NÁRODNÍ CENTRUM KYBERNETICKÉ BEZPEČNOSTI

NÁRODNÍ BEZPEČNOSTNÍ ÚŘAD

- zřízen 1998
- vydává osvědčení fyzické osoby nebo podnikatele o bezpečnostní způsobilosti
- gestor ochrany utajovaných informací
- certifikuje kryptografické prostředky
- schvaluje národní šifrové algoritmy
- od roku 2011 gestor kybernetické bezpečnosti, provozuje NCKB

STRUKTURA NCKB

Odbor kybernetických bezpečnostních politik

- Oddělení národních strategií a politik
- Oddělení regulace, podpory a auditu
- Oddělení cvičení a vzdělávání
- Oddělení mezinárodních organizací a práva
- Oddělení strategických informací a analýz

Odbor vládní GovCERT.CZ

- Oddělení reaktivní
- Oddělení vývoje a bezp. testování
- Oddělení analytické
- Oddělení analýzy síťového provozu

+ MIMO NCKB

Národní CERT: CSIRT.CZ

Vojenské zpravodajství: NCKS

CESNET-CERT
O2.cz CERT
SEZNAM.CZ-CSIRT
CZ.NIC-CSIRT
CSIRT-MU
ACTIVE24-CSIRT
CSOB-Group-CSIRT
..

Ministerstvo vnitra: CTHH

STRUKTURA NCKB

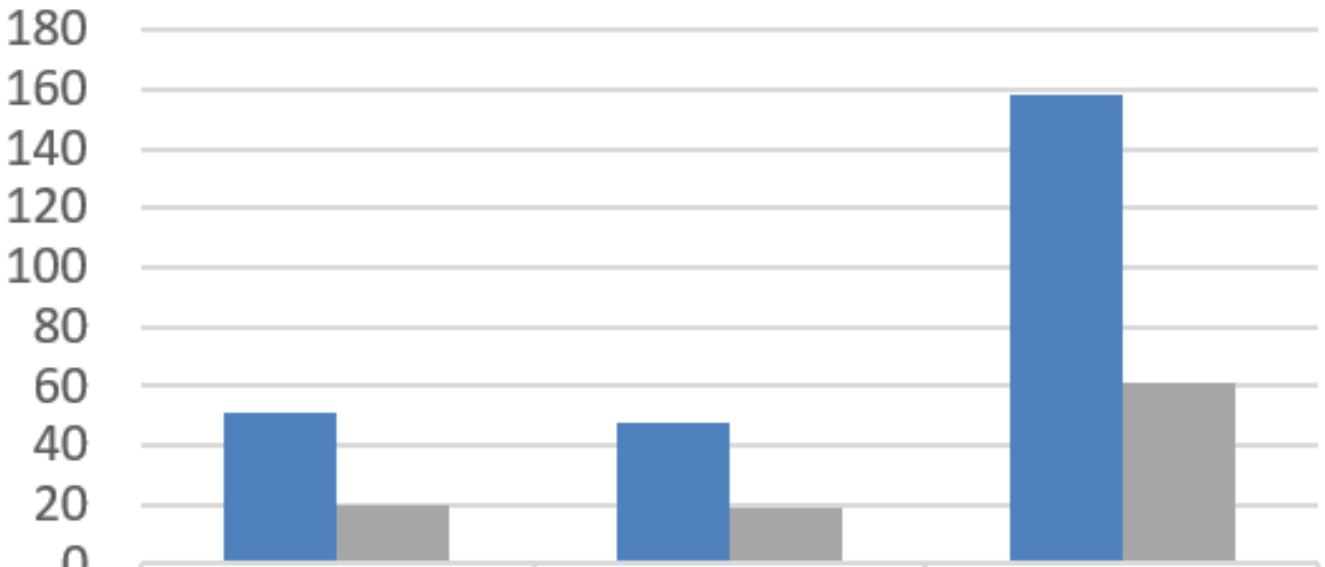
Odbor kybernetických bezpečnostních politik

- strategie, analýzy, výzkum
- věcná a právní doporučení
- kyber. bezpečnostní politiky napříč subjekty pod ZKB
- každoroční Zprávy o stavu kybernetické bezpečnosti ČR
- publikační činnost
- mapování a určování KII/VIS

Odbor vládní GovCERT.CZ

- technická asistence při řešení bezpečnostních incidentů
- penetrační testy
- analýza malware
- sdílení dat
  - BotnetFeed
  - ShadowServer

Aktuální počty systémů a správců KII/VIS



	KII - soukromý sektor	KII - veřejný sektor	VIS
Počet systémů	51	48	158
Počet správců	20	19	61

STRUKTURA NCKB

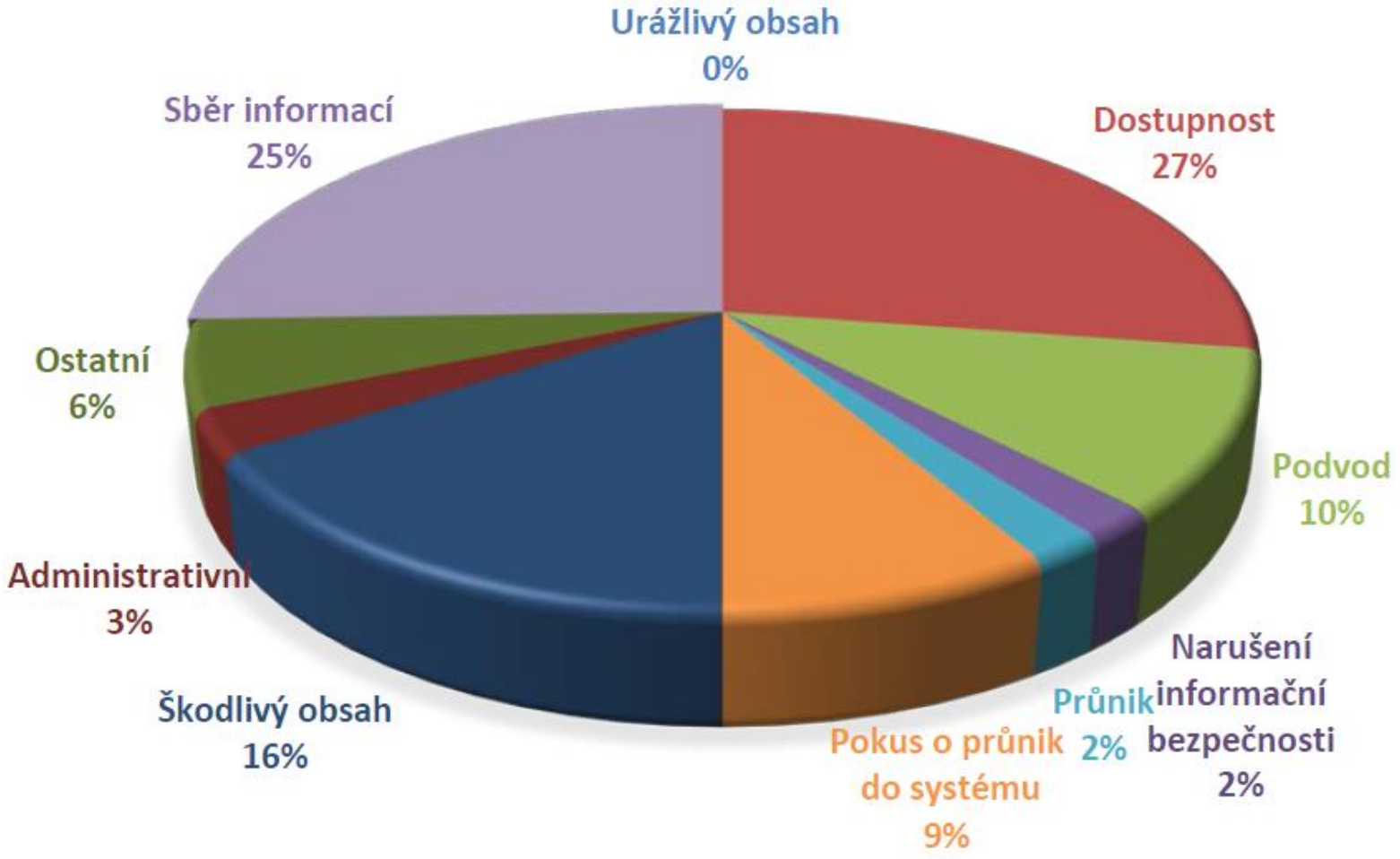
Odbor kybernetických bezpečnostních politik

- strategie, analýzy, výzkum
- věcná a právní doporučení
- kyber. bezpečnostní politiky napříč subjekty pod ZKB
- každoroční Zprávy o stavu kybernetické bezpečnosti ČR
- publikační činnost
- mapování a určování KII/VIS

Odbor vládní GovCERT.CZ

- technická asistence při řešení bezpečnostních incidentů
- penetrační testy
- analýza malware
- sdílení dat
  - BotnetFeed
  - ShadowServer

KLASIFIKACE INCIDENTŮ



STRATEGICKO-PRÁVNÍ RÁMEC

Zákon 181/2014 Sb. o kybernetické bezpečnosti + návazné vyhlášky

Bezpečnostní strategie ČR

Národní strategie kybernetické bezpečnosti ČR pro období let od 2015 až 2020 + návazný Akční plán

ZÁKON O KYBERNETICKÉ BEZPEČNOSTI

PROČ

- ↑ závislost na ICT = ↑ kritičnost selhání
- ↑ počet kybernetických útoků
- právní zakotvení působení vládního a národního CERTu

CÍLE

- ustanovit základní kybernetická bezpečnostní opatření
- zlepšit detekci a hlášení kybernetických bezpečnostních incidentů
- není cílem zasahovat do obsahu

ZÁKON O KYBERNETICKÉ BEZPEČNOSTI

PRINCIPY

- individuální zodpovědnost správců za sítě & systémy
- technologická neutralita
- minimalizace zásahu do práv soukromoprávních subjektů (cestou standardizace, nikoliv certifikace)

POVINNÉ OSOBY

- správci KII a správci VIS
- do budoucna: provozovatelé základních služeb (+ správci/provozovatelé jejich informačních systémů) a poskytovatelé digitálních služeb

STRATEGICKO-PRÁVNÍ RÁMEC

Zákon 181/2014 Sb. o kybernetické bezpečnosti + návazné vyhlášky

Bezpečnostní strategie ČR

Národní strategie kybernetické bezpečnosti ČR pro období let od 2015 až 2020 + návazný Akční plán

NÁRODNÍ STRATEGIE KYBER. BEZPEČNOSTI

- chránit národní KII a VIS
- spolupracovat se zahr. partnery
- bojovat s informační kriminalitou
- vybudovat národní schopnosti v kybernetické obraně
- zajistit bezpečný kyberprostor stimulující českou ekonomiku
- zvyšovat osvětu a digitální gramotnost

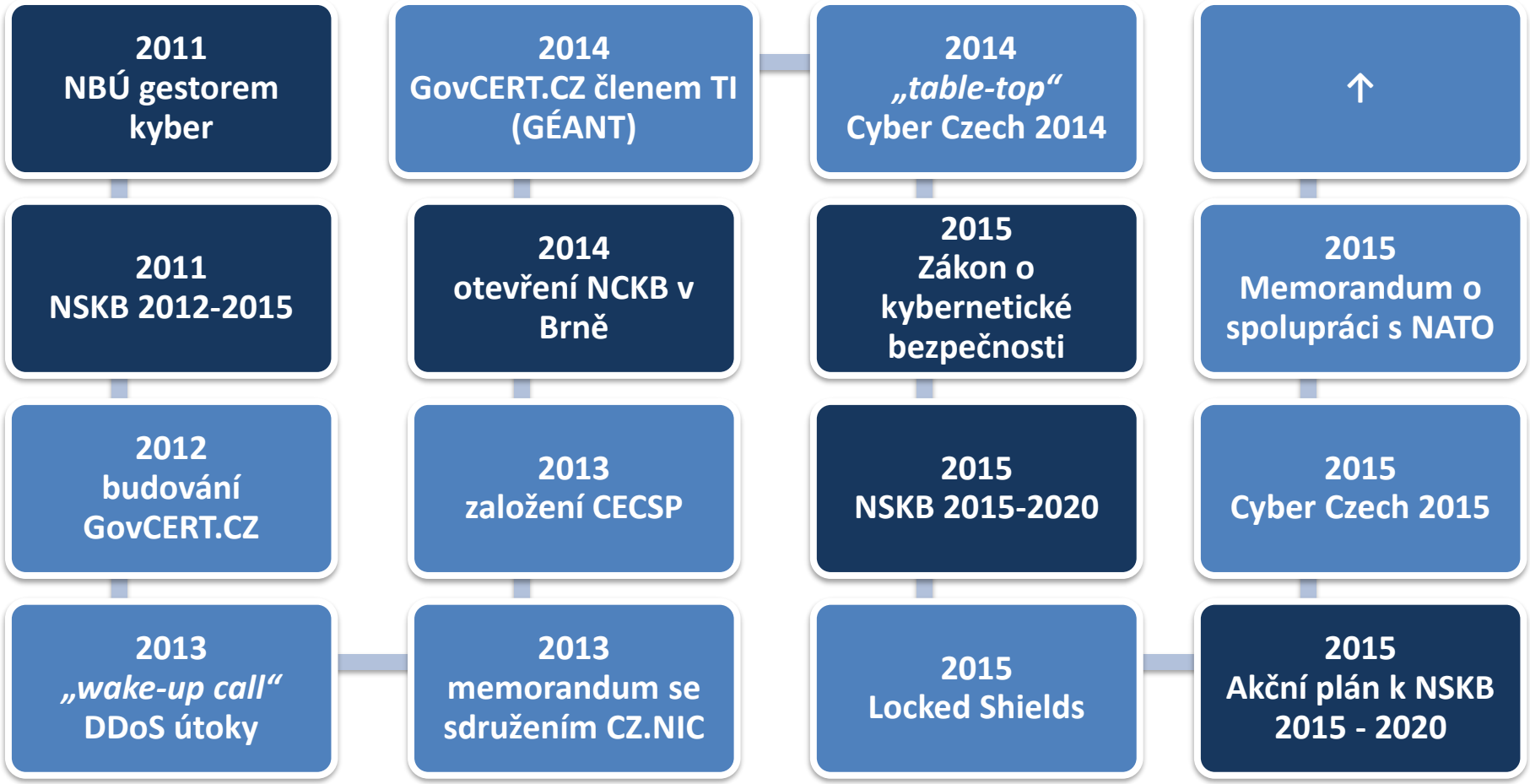
NÁRODNÍ STRATEGIE KYBER. BEZPEČNOSTI - VÝZVY

1. ČR jako možný testovací objekt
2. nedostatečná důvěra veřejnosti ve stát
3. ↑ počet uživatelů internetu, ICT technologií a ↑ kritičnost jejich selhání
4. ↑ počet uživatelů mobilních platforem a ↑ množství mobilního malware
5. možnosti zneužití zadních vrátek hardware pro exfiltraci informací
6. koncept *„internetu věcí“*
7. bezpečnostní rizika spjatá s přechodem z protokolu IPv4 na IPv6
8. bezpečnostní rizika spjatá s elektronizací veřejné správy (eGovernment)
9. nedostatečné zabezpečení malých a středních podniků
10. big data, skladování dat v nových prostředích

AKČNÍ PLÁN K NÁRODNÍ STRATEGII 2015-2020

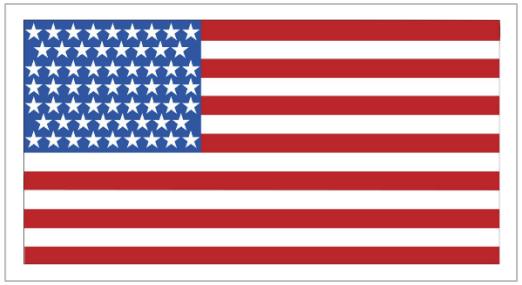
Hlavní cíle	Kód	Úkoly	Odpovědný subjekt	Časový rámec
A. Zajištění efektivity a posilování všech struktur, procesů a spolupráce při zajišťování kybernetické bezpečnosti				
Vytvořit efektivní model spolupráce na národní úrovni mezi jednotlivými subjekty kybernetické bezpečnosti – pracoviště typu CERT a CSIRT, subjekty KII apod. – a posilovat jejich stávající struktury a procesy.	**A.1.01**	Vytvořit v koordinaci s ostatními subjekty schéma a podrobný model spolupráce v rámci zajišťování kybernetické bezpečnosti.	NBÚ/NCKB *ve spolupráci s:* MV MZV MO MPO Zpravodajské služby	Q3 2015
	A.1.02	Provést analýzu agend v rámci problematiky kybernetické bezpečnosti a na jejím základě definovat národní zájmy a priority v této oblasti.	NBÚ/NCKB *ve spolupráci s:* MO MZV MPO Zpravodajské služby	Q4 2015
	A.1.03	Provádět technická i netechnická národní cvičení kybernetické bezpečnosti.	NBÚ/NCKB *ve spolupráci s:* MO MV Zpravodajské služby	průběžně

MILNÍKY


2011
NBÚ gestorem kyber
2011
NSKB 2012-2015
2012
budování GovCERT.CZ
2013
„wake-up call“ DDoS útoky
2013
memorandum se sdružením CZ.NIC
2013
založení CECSP
2014
otevření NCKB v Brně
2014
GovCERT.CZ členem TI (GÉANT)
2014
„table-top“ Cyber Czech 2014
2015
Locked Shields
2015
NSKB 2015-2020
2015
Zákon o kybernetické bezpečnosti
↑
2015
Memorandum o spolupráci s NATO
2015
Cyber Czech 2015
2015
Akční plán k NSKB 2015 - 2020

MEZINÁRODNÍ SPOLUPRÁCE

CECSP



MEZINÁRODNÍ SPOLUPRÁCE

CYBER ATTACHÉ

- **navazuje a udržuje spolupráci** s relevantními institucemi
- zajišťuje **předávání informací** o kybernetické bezpečnosti
- **reprezentuje NBÚ/NCKB**, respektive ČR na relevantních akcích
- sleduje a vyhodnocuje dodržovaní vzájemných smluv
- asistuje v oblasti kybernetické bezpečnosti při vzájemných návštěvách českých a zahraničních představitelů
- Izrael (Tel Aviv), USA (Washington), NATO/EU (Brusel)

CVIČENÍ – MEZINÁRODNÍ

CECSP 2015 EXERCISE

LOCKED SHIELDS

CYBER COALITION

CECSP Exercise

- téma ročníku 2015: komunikace
- účastníci: ČR, Maďarsko, Rakousko, Slovensko, Polsko

Locked Shields

- největší technické cvičení v oblasti kybernetické obrany NATO
- 2016: přes 500 účastníků
- organizované CCD COE NATO v Talinnu
- Blue / Red team scénář

Cyber Coalition

- největší cvičení kybernetické obrany NATO
- 2016: přes 700 účastníků
- účast členských zemí
- operační, technické i právní scénáře
- stát, CSIRT.CZ, CSIRT-MU

CVIČENÍ – MEZINÁRODNÍ

Cyber Europe

- připravuje ENISA
- 29 zemí na evropské úrovni
- tři části: technická, operační a taktická část

Crisis Management Exercises

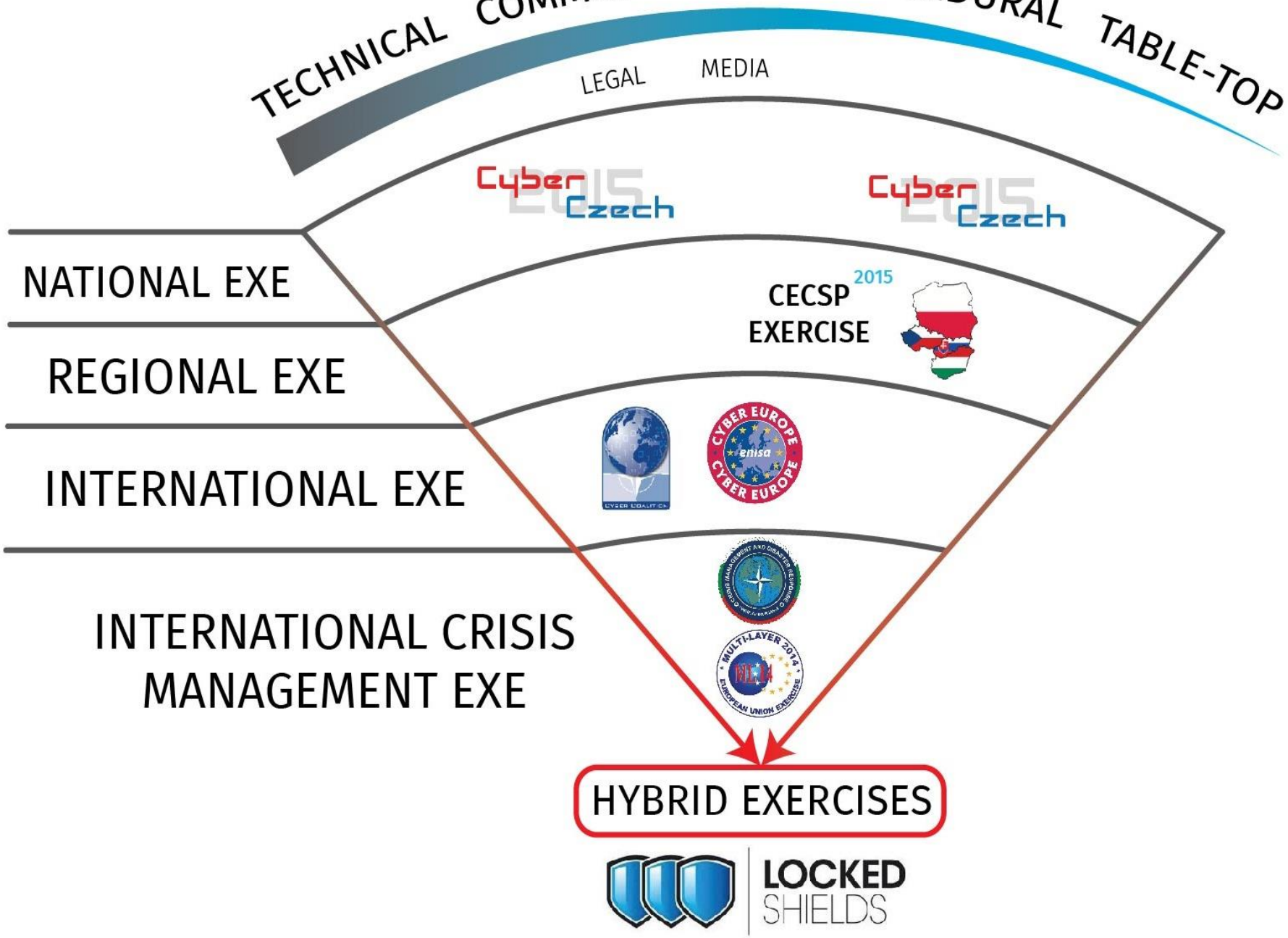
- cvičení krizového řízení včetně kyber. scénářů
- EU: MultiLayer Crisis Management Exercise
- NATO: Crisis Management Exercises

CVIČENÍ – NÁRODNÍ

2016
COMM
CZECH

- **technická část – Brno**
  - s ÚVT MU na Kybernetickém polygonu
  - 6 obranných týmů po 6 hodin čelilo nárůstajícím aktivitám útočníků
- **strategická část – Praha**
  - rozhodovací procesy při řešení krize
  - 6 skupin, které musely spolupracovat

- **komunikační cvičení**


TECHNICAL
COMMUNICATION
PROCEDURAL
TABLE-TOP
LEGAL
MEDIA
Cyber Czech 2015
Cyber Czech 2015
NATIONAL EXE
CECSP 2015
EXERCISE
REGIONAL EXE
INTERNATIONAL EXE
CYBER EUROPE
enisa
CYBER EUROPE
INTERNATIONAL CRISIS
MANAGEMENT EXE
MULTI-LAYER 2014
EUROPEAN UNION EXERCISE
HYBRID EXERCISES
LOCKED
SHIELDS

Děkujeme za pozornost!

www.nbu.cz
www.govcert.cz