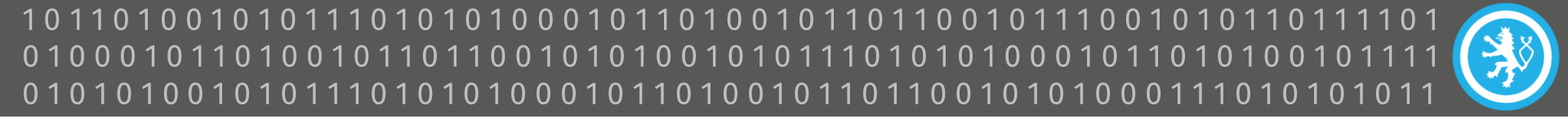
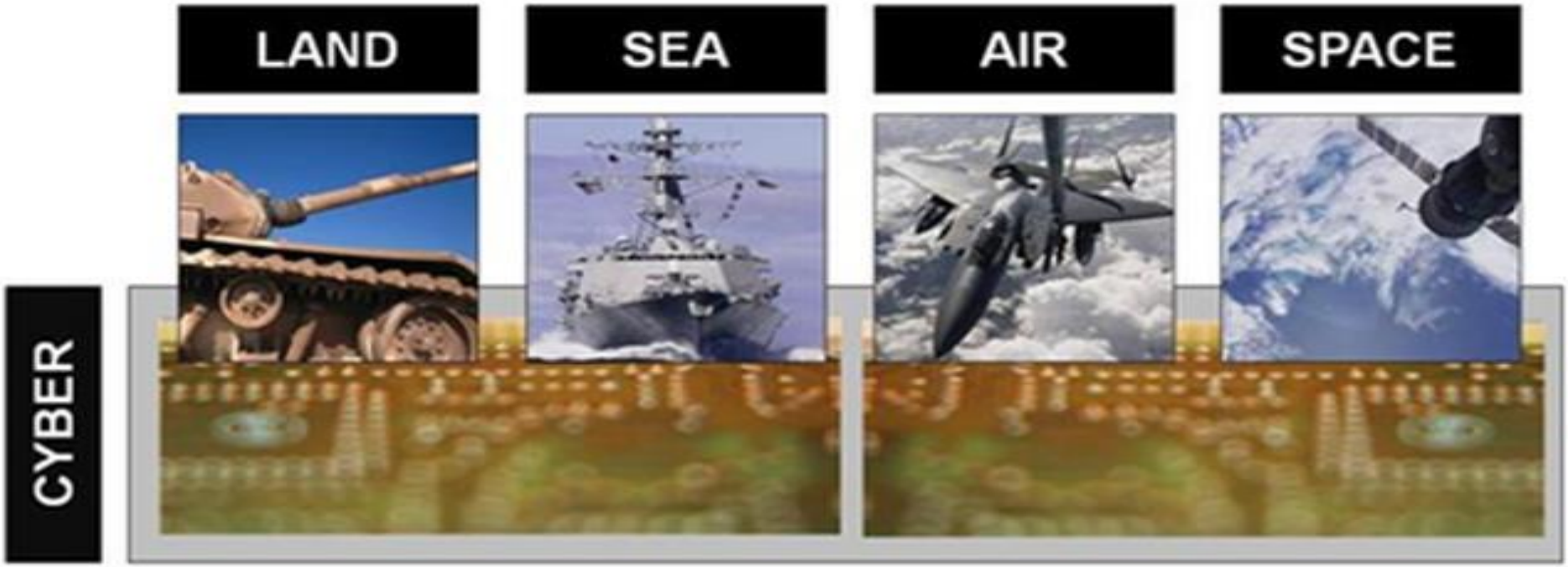


Kybernetická obrana

Národní úřad
pro kybernetickou
a informační bezpečnost

NATO 3.0

- 2002 – Praha: zahrnuta „CYBER“ problematika do NATO agendy
- 2007 – útoky na Estonsko
- 2008 – Bukurešť: větší apel na cyber security/defense klíčových systémů + Rapid Reaction Teams
- 2010 – Lisabon: integrována kybernetická obrana plánování a vytvořena samostatná politika kybernetické obrany NATO
- 2014 – Wales: článek 5
- 2016 – Varšava: kyberprostor novou operační doménou


LAND
SEA
AIR
SPACE
CYBER

Article 3

In order more effectively to achieve the objectives of this Treaty, the Parties, separately and jointly, by means of continuous and effective self-help and mutual aid, will maintain and develop their individual and collective capacity to resist armed attack.

Souhrn úkolů vyplývajících z dokumentů NATO a EU

- zodpovědnost za vlastní sítě,
- odolnost a bezpečnost informací,
- sdílení informací, vzdělávání,
- spolupráce s průmyslem a akademickou sférou,
- začlenění Cyber Defence do plánování a vedení operací,
- začlenění Cyber Defence do vojenských cvičení,
- jasná struktura velení a řízení v kybernetické oblasti,
- schopnost tvorby společného obrazu o stavu vlastních sítí a kybernetického prostoru.

Kyberprostor a jeho specifika

- Clausewitz X neustále se měnící prostředí
- Digitální bitvu nelze vyhrát analogovými nástroji a myšlením

Výhody	Nevýhody
Nové technologie zvyšují obranné schopnosti a kapacity	Obsahují nové zranitelnosti a hrozby (stejné jako v civilním sektoru)
Vzrůstající konektivita zvyšuje efektivitu	Bez obranných/útočných schopností je stát úměrně zranitelný

Kyberprostor a jeho specifika

- Hans Guderian – Blitzkrieg
- Redefinoval Armored warfare
  - Použití nekonvenčním způsobem
  - Důležitý je způsob jak technologie militarizujeme
- Receptem na úspěch není čekání na nějakou revoluční technologii
- Nutnost oproštění se od tradičního myšlení

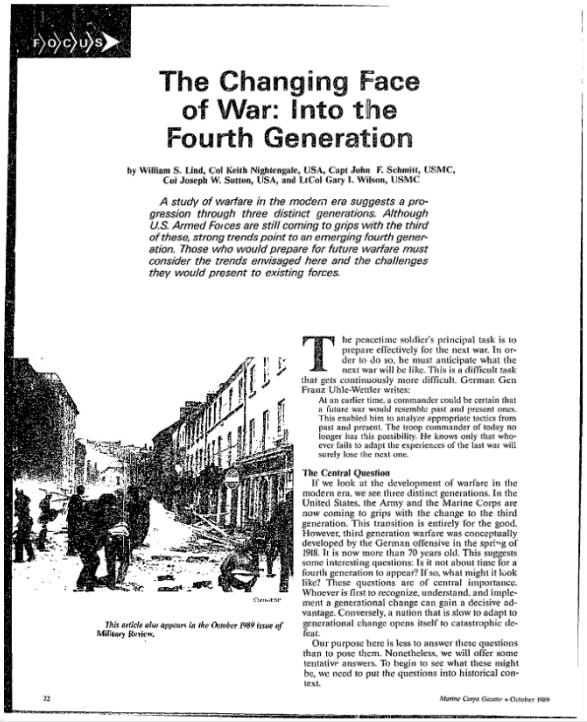
- = problém voj. složek vyrovnat se kyberprostorem jako takovým

Čtyři generace bojiště:

1. Vzestup národních států, top-down vojenská struktura, limitované zbraně, armády složené z nevolníků, vrcholem Napoleonské války
2. Konec 19. století, zahrnuta artilerie, kulomety, lepší logistika, vývoj zbraní hromadného ničení, vrcholem 1WW
3. Německo za 2WW – blietzkrieg doktrína / shock-maneuver taktita
4. 1989 – The Changing Face of War: Into the Fourth Generation (Marine Corps Gazette)

Whole of the enemy's society… distinction between civilian and military disappear… TV news may become a more powerful operational weapon than armored division…

…here comes the CYBER warfare



FOCUS

The Changing Face of War: Into the Fourth Generation

by William S. Lind, Col Keith Nightengale, USA, Capt John F. Schmitt, USMC, Col Joseph W. Sutton, USA, and LtCol Gary I. Wilson, USMC

A study of warfare in the modern era suggests a progression through three distinct generations. Although U.S. Armed Forces are still coming to grips with the third of these, strong trends point to an emerging fourth generation. Those who would prepare for future warfare must consider the trends envisaged here and the challenges they would present to existing forces.

The peacetime soldier's principal task is to prepare effectively for the next war. In order to do so, he must anticipate what the next war will be like. This is a difficult task that gets continuously more difficult. German Gen Franz Uhle-Wettler writes:

At an earlier time, a commander could be certain that a future war would resemble past and present ones. This enabled him to analyze appropriate tactics from past and present. The troop commander of today no longer has this possibility. He knows only that whoever fails to adapt the experiences of the last war will surely lose the next one.

The Central Question

If we look at the development of warfare in the modern era, we see three distinct generations. In the United States, the Army and the Marine Corps are now coming to grips with the change to the third generation. This transition is entirely for the good. However, third generation warfare was conceptually developed by the German offensive in the spring of 1918. It is now more than 70 years old. This suggests some interesting questions: Is it not about time for a fourth generation to appear? If so, what might it look like? These questions are of central importance. Whoever is first to recognize, understand, and implement a generational change can gain a decisive advantage. Conversely, a nation that is slow to adapt to generational change opens itself to catastrophic defeat.

Our purpose here is less to answer these questions than to pose them. Nonetheless, we will offer some tentative answers. To begin to see what these might be, we need to put the questions into historical context.

This article also appears in the October 1989 issue of Military Review.

32

Marine Corps Gazette • October 1989

IW vs. CW

- IW: *„Cílená snaha o podkopání a neutralizaci systému velení a řízení nepřítele za účelem chránění a koordinace činností velícího a řídícího systému přátelských sil.“*
- *„Koherentní, synchronizované spojení fyzických a virtuálních akcí za účelem přimět státy, organizace či jednotlivce provést/neprovést akce, pomocí nichž dosáhneme svých cílů. A zároveň zabráníme oponentovi v provádění působení IW/IO.“*
- IW může zahrnovat:
  - shromažďování taktických informací a dat,
  - kontrolu informací,
  - šíření propagandy a dezinformace k demoralizaci nebo manipulaci s oponentem a veřejností,
  - Podrývání/snižování kvality informací oponenta,
  - Zamezit oponentovi možnost shromažďovat informace.

IW vs. CW

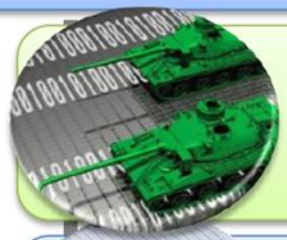
- IW mnohem širším termínem
- CW (většinou) jako podmnožina IW
- Vice chairman of the US Joint Chiefs of Staff, Gen. James E. Cartwright (2010): *„Ozbrojený konflikt vedený zcela nebo jen částečně kybernetickými prostředky. Vojenské operace vedené k odepření nepřátelským silám efektivního využívání systémů v kyberprostoru a kybernetických zbraní v konfliktu. Patří sem počítačové útoky, kybernetická obrana a další kybernetické akce.*"

Výhody CW

- Low entry cost
- Nasazení levnější než konvenční zbraně (open-source)
- Nevyžaduje velké množství vojáků
- Může být využito k dosažení okamžitého efektu, chybí inherentní zpoždění spojené s fyzickým nasazením jednotek
- Potenciál provádění anonymních „stealth“ operací
- Disproporční efekt – dominovat mohou i státy bez významné konvenční síly
- Lze využít k redukci, na místo či k vyhnutí se kinetickým operacím (duty to hack?)
- Nepřátelské systémy mohou být „narušeny“, nikoliv „zničeny“ – menší poválečné/postkonfliktní škody a potřeba restorace

KYBERNETICKÁ BEZPEČNOST STÁTU

Působení zpravodajských služeb



Kybernetická obrana

Kybernetická kriminalita

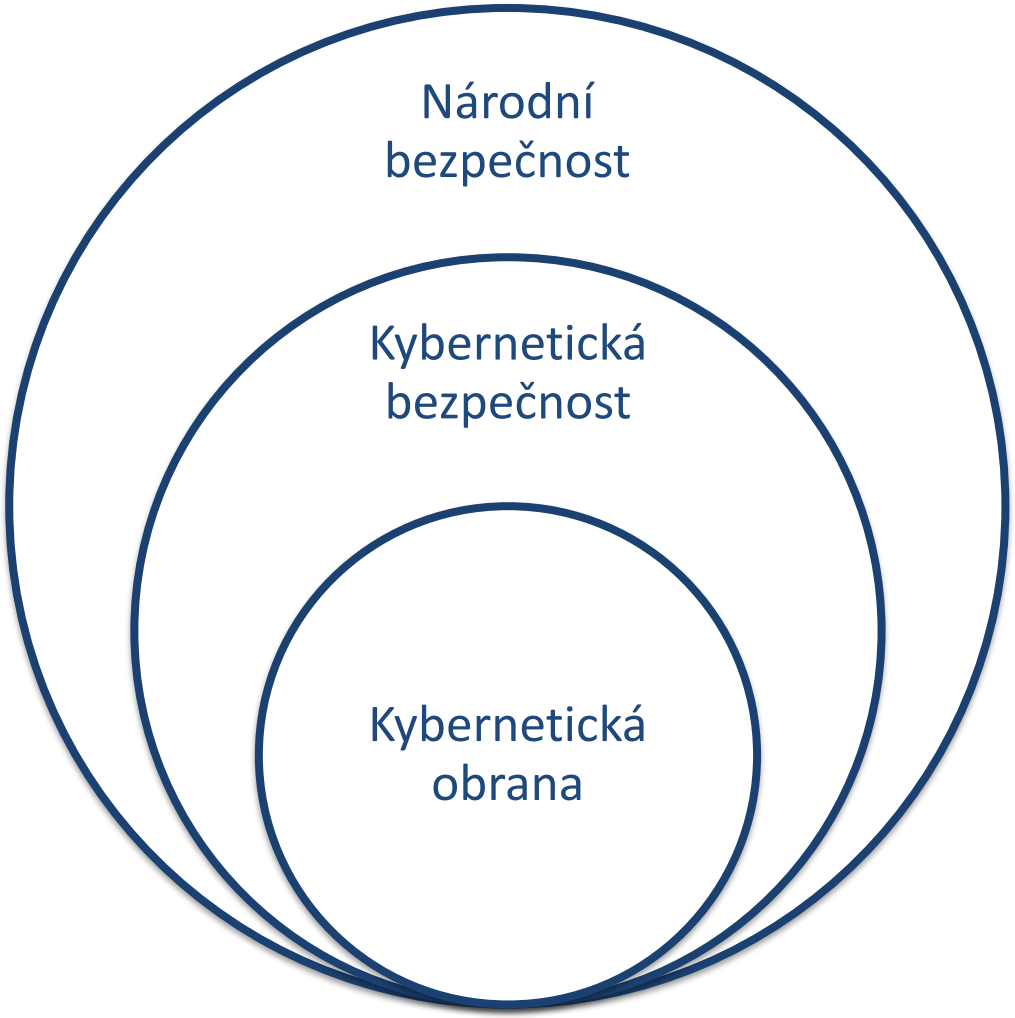
Kybernetická bezpečnost
(KB KII, VIS, Incident Handling,…)

čas

Kybernetický
bezpečnostní incident

proaktivní oblast

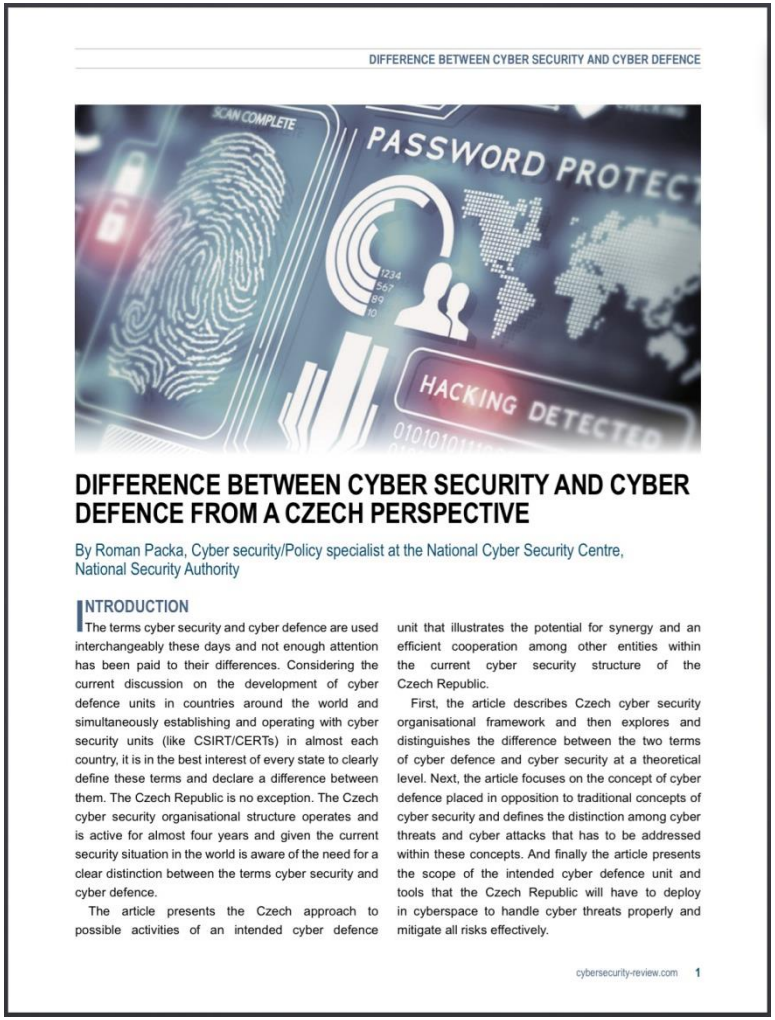
reaktivní oblast


Národní
bezpečnost
Kybernetická
bezpečnost
Kybernetická
obrana

KYBERNETICKÁ BEZPEČNOST vs. OBRANA

Kybernetická obrana z pohledu ČR:

- Závažné kybernetické útoky mířené proti informacím, datům, systémům a sítím, které:
  - jsou považovány za cílené / prováděné „na míru“ a mají závažné konsekvence vůči stavu bezpečnosti v zemi;
  - probíhají v masivním měřítku a nelze je zvládnout běžnými prostředky, tj. po vyčerpání standardních opatření a nástrojů složek kybernetické bezpečnosti;
  - mají významný vliv na strategická aktiva a národní zájmy;
  - ovlivňují obranyschopnost země, či řízení a koordinaci vojenských sil.



DIFFERENCE BETWEEN CYBER SECURITY AND CYBER DEFENCE

DIFFERENCE BETWEEN CYBER SECURITY AND CYBER DEFENCE FROM A CZECH PERSPECTIVE

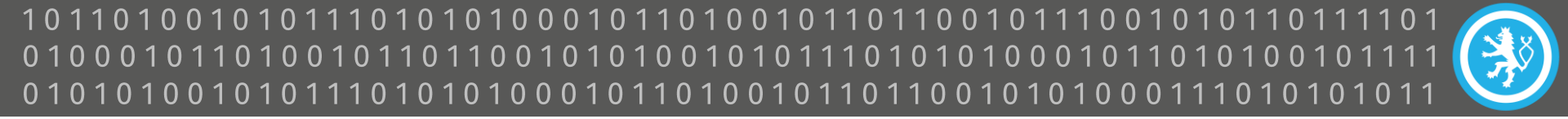
By Roman Packa, Cyber security/Policy specialist at the National Cyber Security Centre, National Security Authority

INTRODUCTION

The terms cyber security and cyber defence are used interchangeably these days and not enough attention has been paid to their differences. Considering the current discussion on the development of cyber defence units in countries around the world and simultaneously establishing and operating with cyber security units (like CSIRT/CERTs) in almost each country, it is in the best interest of every state to clearly define these terms and declare a difference between them. The Czech Republic is no exception. The Czech cyber security organisational structure operates and is active for almost four years and given the current security situation in the world is aware of the need for a clear distinction between the terms cyber security and cyber defence.

The article presents the Czech approach to possible activities of an intended cyber defence unit that illustrates the potential for synergy and an efficient cooperation among other entities within the current cyber security structure of the Czech Republic.

First, the article describes Czech cyber security organisational framework and then explores and distinguishes the difference between the two terms of cyber defence and cyber security at a theoretical level. Next, the article focuses on the concept of cyber defence placed in opposition to traditional concepts of cyber security and defines the distinction among cyber threats and cyber attacks that has to be addressed within these concepts. And finally the article presents the scope of the intended cyber defence unit and tools that the Czech Republic will have to deploy in cyberspace to handle cyber threats properly and mitigate all risks effectively.



Cyber defense starter pack:

- Vytvořit kybernetické kapacity na provádění ofenzivních / defenzivních akcí
- Vytvořit centralizovanou strukturu velení pro tyto kapacity s jadsnými požadavky na political-level schvalování akcí
- Zahrnutou tyto kapacity do doktríny / právního rámce (soulad s MPV)
- Vytvoření Cybercommand
  - Cílem centralizovat zdroje, propojit stávající kapacity a vytvořit nové
  - Výhody:
    - Kyberkapacity musí být integrovány do všech domén / i pro kyberprostor
    - Zlepšuje koordinaci
    - Efektivita získávání nových nástrojů, training jednodušší

cesnet

jak ubráníme naše sítě

čemu se vyhnout ?

těmto a podobným představám...

ČESKÁ REPUBLIKA a KO:

- Vojenské zpravodajství / Národní centrum kybernetických operací
- GŠ AČR / Velitelství kybernetických sil a informačních operací
- MO CIRC

- NÚKIB / GovCERT.CZ
- Zpravodajské služby

MIL-CIV spolupráce (dříve)

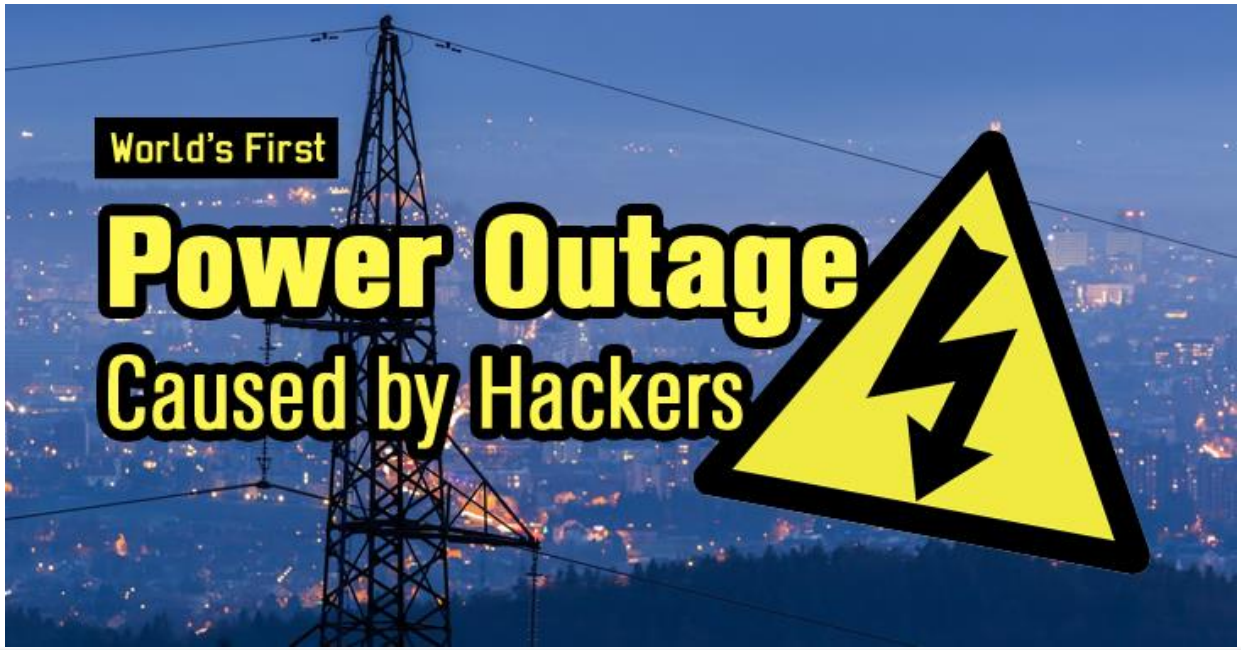
- Válčení exkluzivní záležitostí
- Spolupráce v CSIRT komunitě
- Vojenské IS/KS vyjmuty z KI

MIL-CIV spolupráce (současné trendy)

- Sun Tzu: *"The supreme art of war is to subdue the enemy without fighting"*
- Armáda je stále více závislá na civilní KII
- Zejména v iniciačních fázích konfliktů kybernetické útoky na IS/KS KII (**energetika**, finance, doprava, telekomunikace, zdravotnictví…) s cílem:
  - Narušit systém velení a řízení (C&C)
  - Snížit konvenční vojenský potenciál a bojeschopnost státu
  - Oslabit politickou vůli
  - Podrýt morálku a oslabit psychiku obyvatelstva
  - …

Ukrajina: elektrická rozvodná síť

- Více než 80 000 domácností bez elektřiny na pár hodin
- Jednoduchý útok – selhání lidského faktoru
- Sandworm team (proruští hackeři)



MIL-CIV spolupráce (současné problémy a výhody)

- Klasifikování informaci / předávání informací
- Rigidní styl velení

X

- Synchronizace s ostatními národními aktéry a vytvoření efektivního modelu spolupráce / krizový management+cvičení
- Lepší situační povědomí o bezpečnostní situaci ve státě
- Snazší incident handling
- Deterrence

Role armády v kybernetické obraně / ČR

Chránit a zabezpečit své informace, systémy a sítě	**MO + AČR + VZ** (spolupráce s NÚKIB)
Přizpůsobovat plánování / organizaci, výcvik a vybavení vojenských sil současným „cyber“ výzvám	**MO + AČR + VZ**
Disponovat útočnými kybernetickými schopnostmi při vojenských operacích	**AČR + VZ**
Bránit stát před závažnými kybernetickými útoky	**VZ** (spolupráce s NÚKIB)
Sběr informací (jakéhokoliv typu) o závažných kybernetických hrozbách	**VZ** (koordinace s ZS, NÚKIB, AČR, MO)

„A force without adequate cyber capabilities is more dangerous to itself than to its opponents.“

James A. Lewis

Rozdělení vojenských (kyber) jednotek dle mise a kapacit

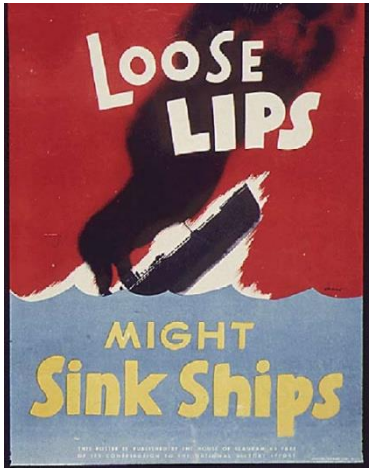
Typ	Popis	Příklady
Vojenská CSIRT pracoviště	- Zajišťování kybernetické bezpečnosti vojenských systémů a sítí - Detekce a řešení incidentů spolu s kontinuálním navyšování robustnosti a odolnosti vojenské infrastruktury	Centrum-CIRC FR-MIL-CERT
Vojenské jednotky kybernetické obrany	- Zajišťování kybernetické obrany státu - Nasazování ofenzivních kapacit v kyberprostoru k defenzivním i ofenzivním účelům	USCYBERCOM Defense Cyber Command (DCC)

+ CSIRT.MIL.SK

Kybernetická obrana

Situace	Válka / Ozbrojený konflikt	Mírový stav	
Technika kybernetické obrany	Kybernetické síťové operace / nasazení kybernetických zbraní	Aktivní kybernetická obrana / hack back	Defenzivní kybernetická obrana / fortifikace

- Information warfare /IO
  - Psychological Operations (PSYOPS)
  - Operations Security (OPSEC)
  - Computer Network Operations (CNO)
    - Computer network Attack (CNA)
    - Computer Network Defense (CND)
    - Computer Network Exploitation (CNE)
  - Military deception (MILDEC)
  - Electronic Warfare (EW)



Kybernetické síťové operace (CNO)

- Ofenzivní akce prováděné (výhradně) v období války / konfliktu
- Technika CW, ale i politické rozhodnutí
- Exkluzivní vojenský nástroj
- Zahrnuje schopnost:
  - **(1) zaútočit a narušit nepřátelské počítačové sítě a systémy (CNA);**
  - (2) chránit své vlastní vojenské informační systémy (CND);
  - **(3) využívat nepřátelské počítačové sítě ke shromažďování informací a dat, např. skrze nasazení sofistikovaného malware (CNE).**

Kybernetické síťové operace (CNO)

- CNA
  - Agresivní/ofenzivní vojenské operace v kyberprostoru
  - Účel: 3Ds: Damage, Destroy, Disrupt

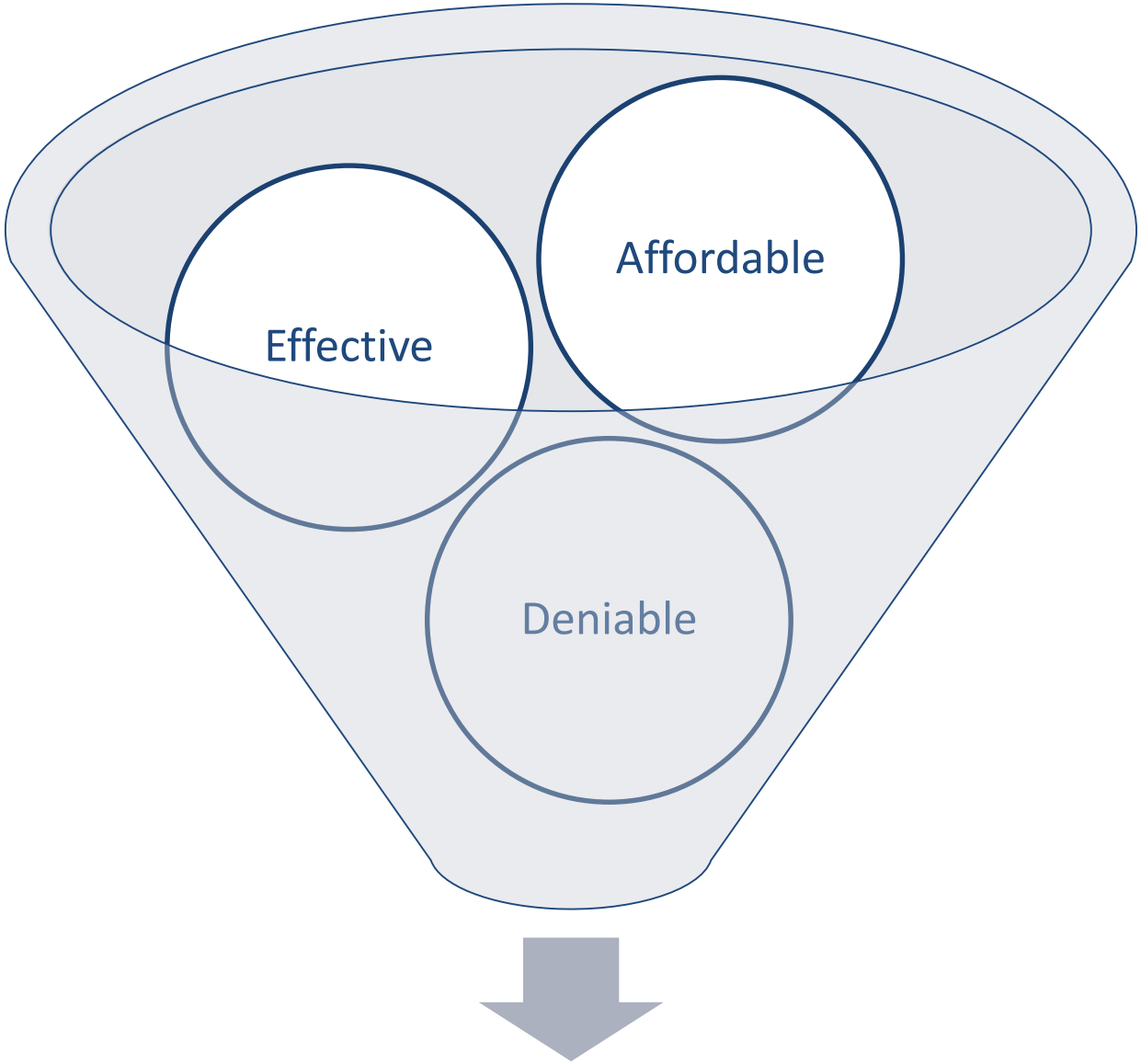
- CNE
  - intelligence, odposlouchávání (espionage) a rekognoskace pomocí síťových nástrojů
  - Účel: zisk strategických informací a dat, informací o zranitelnostech, jak systém pracuje/konfigurace, apod.
- Příklady: Stuxnet, Ukrajina 2016, Sony Hack

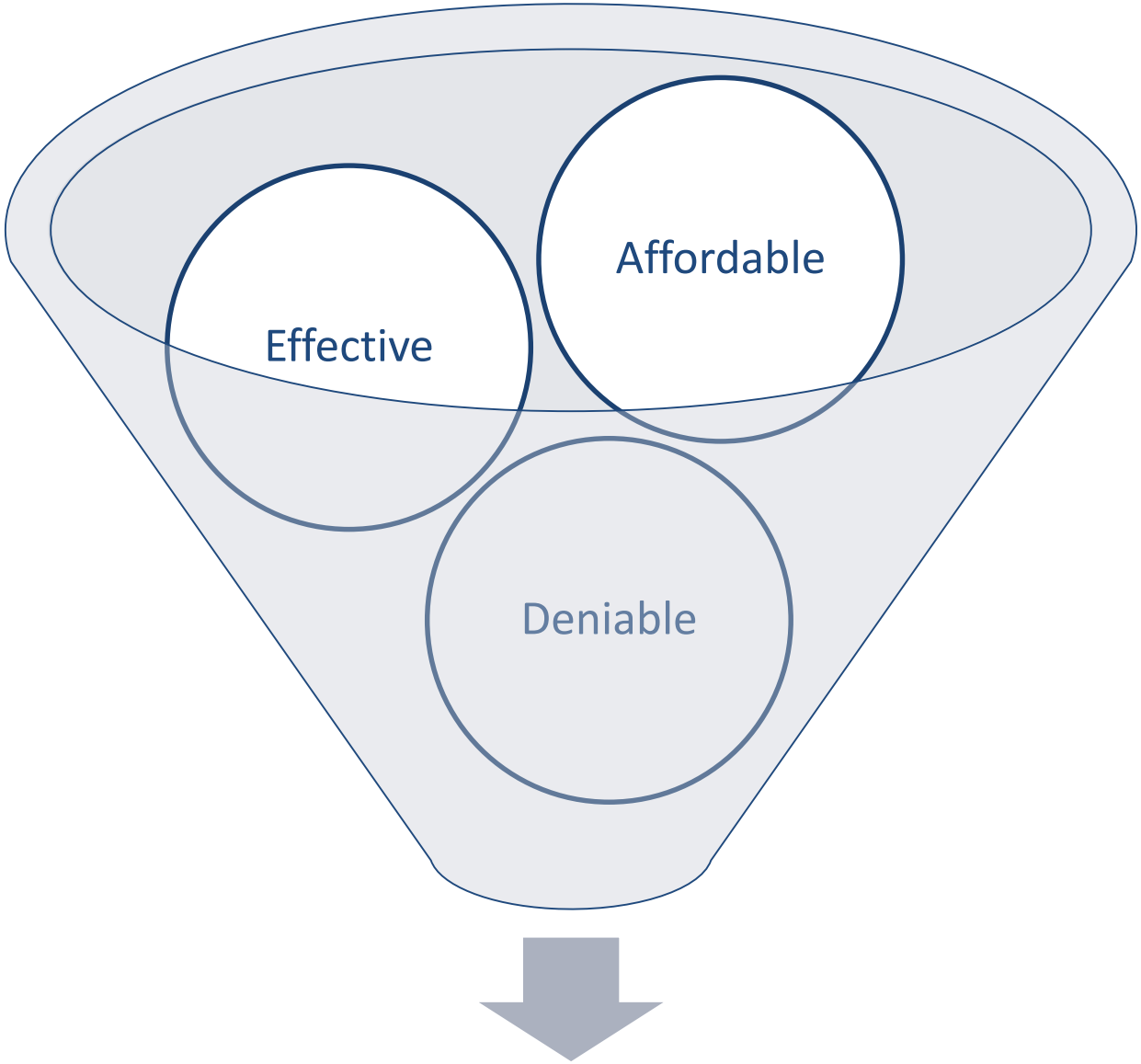
Advanced military cyber capabilities / kybernetické útoky

- Využitelné pro defenzivní i ofenzivní účely
- „Support weapon“/ limitované fyzické účinky (prozatím)
- Rozšiřuje „fog of war“ – vytváří nerozhodnost, zpomalují reakci
- Vytváří vojenskou převahu, může snižovat bojeschopnost a připravenost
- Využitelné pro manipulaci s veřejným míněním a autoritou/legitimitou oponenta (před nár. i mez. publikem)
- Trend vytváření ofenzivních kybernetických kapacit státy
- Malware kampaně: Shady RAT, Red October, APT1, Flame, PRISM, DarkSeoul, Sony Pictures, Stuxnet, …

Advanced military cyber capabilities / kybernetické útoky

Způsoby využívání malware k vojenským účelům
Kybernetická špionáž nebo jiné narušení bezpečnosti, které jsou prováděny skrze kyberprostor za cílem zisku státních dokumentů a jiných informací citlivého či utajovaného charakteru
On-line sabotáž komunikačních systémů prováděná státními aktéry za účelem způsobit škodu či nevýhodu v boji (cílí především na vojenské informační a komunikační sítě a KII).
Kybernetické útoky na fyzická zařízení směrem k jejich zničení či vyřazení z provozu (zejména průmyslové řídicí systémy spadající do KII).


Affordable
Effective
Deniable



IDEAL WEAPON

Technika:

Aktivní kybernetická obrana (ACD / hack back)

- Defenzivní technika zahrnující ofenzivní komponentu (použití za hranicí sítě oběti)
- Vyhledání zdroje útoku/analýza a jeho neutralizace
- Hack-back státního/státem sponzorovaného aktéra může mít závažné konsekvence
- Možnost i kinetické/fyzické reakce
- Nasazení musí být pečlivě zváženo (vs. resilience/fortifikace)
- Není exkluzivní vojenskou záležitostí
- Obránci musí mít schopnost a zdroje k provádění ofenzivních akcí proti hrozbám a působení v domácích i nepřátelských sítích

Technika:

Aktivní kybernetická obrana (ACD / hack back)

- Analogie se vzdušnou obranou (AMD)
  - Shooting down / diverting incoming missiles
  - Jamming hostile radar / communication
  - Patriot (země-vzduch) = příklad aktivní obrany

Technika:

Aktivní kybernetická obrana (ACD / hack back)

- Problém atribuce

???

U.S. firm blames Russian 'Sandworm' hackers for Ukraine outage

Jim Finkle

3 MIN READ

A man types on a computer keyboard in Warsaw in this February 28, 2013 illustration file picture. REUTERS/Kacper Pempel

The Telegraph

China's global cyber-espionage network GhostNet penetrates 103 countries

A vast Chinese cyber-espionage network, codenamed GhostNet, has penetrated 103 countries and infects at least a dozen new computers every week, according to researchers.

The sophisticated computer attacks have been 'devastatingly effective' Photo: CLARE KENDALL

APT Sauron

- Státem vyvinutý, vysoce sofistikovaný špionážní malware, který působil neodhalen min. od roku 2011. Odhalen až 2015 v nejmenované vládní síti.
- Cílí na utajované systémy a data vládních, vojenských, výzkumných, telekomunikačních a finančních organizací.
- Doposud odhalen v Rusku, Číně, Švédsku, Belgii, Íránu a Rwandě.

```
KBLOG_ROTATE_SECS = 10800
tmp_dir = os.getenv("WINDIR") .. "\\temp\\"
drive = "C:\\"
SAURON_KBLOG_KEY = "mISfx1q2Ef/QJPO4gi6DMKD5lx
create_log = function(l_1_0, l_1_1, l_1_2, l_1
  local f = ""
  repeat
    w.sleep(1000)
    t1 = "b"
    t2 = "k"
    t3 = "a"
```

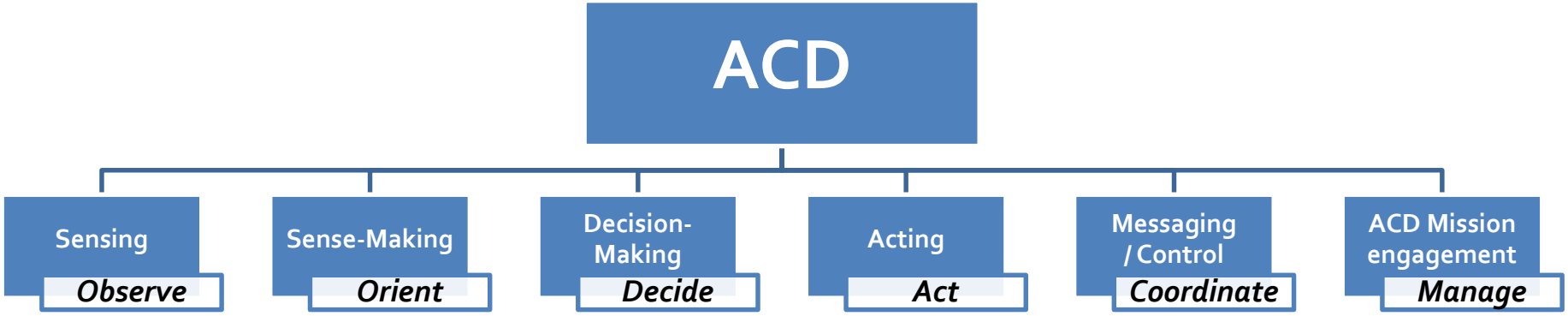
ENERGETIC BEAR


Deep
Panda

CHOLLIMA

CHOLLIMA

SILENT KITTEN


ACD
Sensing
Observe
Sense-Making
Orient
Decision-Making
Decide
Acting
Act
Messaging / Control
Coordinate
ACD Mission engagement
Manage

Sensing – kontinuální pozorování s cílem poskytnout povědomí o situaci (sensory, data, informace, lidé)

Sense-Making – použití analytiky na porozumnění situace v kontextu

Decision-Making – každý DM má své potřeby, cíle, kontext (národní politika vs. operační potřeby)

Acting – zahájení reakce

Messaging/Control – zajišťování vzájemného povědomí, komunikace, koordinace

ACD Mission engagement – provádění/udržení ACD operace, kontinuální kontrola

Technika:

Defenzivní kybernetická obrana / fortifikace

- Praxe chránění aktiv v rámci ohraničeného perimetru (např. firewall)
- Zaměřeno na kvantifikaci rizik a předpovídání hrozeb
- Prováděna za účelem prevence škodlivého narušení sítě/systému

Budoucí role CW:

- Force multiplier **X** nahrazení konvenčních operací
- Obecný konsensus: kybernetické zbraně se nestanou exkluzivním nástrojem válčení
- Kybernetické síly se již staly vojenskou kapacitou, a proto musí být integrovány do voj. strategie a plánování
- Kybernetické zbraně budou doplňovat konvenční

VÝVOJ OPERAČNÍHO PROSTŘEDÍ
Charakter budoucích konfliktů

- Časová komprese – enormní akcelerace nasazování zbraní a dalších doprovodných účinků;
- Rozšíření v prostoru – až globální rozměr (precizní útoky dlouhého rozsahu) přes přesný dlouhý dohled a propojenost,
- Účinnější (více smrtící) útoky, pokročilejší zbraňové systémy, větší kritičnost selhání techniky;
- Rutinně propojené (i napadané) domény (air, land, sea, space and cyber);
- Interaktivní i mimo fyzickou dimenzi konfliktu – morální rozměr, hodnoty a víra / role IW.

Taktické implikace

- Finders vs. Hiders
- Ofenzíva – pečlivé plánování, preciznost útoků
- Defenzíva – vysoká míra automatizace až autonomita
- Větší dosah, rychlost, přesnost a síla útoků
  - AI vizuální rekognoskace
  - Senzory a autonomní rozhodování
- Atraktivnost městských oblastí pro hiders
- Rozptýlení sil (hiders) za účelem přežití / větší síly v nevýhodě

Taktické implikace

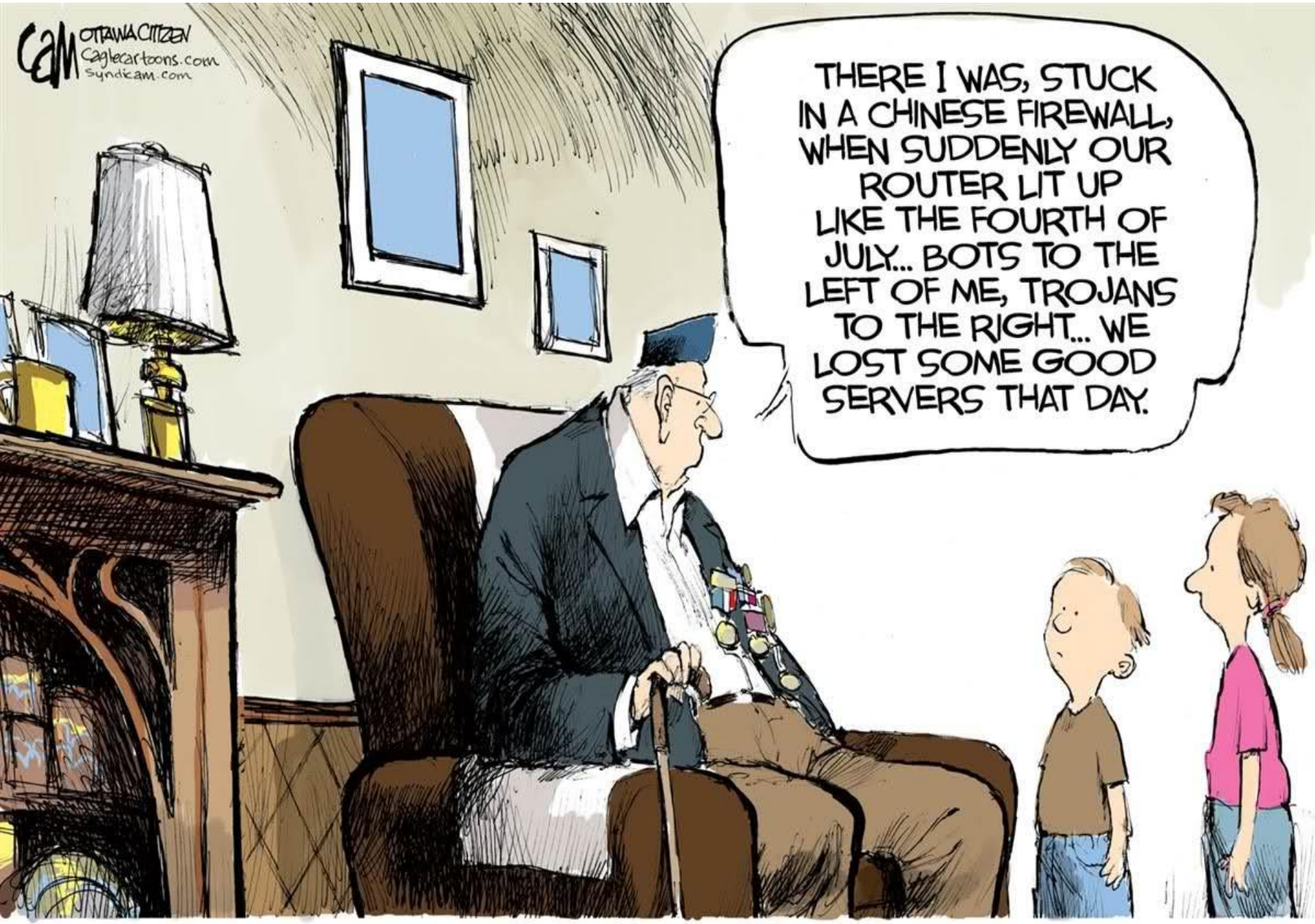
- v IW a CW výhoda stále u strikers/hiders
  = pomáhá překonat výhody defenzívy
  ve fyzickém prostředí
- Stálé pokusy o narušení komunikačních spojení a nové technologie
  (quantum based communication)
- „Going dark" – konektivita normou
  – úmyslné odpojování jednotek k zachování bezpečnosti
- „Fog of war" – CW umocní nejistotu na bojišti / snížené situační povědomí a koordinace jednotek
- Algoritmické bojiště – AI upravované rozhodování v boji bude pro dominanci na bojišti zásadní

Operační implikace

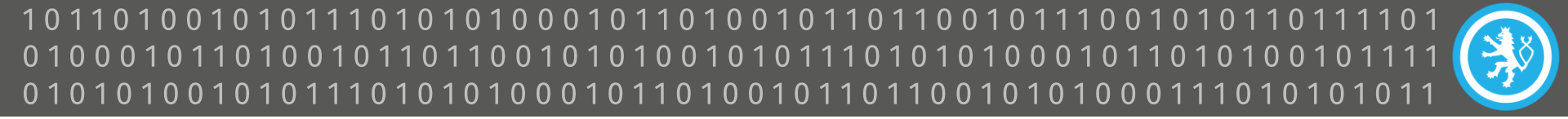
- Globální bojiště / fyzicky i virtuálně
  - Joint command and control přístup se bude i nadále vyvíjet
  - Kulturní velmoci / transregionální ideologie – značná moc v informační, morální rovině konfliktů
  - Multidimenzionální kampaně – informační boj na globální úrovni
    - precizní ideologie a narativy podporované CW, IO, PsyOps
    - Cílem zmást nepřítele, paralyzovat dec-mak proces, odepřít schopnost cílit zpět
    - Cílení i mimo bojiště
    - Weaponizace informací skrze kybernetické nástroje, sociální média
- Konec éry dominance v single doméně / velká propojenost

Strategické implikace

- Válka se nevyhlašuje, konvenční konflikty výjimkou
- Rozdělení na vnitřní a vnější bezpečnost neexistuje
- Regular /Irregular warfare ztrácí rozlišení a nastupuje hybridní spojení = Konflikt má široké spektrum od mírových/legálních aktivit přes násilné, masové otřesy, občanské války až k unlimited warfare.
  - nejasné hranice mezi mírovým „soutěžením" a agresí
- Iluze o nadvládě – i doposud nevýznamní aktéři mohou provádět ničivé, např. kybernetické útoky a mohou se stát významnými hráči na globálním bojišti
  - prostor k realizaci ambicí i lokálních aktérů, z čehož pak vyplývá rostoucí komplexita, provázanost a obtížná předvídatelnost bezpečnostního prostředí.



FUTURE WAR STORIES



Děkuji za pozornost!

Roman Pačka
mail: r.packa@nukib.cz / 333252@mail.muni.cz
web: www.govcert.cz
twitter: @GOVCERT_CZ