# Kybernetická obrana, kybernetické útoky jako součást hybridní války a shrnutí předmětu a analýza aktuálních událostí a trendů

**Ing. Dušan Navrátil**

# Kybernetická obrana

**Kybernetická obrana je ochrana státu proti pokročilým závažným a nepřátelským kybernetickým útokům. Reaktivní část kybernetické obrany přichází na řadu ve chvíli, kdy útok byl úspěšný a je potřeba ho odrazit nebo vyvinout takové aktivity, aby bylo útoku předejito. Smyslem je aktivní působení v kybernetickém prostoru proti útočícím entitám a proti infrastruktuře používané k útokům. Důležitá je role odstrašení.**

**V Kybernetické obraně sehrávají rozhodující roli vojenské složky:**

- **Chránit a zabezpečit své informace, systémy a sítě.**
- **Přizpůsobit plánování, organizaci, výcvik a vybavení vojenských sil současným „cyber“ výzvám.**
- **Disponovat útočnými kybernetickými schopnostmi.**
- **Bránit stát před závažnými kybernetickými útoky.**
- **Sbírat informace (jakéhokoli typu) o závažných kybernetických hrozbách.**

# Kybernetická obrana

- **Kybernetický prostor byl vyhlášen jako 5. doména na Varšavském sumitu NATO (červen 2016). Ve 4 tradičních doménách konfliktu je hranice a limity jasně dané, v kybernetického prostoru však veškeré hranice absentují a limity jsou nejasné. Kybernetický prostor a ICT dnes propojují všechny oblasti boje, zajišťují její funkčnost, a zároveň jsou na něm i kriticky závislé.**

- **Na Varšavském sumitu NATO byl přijat Závazek ke kybernetické obraně, jehož úkolem je posílit národní schopnosti kybernetické obranya podpořit spolupráci mezi spojenci v této oblasti. Hlavní odpovědnost leží na národní úrovni, NATO hraje podpůrnou roli. (v ČR vzniklo Velitelství kybernetických sil a informačních operací a Vojenské zpravodajství plní některé role v kybernetické obraně)**

- **Byly vytvořeny kybernetické síly rychlého nasazení NATO. Jsou do 24 hodin být schopny nasazení na žádost státu NATO. V případě nasazení v nečlenské zemi musí to odsouhlasit Severoatlantická rada.**

# Kybernetická obrana

- **Kybernetické útoky jsou v aliančním chápání klíčovým prvkem hybridního spektra.**
- **Cvičení NATO Cyber Coalition  a Locked Shields.**
- **V případě ofenzivních kybernetických schopností NATO spoléhá na národní kapacity, které technologicky nejvyspělejší spojenci dávají dobrovolně k dispozici.**
- **Dle závěrů NATO na sumitu ve Walesu (2014) mohou kybernetické útoky nově aktivovat článek 5 Washingtonské smlouvy o kolektivní obraně.**

# Kybernetická obrana

**Otázka mírového a válečného stavu.**

**Možnost provádět informační operace v kyberprostoru – schopnost operovat proti geograficky vzdáleným cílům bez nasazení fyzických prostředků – zmenšuje se možnost prozrazení a přisouzení útoku a tím cílení možného protiútoku – možnost útoku na fyzickou infrastrukturu – její narušení či zničení – to vše pod hranicí ozbrojeného útoku.**

**Ofenzivní operace (aktivita) v kyberprostoru – manipulace, odepření, přerušení, degradace nebo zničení infrastruktury, informačních a komunikačních systému sítí a prostředků – cílem jsou jak vojenské tak i civilní infrastruktura státu.**

**Odstrašení- „Pokud chceš mír připravuj se na válku!“**

# Hybridní válka

**Hybridní, alternativní či nelineární válka je druh ozbrojeného konfliktu vedeného útočníkem za kombinace konvenčních a nekonvenčních prostředků se synergie efektem (hybridní hrozby), přičemž hlavní roli hrají nevojenské nástroje. Mezi ně patří např. psychologické operace, informační válka a propaganda, kybernetické útoky, kriminální a teroristické aktivity, ekonomické sankce a další. Vojenské akce útočníka probíhají nepřiznaně, jsou vedeny především nepravidelnými silami a kombinují symetrické a asymetrické způsoby vedení bojových akcí proti celé cílové společnosti.**

**Hybridní hrozbu lze definovat jako „různorodou a dynamickou kombinaci pravidelných sil, neregulérních sil, kriminálních živlů nebo kombinace těchto sil a prvků sjednocených za účelem dosažení vzájemně prospěšného výsledku.**

**Hybridní hrozby jsou metody a činnosti zaměřené na zranitelná místa soupeře, kde je rozsah metod a činností široký.**