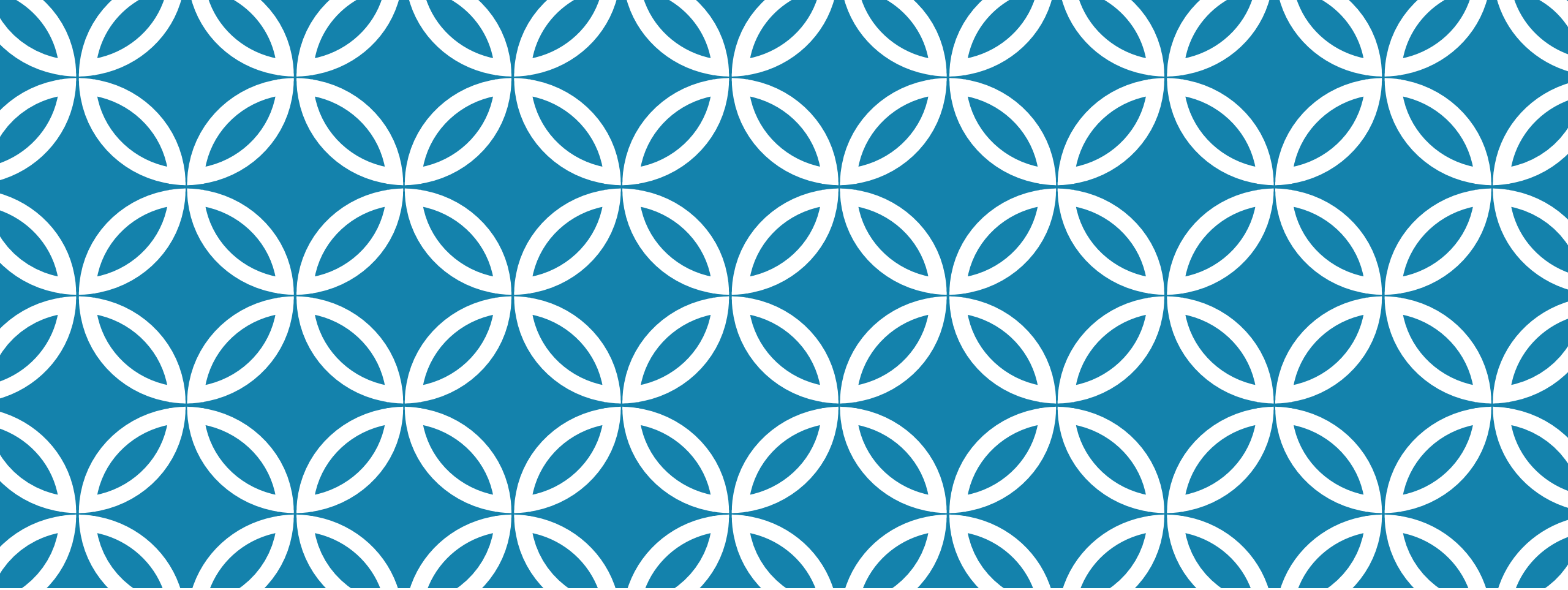
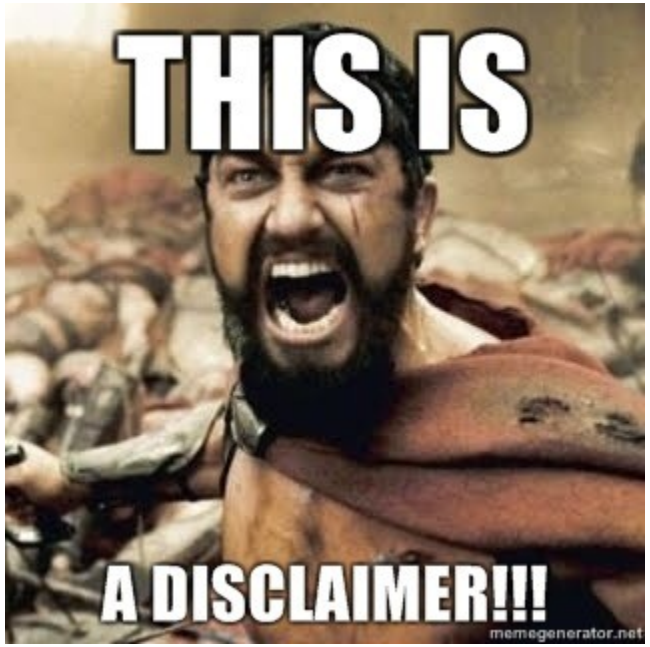


# TBN, IOBT, UA




Názory prezentované v této přednášce jsou výhradně názory autora, a nemusí tak nutně reprezentovat stanoviska a názory SkKySIO, potažmo VeX.

# OBSAH

Co jsou bojové sítě;

Co je IoBT;

Kybernetická bezpečnost bojových sítí;

Doktrína RF;

Cyber & UA;

Q&A;

# TYPOLOGIE SÍTÍ (SEGMENTŮ) V ARMÁDÁCH

Podle typu uživatelů, které do nich pouštíme (zóny)?;

Podle (ne)směrování do internetu?;

Podle stupně utajení – jaký typ informací na IKT zpracovávám a jaké přes síť posílám?;

- Zákon 412/2005 Sb.
- TLP;
- TEMPEST;

Podle typu činnosti?

- C2 x boj;

Podle stálosti?;

- Stacionární sítě;
- Mobilní/polní sítě;

# BOJOVÉ SÍTĚ

Armády/vojáci využívají bojové sítě k tomu, aby:

a) detekovali, co se děje na bojišti;
b) zpracovali získaná data do informací, na základě kterých lze jednat (actionable intell);
c) na základě těchto informací se rozhodli o tom, co budou dělat (course of action);
d) toto rozhodnutí komunikovali napříč jednotkami;
e) provedli dané jednání;
f) zhodnotili ho.

Koncept bojových sítí není novinka, byl tu vždy;

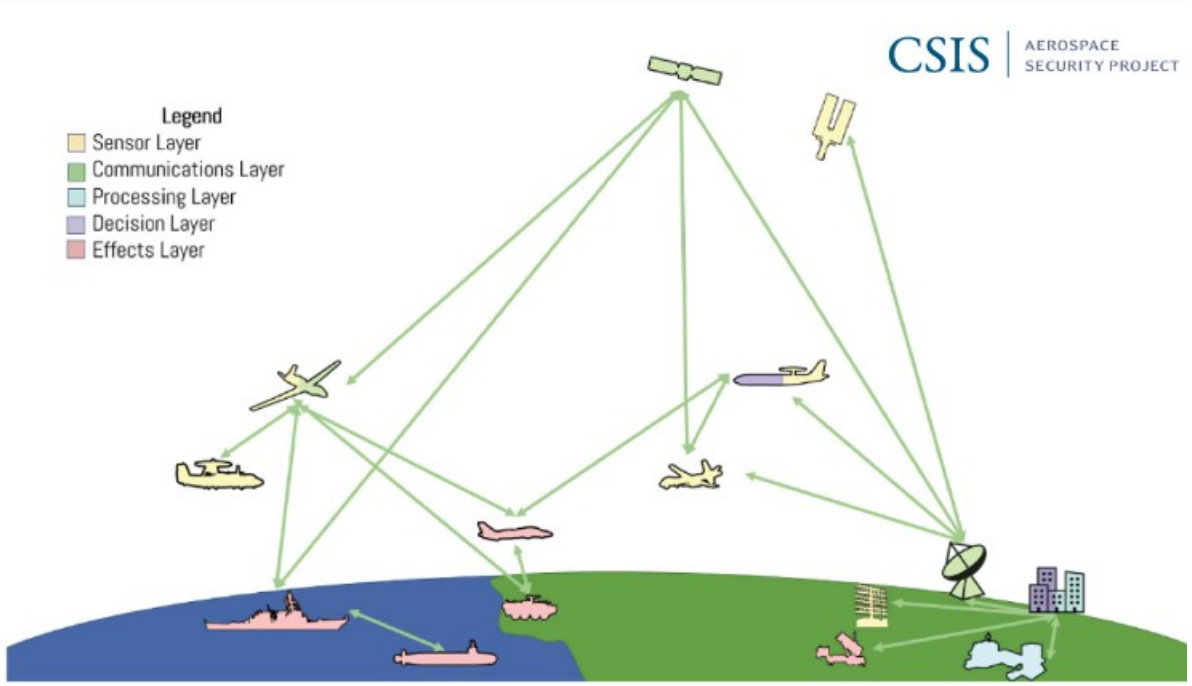
# BOJOVÉ SÍTĚ – CO TO JE

Formální definice: „soubor vzájemně propojených KIS, které podporují bojové operace na taktické úrovni“

Pracovní definice: „různé počítače na bojišti, které sbírají, zpracovávají, vyhodnocují, přeposílají, zobrazují nebo ukládají data“

Sběr, zpracování a přenos informací near real-time → situační povědomí, koordinace, rozhodování;

- Rychlejší OODA → výhra? X information overload;



# VRSTVY BOJOVÉ SÍTĚ

Senzorická – sběr dat o dění na bojišti prostřednictvím senzorů;

Komunikační – datové linky přeposílající data napříč KIS (operátory);

Vrstva zpracování – analýza, agregace, syntéza dat („on-prem“, cloud)

Rozhodovací;

- Human in the loop;
- Human on the loop (semi-autonomní);
- Human outside the loop (plná autonomie);

Vrstva efektů

- kinetické (rakety) X nekinetické (cyber, ebáci);
- letální X neletální

# IOBT

IoT: Věc s vestavěnými senzory, HW&SW a síťovou konektivitou, což jim umožňuje sbírat a sdílet data

IoBT = IoT na bojišti

https://www.youtube.com/watch?v=AwTokY2xXQw&ab_channel=Ansys

https://internetofdon.gs/reports/

# IOBT

Wearables na gumách – smartwatch, IP kamery;

Síťová infrastruktura;

Všechno spadající do kategorie bezosádkové - UAVs, UGVs, UUVs atp.;

C4ISTAR komponenty – tablety, smartphones;

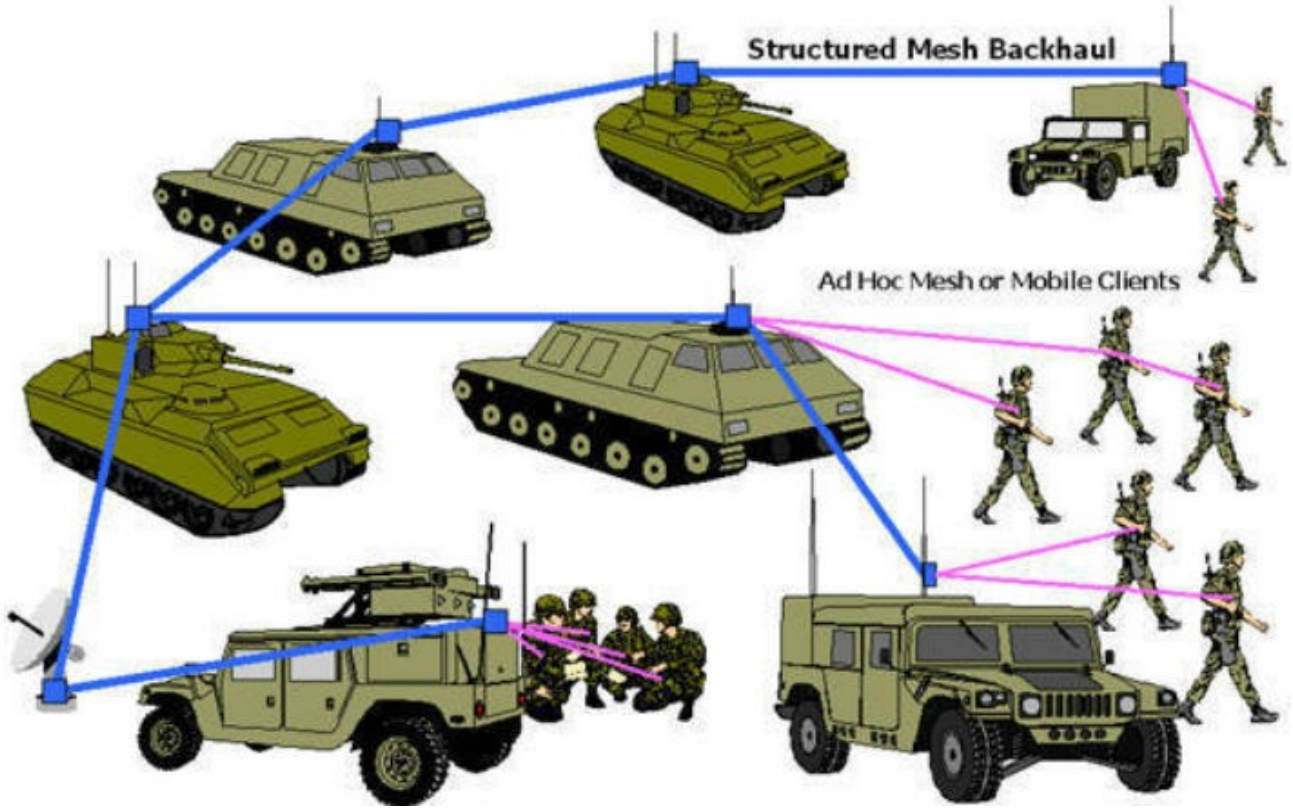
Satelity;

Zbraňové platformy – vrtáky, stíhací letouny, tanky, BVP atp.

# VSUVKA MANET / FANET

Mobile Ad Hoc Network / FIying Ad Hoc Network;

= P2P síť



# BUDOUCÍ TBNS

Vyšší konektivita

- Pro větší bojovou efektivitu můžeme (budete muset?) začít propojovat i systémy, které byly předtím odděleny;

Více zařízení (viz IoBT část)

Typově „nové“ systémy a služby

- Plně či semi autonomní systémy;
- Swarmy;
- Machine & deep learning;
- Cloud;

# PROBLÉMY A VÝZVY TBN

Integrace sítí;

Bandwidth;

Škálovatelnost a elasticita;

Visibility;

Heterogenita zařízení;

Počty zařízení na bojišti (IKT);

Kybernetická bezpečnost;

# KYBERNETICKÉ HROZBY

TBN a IoBT jako „bojiště v bojišti“

I – protivník mi diktuje informace (data);

A – protivník mi může odepřít přístup k mým informacím (datům), službám, systémům;

C – protivník zná moje informace (data);

# VEKTORY ÚTOKU NA TBN

Supply Chain – HW, SW;

Navázané sítě a systémy;

Přenosná média (old but gold);

IoBT;

# CYBER ASPEKT

Kybernetická bezpečnost hraje druhou kolej;

Samotná aplikace bezpečnostních opatření představuje v TBN rizika;

- Sepnutí EDR pravidla kvůli black boxu; vytěžování bandwidth;

Nepřenositelnost standardních enterprise bezpečnostních opatření;

- Autentizace?
- Autorizace?
- Accounting?

Obtížnost napadení sítě → ROSI?

# Q&A TIME

Dotazy k předchozí části?

# RF – DOKTRINÁLNÍ UKOTVENÍ

Informačně-kinetické operace

Informačně-technické operace

Informačně-psychologické operace

Holistický přístup – kombinace operací pro dosažení požadovaného efektu (imho v konečném důsledku na „duševní síly protivníka“ – morál bojovat).

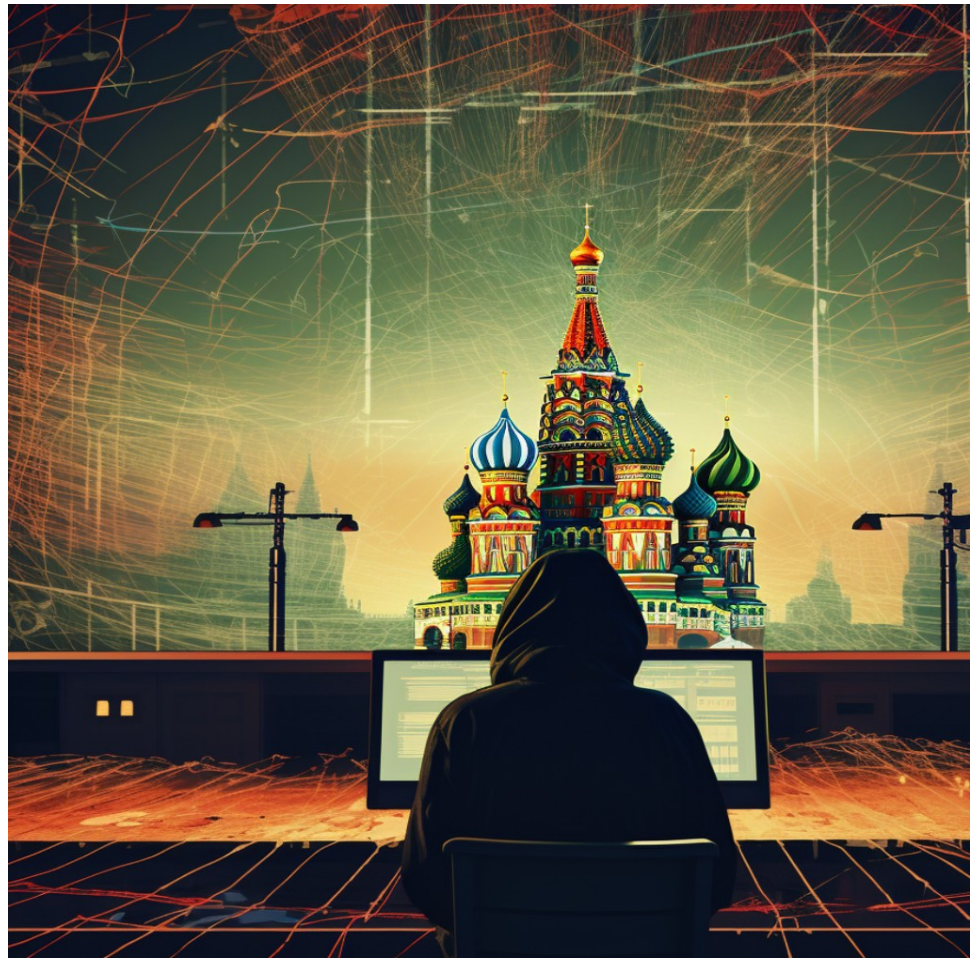
# 5TH DOMAIN – RUSKÉ AKCE

Přípravná fáze (březen 2021 – 23. únor 2022)

Počátek invaze (24. únor – duben 2022 )

Donbass (Duben – červenec)

UA counter offensive (srpen – listopad)



# 5TH – UA COUNTERMEASURES

Dohnání základů a následování best practise

- Jak státní instituce pracují za normálního stavu X krizového stavu;

Odborná pomoc Západu

- Vojenská pomoc
- Nevojenská pomoc – Microsoft, ESET, Google aj.

Přesun dat/databází do cloudu (nadto do zahraniční jurisdikce);

Dobrá kombinace zelené a cyber (OPSEC);

Legislativní změny – umožňující zapojení soukromého a veřejného sektoru do DCO;

# 5TH DOMAIN - MILITARY

Nezaznamenány výraznější útoky na polní sítě / DoD infrastrukturu

- Doktrinální myšlení?
  - Útok na dual use/civilní infastrukturu má potenciálně větší dopad na ozbrojený konflikt?
    - Narušení KI (finance, zdrav, energie, potraviny) →podlomíte vůli fyzické základny vzdorovat
- Doktrinální myšlení + strategie?
  - shock and awe + OCO na KI → Effect Base Operations
- Výnosnost?
  - Vyplatí se v současnosti útočit na polní sítě? (náklady X efekt)
  - Není lepší útočit na KI + ICS (OT)?

# 5TH DOMAIN & STRATEGIC IMPLICATIONS

RF se zaměřila na širší fyzickou základnu státu (širokou společnost) jako center of gravity → realizace efektů byla odepřena → fungovalo by to?

- Strategické bombardování WW2?

Diletantismus v OPSECU RF

- Mobily a vyzařování → umřeš rychle
- Potřeba počítat s chováním vojáků jako „uživatelů“

RF a podkopání konceptu vlivových/IO/PSYOPS?

- Když RF něco popře/přizná, je to pravý opak → to nechceš

# 5TH DOMAIN & STRATEGIC IMPLICATIONS

Špatná volba  zelené strategie kampaně → 5. to schytá stejně jako ostatní domény;

Problém OCO v rozjeté kampani; - intell sup, rozhodování velitelů;

Proxy / haktivismus jako aktér v konfliktu;

Targetting – dual-use: SCADA/OT/ICS?

Balancování akce a přístupů (event/effect based vs presence based ops)

Network access;

Ressiliance > cybersecurity

# Q&A

Bylo všechno jasné?

Pokud by byly dotazy k této anebo k předchozí přednášce a jste introverti a nemáte rádi lidi (jako já) a nechcete se ptát před zbytkem genpop → afterclass debrief, mail

# ZDROJE


Harrison, Todd. (2021, August 5). Battle Networks and the Future Force. Csis.org (https://www.csis.org/analysis/battle-networks-and-future-force).

Scharre, Paul. (2018). Army of None: autonomous weapons and the future of war. New York: W.W. Norton & Company.

Halpin, Edward et al. (2006). Cyberwar, netwar, and the revolution in military affairs. New York: Palgrave Macmillan.

Black, Dan. (2023). Russia‘s War in Ukraine: Examining the Success of Ukrainian Cyber Defences.

# POVINNÁ LITERATURA

Black, Dan. (2023). Russia‘s War in Ukraine: Examining the Success of Ukrainian Cyber Defences.

Harrison, Todd. (2021, August 5). Battle Networks and the Future Force. Csis.org (https://www.csis.org/analysis/battle-networks-and-future-force).

Voo, Julia. (2023). Lessons from Ukraine‘s Cyber Defense and Implications for Future Conflict. In: Evolving Cyber Operations and Capabilities. James Lewis and Georgia Wood (Eds.). Center for Strategic and International Studies, pp. 15-23 (https://www.csis.org/analysis/evolving-cyber-operations-and-capabilities)