

KYBERBEZPEČNOST A NATO

Jak Severoatlantická aliance chrání svůj kyberprostor



Alianční cvičení Steadfast Jupiter-Jackal, prosinec 2020.

Zdroj: NATO Communications and Information Agency

Kyberútoky představují rostoucí riziko nejen pro zajištění obrany a bezpečnosti členských zemí NATO, ale i pro celkové fungování společnosti a ekonomiky. Kybernetický útok může mít ničivější dopady než ten konvenční a je zároveň méně nákladný a rychleji proveditelný. Kyberútok na jednu zemi se navíc může snadno rozšířit a postihnout i další spojence. Na druhou stranu kyberprostor a informační technologie dnes zajišťují funkčnost velké části ozbrojených sil a propojují všechny oblasti boje.

Severoatlantická aliance proto zařadila kyberprostor mezi „operační domény“ a [rozvoj schopností na kyberobranu](#) tak nyní považuje za stejně důležitý krok jako obranu na zemi, na moři, ve vzduchu a blízkém vesmíru. Členské

země se zavázaly prioritně posilovat bezpečnost svých národních sítí a navyšovat odolnost proti kybernetickým útokům (tzv. [Cyber Defence Pledge](#) z roku 2016). Z hlediska bezpečnosti je významné, že se na kyberútoky [vztahuje článek 5](#) Washingtonské smlouvy – čili útok na jednoho spojence může být považován za útok na celou Alianci.

Role NATO na poli kyberobran

1) Ochrana aliančních sítí proti útokům

Na síťovou infrastrukturu NATO spoléhají desetitisíce osob na více jak [60 různých lokacích](#) – nejen v centrále Aliance v Bruselu, ale například i na aliančních velitelstvích v Evropě a USA či všude tam, kde probíhají operace NATO. Alianční systémy čelí [až stovkám útoků měsíčně](#). Od pokusů napadení na nízké úrovni, až po technologicky propracované útoky. Většina z nich je zaznamenána a řešena automaticky, některé ovšem vyžadují analýzu a reakci expertního týmu.

2) Jak NATO pomáhá členským zemím?

- » podporou sdílení informací o hrozbách v reálném čase, včetně výměny osvědčených postupů
- » NATO disponuje týmy kybernetické obrany (*NATO Cyber Rapid Reaction teams*), které mohou rychle pomoci spojencům při řešení kybernetických útoků
- » sestavováním cílů pro rozvoj kyberschopností členských zemí, což usnadňuje celoalianční spolupráci a další rozvoj schopností (př. prostřednictvím tzv. *NATO Defence Planning Process*)
- » podporou vzdělávání a školení (např. prostřednictvím aliančních škol v Německu, Portugalsku a Itálii), plus organizací cvičení (např. každoroční mezinárodní cvičení [Cyber Coalition](#)), které spojencům umožňují zlepšovat jejich schopnosti

Bezpečnost a obrana kyberprostoru

Trend digitalizace či robotizace život v mnohém usnadňuje, zároveň však přináší nová rizika i hrozby. Závislost společnosti na digitálních informačních systémech se stále zvyšuje a kybernetické útoky se zároveň stávají běžnějšími, sofistikovanějšími a závažnějšími. Přitom narušení komunikace či zneužití dat může ovlivnit procesy rozhodování a následně ohrozit například život nebo majetek obyvatel či dokonce států. Ochrana informačních systémů před zneužitím, ať už softwarovým či hardwarovým, nebo odcizením informací v těchto systémech uložených, je proto klíčem k zajištění bezpečnosti v kyberprostoru. **Zajištěním bezpečnosti a obrany v kyberprostoru, tedy ochranou informací, systémů a infrastruktury, se proto stále intenzivněji zabývají jak odborné instituce, tak na nejvyšší úrovni i vlády a Severoatlantická aliance.**

Hlavní nástroje kyberobrany pod hlavičkou NATO

Alianční politiku v oblasti kybernetické obrany provádějí politické, vojenské a technické orgány NATO, pro své operace může ale využívat i národní kybernetické capacity.

Celkový politický dohled na nejvyšší úrovni poskytuje Severoatlantická rada, jejím specializovaným poradním orgánem ve věcech kybernetické obrany je **Výbor pro kybernetickou obranu** (*Cyber Defence Committee – CDC*).

- » **Rada pro řízení kybernetické obrany** (*Cyber Defence Management Board – CDMB*) koordinuje kybernetickou obranu na pracovní úrovni. Skládá se ze zástupců všech hlavních těles v oblasti kybernetické bezpečnosti v rámci NATO. CDMB mimo jiné podepisuje s členskými státy i tzv. Memoranda o porozumění s cílem usnadnit výměnu informací, vylepšit prevenci incidentů a koordinaci případné pomoci.
- » **NATO Computer Incident Response Capability** (NCRIC) je skupina dvou set expertů v belgickém Monsu s úkolem zajišťovat ochranu sítí NATO a poskytovat členským státům a spojencům aktuální informace a analýzu kybernetických výzev.
- » **NATO Cyberspace Operations Centre** je připravované operační středisko, které bude od roku 2023 posilovat kyberobranu NATO a poskytovat vojenskému velení informace na podporu aliančních operací a misí. Centrum by také mělo koordinovat operační činnost NATO v kyberprostoru a zvyšovat odolnost operací vůči kybernetickým hrozbám.
- » **Centrum excellence NATO pro kybernetickou obranu (CCDCOE)** v Estonsku, jež se po [zkušnostech s kyberútoky v roce 2007](#) dnes profiluje jako alianční lídr v oblasti kybernetické bezpečnosti. Centrum realizuje výzkumné, vzdělávací či konzultační aktivity. Jeho základem jsou experti z 29 států, připojeny jsou i některé nečlenské státy, př. [Japonsko](#). Jelikož [centra excellence](#) nejsou součástí alianční struktury velení, nemají mandát k operacím a účast nealiančních států např. na kybercvičeních je proto bezproblémová.



Příklady kyberútoků

Kybernetické útoky sledují různé cíle, od vojenských (např. útoky na celé země), přes kriminální (např. krádeže) až po ekonomické (např. kyberšpionáž) a jiné, často se vzájemně překrývající. Mohou mít závažný dopad i na každodenní život (např. ochromení státní správy v Estonsku v r. 2007, vyrazení dodávek elektřiny pro statisíce obyvatel na Ukrajině v letech [2015](#) a 2016), nebo cílené na specifické schopnosti (poškození iránského jaderného programu malwarem Stuxnet kolem roku 2010).

Útoků není ušetřena ani ČR, zdejší orgány řešily jen [v roce 2019 přes dvě stě útoků](#) na instituce i firmy. Životu nebezpečné mohou být útoky na počítačové sítě zdravotnických zařízení, zvláště v době pandemie, které NATO [odsoudilo](#) (v ČR viz příklad nemocnic v [Benešově](#) a [Brně](#)).

Česká republika

Česká republika se ochraně kyberprostoru intenzivně věnuje jak v civilní, tak vojenské rovině. Klíčovým dokumentem je [zákon o kybernetické bezpečnosti](#). Hlavními aktéry jsou:

- » **Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB)**, ústřední orgán mající na starost kybernetickou bezpečnost a dohled (jde například o ochranu kritické infrastruktury a orgánů veřejné správy)
- » **Vojenské zpravodajství (VZ)**, které zajišťuje kybernetickou obranu ČR a za tím účelem zřizuje *Národní centrum kybernetických operací (NCKO)*
- » **Velitelství kybernetických sil a informačních operací (VeKySIO)** Armády ČR má společně s VZ na starost obranu a vedení vojenských kybernetických operací; v přípravě je také novela kybernetického zákona, jež by [vojákům umožnila na útočníka udeřit](#)
- » **Národní centrála proti organizovanému zločinu**, která má na starosti kriminalitu, zřídila speciální *Sekci kybernetické kriminality*

ČR: strmý růst

Zatímco v posledních osmi letech obecná kriminalita klesla o více než 40 %, ta v kyberprostoru [narostla o neuvěřitelných 460 %](#). Sekce kybernetické kriminality Národní centrály proti organizovanému zločinu tak v roce 2019 řešila 8417 trestných činů z oblasti kyberkriminality.

Bibliografie a zdroje k tématu:

- » Národní úřad pro kybernetickou a informační bezpečnost (<https://www.nukib.cz/cs/>) a jeho bezpečnostní doporučení (<https://www.nukib.cz/cs/infoservis/doporuceni/>)
- » North Atlantic Treaty Organization (2020): Cyber defence. Nato.int, 25. 9. 2020. (https://www.nato.int/cps/en/natohq/topics_78170.htm)
- » North Atlantic Treaty Organization (2020): NATO Cyber Defence Factsheet. (https://www.nato.int/nato_static_fl2014/assets/pdf/2020/8/pdf/2008-factsheet-cyber-defence-en.pdf)
- » Fertasi, Nadja El – De Vivo, Diana (2016): Cyber resilience: protecting NATO's nervous system. NATO Review. (<http://www.nato.int/docu/review/2016/Also-in-2016/nato-cyber-resilience-security/EN/index.htm>)
- » Zaharia, Andra (2020): 300+ Terrifying Cybercrime and Cybersecurity Statistics & Trends. Comparitech.com, 29. 7. 2020. (https://www.comparitech.com/vpn/cybersecurity-cyber-crime-statistics-facts-trends/#Cost_of_cybercrime_stats)