhadnout, zda by mohla situace v budoucnu eskalovat. Obrana v Evropě se neustále zdokonaluje a ochrana produktovodů patří k významným otázkám v oblasti energetické ochrany. Závažný fyzický útok by musel být dobře zorganizovaný a koordinovaný, přičemž jednou z možností by bylo simultánně napadnout více míst zároveň. Cílem útoku by byl především psychologický dopad na společnost. V Evropě je důležité si uvědomit, že útok na ropovod nemusí mít takový efekt kvůli diverzifikaci energetických zdrojů. Problém mohou představovat mezistátní body, ve kterých se produktovody spojují a kde by mohlo dojít k závažnější škodě.

Otázka č. 3: Dají se tyto hrozby efektivně předvídat?

Odborník č. 1: Do určité míry ano, ale myslím si, že predikce je omezená. Pokud bychom mluvili o fyzických útocích, základním problémem je ochrana území, na kterém se daný systém rozkládá. Není v lidských ani ekonomických silách žádného státu zajistit stoprocentní ochranu.

Odborník č. 2: Domnívám se, že tyto hrozby efektivně předvídat nelze. Pouze přísnými, což samozřejmě znamená také drahými, bezpečnostními opatřeními lze zvýšit pravděpodobnost, že bude připravovanému útoku zabráněno.

Odborník č. 3: Predikce těchto událostí je do značné míry omezená. Do určité míry lze pozorovat trendy a přístupy teroristických organizací k útokům na produktovody v postižených oblastech. Zejména ovšem záleží na kvalitě bezpečnostních opatření.

Otázka č. 4: Existují nějaká protiopatření? Má Evropa prostředky k tomu se proti tomuto typu útoků bránit?

Odborník č. 1: Fyzická ochrana je v tomto případě problematická. Technická ochrana je zajisté možná, ale asi nejúčinnějším nástrojem k ochraně těchto systémů jsou zpravodajské služby. Ty mohou na základě informací podobným útokům dokonce i předcházet.

Odborník č. 2: Rozhodně existují protiopatření, například přísná režimová opatření, kdo smí a kdo nesmí do příslušných areálů vstupovat, kamerová ochrana vlastních produktovodů, nadstandardní zabezpečení počítačových řídících systémů atd. Tato opatření jsou však velmi drahá, avšak jak řekl náš přední expert na energetickou bezpečnost Václav Bartuška, energetická bezpečnost je svým způsobem luxus.

Odborník č. 3: Protiopatření určitě existují v podobě fyzické a technické ochrany. V Evropě je ochrana produktovodů na vysoké úrovni a troufám si tvrdit, že se neustále zdokonaluje. Produktovody jsou zakopané hluboko pod zemí a jsou chráněné pomocí plotů a dronů.

Otázka č. 5: Představují větší hrozbu fyzické nebo kybernetické útoky?

Odborník č. 1: Myslím, že fyzický a kybernetický útok na produktovody nelze od sebe oddělit. Nejhorším scénářem, který si můžete představit, je kombinace fyzického i kybernetického útoku. Takže obě formy spolu souvisí.

Odborník č. 2: Domnívám se, že v současném světě při dnešním rychlém vývoji technologií, představují větší hrozbu kybernetické útoky. Situace se však logicky liší teritorium od teritoria. To samozřejmě neznamená, že hrozbu fyzických útoků je možno podceňovat – tento typ útoků hrozí zejména v zemích tzv. „třetího světa“, jsme toho svědky například v Nigérii. Ve vyspělých částech světa poroste stále více hrozba kybernetických útoků na kritickou infrastrukturu.

Odborník č. 3: Jak jsem již avizoval v předchozí otázce, fyzická ochrana produktovodů v Evropě je na vysoké úrovni. V Evropě by kybernetický útok představoval větší ohrožení. V jiných regionech, kde dochází k častým útokům na tyto systémy, nelze vyloučit hrozby fyzických útoků jakožto závažnější formu ohrožení.

Výsledky průzkumu

Otázka č. 1: V čem vidíte hlavní výzvy v oblasti útoků na produktovody?

Všichni odborníci se shodují, že zabezpečení produktovodů patří k nejvýznamnější výzvám v oblasti útoků na produktovody. První odborník zdůrazňuje význam energie pro moderní společnost, jejíž narušení by způsobilo výrazné omezení potřeb lidí vzrůst napětí ve společnosti, představující možnosti radikalizace společnosti a s tím spojenou nepředvídatelnost vývoje událostí. Zbývající respondenti poukazují na rozdílnost konfliktů z hlediska regionu, v němž se útoky uskutečňují. Zatímco v severní Africe nebo na Blízkém východu jde zejména o zisky z prodejů strategických surovin a ublížení ekonomikám daných států, v Evropě by k cílům patřilo vyvolání nespokojenosti obyvatelstva, což se shoduje s názorem prvního experta.

Otázka č. 2: Myslíte si, že cílené útoky na produktovody budou přibývat i v Evropě?

První dva odborníci poukazují ve svých odpovědích na potenciální hrozbu výskytu islámských bojovníků na evropském kontinentu, v souvislosti s migrační vlnou. S tím souvisí také možnost fyzického útoku na produktovody, nicméně větší hrozbu v Evropě spatřují u kybernetických útoků. První odborník odkazuje na soutěžení mezi státy, které způsobují tenze, z nichž může vyústit konflikt. Důležitá je i zmínka o útoku na produktovody z hlediska stanovení politických požadavků a vydírání. Poslední respondent zdůrazňuje psychologický efekt na obyvatelstvo jakožto hlavní cíl případného fyzického útoku. Zároveň poukazuje na nutnost koordinace fyzického útoku a hlavní hrozbu v této oblasti spatřuje v simultánním útoku na několik bodů najednou, zejména pak na důležité místa, ve kterých je větší koncentrace produktovodů.

Otázka č. 3: Dají se tyto hrozby efektivně předvídat?

U této otázky se všichni oslovení experti do určité míry shodují v tom, že možnosti predikce těchto hrozeb jsou omezené. Respondenti rovněž potvrzují stěžejní důležitost bezpečnostních opatření, zajišťující ochranu produktovodů. Současně však podotýkají, že zajištění těchto ochranných prvků je finančně nákladná záležitost a zajištění stoprocentních ochrany není z ekonomického hlediska v silách žádného státu.

Otázka č. 4: Existují nějaká protiopatření? Má Evropa prostředky k tomu se proti tomuto typu útoků bránit?

Také u této otázky se všichni oslovení experti částečně shodují ve svých odpovědích. Zásadní roli zde hrají fyzické a technické bezpečnostní opatření, které jsou sice finančně nákladné, ale jejich kvalita se neustále vylepšuje. První odborník vidí nejvýznamnější roli ochrany produktovodů ve zpravodajských službách. Díky zprostředkovaným informacím je možné předvídat hrozby a případným útokům úplně předejít.

Otázka č. 5: Představují větší hrozbu fyzické nebo kybernetické útoky?

Odpověď na tuto otázku se liší zejména v závislosti na oblasti či teritoriu, o kterém je řeč. První odborník poukazuje na význam obou těchto forem útoků a na jejich neoddělitelnost. Současně spatřuje největší hrozbu v kombinovaném fyzickém a kybernetickém útoků, který by mohl mít zásadní dopad na kritickou infrastrukturu. Ostatní respondenti zdůrazňují, že ve vyspělých částech světa představují větší hrozbu kybernetické útoky, kdežto v chudších regionech, v nichž dochází k útokům na produktovody, jsou stále větší hrozbou fyzické útoky.

5 Přístupy k ochraně produktovodů a návrhy na protiopatření

V této kapitole bude prostor věnován přístup k ochraně produktovodů, které lze rozdělit do tří kategorií na fyzické, technické a informační. V souvislosti s jednotlivými typy ochrany produktovodů je zde vypracována analýza těchto typů ochrany a návrhy na protiopatření. Poslední část této kapitoly je koncipována jako sonda do soukromé sféry. Je zde poskytnut detailní náhled na soukromý subjekt, nabízející moderní bezpečnostní opatření v oblasti ochrany produktovodů. Tato část kapitoly slouží jako názorná ukázka technologie, kterou lze v současnosti aplikovat k ochraně produktovodů a zároveň nastavuje úroveň, k jejíž dosažení by měl aspirovat každý provozovatel produktovodů.

5.1 Fyzická ochrana a návrhy na protiopatření

Fyzická ochrana produktovodů by se dala definovat jako systém bezpečnostních opatření, využívající lidských sil k zabezpečení ochrany. Tato forma ochrany produktovodů představuje nedílnou součást zabezpečení, nicméně i tak představuje problematickou otázku. Jednou z klíčových vlastností produktovodů je jejich délka, což z logického pohledu představuje závažný problém pro efektivní řešení fyzické ochrany těchto systémů. Náročnost ovšem spočívá také v ekonomické stránce věci, neboť zajisti fyzickou ochranu po celé produktovodů je z finančního hlediska prakticky nemožné. Regiony zde hrají velkou roli, neboť každý stát přistupuje k fyzické ochraně rozdílným způsobem. Evropské státy disponují kvalitní fyzickou ochranou produktovodů, k čemuž napomáhá fakt, že strategicky významné produktovody jsou v Evropě ve velké míře zakopány pod zemí. Naprostým opakem je situace ve státech „třetího světa“, kde jsou produktovody spíše nad zemí, kde jsou vystaveny podstatně většímu riziku.

Některé formy fyzické ochrany jsem již zmiňoval u podkapitoly o krádežích z produktovodů, ale pro lepší orientaci jsou zmíněné i v této kapitole. K fyzické ochraně bezpochyby patří pozemní hlídky, ostraha a letecký dohled.[85] Všechny tyto varianty jsou samozřejmě v určitém ohledu účinné a jsou platnou součástí ochrany produktovodů. Na druhou stranu je nutné podotknout, že ku příkladu pozemní hlídky budou z logistického hlediska usměrněné do stěžejních částí systému, jakými jsou řídící střediska nebo zásobovací sklady. Odlehlé části produktovodu ovšem zůstanou nechráněné a nelze předpokládat, že by se s tímhle problémem z hlediska pozemních hlídek dalo něco dělat. Letecké hlídky dokáží pokrýt podstatně větší vzdálenost, ale stále nejde o ideální řešení, schopné neustále pokrývat veškerý rozsah produktovodů. Ostraha se z pravidla pohybuje na kontrolních stanovištích a v areálu konkrétních zařízení, přičemž jejich úloha spočívá v hlídkování oblasti okolo areálu v roli bezpečnostního ochranného doprovodu.[86] U fyzické ochrany lze protiopatření navrhnout paradoxně ve formě menšího využití lidí a zapojení ideálních technických prostředků, které efektivněji dokáži plnit stanovené úlohy. V případě pozemních hlídek se

[85] Metodika zajištění ochrany kritické infrastruktury v oblasti výroby, přenosu a distribuce elektrické energie. Praha: Deloitte, 2012; DocPlayer. https://docplayer.cz/17588799-24-10-2012-metodika-zajisteni-ochrany-kriticke-infrastruktury-v-oblasti-vyroby-prenosu-a-distribuce-elektricke-energie.html

[86] ŘEHÁK, David. Kritická infrastruktura elektroenergetiky: určování, posuzování a ochrana. Ostrava: Sdružení požárního a bezpečnostního inženýrství, 2013. Spektrum. ISBN 978-80-7385-126-2.

nabízí varianta dronů, které by neměly chybět v rámci zabezpečení objektů kritické infrastruktury.

Zvláštní variantu tvoří mechanické zábranné prostředky. Mezi mechanické zábranné prostředky patří bariéry, ploty, brány, ale i turnikety, mříže, zámky a uzamykací systémy a další. Účelem těchto ochranných prostředků je zamezit vstupu do chráněných prostorů nebo objektů. Ve své podstatě se jedná o systémy, které lze do určité míry neustále zdokonalovat, což z nich činí důležitou součást ochrany produktovodů.[87] Bariéry nebo ploty lze navíc postavit po celé délce produktovodů, respektive podél jejich nadzemní části. Nevýhodou mechanických zábranných prostředků spatřuji v jejich nedostatečnosti samo o sobě. Dle mého názoru se jedná o účinné bezpečnostní opatření, pokud jsou doplněny další formou ochrany. Pokud bych měl tuto myšlenku rozvést na příkladu, tak oplocení produktovodů samo o sobě nedokáže zabránit útoku, obzvlášť pokud půjde o organizované zločince. Tento fakt je ještě zřetelnější na odlehlých místech, kde nebude hrát zásadní roli ani časové zdržení při zneškodňování těchto mechanických zábranných prostředků.

5.2 Technická ochrana a návrhy na protiopatření

Technická ochrana produktovodů nabízí celou škálu možných řešení, obzvláště oproti fyzické ochraně. Nespornou výhodou je automatizace těchto systémů a absence nutnosti lidských sil, respektive jejich neustálou přítomnost. Technologie se vyvíjí, což má pochopitelně příznivý vliv i na ochranné prostředky. Mezi typické formy technické ochrany patří kamerové systémy, kabely s optickým vláknem, detekční systémy, zabezpečení zabraňující vstupu do objektů a mnoho dalších.[88]

Kamerové systémy patří k jedné z nejběžnějších forem technické ochrany, a jejich využití pochopitelně spadá i do ochrany produktovodů. Význam kamer v rámci ochrany v moderní společnosti je nesporný a pouze těžko si lze představit významné zařízení nebo objekt bez kamerových systémů. Existuje celá řada různých kamerových systémů, přičemž nejmodernější kamery jsou schopné snímat obraz a teplotu na velkou vzdálenost.[89]

Nevýhodou těchto systémů je, že je nelze aplikovat po celé délce produktovodů. Z ekonomického hlediska by taková varianta nedávala smysl a podobně jako u oplocení, kamera sama o sobě nezabrání útoku na produktovody a dá se předpokládat, že nebude náročné ji vyřadit z provozu.

[87] Metodika jednotného určování zařízení pro výrobu, přenos a distribuci elektřiny národní a evropskou kritickou infrastrukturou a zajišťování fyzické ochrany těchto zařízení. Praha: Ministerstva vnitra České republiky, 2013; ResearchGate. https://www.researchgate.net/publication/266852546_Metodika_jednotneho_urcovani_zarizeni_pro_vyrobu_prenos_a_distribuci_elektriny_narodni_a_evropskou_kritickou_infrastrukturou_a_zajistovani_fyzicke_ochrany_techto_zarizeni

[88] ŘEHÁK, David. Kritická infrastruktura elektroenergetiky: určování, posuzování a ochrana. Ostrava: Sdružení požárního a bezpečnostního inženýrství, 2013. Spektrum. ISBN 978-80-7385-126-2.

[89] Metodika zajištění ochrany kritické infrastruktury v oblasti výroby, přenosu a distribuce elektrické energie. Praha: Deloitte, 2012; DocPlayer. https://docplayer.cz/17588799-24-10-2012-metodika-zajisteni-ochrany-kriticke-infrastruktury-v-oblasti-vyroby-prenosu-a-distribuce-elektricke-energie.html

Detekční systémy jsou technická opatření, které mohou detekovat vibrace v produktovodu, pohyb v zařízení nebo změny tlaku v produktovodech. Jedná se o zařízení, které jsou důležitým prvkem v ochraně produktovodů. Jak je již z názvu patrné, jejich cílem je detekovat informace a anomálie, které mohou ohrozit funkčnost produktovodu. Detekční systémy jsou zpravidla napojené na řídící střediska, kde dochází ke zpracování veškerých dat, zachycených pomocí těchto prostředků. Jedná se o důmyslné technické systémy, které hrají klíčovou roli při identifikaci možných rizik.[90] Nevýhodu může představovat nedostatečná citlivost detekčního zařízení. Systém může být například nastaven na reakci na větší změny tlaku, nicméně menší změny zůstanou nepovšimnuty.[91] Toto může hrát roli například u krádeží produktovodů, kdy detekční systém je nastaven na měření vibrací, avšak u krádeží menšího rozsahu nedojde k takovým vibracím, aby detekční prvek tuto situaci zachytil.

Významný technologický posun vpřed lze pozorovat u systému bezpilotních letounů. Drony se řadí k perfektním technickým prvkům ochrany, které je možné ovládat dálkově, jsou vysoce programovatelné a poskytují kvalitní snímky oblasti a dokáží upozornit na případná nebezpečí. Dalším významným technickým prvkem ochrany jsou satelity, které poskytují snímky ve vysoké kvalitě a mohou neustále monitorovat jakýkoliv úsek produktovodu. Satelity jsou navíc schopné rozpoznat změny v povrchu, respektive dokáží identifikovat události, ve kterých by se útočník snažil například prokopat k nějakému produktovodu.[92]

5.3 Informační systémy a návrhy na protiopatření

Informační systémy se dostávají v oblasti ochrany produktovodů do popředí, neboť jedním z aktuálních trendů je digitalizace systémů. V souvislosti s nárůstem kybernetických hrozeb ovšem digitalizace zvětšuje pravděpodobnost ohrožení tímto druhem útoku. Produktovody zpravidla používají informační software SCADA, prostřednictvím kterého lze monitorovat a ovládat technologii produktovodu z řídícího centra. Systém SCADA umožňuje také rychlý přenos dat, možnost dálkové údržby a konfigurace produktovodů a zároveň měří a vypočítává životnost produktovodů na základě provozu a celkové zátěže.[93] Lze předpokládat, že produktovody obsahují další informační systémy v podobě ochranného softwaru, avšak informace o těchto programech jsou udržovány v tajnosti jakožto ochrana vůči zneužití informací.

Protiopatření se v této oblasti nabízí například ve větší investici do ochrany vůči kybernetickým hrozbám. V současnosti se společnost ocitá v situaci, kdy klasické ochranné prostředky v této oblasti již nestačí. Spoléhat se na firewally a antivirové softwary přestává být dostačujícím řešením a organizace musí učinit krok vpřed k zajištění ochrany

[90] ŘEHÁK, David. Kritická infrastruktura elektroenergetiky: určování, posuzování a ochrana. Ostrava: Sdružení požárního a bezpečnostního inženýrství, 2013. Spektrum. ISBN 978-80-7385-126-2.
[91] Learning from Pipeline Failures. Penspen Integrity, 2008. http://www.penspen.com/wp-content/uploads/2014/09/learning-from-failures.pdf
[92] Aratos Pipeline Protection Platform. Aratos Technologies, 2015. https://www.aratoshls.com/Aratos_Pipeline_Security_Platform_Presentation_-_2015c.pdf
[93] MERO Česká republika. https://mero.cz/

produktovodů.[94] Jako řešení se nabízí také sdílení informací a poznatků o ochraně proti kybernetickým útokům. Pokud budou provozovatelé produktovodů navzájem spolupracovat, mohou zvýšit úroveň zabezpečení a tím současně posílit svá aktiva. Dalším protiopatřením může být vyvinutí geografického informačního systému, který dokáže monitorovat oblasti a identifikovat konkrétní úseky, ve kterých došlo k poškození nebo narušení funkčnosti produktovodu.[95] Podobný geografický informační systém nabízí k ochraně produktovodů například soukromý subjekt Aratos Technologies S.A., jejichž nabízené služby jsou rozebrány v další části této studie.

Závěrem lze dodat, že jednotlivé formy bezpečnostních opatření nelze posuzovat jednotlivě. Řada z těchto systémů funguje kvalitně na vlastní bázi, nicméně samy o sobě mohou být zranitelné a nebudou dosahovat žádoucí účinnosti. Důležitým bodem je zkombinovat tyto systémy do jednoho komplexního celku, tvořící bezpečnostní systém daného objektu, v tomto případě produktovodů a jejich řídících center a jiných důležitých zařízení. V takovém případě se negativní stránky jednotlivých opatření neprojeví do takové míry, neboť jsou podpořeny funkcí dalších systémů, které tato negativa zmírňují. Bezpečnostní systém je silný pouze jako jeho nejslabší celek.

5.4 Aratos Technologies S.A. – Systém dozoru nad produktovody

Soukromý subjekt Aratos Technologies S.A. je evropská společnost, která je součástí skupiny Aratos, do které dále patří například společnost Aratos Homeland Security. Organizace byla založena v roce 2003 a k jejich činnostem patří poskytování produktů a služeb navržených podle požadavků a potřeb jejich zákazníků. Angažují se mimo jiné také v ochraně kritické infrastruktury a produktovodů.[96] V rámci ochrany nabízí systémy bezpilotních letadel zhotovené na zakázku, unikátní satelitní využití a jiné moderní technologie (bezpilotní vozidla, systém automatické identifikace a rozpoznání obličeje, optická vlákna nebo radary určené pro pozemní dozor) k dohledu a ochraně jakéhokoliv prvku kritické infrastruktury. Společnost avizuje využití nejmodernějších přístupů a techniky k ochraně kritické infrastruktury a poskytují kvalitní řešení vůči rizikům ohrožující prvky kritické infrastruktury. Zajímavostí je nabídka unikátních bezpečnostních opatření, a to ve vesmírném sektoru, vzdušném sektoru, pozemním sektoru i podzemním sektoru.[97]

Jednou z nabízejících služeb této společnosti je platforma ochrany potrubí v rámci systému dozoru nad produktovody. Tento systém mimo jiné využívá:

- Inteligentní softwarovou platformu pro vyhledávání a indexování informací.
- Satelitní data a zpracování satelitních snímků ve vysokém rozlišení.

[94] Are Our Nation's Oil and Gas Pipelines Safe From Cyber-Attack? Comptia, 24. X. 2018. https://www.comptia.org/about-us/newsroom/blog/comptia-blog/2018/10/24/are-our-nation-s-oil-and-gas-pipelines-safe-from-cyber-attack
[95] Pipeline Surveillance System. Aratos Technologies, 2018. https://aratos.gr/index.php/solutions/pipeline-surveillance-system
[96] Aratos Technologies, 2019. https://aratos.gr/index.php/company
[97] Who We Are. Aratos Homeland Security; Aratos Technologies, 2018. https://www.aratoshls.com/whowr.html#

- Vlastní vyvinutý geografický informační systém, který zobrazuje aktuální stav produktovodů. Mezi další funkce geografického informačního systému patří zobrazení úseků, v nichž došlo k poškození, včetně zobrazení výstrah a varování a následné informování subjektu. Zároveň obsahuje digitální mapy zájmových oblastí a umožňuje jejich vizualizaci.
- Systém bezpilotních letadel pro monitorování produktovodní sítě v těsné blízkosti.[98]

Vesmírný sektor ochrany produktovodů operuje na bázi satelitů. K výhodám těchto satelitů se řadí globální pokrytí, akurátní indikace detekce změny povrchu (například kopání), denní dohled a automatizované procesy skrze interaktivní rozhraní geografického informačního systému. Využití radaru se syntetickou aperturou poskytuje cenné údaje o detekci úniků, koroze a dalších hrozeb.[99]

Vzdušný sektor ochrany produktovodů se vyznačuje zejména zmiňovaným používáním programovatelných a dálkově ovládaných dronů. Bezpilotní letadla podle společnosti Aratos Technologies S. A. disponují mnohými výhodami, mezi které patří:

- Nahrazení fyzické hlídky za minimální cenu.
- Snímky s vysokým rozlišením umožňují detailní kontrolu objektů na zemi.
- Velké možnosti konfigurace.
- Mohou být vybaveny různými typy senzorů – optické, zvukové, infračervené kamery (úniky ropy a plynu se dobře projevují na infračerveném světle kvůli teplotním rozdílům mezi půdou a kapalinou).
- Nepřetržitý přenos dat do kontrolních center.
- Integrovaný software pro zpracování obrazu, který dokáže identifikovat cíle a další.[100]

Je patrné, že drony mohou mít zásadní využití v ochraně produktovodů. Pozemní sektor ochrany produktovodů představuje kombinaci fyzické a technické ochrany. V případě nabídky organizace Aratos Homeland Security se jedná zejména o železné oplocení, kabely s optickým vláknem, řídící věže, pozemní radary a kamerové systémy s dlouhým dosahem, vybavené senzory citlivé na teplotu. Co se týče podzemního sektoru, jedná se především o detekční senzory vibrací, jejichž účelem je upozornění na případný únik látek. Dále se jedná o senzory rozpoznávající teplotní změny v produktovodech a případná možnost přesné identifikace postiženého úseku.[101]

[98] Pipeline Surveillance System. Aratos Technologies, 2018.
https://aratos.gr/index.php/solutions/pipeline-surveillance-system
[99] Aratos Pipeline Protection Platform. Aratos Technologies, 2015.
https://www.aratoshls.com/Aratos_Pipeline_Security_Platform_Presentation_-_2015c.pdf
[100] Remotely Piloted Aircraft Systems (RPAS). Aratos Platform RPAS. Aratos Technologies, 2018.
https://aratosrpas.com/
[101] Aratos Pipeline Protection Platform. Aratos Technologies, 2015.
https://www.aratoshls.com/Aratos_Pipeline_Security_Platform_Presentation_-_2015c.pdf

Závěr

Útoky na produktovody patří k aktuálním geopolitickým problémům. Liniové stavby představují nejrychlejší formu distribuce strategických surovin (ropa a zemní plyn) a z tohoto důvodu jsou produktovody důležitou součástí kritické infrastruktury. Závažnost této problematiky se značným způsobem liší v závislosti na regionech. Nejvíce zasažení oblasti jsou v severní Africe (zde se jedná zejména o Nigérii, ale také Alžírsko nebo Egypt), na Blízkém východě (Sýrie, Irák, Saudská Arábie nebo Jemen), v jihovýchodní Asii (především Indonésie) a v jižní Americe (Mexiko a Kolumbie). Je důležité zmínit, že každý z těchto regionů se potýká s jinou formou útoků na produktovody a situace může výrazně fluktuovat v závislosti na aktuálním politickém dění v těchto státech. Příkladem může být Nigérie, kde během posledních tří let docházelo k dohodám o příměří mezi vládou a místní ozbrojenou organizací, nicméně dohoda byla několikrát porušena ojedinělým útokem na produktovod a současná situace může být stále považována za vypjatou. Nyní již ke stanoveným hypotézám.

Hypotéza č. 1: Tuto hypotézu jsem na základě poznatků v práci verifikoval. Útoky na produktovody jsou v dnešním světě problémem několika vybraných zemí, mezi nimiž není žádný stát z Evropy. V Evropě k žádnému přímému útoku na produktovody nedošlo, třebaže nelze tuto alternativu v budoucnosti vyloučit. V posledních měsících jsou například viditelné mezinárodní tenze v politickém prostředí ohledně výstavby plynovodu Nord Stream 2.

Hypotéza č. 2: Tuto hypotézu jsem na základě poznatků v studii verifikoval. Fyzická a technická ochrana produktovodů v Evropě je na vysoké úrovni. Produktovody jsou navíc ve velké části zakopané pod zemí, tudíž případný fyzický útok by musel být koordinovaný a zasáhnout slabé místo celého systému. Kybernetické útoky jsou nejenom v energetice globálně na vzestupu. Produktovody se digitalizují, což umožňuje pohodlnější automatizované ovládání, na druhou stranu digitalizace systémů zanechává produktovody náchylnější ke kybernetickému útoku. V Evropě lze předpokládat, že kybernetický útok je v této oblasti pravděpodobnější a lze očekávat ničivějšího účinku než v případě útoku fyzického.

Ačkoliv se v současnosti soustřeďují útoky na produktovody výhradně ve státech, které produkují velké množství ropy a zemního plynu, je těžké predikovat, zda se tento stav bude měnit či nikoliv. Na území Evropy shledávám největší výzvu v kybernetickém ohrožení. Nejenom z konkrétních případů uvedených v této studii je patrné, nakolik ničivé dopady může mít kvalitně provedený kybernetický útok. Cílem studie bylo ověřit nebo vyvrátit stanovené hypotézy, čehož jsem dle mého názoru docílil. Dále bylo cílem analyzovat bezpečnostní opatření v rámci ochrany produktovodů. U nich jsem stanovil slabé a silné stránky a snažil se navrhnout možnosti na případné vylepšení. Závěrem jsem měl za cíl analyzovat aktuální situaci ve vybraných regionech, mezi které jsem zařadil Nigérii a Mexiko a zároveň poukázat na závažnost útoků na produktovody pro společnost, čehož jsem dle mého názoru docílil.