

Celostní kybernetická bezpečnost z pohledu státu

Miroslav Nečas

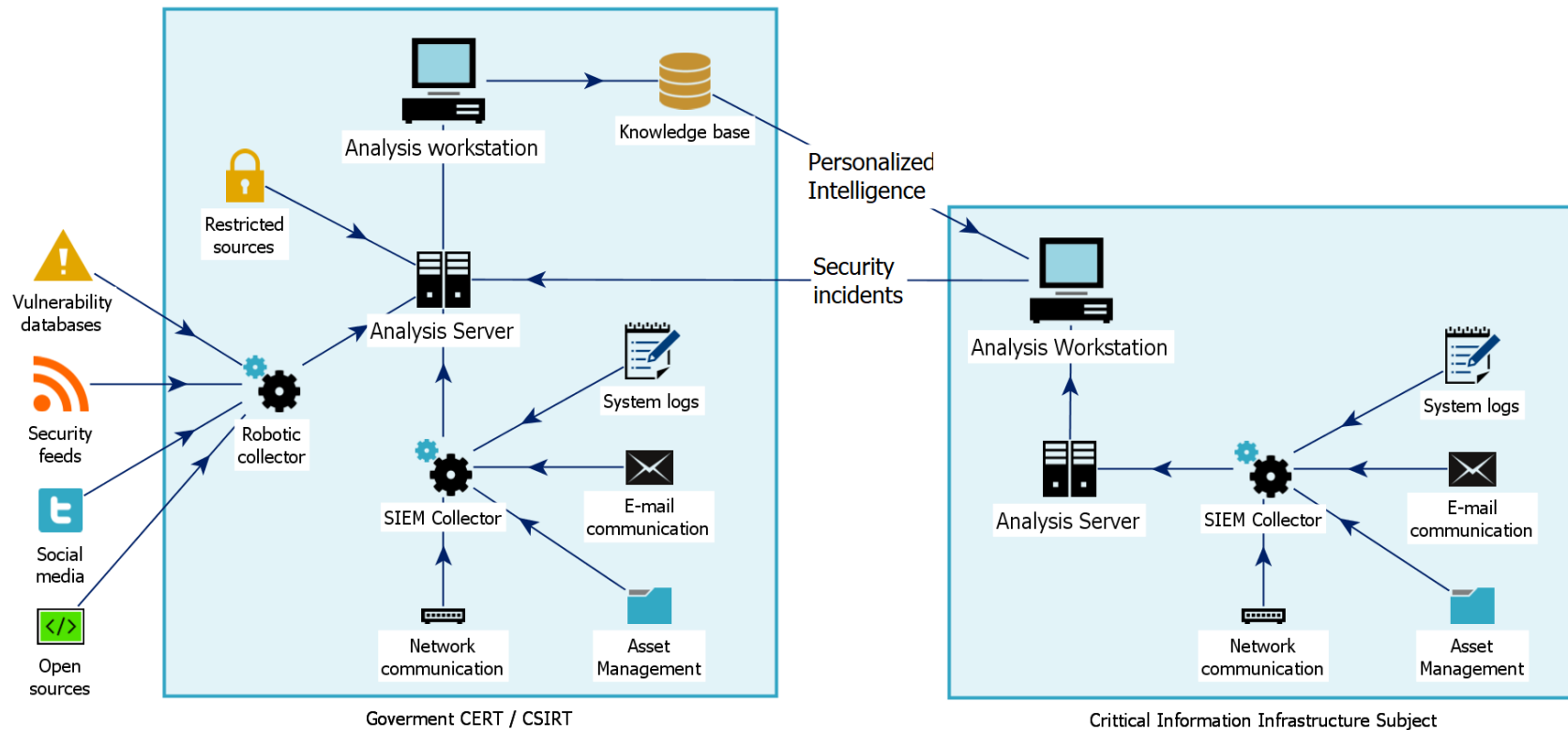
Kybernetická bezpečnost VII
26. 9. 2019

find ►
understand ►
use ►

Cíle kyberbezpečnosti z pohledu firmy

- ▶ Ochrana podnikání
 - ▶ Kontinuita výrobních procesů, dostupnost služeb, pověst organizace...
- ▶ Ochrana majetku
 - ▶ Peníze, výrobní zařízení, materiál, duševní vlastnictví, investice...
- ▶ Ochrana životů, zdraví a osobnostních práv
 - ▶ Zaměstnanců, zákazníků i třetích osob

Analytický, řešerší a monitorovací systém



Cíle kyberbezpečnosti z pohledu státu

- ▶ Bezpečné a stabilní prostředí pro podnikání a život
 - ▶ Dostupnost digitální infrastruktury, dostupnost služeb státu, fungující registry, ochrana a vymahatelnost práva v kyberprostoru
- ▶ Obrana státu proti vnějšímu napadení
 - ▶ Kybernetická obrana státu, plnění závazků kolektivní obrany
- ▶ Zajištění společenské soudržnosti
 - ▶ Důvěra v orgány státu, pocit sounáležitosti a spoluzodpovědnosti ve vztahu ke společným cílům a hodnotám občanů státu

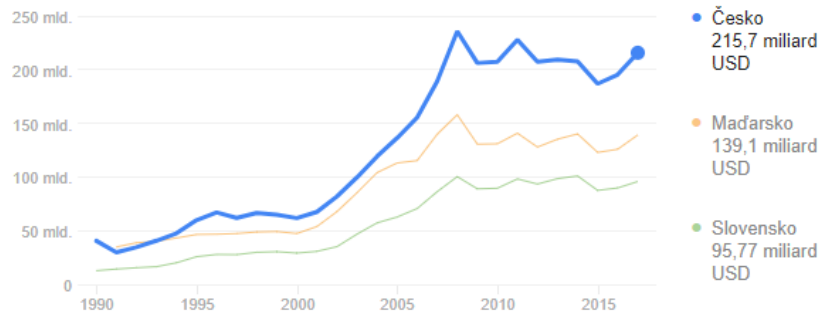


Ovlivňuje fungování státu na ekonomiku?

Česko HDP 1990 #48 2017 #44

Česko / Hrubý domácí produkt

215,7 miliard USD (2017)



 Prozkoumat další

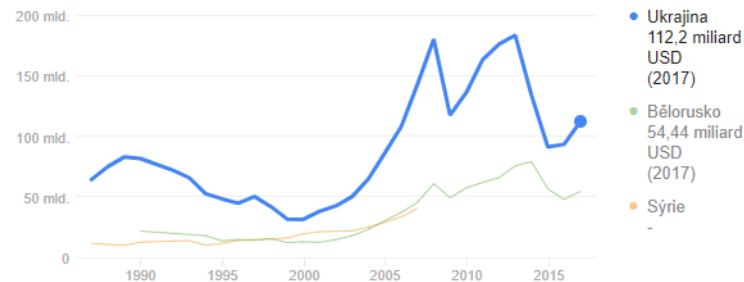
Zdroje informací: Skupina Světové banky

[Zpětná vazba](#)

Ukrajina HDP 1990 #32 2017 #58

Ukrajina / Hrubý domácí produkt

112,2 miliard USD (2017)



 Prozkoumat další

Zdroje informací: Skupina Světové banky

[Zpětná vazba](#)

Digitální ekonomika



- ▶ 7 % světového HDP v roce 2017
- ▶ Průměrný růst 1998-2017 o 9,9 % ročně vs. 2,3 % ekonomika celkem
- ▶ Hlavní dopady
 - ▶ Redukce počtu a marží prostředníků mezi výrobcem a zákazníkem
 - ▶ Zvýšení mobility pracovní síly a kapitálu
 - ▶ Globalizace výrobků vs. sdílená ekonomika služeb



Internet
Connectivity



Public Services



Smart Water
Management



Traffic Management
& Navigation



Cybersecurity



Smart Buildings



Urban Planning



Smart Mobility



Environmental
Sensors



Smart Parking



Smart Waste
Management



Smart Energy/Grid
Management

Kde končí digitální ekonomika?



Máme-li zabezpečit

- ▶ Bezpečné a stabilní prostředí pro podnikání a život
 - ▶ Dostupnost infrastruktury, dostupnost služeb státu, fungující registry, ochrana a vymahatelnost práva
- ▶ Obranu státu proti vnějšímu napadení
 - ▶ Obrana státu, plnění závazků kolektivní obrany
- ▶ Společenskou soudržnost
 - ▶ Důvěru v orgány státu, pocit sounáležitosti a spoluzodpovědnosti ve vztahu ke společným cílům a hodnotám občanů státu



Jaké informace k tomu potřebujeme?

Jak je získáme?

Jak je budeme sdílet?

Platforma pro řízenou výměnu informací



- ▶ Spolupráce zpravodajských a bezpečnostních složek:
 - ▶ Reakce na bezpečnostní události
 - ▶ Realizace společných operativních a taktických cílů
 - ▶ Zvyšování kompetence v klíčových oblastech

- ▶ Otevřená nadstavba platformy Tovek, která umožňuje
 - ▶ Vytvářet ad-hoc týmy pro realizaci společných projektů
 - ▶ Kontrolovaně a asynchronně sdílet informace a znalosti
 - ▶ Využívat služby pro sběr, monitoring a zpracování informací

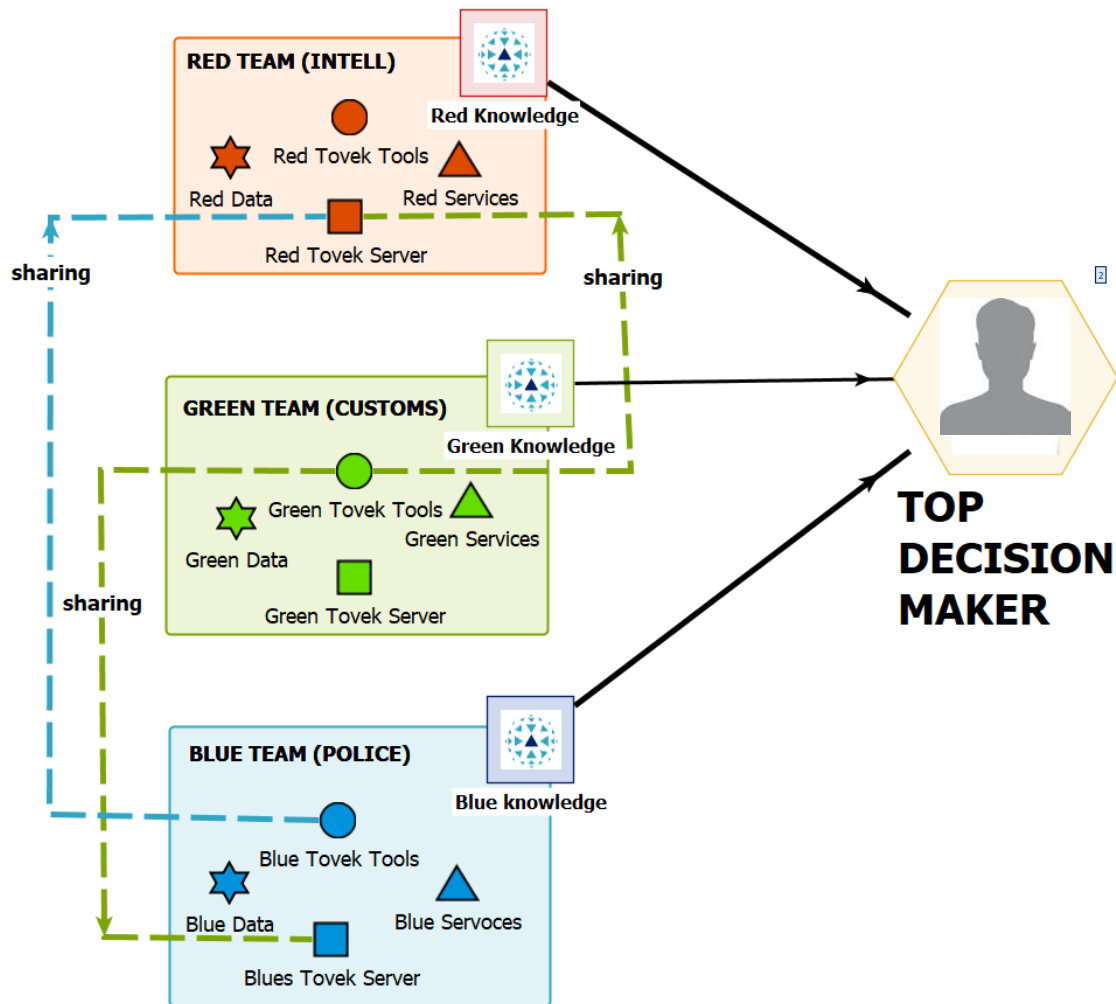
- ▶ Efektivní sběr aktuálních informací z operačního prostoru
 - ▶ IT Infrastruktura / OSINT / SIGINT / systémy a služby třetích stran
 - ▶ Zapojení uživatelů přes sociální sítě a kontaktní seznamy (crowdsourcing / remoteindexing)
- ▶ Umělá inteligence
 - ▶ Vyhodnocování multimediálních informací
 - ▶ Popojování s informacemi textové povahy a strukturovanými daty
- ▶ Vytváření a sdílení poznatků a znalostí
 - ▶ Řízené sdílení informační, znalostní a poznatkové báze
 - ▶ Tvorba výstupů podporujících rozhodovací cyklus

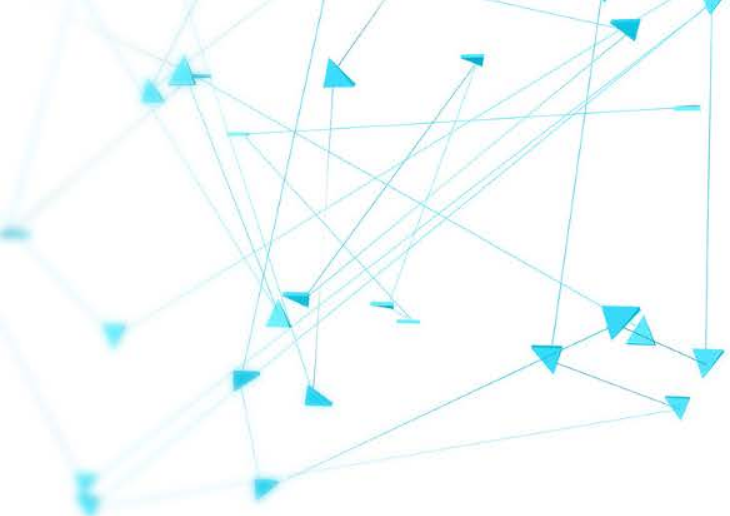


Sdílení informací na národní úrovni

Sít' nezávislých,
spolupracujících
subjektů

„Need to Know“
vs.
„Need to Share“





Děkuji vám za pozornost

Celostní kybernetická bezpečnost

Miroslav Nečas
necas@tovek.cz

www.tovek.cz