DECT

MUNI LAW

Národní centrum kompetence pro kyberbezpečnost

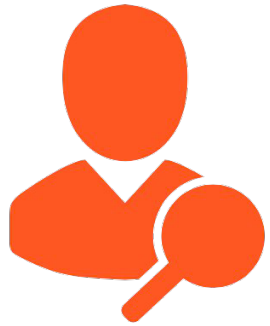
e4j

# KYBERNETICKÁ BEZPEČNOST A KYBERNETICKÁ OBRANA

VÁCLAV STUPKA

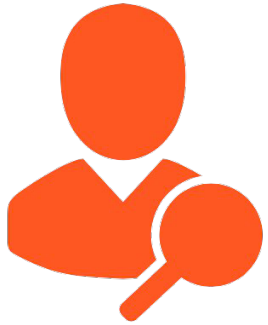
# POJEM KYBERNETICKÉ BEZPEČNOSTI

- “ochrana počítačových systémů před poškozením a narušením provozu hardwaru, softwaru nebo informací”
- Dvě složky:
  - Prevence
  - Reakce (obranná, nikoliv primárně represivní)
- Bezpečnostní incident vs. událost
- Více úrovní: jednotlivec, organizace, státy, mezinárodní společenství



# JEDNOTLIVEC A ORGANIZACE

- Vlastní zajištění bezpečnosti systémů
- Zásadně nevynucené státní mocí
- Možnost vzniku odpovědnosti (škoda, osobní údaje, správní, trestní) – příklad kauza Huawei
- Postavení definiční authority – specifické postavení

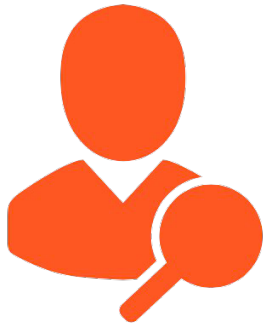


# STÁT

- Možnost uplatnění státní moci

- Ochrana lidských práv a suverenity
- Ochrana vlastíních kritických infrastruktur
- Donucení provozovatelů služeb k bezpečnostním opatřením

- Je zapojení státu nutné?
- Relativně velké regionální rozdíly.

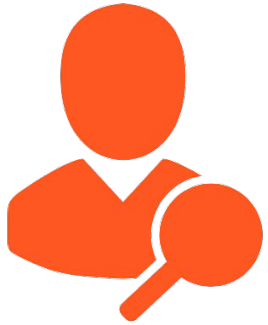


# MEZINÁRODNÍ SPOLEČENSTVÍ

- Instrumenty mezinárodního práva
- Regionální instrumenty

- Problematika regulace kyberprostoru
- Due-diligence a atribuce
- Harmonizace a spolupráce

- Problém nekompatibilních přístupů

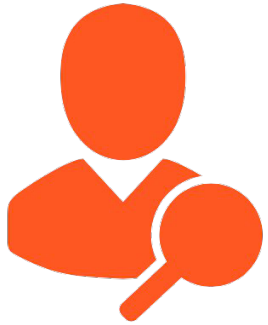


# POJEM KYBERNETICKÉ BEZPEČNOSTI V ČR

- „[k]ybernetická bezpečnost pomáhá identifikovat, hodnotit a řešit hrozby v kyberprostoru, snižovat kybernetická rizika a eliminovat dopady kybernetických útoků, informační kriminality, kyberterorismu a kybernetické špionáže ve smyslu posilování důvěrnosti, integrity a dostupnosti dat, systémů a dalších prvků informační a komunikační infrastruktury. Hlavním smyslem kybernetické bezpečnosti je pak ochrana prostředí k realizaci informačních práv člověka.“ (NSKB)
- CIA triáda

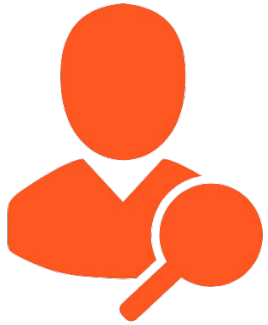
# LIMITY REGULACE

- Teritoriálně omezená suverenita
- Mezinárodní spolupráce
- Ochrana základních práv
- Vliv definičních autorit
- Problematika proporcionality



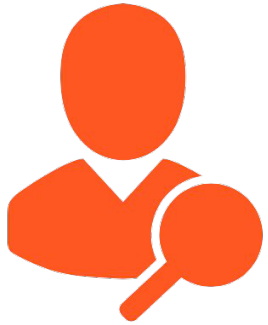
# VÝVOJ V ČR

- Národní strategie informační bezpečnosti (2005) + AP
- Usnesení vlády 205/2010 o řešení problematiky kybernetické bezpečnosti (gestor MV, koordinační rada)
- Memorandum o CSIRT.CZ (2010)
- Přechod gesce na NBÚ (2011)
- Strategie pro oblast KB (2011) + AP
- Věcný záměr ZoKB (2012)
- CSIRT.CZ GovCERT.cz
- ZoKB (2015)
- Směrnice NIS (2017) + Cybersecurity act (2019)



# VÝVOJ V EU

- ENISA (2004)
- Digitální program pro Evropu (2010)
- Strategie kybernetické bezpečnosti (2013) – ENISA, EUROPOL, EDA
- Směrnice NIS (2017)
- Cybersecurity package (2017)
- Cybersecurity act (2019)

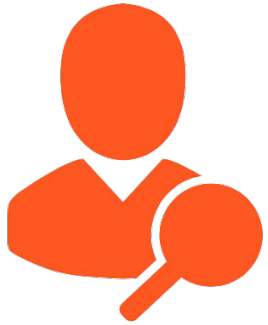


# ZÁKLADNÍ PRINCIPY

- Technologická neutralita
- Ochrana informačního sebeurčení
- Ochrana nedistributivních práv
- Minimalizace státního donucení
- Autonomie vůle regulovaných subjektů
- Bdělost ve vztahu k zahraničí

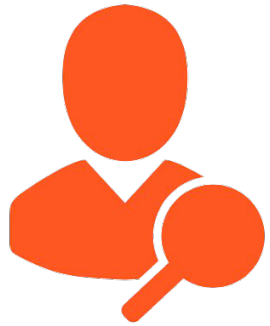
# RELEVANTNÍ ORGÁNY

- NBÚ -> NÚKIB
- OČTŘ
- Zpravodajské služby
- Armáda
- ČTÚ
- Ostatní OVM
- Soukromá sféra



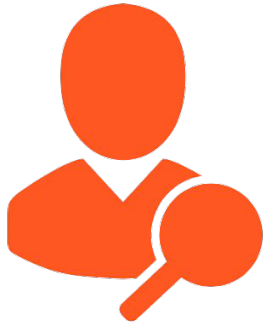
# POJEM KYBERNETICKÉ OBRANY

- Využití bezpečnostních nástrojů k předcházení, zastavení nebo odvrácení kybernetického útoku ohrožujícího zajišťování obrany státu
- Různá chápání:
  - NATO,
  - USA,
  - Rusko,
  - EU…



# KYBERNETICKÁ OBRANA V ČR

- Gesce: VZ – Národní centrum kybernetických operací (NCKO)
- Spolupráce – AČR, zpravodajské služby (BIS, ÚZSI)
- Utajené postupy – budování kapacit
- Kromě toho ochrana vlastních infrastruktur – MO/AČR



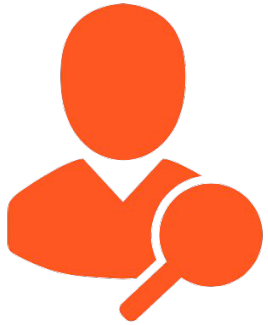
# KYBERNETICKÁ OBRANA - ZOVZ

- Pravomoci VZ
  - Detekce
  - Vyhodnocování
  - Opatření k odvracení

- Spolupráce s různými relevantními subjekty:
  - Při provádění činností a opatření
  - Při detekci s podnikateli podle ZoEK (na základě dohody, povinně v případě rizika prodlení)

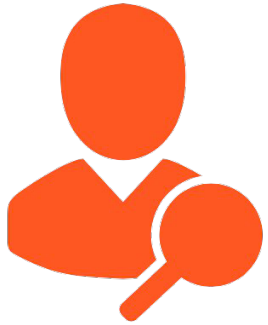
Informační povinnost, inspektor

Náhrada škody a nemajetkové újmy



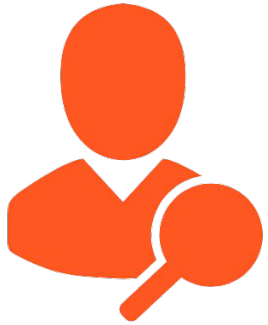
# DETEKCE

- Možnost instalace vlastních zařízení pro detekci v komunikačních sítích (není-li možné uzavřít dohodu, nebo tato není efektivní)
- Zaznamenávaná metadata:
  - popisující **informace a souvislosti nezbytné pro přenos dat, jejich strukturu a čas o zachyceném provozu v telekomunikacích**, a to pouze **v rozsahu souvisejícím s detekovaným kybernetickým útokem nebo hrozbou** na základě stanovených ukazatelů; **součástí není obsah přenášených dat**
  - Provozu detekčního nástroje a o manipulaci s ním
- Negativní vymezení: odposlech, aktivní zásah
- Nutnost zachování CIA triády telekomunikací
- Nesmí být zasahováno do činnosti subjektů podle ZoEK
- ISP povinnost vytvořit rozhranní pro připojení zařízení pro detekci
  - (na základě rozhodnutí MO, lhůty, náhrada nákladů)



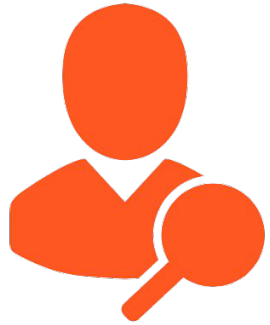
# OPATŘENÍ

- Na základě výsledku vyhodnocení detekovaných útoků nebo hrozeb
  - Předání informace relevantním státním orgánům, Národnímu CERTU, případně subjektu schopnému reakce na útok nebo hrozbu (nejsou-li naplněny podmínky aktivního zásahu)
  - Hrozí-li prodlení -> aktivní zásah
- Podmíny pro realizaci aktivního zásahu:
  - Existence ohrožení důležitých zájmů státu ve značném rozsahu
  - Útok nebo hrozba bezprostředně hrozí nebo trvá
  - Nelze odvrátit ve spolupráci s ozbrojenými silami a aktivní zásah je jediná možnost
  - Souhlas ministra obrany



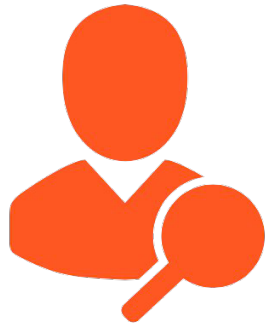
# INFORMAČNÍ POVINNOSTI

- Předávání informací o aktivním zásahu
  - O zahájení: vládu, NÚKIB a zpravodajské služby
  - O provedení: ministr obrany -> vláda, náčelník GŠ, ředitel NÚKIB, ostatní zpravodajské služby, v nezbytném rozsahu Národní CERT
- Obecně informace a součinnost pro NÚKIB a Policii ČR v rozsahu jejich působnosti
- Předání dat a realizace aktivních zásahů se eviduje
- Zpráva o činnosti – vláda a prezident (ročně)
- Zpráva o plění úkolů – ministr obrany (pololetně)



# INSPEKTOR PRO KYBERNETICKOU OBRANU

- Jmenuje vláda na 5 let, voják VZ podřízen ministrovi obrany
- VZ – poskytuje informace, přístup, materialní a personální vybavení
- Vypracovává zprávu o nedostatcích a návrhy na zlepšení ministrovi obrany
- Povinnosti:
  - Prověřuje správnost postupů VZ
  - Ověřuje účinnost bezpečnostních opatření, navrhuje jejich aktualizaci
  - Poskytuje poradenství v oblasti ochrany dat a informací
  - Spolupracuje v oblasti bezpečnosti s povinnými osobami
  - Obrací se na něj ISP při obavě o bezpečnost (podnět) – řešení podateli a PS



# DÍKY ZA POZORNOST

STUPKA@NC3.CZ