

**Bezpečnostní systém České
republiky, praktické zkušenosti
s jeho fungováním a institucionální
zajištění kybernetické bezpečnosti
v České republice**

Ing. Dušan Navrátil

Kybernetickou bezpečnost je nutno chápat v souvislostech.

Kybernetické hrozby jsou součástí hybridních hrozeb. Obrana proti hrozbám (zjednodušeně útokům vedeným kombinací různých metod), které mohou být konvenční i nekonvenční.

Konkrétní příklad:

Ruský útok na Ukrajinu v roce 2022.

Konvenční (kinetický útok byl doprovázen množstvím nekonvenčních útoků:

- . DDoS útoky na celém území Ukrajiny již od rána 23. února 2022 (den před útokem)**
- . destruktivní kybernetické útoky – malware wiper a boot sector altering – cílem útoku ukrajinští poskytovatelé služeb, kritická infrastruktura a vládní organizace (pouze území Ukrajiny na rozdíl od války 2014) – největší útoky mezi 22. a 24. únorem a poté 6 týdnů**

Pozn. Nejsofistikovanější malware Infustroyer zaměřující se systémy Windows, Linux a Solaris, zaměřoval se na provozní technologie používané k monitorování energetické sítě.

- . ničivé útoky na modemy satelitního systému Viasat – v okamžiku zahájení kinetického útoku – způsobil zásadní problémy v komunikaci – vedlejší účinek bylo narušení provozu 5800 větrných turbín v Německu**

Pozn. Mnoho kybernetických útoků bylo koordinováno s konvenčními útoky.

Další nekonvenční útoky:

- . Kybernetická špionáž – zintenzivnění činnosti – cíle kromě Ukrajiny především Polsko, USA, Pobaltské země, Skandinávie, Turecko, MZV zemí NATO**
- . Haktivismus – na obou stranách – připojily se i kyberzločinecké organizace**
- . Dezinformace a informační válka – cíle ukrajinský lid, ruský lid, Západ a Třetí svět**

Pozn. Šíření ruské propagandy se zvýšilo po zahájení války na Ukrajině o 216% a v USA o 82%.

Adekvátní obrana musí být schopna koordinované detekce, analýzy, reakce a musí koordinovat napříč jednotlivé části bezpečnostního systému!!!

Daná kombinace hrozeb málokdy spadá pouze do gesce jedné instituce, účinná reakce skoro pokaždé vyžaduje mezirezortní koordinaci, mnohdy koordinaci širší napříč celou státní správou, popř. celou veřejnou správou, popř. celou společností, popř. i koordinaci mezi státy.

Obecné problémy bezpečnostních systémů státu

Funkčnost nebo nefunkčnost mezirezortní, nebo i širší koordinace je většinou odrazem celého bezpečnostního systému.

Základní problémy:

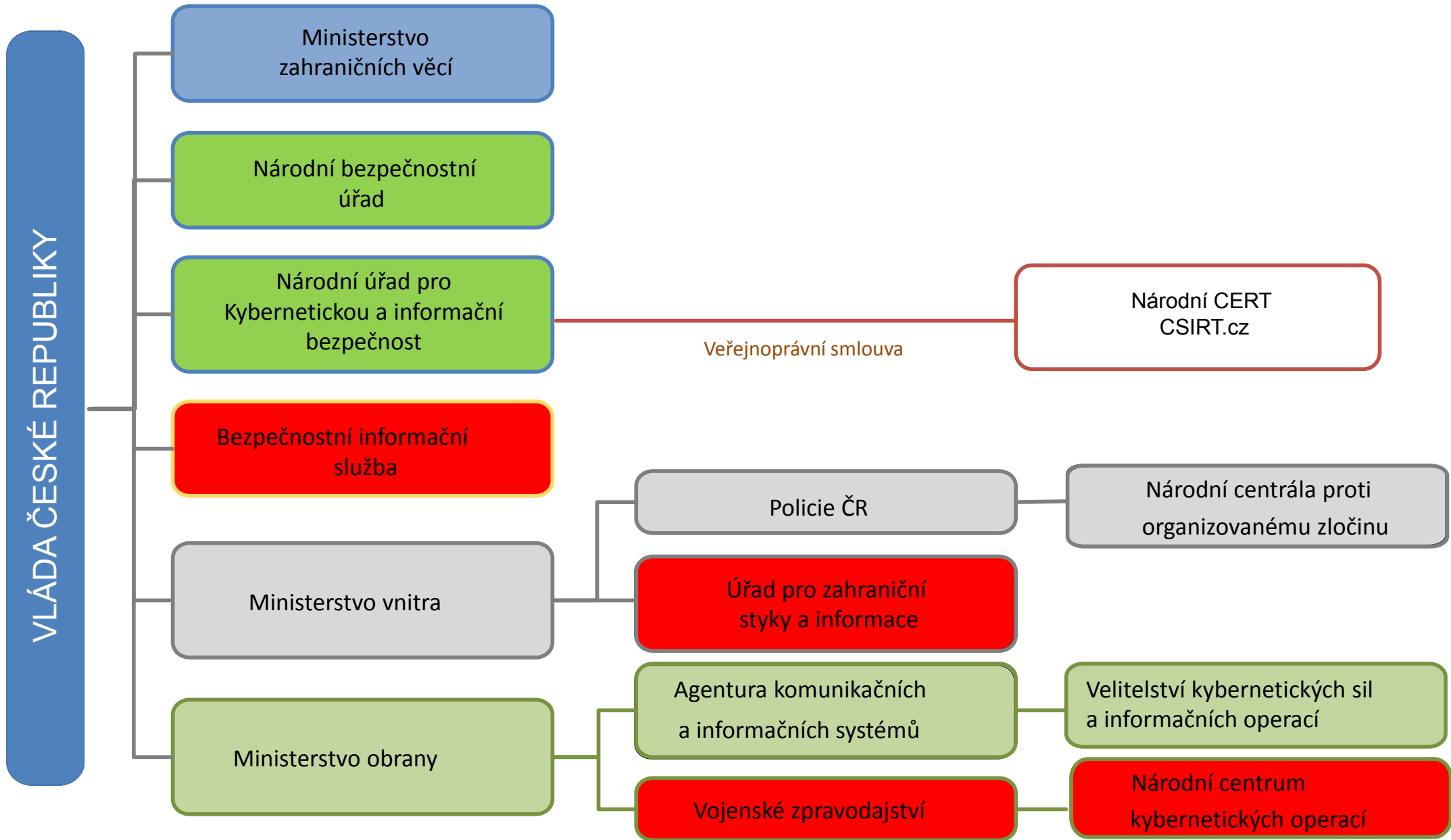
- . otázka rozdělení gescí mezi jednotlivé instituce**
- . otázky (ne)stanovení hlavní koordinační role různých institucí za bezpečnostní politiky**
- . rivalita mezi jednotlivými částmi systému**
- . otázka duplicity či absence gescí za jednotlivé určitou oblast**
- . otázka formálních gescí versus reálné vykonávání dané gesce**
- . koordinace zpravodajských služeb**
- . stanovení priorit a úkolů zpravodajským službám**
- . kontrola zpravodajských služeb**

Jak funguje bezpečnostní systém v České republice?

Jaké má nedostatky?

Jak je Česká republika schopna čelit novým hrozbám?

Jak je zajištěna kybernetická bezpečnost v ČR?



Ministerstvo zahraničních věcí

Věnuje se primárně zprostředkování informací se zahraničí a komunikaci s ním.

Je gestorem Bezpečnostní strategie České republiky (poněkud nesystémové řešení)

Není koordinátorem bezpečnostní politiky

Kybernetické útoky na sítě ministerstva ze strany Ruska a Číny

Národní bezpečnostní úřad

Zodpovídá za ochranu utajovaných informací
(vznikl v roce 1998)

Činnost:

- . provádění bezpečnostních prověrek pro osoby a firmy dle standardů NATO.**
- . vydává certifikáty pro přístup k utajovaným informacím NATO a EU**
- . administrativní bezpečnost**
- . fyzická bezpečnost**
- . vede registr dokumentů NATO**
- . garant národní šifry *(přešlo na NÚKIB v roce 2017)***
- . tempest *(přešlo na NÚKIB v roce 2017)***
- . certifikace informačních systémů obsahujících utajované informace *(přešlo na NUKIB v roce 2017)***
- . kybernetická bezpečnost *(od roku 2011 do roku 2017 – NÚKIB)***

Národní úřad pro kybernetickou a informační bezpečnost

Zabývá se kybernetickou bezpečností a další činností
(vznikl v roce 2017 oddělením od NBÚ)

Podrobněji později

Ministerstvo vnitra

- . oblast vnitřní bezpečnosti**
- . oblast veřejné správy**
- . oblast eGovernmentu - přechází do DIA (Digitální a informační agentura)**

Složky v podřízenosti:

- . Policie ČR (zabývá se kromě jiného i kybernetickou kriminalitou)**
- . Hasičský záchranný sbor ČR**
- . Úřad pro zahraniční styky (ředitel přímo podřízen ministrovi)**

Státní podnik zřízený ministerstvem:

NAKIT (Národní agentura pro komunikační a informační technologie s. p.) – přechází do DIA

Ministerstvo vnitra

V minulosti řešilo především hrozby terorismu a migrace, které v ČR nebyly vážné, spíše mediální a politická poptávka. Oboje bylo doprovázeno dezinformacemi, které měly původ v zahraničí. Nebyla vůle to řešit, ani koordinovat. Obecně MV má tendenci neřešit nové hrozby a nevíle převzít zodpovědnost - „odstrkávat vše od sebe“

Odpor bezpečnostní politiky – oddělení hybridních hrozeb.

Dnes vládní zmocněnec pro dezinformace – žádné kompetence – výsledek?

Příprava zákona o dezinformacích?

Ministr vnitra svolává Ústřední krizový štáb pokud řeší aktuální hrozby a rizika v oblasti vnitřní bezpečnosti. Problém s ministrem obrany.

Bezpečnostní výzkum

Ministerstvo obrany

Zabezpečuje obranu ČR

Kromě jiného:

- . řídí Armádu ČR**
- . podílí se na návrhu obranné politiky státu**
- . koordinuje činnost ústředních orgánů samosprávy a právnických osob důležitých pro obranu státu při přípravě k obraně**
- . řídí Vojenské zpravodajství**

Ministerstvo obrany

Armáda ČR

Od 1. července 2019 vzniklo **Velitelství kybernetických sil a informačních operací AČR** na základě definování kybernetického prostoru jako 5. operační domény summitem NATO ve Varšavě.

Hlavní úkoly:

- . působení v kybernetickém prostoru a informačním prostředí
- . začleňování se do vedení společných operací, které zasahují i kybernetickou doménu
- . chránit vlastní síly a prostředky v kybernetickém prostoru
- . podporovat strategickou a vést operační komunikaci

Vojenské zpravodajství

Národní centrum kybernetických operací (NCKO)- kybernetická obrana – vytvoření účinného systému obrany kybernetického prostoru, tak aby ČR byla schopna zastavit , případně odvrátit kybernetické útoky.

Další zajímavé aktivity – SIGINT (signální zpravodajství) a IMINT (obrazové zpravodajství)

Zpravodajské služby

Bezpečnostní informační služba - podřízena premiérovi

(vnitřní)

Úřad pro zahraniční styky a informace – podřízena ministru vnitra

(vnější)

Vojenské zpravodajství – podřízeno ministru obrany

(vnější a vnitřní)

HUMINT,SIGINT,OSINT,IMINT

historický vývoj

zavěšení

nemají výkonné pravomoci

spolupráce a nespolupráce

koordinace

úkolování

stanovování priorit

kontrola

efektivita

PR

Úřad vlády

Poradce pro bezpečnostní a zahraniční politiku od 1.ledna 2022

- . skupina pro koordinaci zpravodajských služeb (vzniká) ? zavěšení**
- .odbor bezpečnostních politik- zajišťuje sekretariát BRS**

Společná zpravodajská skupina Výboru pro zpravodajskou činnost BRS –zabývá se pouze terorismem

Bezpečnostní rada státu

členové:

- . **předseda vlády**
- . **ministr vnitra**
- . **ministr obrany**
- . **ministr zahraničních věcí**
- . **ministr dopravy**
- . **ministr průmyslu a obchodu**
- . **minist zdravotnictví**
- . **ministr sociálních věcí**
- . **ministr pro místní rozvoj**

Jednání BRS se zúčastňují stálí event. nestálí hosté.

BRS zřizuje výbory:

Výbor pro koordinaci zahraniční a bezpečnostní politiky

Výbor pro zpravodajskou činnost

Výbor pro kybernetickou bezpečnost

Výbor pro vnitřní bezpečnost

Výbor pro obranné plánování

Výbor pro civilní nouzové plánování

Nedostatky bezpečnostního systému

Pozitiva

- . vznik Národního úřadu pro kybernetickou a informační bezpečnost (*iniciativa jednotlivců*)**
- . vznik Velitelství kybernetických sil a informačních operací AČR (*na základě požadavku NATO*)**
- . vznik Národního centra kybernetických operací (*na základě iniciativy jednotlivců a požadavku NATO*)**
- . jmenování bezpečnostního poradce premiéra a zřízení skupiny pro koordinaci zpravodajských služeb (*politická vůle po vypuknutí války na Ukrajině*)**

Nedostatky bezpečnostního systému

Negativa

Pozn. Česko dlouho nečelilo (teprve nyní čelí) závažným krizím a bylo relativně bezpečným místem k životu. To však platilo pro konvenční hrozby. Existovaly nové nestandardní hrozby, kombinované, hybridní, ale nebyla politická vůle je řešit, byly bagatelizovány popř. popírány.

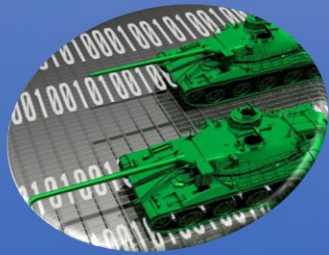
- . hluboce zakořeněný rezortismus – původ v politické rovině – koaliční vlády – každá vládní stran jedno ze silových ministerstev – kooperace ovlivněna je ovlivněna politické mírou ochoty kooperovat mezi členy vlády - každý ministr odpovídá poze za svoji působnost – kolektivně v rámci vlády necítí odpovědnost za celou bezpečnostní politiku**
- . Úřad vlády nemá dostatečné koordinační a analytické kapacity – neposkytuje premiérovi zázemí pro řízení a koordinaci bezpečnostní politiky státu - ministerstva nemají motivaci sladit své postupy do synergie**
- . neschopnost provést potřebné strukturální změny v bezpečnostním systému - není příprava na nové hrozby a rizika – nedostatek strategického myšlení – pohodlnost – kdo nic nedělá a hlavně o ničem nerozhodne neudělá chybu a tím nemá problém - alibismus**

Nedostatky bezpečnostního systému

- . bezpečnostní politika je tvořena tichým koncenzem skupiny hlavních gestorů bezpečnosti – nebudou si zasahovat do svých oblastí působnosti – nebudou se příliš snažit o nadrezortní koordinaci – to zabraňuje sporům a konkurenci – vylučuje efektivně řešit cokoliv co přesahuje působnost – eventuelně koordinaci podřídít sám sobě**
- . odmítání čehokoliv nového – způsobuje to problémy nedej bože nutnost rozhodovat a převzít zodpovědnost**
- . řešení dezinformací?**

Je nutný komplexní přístup k realizaci bezpečnostní politiky, ale nejen státu, ale celé společnosti do obrany státu. Naše bezpečnostní situace se prudce změnila – prudce zhoršila!

Kybernetická bezpečnost



Kybernetická
obrana



Ochrana kritické
informační
infrastruktury



Kybernetická
kriminalita



Působení
zpravodajských
služeb



Dotazy?

Diskuze.