

**Moderné vojny sa neodohrávajú
len na fronte**

eFOCUS

Branislav Kulich

Predstavenie

mjr. Ing. Branislav Kulich

náčelník oddelenia kybernetickej obrany OSSR

Základňa stacionárnych KIS Trenčín

- 1999-2014 AVO, Log&SIEM, Analýzy incidentov,..
- 2014-2016 CSIRT.MIL
- 2017 Oddelenie implementácie informačnej bezpečnosti

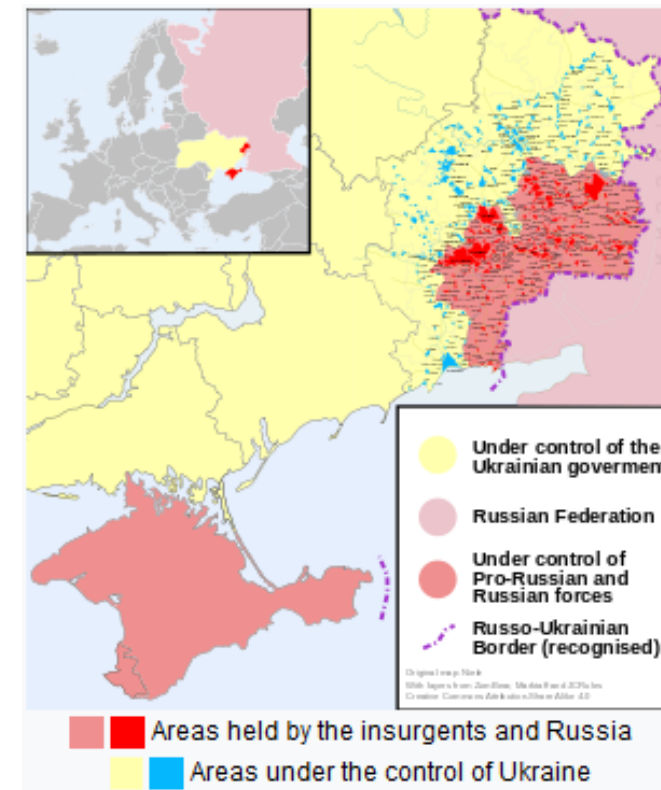
Štruktúra prezentácie

- Moderné vojny a konflikty vs. Digitálny front
 - NATO a kybernetická bezpečnosť , spolupráca
 - **Ozbrojené sily SR , kybernetická bezpečnosť a jej budúcnosť**
-
- Aktuálne hrozby
 - **Návrhy opatrení**

Moderné vojny a konflikty vs. Digitálny front

Ukrajina vs. Rusko 2013-2017

- Kybernetická vojna?
- Incidenty vs. Priebeh konfliktu (Rusko, NATO, EU)
- APT (špecifické ciele, časový úsek prípravy a pôsobenia, sofistikovanosť, na pozadí štát, armáda, skupiny s kapacitami štátu, koordinácia tímov, schopnosť prispôsobenia sa obrane a prostrediu, zložitosť identifikácie páchatel'ov)



Moderné vojny a konflikty vs. Digitálny front

Ukrajina vs. Rusko 2013-2017

- Computer network operations
- Electronic warfare
- Psychologické operácie
- Kamufláž, klamné a utajované operácie
- Propaganda, masmédiá, zombifikácia, psycholingvistické programovanie

Moderné vojny a konflikty vs. Digitálny front

Ukrajina vs. Rusko 2013-2017

- Kreml trotling
- Ukrajinská kybernetická armáda a Informačné vojská Ukrajiny
- Anonymous Ukraine
- Cyber-Berkut
- Aktivitiy Sandworm team
- Snake malware a APT28

NATO a kybernetická bezpečnosť

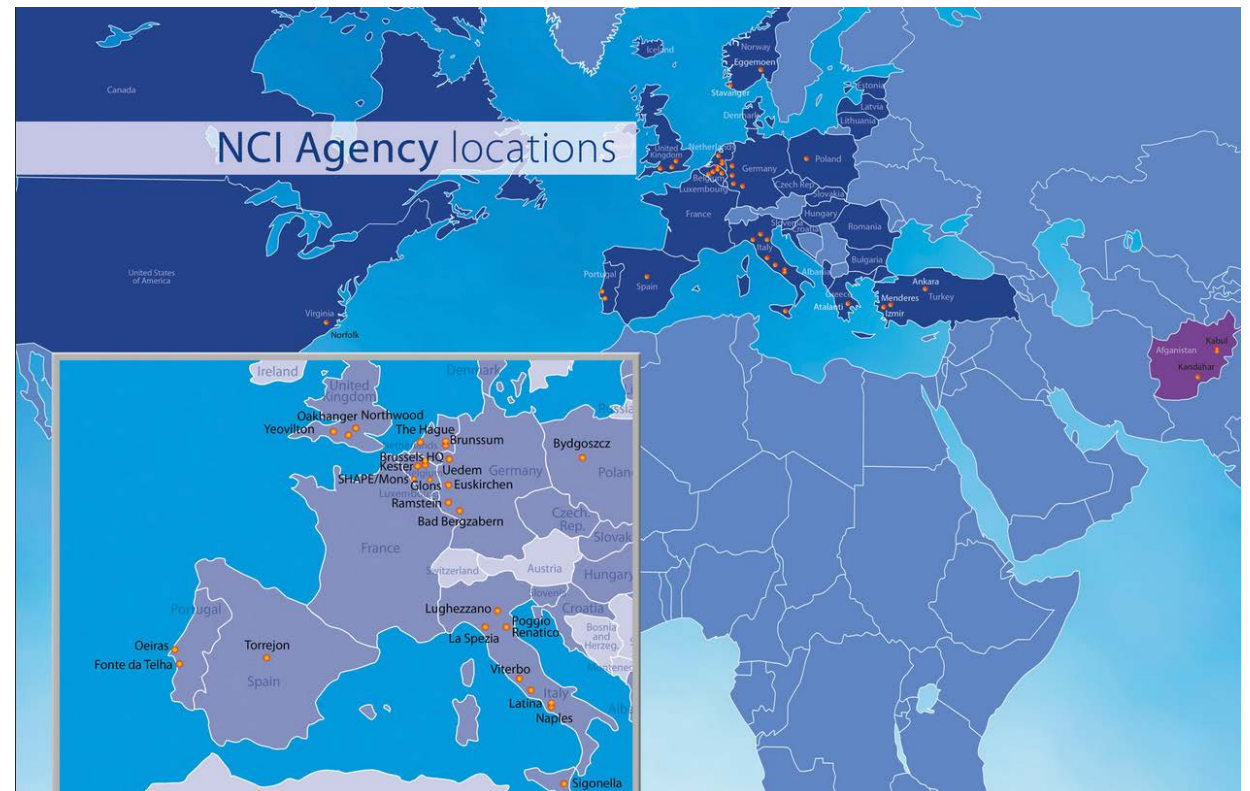
- **NCIA - NATO Communications and Information Agency's**
- **CCDCOE - NATO Cooperative Cyber Defence Centre of Excellence**



NATO a kybernetická bezpečnosť

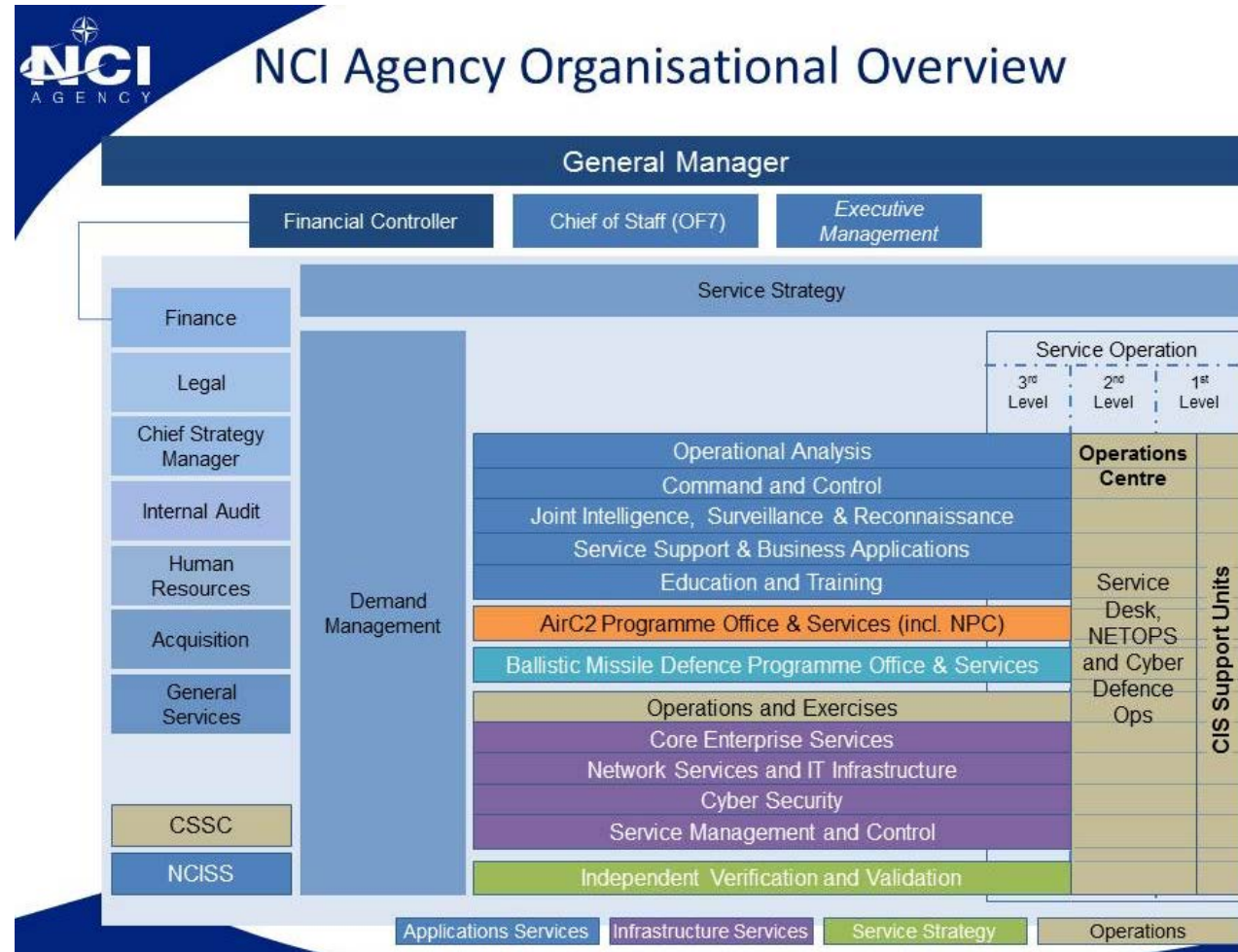
NCIA - NATO Communications and Information Agency's

- v 25 krajinách EU, USA, j.v. Ázia
- podpora NATO operácií
- Centrála - Brusel, Mons a Hague
- I.c. C4ISR delivery/Service lines
- Agency service catalogue
- Cyber Coalition
- NCIRC Daily News



NATO a kybernetická bezpečnost

NCIA - NATO Communications and Information Agency's



NATO a kybernetická bezpečnosť

CCDCOE - NATO Cooperative Cyber Defence Centre of Excellence



- Tallinn, Estónsko
- 14.5.2008 memorandum EST, GER, IT, LT, LI, SK, ESP
- 28.10.2008 akreditácia NATO
- 2010 Baltic Cyber Shield (CCDC)
- 2010 1. Locked Shields
- 2013 Tallinn manual, EDA
- -2017 GR, TUR, FIN, CZ, AUT, FR, UK, NL (sponsoring nation alebo participant)

NATO a kybernetická bezpečnosť

CCDCOE - NATO Cooperative Cyber Defence Centre of Excellence



- CIIP kurzy
- Cyber defence exercises (Locked Shields, Crossed Swords, Cyber Coalition)
- Cyber defence workshops
- Technical a právnické kurzy
- CD kurzy pre operačná úroveň
- Výskumné projekty
- Konferencie (Cycon)
- CD strategické dokumenty

Ozbrojené sily SR a kybernetická bezpečnosť

Minulosť

- Odbor informačnej bezpečnosti 2000-2017
- Internet, elektronická pošta, antivírus
- CRBS centrálné riadenie bezpečnosti siete, LOGs, SIEM, NAC, ..
- PKI infraštruktúra verejných kľúčov, ZEP, ACA
- CIRC 2014-2016 CSIRT.MIL

Ozbrojené sily SR a kybernetická bezpečnosť

Súčasnosť

- Reorganizácia leto 2017
- Odbor informačnej bezpečnosti 2017-2018
- Personálne výzvy
- Revízia informačnej bezpečnosti
- Reorganizácia projektov

Ozbrojené sily SR a kybernetická bezpečnosť

Budúcnosť

- Odbor informačnej bezpečnosti 2018 a ďalej
- Implementácia CSC20 (kritické bezpečnostné opatrenia) CISecurity.org
- Zázrak s ľudskými zdrojmi vs. Outsourcing

Ďakujeme za pozornosť

Branislav.Kulich@mil.sk

