POTREBUJEME VIAC ODBORNÍKOV NA KRITICKÚ INFRAŠTRUKTÚRU

Analýza zraniteľností Slovenska voči možnému hybridnému pôsobeniu proti kritickej infraštruktúre.

V rámci pravidelného seriálu o hybridných hrozbách sa v šiestej kapitole zameriame na to, ako je v SR zabezpečená kritická infraštruktúra proti útokom, ktoré môžu byť vykonané v rámci hybridného pôsobenia. Analýza neprináša hodnotenie stavu fyzickej ochrany kritickej infraštruktúry pracovníkmi na to určenými, ani hodnotenie systémov použitých na jej ochranu.

Zhrnutie:

Vyhodnotenie situácie v oblasti ochrany slovenskej kritickej infraštruktúry pred hybridným pôsobením ukazuje, že zraniteľnosti identifikované v hĺbkovej analýze hybridných hrozieb, ktorú ministerstvo vnútra publikovalo v roku 2023, vo veľkej miere stále pretrvávajú.

Znefunkčnenie špecializovaných útvarov určených na riešenie hybridných hrozieb spôsobilo, že štát sa momentálne zaoberá problematikou hybridného pôsobenia proti kritickej infraštruktúre iba na úrovni osobnej angažovanosti jednotlivých zamestnancov.

Slovensko čelí významným výzvam v oblasti ochrany kritickej infraštruktúry. Súčasná legislatíva a financovanie zaostávajú za vývojom bezpečnostného prostredia a hybridného pôsobenia. Nový zákon z roku 2024 síce reflektuje tieto hrozby, avšak jeho prijatie prišlo neskoro. Problémy pretrvávajú najmä v podfinancovaní, nedostatku odborníkov a nedostatočnej koordinácii medzi štátnymi orgánmi. Incidenty, ako kybernetický útok na kataster, poukazujú na slabiny v kybernetickej bezpečnosti. Navyše, odporúčania na zlepšenie krízového riadenia a zvýšenie odolnosti ostávajú často nerealizované.

Súčasný stav robí Slovensko výrazne zraniteľné voči hybridnému pôsobeniu proti kritickej infraštruktúre.

Je nevyhnutné, aby sa táto problematika dostala do popredia a stala sa prioritou, ktorá bude riešená naprieč štátnou správou SR, najmä ministerstvom vnútra. Bude potrebné navýšiť a udržať odborný personál, zabezpečiť potrebné finančné prostriedky na ochranu kritickej infraštruktúry a nastaviť funkčný a udržateľný systém jej ochrany.

A. Ako môže byť kritická infraštruktúra ohrozovaná hybridným pôsobením?

Vo vyspelých krajinách sú identifikované objekty kritickej infraštruktúry, ktoré zohrávajú zásadnú úlohu pri zabezpečovaní bezpečnosti, fungovania spoločnosti a stability hospodárstva štátu. Podľa platnej slovenskej legislatívy sa za kritickú infraštruktúru považujú najmä inžinierske stavby, služby vo verejnom záujme a informačné systémy v rámci sektora kritickej infraštruktúry, ktorých narušenie alebo zničenie by malo vážne negatívne dopady na hospodárske a sociálne funkcie štátu. Takéto ohrozenie by zároveň ovplyvnilo kvalitu života obyvateľov, najmä z hľadiska ochrany ich života, zdravia, bezpečnosti, majetku a životného prostredia. Tieto objekty sa nachádzajú v rôznych sektoroch hospodárstva, ako sú doprava, elektronické komunikácie, energetika, pošta, priemysel, informačné a komunikačné technológie, voda a atmosféra, zdravotníctvo či financie.

Kritická infraštruktúra môže byť vystavená hybridným hrozbám rôznymi spôsobmi. Uvádzame niekoľko príkladov, ako takéto pôsobenie môže prebiehať:

- **Špionáž**: Zahraničný aktér môže získať citlivé údaje, napríklad plány bezpečnostných opatrení alebo spôsobu fungovania jednotlivých kľúčových systémov. To môže oslabiť kontrolu nad infraštruktúrou a umožniť realizáciu ďalších útokov. Ak špionážne aktivity odhalia strategické ekonomické informácie, môže to viesť k manipulácii trhu s energiami alebo potravinami, čo následne ohrozí stabilitu hospodárstva.

- **Sabotáž**: Hybridné hrozby môžu zahŕňať aj fyzické útoky na kritickú infraštruktúru, napríklad sabotáže plynovodov, elektrického vedenia alebo vodárenských zariadení, ktoré môžu mať za následok narušenie dodávok základných služieb.

- **Kybernetické útoky**: Útočníci môžu napadnúť IT systémy kritickej infraštruktúry, ako sú elektrárne, nemocnice či vodárne, a spôsobiť ich výpadok, zníženie kapacity alebo skreslenie dát. Napríklad kyberútok na energetické siete môže viesť k rozsiahlym výpadkom elektriny alebo kľúčových systémov.

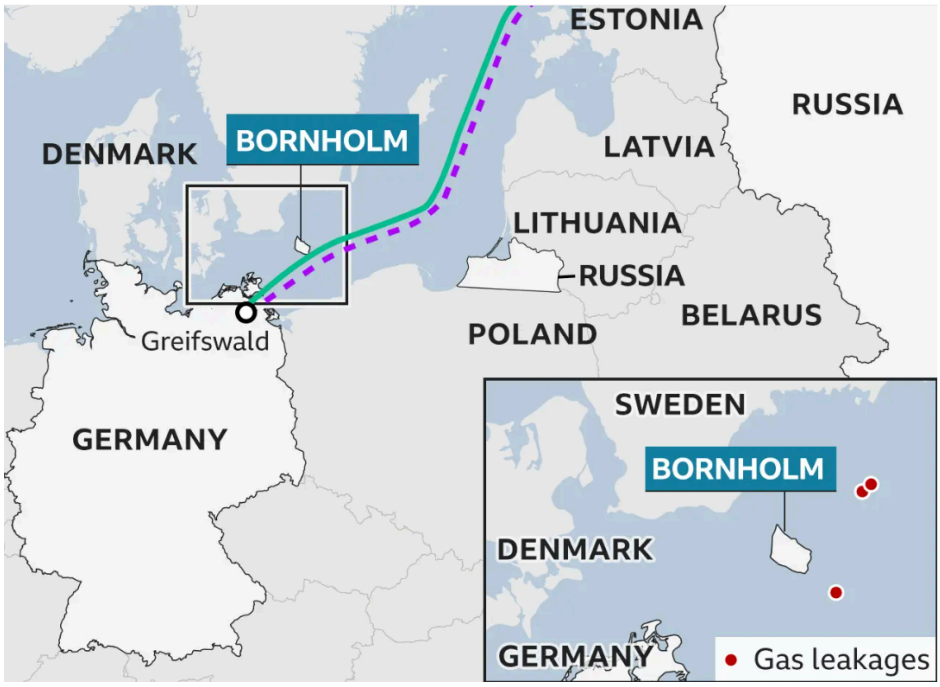
- **Dezinformačné kampane**: Dezinformácie môžu oslabiť dôveru verejnosti v kľúčové služby alebo v reakčné kapacity štátu. Príkladom môže byť šírenie falošných informácií o „nefunkčnosti“ alebo „ohrození“ zdravotníckych služieb či distribúcie potravín.

Takéto útoky môžu viesť k prerušeniu základných služieb, ohrozeniu zdravia a životov obyvateľov, ekonomickým stratám, narušeniu verejného poriadku, zvýšeniu paniky a oslabeniu dôvery verejnosti v štát. **Dôsledky útokov na kritickú infraštruktúru môžu byť súčasťou širšieho strategického zámeru nepriateľského zahraničného aktéra**.

B. Prípady útokov na kritickú infraštruktúru v zahraničí

Útoky na plynovody Nord Stream

Mnohé svetové médiá priniesli 26. septembra 2022 informácie o sérii podmorských výbuchov s následným únikom plynu na troch zo štyroch potrubí plynovodov Nord Stream 1 a Nord Stream 2, ktoré tak boli vyradené z prevádzky. Tieto plynovody, ktoré spájajú Rusko a Európu, mali za úlohu prepravovať zemný plyn z Ruska do Nemecka cez Baltské more a väčšinu v nich vlastnila ruská štátna plynárenská spoločnosť Gazprom. Miesta únikov sa nachádzali v medzinárodných vodách neďaleko ostrova Bornholm, avšak v ekonomických zónach Dánska a Švédska.



Zdroj: BBC, https://www.bbc.com/news/world-europe-63044747

Pred výbuchmi boli potrubia naplnené zemným plynom, no pre okolnosti ruskej agresie na Ukrajine nebol cez ne prepravovaný žiaden plyn. Úniky nastali deň pred otvorením Baltic Pipe, plynovodu medzi Poľskom a Nórskom cez Dánsko, ktorý je alternatívou k dodávkam z Ruska. Rusko žiadalo na pôde OSN medzinárodné vyšetrovanie, no táto žiadosť bola zamietnutá. Samostatné vyšetrovania spustili Dánsko, Nemecko a Švédsko, pričom výbuchy označili za sabotáž. Vo februári 2024 dánske a švédske vyšetrovania ukončili bez určenia vinníka, ale nemecké vyšetrovanie stále pokračovalo. V médiách zverejnené informácie naznačujú, že za sabotážou môžu byť niektorí príslušníci ukrajinských ozbrojených síl, a že akcia bola vykonaná bez súhlasu vedenia Ukrajiny.

Útoky na podmorské káble

Okrem útokov na podmorské potrubia plynovodov, bolo v minulom roku zaznamenané aj významné poškodzovanie podmorských optických a elektrických káblov. Aj v tomto prípade boli postihnuté krajiny EÚ.

Poškodenie dvoch podmorských optických káblov v Baltskom mori v polovici novembra 2024 vyvolalo obavy z možnej sabotáže, ktorú vyšetruje Švédsko ako útok na kritickú infraštruktúru. Jeden z káblov, dlhý 218 kilometrov, spája Litvu so Švédskom, druhý s dĺžkou 1 200 kilometrov, prepája Helsinki s nemeckým Rostockom. Podozrenie padlo na posádku čínskej nákladnej lode Yi Peng 3, ktorá sa plavila v oblasti s vypnutým lokalizačným systémom, a zároveň na Rusko, ktoré už v minulosti vykazovalo podozrivé aktivity v Baltskom mori. Predmetná loď vyplávala 15. novembra z ruského prístavu Usť-Luga pri Petrohrade a po zistení poškodenia káblov ju zadržali švédske úrady. Tie zároveň zaslali do Pekingu oficiálnu žiadosť o spoluprácu pri objasňovaní incidentu. Čína žiadosť na spoluprácu akceptovala. Na zistení príčiny poškodenia podmorských káblov sa podieľa aj Agentúra Európskej únie pre justičnú spoluprácu v trestných veciach (Eurojust). Napriek tomu, že čínska loď odplávala zo švédskych vôd, vyšetrovanie pokračuje. Oba optické káble boli koncom novembra 2024 opravené.

Čínska loď Yi Peng 3, v popredí dánska hliadková loď neďaleko Jutského polostrova. (Zdroj: TASR/AP)

Podobný incident sa stal aj koncom decembra 2024, keď bol **prerušený podmorský elektrický kábel Estlink 2**, ktorý od roku 2014 prepája Estónsko s Fínskom, pričom dotknuté krajiny, nevylučujú zámerný čin. Fínske úrady objavili na mieste poškodenia kábla podozrivú stopu po ťahaní lodnej kotvy dlhú desiatky kilometrov práve v mieste, kde sa pohyboval v tom čase tanker Eagle S. Fínska pobrežná stráž loď plaviacu sa pod vlajkou Cookových ostrovov zadržala a jej posádku, ktorú tvoria občania Gruzínska a Indie, vyšetruje. Fínsko predpokladá, že tanker je súčasťou tzv. ruskej tieňovej flotily. Tú Moskva používa na obchádzanie sankcií, napríklad pri preprave ropy. Kábel bol začiatkom roku 2025 opravený.

Položenie podmorského kábla Estlink 2 významne posilnilo energetické prepojenie regiónu a znížilo závislosť Estónska od ruských dodávok, zatiaľ čo podmorské optické káble prenášajú viac ako 95 % globálnej internetovej prevádzky. Ak by došlo k masívnemu narušeniu tejto infraštruktúry, mohlo by to ochromiť ekonomiku a vyvolať chaos v celej Európe. To si uvedomuje aj NATO, ktoré podniklo v Baltskom mori kroky k ochrane kritickej infraštruktúry.

C. Aký je stav na Slovensku?

Téma ohrozenia kritickej infraštruktúry na Slovensku sa dostala v posledných rokoch do popredia v súvislosti s ruskou inváziou na Ukrajinu. Viaceré incidenty, ktoré sa udiali v zahraničí v súvislosti s útokmi na kritickú infraštruktúru, ukázali aj zraniteľnosti Slovenska v tejto oblasti. Slovensko nie je dostatočne pripravené na intenzívny vývoj v oblasti hrozieb pre kritickú infraštruktúru.

Z hľadiska legislatívy, bol zákon o kritickej infraštruktúre z roku 2011 v kontexte bezpečnostného vývoja posledných rokov už prekonaný, pretože nereflektoval bezpečnostnú realitu posledných rokov. Vývoj bezpečnostnej situácie v Európe a vo svete po roku 2014, kedy Ruská federácia značne zintenzívnila svoje nepriateľské pôsobenie proti členom EÚ a NATO, priniesol zvýšené riziko hybridného pôsobenia na prvky kritickej infraštruktúry. Pôvodný zákon z roku 2011 sa síce zameriaval na prevenciu a ochranu kritickej infraštruktúry hlavne proti terorizmu, nebral však do úvahy riziko hybridného pôsobenia. Hybridné pôsobenie ako hrozba bolo zavedené do zákona o kritickej infraštruktúre platnom od roku 2025, pričom dôvodová správa k novému zákonu označuje hybridné hrozby ako jednu z hlavných hrozieb pre kritickú infraštruktúru na Slovensku. Skutočnosť, že nová legislatíva bola prijatá až v roku 2025 ukazuje, že politická podpora na riešenie tejto problematiky nebola naprieč rôznymi vládami na Slovensku prioritou. K rovnakému záveru dochádza aj správa Najvyššieho kontrolného úradu SR z marca 2024.

Analýza dostupných údajov o kritickej infraštruktúre odhaľuje pretrvávajúce problémy v oblasti financovania, ktoré sa prejavujú nedostatočnými rozpočtovými alokáciami v jednotlivých rezortoch. Podobne aj nový zákon č. 367/2024 Z.z. o kritickej infraštruktúre nepredpokladá žiadne vplyvy na rozpočet verejnej správy, čo indikuje zaužívaný trend o nedostatočnom financovaní tejto problematiky zo strany štátu a nezáujem o rozvoj tejto problematiky.

Ruská invázia na Ukrajinu zvýšila ohrozenie kritickej infraštruktúry

Vo februári 2022, krátko pred začiatkom ruskej invázie na Ukrajine, vydal Národný bezpečnostný úrad (NBÚ) varovanie pre prevádzkovateľov kritickej infraštruktúry vzhľadom na bezpečnostnú situáciu v súvislosti s chystanou inváziou Ruska na Ukrajinu. Podobne v novembri 2024 NBÚ varoval pred zvýšeným rizikom kybernetických útokov v regióne strednej Európy, pričom vydal odporúčania pre prevádzkovateľov základných elektronických služieb v rámci kritickej infraštruktúry na Slovensku, aby dôkladne zabezpečili svoje siete a systémy. NBÚ uviedol, že „pokračujúca vojna na Ukrajine je príznačná nielen devastujúcimi fyzickými útokmi Ruska na infraštruktúru a obyvateľstvo Ukrajiny, ale aj kontinuálnymi kybernetickými útokmi, ako na jej infraštruktúru, tak aj na infraštruktúru členských štátov Európskej únie a NATO.“ Európska agentúra pre bezpečnosť sietí a informácií (ENISA) informuje o 11 079 kyber incidentoch len za rok 2024 v EÚ, SR a sektory kritickej infraštruktúry nevynímajúc.

Kybernetický útok na kataster v roku 2025

V januári 2025 bol informačný systém Úrad geodézie, kartografie a katastra SR zasiahnutý rozsiahlym kybernetickým útokom zo zahraničia. Pracoviská katastrálnych odborov boli

preventívne dočasne zatvorené. Podľa oficiálnych vyjadrení, vlastnícke vzťahy ani databáza katastra neboli zasiahnuté. Situácia si vyžiadala okamžitý zásah krízového štábu a bezpečnostných zložiek. Útok, identifikovaný ako ransomvérový, pravdepodobne zablokoval prístup k systémom a dátam, čím paralyzoval ich využívanie.

V reakcii na tento incident minister vnútra Matúš Šutaj Eštok navrhol prevod zodpovednosti za kybernetickú ochranu kritickej infraštruktúry na Ministerstvo vnútra SR. Tento návrh však poukazuje na možné nedostatočné pochopenie princípov kybernetickej bezpečnosti. Zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti, ktorý komplexne upravuje túto oblasť, stanovuje základné bezpečnostné požiadavky a opatrenia na ochranu informačných, komunikačných a riadiacich systémov. V tejto oblasti má kompetencie Národný bezpečnostný úrad, ktorý koordinuje výkon štátnej správy. Ministerstvo vnútra SR aktuálne nemá potrebné kompetencie, kapacity ani rozpočet na zabezpečenie kybernetickej ochrany kritickej infraštruktúry, čo naznačujú aj vyššie uvedené problémy s financovaním. Presun týchto kompetencií na MV SR by teda mohol byť kontraproduktívny.

Analýzy založené na verejne dostupných dátach poukazujú na problémy katastra, vysvetľujú bezpečnostné medzery, ktoré mohli byť bez väčších problémov zneužité útočníkmi. To nastoľuje otázky kvality vykonaných auditov a implementácie ich záverov a odporúčaní. Podobné zraniteľnosti môžu byť relevantné aj pre iné inštitúcie verejnej správy, kde sú medializované informácie, že IT bezpečnosť bola údajne zverená ľuďom bez potrebnej kvalifikácie a vzdelania. Varovným príkladom je, aj keď nie v oblasti kritickej infraštruktúry, Pôdohospodárska platobná agentúra (PPA), ktorá v minulosti obsadzovala pozície na odbore kybernetickej bezpečnosti ľuďmi bez patričnej kvalifikácie, pričom ochranu kyberbezpečnosti zabezpečoval veterinár a sprievodkyňa. Okrem toho inštitúcia v audite kybernetickej bezpečnosti nedosiahla ani štvrtinu splnených legislatívnych požiadaviek.

Vyhostenie osôb plánujúcich útok na kritickú infraštruktúru

V decembri 2024 Slovensko vyhostilo dve osoby do Maďarska a na Ukrajinu pre podozrenie z prípravy útoku na kritickú infraštruktúru na východe krajiny. Podozriví, medzi ktorými boli cudzinci a slovenský občan, údajne plánovali útoky na energetické zariadenia. Používali drony na monitorovanie objektov, ako sú trafostanica a kompresorová stanica vo Veľkých Kapušanoch, elektráreň Vojany a ďalšie objekty. Pri prehliadkach boli zaistené predmety ako termokamery, balistické vesty a mapy. V reakcii na vyššie uvedený prípad podpredseda NR SR Tibor Gašpar uviedol, že všetky objekty kritickej infraštruktúry na Slovensku budú mať posilnenú ochranu, avšak vláda nezverejnila žiadne ďalšie podrobnosti a podozriví boli prepustení bez obvinenia.

D. Ako štát realizoval opatrenia, ktoré si sám určil?

Nasledovná tabuľka uvádza opatrenia z verejnej verzie hĺbkovej analýzy hybridných hrozieb a ich vyhodnotenie, založené výhradne na informáciách dostupných z otvorených zdrojov.

Zhodnotenie stavu za rok 2024
Opatrenie: Novelizovať Zákon o kritickej infraštruktúre tak, aby odrážal aktuálne bezpečnostné výzvy a trendy v tejto oblasti. **Vyhodnotenie: REALIZOVANÉ** Dňa 27. novembra 2024 NR SR schválila nový Zákon o kritickej infraštruktúre, ktorý transponuje a implementuje právne predpisy EÚ. Zákon nanovo upravuje organizáciu a pôsobnosť orgánov štátnej správy v tejto oblasti. Zákon definuje pri posudzovaní rizika potrebu zohľadniť všetky relevantné prírodné riziká a riziká spôsobené ľudskou činnosťou vrátane hybridných hrozieb. Hybridné hrozby sú v dôvodovej správe k novému zákonu označované za jednu z hlavných bezpečnostných výziev, ktorým Slovensko čelí. Prijatie novej legislatívy tak predstavuje krok správnym smerom, no zároveň k nemu malo dôjsť už v predchádzajúcich rokoch.
Opatrenie: Prevziať odporúčania z Akčného plánu koordinácie boja proti hybridným hrozbám z roku 2022 v oblasti kritickej infraštruktúry, zapracovať problematiku hybridných hrozieb do hodnotení rizík, integrovaných postupov a procesov krízového riadenia a civilnej ochrany. **Vyhodnotenie: NEREALIZOVANÉ** Nový zákon o kritickej infraštruktúre zapracováva hybridné hrozby ako povinnú súčasť hodnotenia rizík. Koncom januára 2024 bol vládou SR schválený “Návrh nového komplexného rámca procesov a postupov pre krízové riadenie Slovenskej republiky”, ktorý predpokladá návrh nového rámca pre riadenie krízových situácii, jeho implementáciu a vytvorenie novej entity podriadenej ministrovi vnútra (Úrad pre riadenie krízových situácii), ktorá bude zodpovedná za celý životný cyklus krízového riadenia v SR. Ani po roku od prijatia tohto návrhu nie je zo strany vlády a MV SR komunikovaný akýkoľvek ďalší postup a jeho implementácia.
Opatrenie: Navýšiť kapacity odborníkov a analytikov v oblasti kritickej infraštruktúry a krízového riadenia naprieč ústrednými orgánmi štátnej správy, zabezpečiť dlhodobú udržateľnosť týchto pozícií.

Vyhodnotenie: NEREALIZOVANÉ

Správa Najvyššieho kontrolného úradu SR z marca 2024 hovorí, že krízové riadenie nebolo reálnou prioritou žiadnej z doterajších vlád, čo spôsobilo jeho úpadok. Podľa správy NKÚ SR sú okresné úrady na odboroch krízového riadenia nedostatočne personálne vybavené na efektívne zvládanie krízových situácií. Z otvorených zdrojov neevidujeme navýšenie počtu zamestnancov v oblasti krízového riadenia.

Nedostatok zamestnancov a rušenie špecializovaných útvarov, ktoré pôsobili v oblasti hybridných hrozieb, bude znamenať nedostatočné budovanie odolnosti a nedostatočný rozvoj spôsobilostí na ochranu kritickej infraštruktúry. Dobrým príkladom je simulácia hybridného pôsobenia z roku 2023, ktorá testovala reakciu na hybridný scenár. Od roku 2023 sa žiadna takáto simulácia neuskutočnila, pričom práve takéto simulácie by sa mali opakovať pravidelne.

E. Ako dosiahnuť pozitívnu zmenu?

Kritická infraštruktúra patrí medzi základné piliere fungovania Slovenska a jej ochrana si vyžaduje zvýšenú pozornosť, kontinuitu a silnú politickú podporu. Nestačí sa zamerať len na technické zabezpečenie jej prvkov, ale aj na posilnenie medzinárodnej spolupráce, pravidelnú aktualizáciu legislatívy a zvýšenie povedomia o jej význame v spoločnosti. Ohrozenia, ako sú kybernetické útoky, extrémne prírodné javy, či hybridné hrozby, môžu mať na kritickú infraštruktúru závažné dopady, a preto je nevyhnutné zabezpečiť jej vysokú odolnosť.

Aby došlo k zvýšeniu odolnosti Slovenska v oblasti kritickej infraštruktúry, štátnej správe dôrazne odporúčame rozpracovať a zaviesť nasledujúce opatrenia:

1. Vyčleniť potrebné financovanie problematiky kritickej infraštruktúry so zameraním na investície do systémov ochrany a prenosu informácií.
2. Zaručiť stabilitu a rozvoj personálnych kapacít prostredníctvom pravidelných školení a náboru nových zamestnancov špecializovaných na ochranu kritickej infraštruktúry.
3. Vykonávať pravidelné cvičenia reakcie štátnej správy SR na simulované hybridné pôsobenie proti kritickej infraštruktúre s účasťou štátnej správy, súkromného sektora a relevantných medzinárodných partnerov.
4. Zabezpečiť, aby z krízového riadenia a ochrany kritickej infraštruktúry bola strategická priorita, ktorá sa nerieši len v reakcii na vzniknuté incidenty, ale najmä prevenciou a budovaním odolnosti.