NATO A KRITICKÁ INFRASTRUKTURA

Proč se ochrana KI stala bezpečnostní prioritou?

Kritická infrastruktura (KI) tvoří základ fungování naší společnosti. Její narušení by ochromilo jak činnost států, tak i běžný život jejich obyvatel.

Kritickou infrastrukturou rozumíme systémy, zařízení a služby, jež jsou pro současnou společnost nezbytné. Patří sem například dodávky elektřiny, vody, doprava, internet nebo zdravotnictví. Pokud by kritická infrastruktura přestala fungovat – ať už vlivem náhodného poškození nebo cíleného útoku – mohlo by to ohrozit bezpečnost lidí, jejich zdraví, zásobování, ekonomiku i činnost státních služeb.

Zatímco před dvaceti lety ohrožovaly kritickou infastrukturu hlavně přírodní katastrofy, dnes čelí cíleným útokům.

Hrozby pro kritickou infrastrukturu

Válka neznamená jen tanky a vojáky. Konflikty se stále častěji vedou i jinými způsoby – pomocí sabotáží, špionáže nebo kyberútoků, které míří na kritickou infrastrukturu. Její nefunkčnost může ochromit činnost bezpečnostních složek, jež tak nejsou schopné reagovat na jiné hrozby, a dotýká se i civilního obyvatelstva. Protivník se tak snaží podkopat morálku společnosti. Nejde ale jen o státy – podobně mohou útočit i teroristické skupiny.

Velkou roli dnes hrají také přírodní vlivy – extrémní počasí, silné bouře, záplavy nebo vlny veder mohou ohrozit elektrárny, nemocnice i komunikační sítě. Další hrozbou může být závislost na technologiích a dodavatelích z nedemokratických států. Ta může vést například k úniku citlivých informací nebo ztrátě přístupu ke klíčovým službám.

Kvůli rostoucím hrozbám začaly NATO a Evropská unie v lednu 2023 spolupracovat na ochraně kritické infrastruktury. Založily společnou pracovní skupinu, která se zaměřuje na čtyři klíčové oblasti: energetiku, dopravu, digitální sítě a vesmír.

Kritická elektřina

V zemích NATO došlo v posledních desetiletích k několika velkým blackoutům, které ukázaly zranitelnost i vzájemnou propojenost energetických sítí. Mezi nejznámější patří italský blackout z roku 2003, kdy kvůli poruše na vedení ze Švýcarska zhasla téměř celá země a 55 milionů lidí se ocitlo bez elektřiny. Podobně rozsáhlý byl i blackout na Pyrenejském poloostrově v roce 2025 způsobený nestabilitou sítě, během něhož skončilo bez proudu 60 milionů lidí.

Ochrana podmořských kabelů

Přes podmořské optické kabely proudí zhruba 95 % celosvětového internetového provozu. Jejich délka, obtížná přístupnost a nízká viditelnost je ale činí zranitelným a potenciálně atraktivním cílem pro státní i nestátní aktéry. Úmyslné poškození může způsobit rozsáhlé výpadky spojení, jejichž opravy by trvaly týdny.

Factbox natoaktual.cz je vydáván Informačním centrem o NATO v Praze jako přehled informací a zdrojů k vybraným tématům.
Není oficiálním vyjádřením NATO ani žádné jiné české nebo zahraniční vládní instituce.
V případě dotazů se neváhejte obrátit na IC NATO na adrese info@natoaktual.cz.

Význam oceánů

Na dně oceánů vedou optické kabely, které přenášejí data mezi kontinenty a tvoří základ globálního internetu. Po celém světě je více než 600 takových kabelů o celkové délce přes 1,48 milionu kilometrů. Zároveň se po moři přepravuje nebo těží více než dvě třetiny světové ropy a zemního plynu.

V červenci 2023 se na summitu NATO ve Vilniusu spojenci dohodli na vytvoření Námořního centra pro bezpečnost podmořské infrastruktury. To spadá pod námořní velení NATO (MARCOM) a má se připravovat na možné útoky a hybridní hrozby pod mořem – například na plynovody nebo internetové kabely. NATO zároveň diverzifikuje způsoby přenosu dat, např. prostřednictvím satelitů.

Operace Baltic Sentry

Historie ukazuje, že „kabelové války" nejsou novinkou – kabely byly sabotovány už během španělsko-americké války (1898) i během první světové války. V posledních letech počet incidentů prudce narostl. V roce 2022 došlo k výbuchům na plynovodech Nord Stream, v roce 2023 byly poškozeny komunikační a elektrické kabely mezi Finskem a Estonskem, přičemž podezření padlo na ruskou stínovou flotilu. Aby tomu NATO předešlo, spustilo operaci Baltic Sentry, která má za cíl lépe chránit podmořskou infrastrukturu, včetně kabelů v Baltském moři. K tomu nasazuje fregaty, námořní hlídková letadla a podvodní drony.

Útoky na plynovod Nord Stream

Nord Stream byl klíčový podmořský plynovod, který přiváděl zemní plyn z Ruska do Německa a dále do Evropy. V roce 2022 došlo k výbuchům a poškození, které byly pravděpodobně výsledkem sabotáže. Tento incident jasně ukázal, jak zranitelná může být podmořská infrastruktura. Útok změnil přístup NATO a Evropské unie k ochraně podmořských zařízení a vyvolal řadu nových opatření.

Ochrana kyberprostoru

Kybernetické útoky mohou narušit provoz nemocnic, elektráren nebo státních úřadů, což může mít vážné důsledky pro národní bezpečnost. Na tyto hrozby se připravuje alianční Centrum kybernetické obrany (CCDCOE) sídlící v estonském Tallinnu, které se zaměřuje na výzkum, výcvik v oblasti kybernetické bezpečnosti.

Locked Shields

Locked Shields je největší a nejkomplexnější mezinárodní cvičení zaměřené na obranu proti kybernetickým útokům. Cvičení simuluje rozsáhlé a realistické kybernetické útoky na klíčovou infrastrukturu – jako jsou elektrárny, nemocnice, letiště nebo státní úřady – a testuje, jak rychle a efektivně jsou týmy schopné reagovat.

Ochrana kritické infrastruktury v ČR

V Česku existuje devět hlavních oblastí kritické infrastruktury, tedy služeb, bez nichž by stát nemohl fungovat: energetika, voda, potraviny a zemědělství, zdravotnictví, doprava, komunikace a IT, finance, nouzové služby a veřejná správa. Pod nouzové služby spadají hasiči, policie, armáda a varovné systémy, které jsou organizované tak, aby fungovaly i během krizových stavů.

Útoky na kritickou infrastrukturu na Ukrajině

Po invazi na Ukrajinu útočí Rusko kromě vojenských cílů i na ukrajinskou kritickou infrastrukturu. Samotnou invazi doprovázela vlna kyberútoků proti státním úřadům či telekomunikačním společnostem. Cílené útoky na teplárny a elektrárny zejména v zimním období pak odstavují řadu regionů od dodávek tepla a elektřiny, čímž trpí zejména civilní obyvatelstvo.

Bibliografie a zdroje k tématu:

- EU-NATO Task Force. Final Assessment Report: On the Resilience of Critical Infrastructure. Brussels: European Commission / NATO, June 2023. https://commission.europa.eu/system/files/2023-06/EU-NATO_Final%20Assessment%20Report%20Digital.pdf
- Cybersecurity and Infrastructure Security Agency. "Critical Infrastructure Sectors." CISA.7. 12. 2025. https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors
- IBM. "What Is Critical Infrastructure?" IBM,7. 12.2025. https://www.ibm.com/think/topics/critical-infrastructure
- Monaghan, Sean, Otto Svendsen, Michael Darrah, and Ed Arnold. 2024. "NATO's Role in Protecting Critical Undersea Infrastructure." CSIS. 19. 12. 2024. https://www.csis.org/analysis/natos-role-protecting-critical-undersea-infrastructure
- NATO. 2024. "Resilience, civil preparedness and Article 3." NATO. 13. 11. 2024. https://www.nato.int/cps/en/natohq/topics_132722.htm
- Ortmann, Matyáš. 2025. "Ochrana kritické infrastruktury v digitální éře: Role NATO a strategie České republiky." CZDEFENCE. 13. 7. 2025. https://www.czdefence.cz/clanek/ochrana-kriticke-infrastruktury-v-digitalni-ere-role-nato-a-strategie-ceske-republiky
- Václavíková, Jana. 2025. "Podmořské kabely neumíme chránit. Počet útoků ukazuje, že bezpečnostní hrozba narůstá, říká expert." IRozhlas. 7. 3. 2025. https://www.irozhlas.cz/zpravy-svet/podmorske-kabely-neumime-chranit-pocet-utoku-ukazuje-ze-bezpecnostni-hrozba_2503070700_jva

Bibliografická citace: natoaktual.cz (2025): NATO a kritická infrastruktura od náhodných výpadků k bezpečnostní prioritě. Factbox natoaktual.cz. 1. vydání, prosinec 2025.