# Postavení NÚKIB ve státní správě, spolupráce s ostatními s ostatními státními orgány a mezinárodní spolupráce

# a varování Huawei

Ing. Dušan Navrátil

# NUKIB

- **Rozhodnutí vlády z prosince 2016 o vzniku samostatného úřadu NUKIB delimitací z NBÚ**
- **V prosinci 2016 v Poslanecké sněmovně Parlamentem ČR byla po prvním čtení novela ZKB (implementace směrnice EU - NIS I.)**
- **Pozměňovací poslanecký návrh předložený ve druhém čtení ve výboru pro bezpečnost definoval nový úřad – NUKIB**
- **Součástí pozměňovacího návrhu byla i novela Zákona o utajovaných informacích 412/2005 Sb.**
- **Novely schváleny v červnu 2017 Senátem Parlamentu ČR a podepsány prezidentem**
- **Platnost novely od 1. srpna 2017 – vznik NUKIB**
- **Leden – červenec 2017 - příprava delimitace NCKB, certifikace IS obsahujících utajované informace, Tempest, krypto a Galileo z NBU**
- **Leden – červenec 2017 – vytvoření nové obslužné sekcee – ekonomika, správa, vnitřní IT a právní věci ještě v rámci NBU a poté delimitováno**
- **Červen 2017 - novela zákona o státním rozpočtu – vlastní rozpočtová kapitola**
- **1. srpna 2017 vznik NUKIB**
- **Říjen 2017 – parlamentní volby**

# NÚKIB

**Ústřední orgán státní správy pro:**

- **kybernetickou bezpečnost**
- **ochranu utajovaných informací v oblasti informačních a komunikačních systémů**
- **kryptografickou ochranu**
- **problematiku neveřejné služby v rámci družicového systému Galileo**

**Sídlo v Brně (3 pracoviště – budoucí výstavba nové budovy v Černých Polích) a dvě pracoviště v Praze**

# NÚKIB

- **Ředitel  jmenovaný vládou po projednání v příslušném výboru PS PČR, odpovědný premiérovi**
- **Ředitel se účastní zasedání BRS, výkonným předsedou RKB A VKB**
- **Právo legislativní iniciativy**
- **Celkem 374 pracovních míst**
- **Rozpočet 611 mil.**
- **Stálá komise PS PČR pro kontrolu NÚKIB**

# NÚKIB

**Struktura úřadu k 1.1.2023 (nejsou uvedeny obslužné útvary)**

**Sekce NCKB**

- **Odbor vládní CERT**
- **Odbor regulace**

**Sekce informačních systémů**

- **Odbor bezpečnosti informačních technologií**
- **Oddělení bezpečnosti satelitních služeb**

**Sekce strategických agent a spolupráce**

- **Odbor mezinárodní spolupráce a EU**
- **Odbor cvičení a vzdělávání**
- **Odbor centrální analytiky**
- **Oddělení národních strategií politik**
- **Oddělení vědy, výzkumu a inovací**

# NÚKIB

**Činnosti odboru centrální analytiky:**

- **Analýza a monitoring kybernetických hrozeb a trendů v kybernetické bezpečnosti**
- **Posuzování jejich politických kontextů či dopady materiálů.**
- **Ve spolupráci s CERT rozvíjí pokročilou analytickou kapacitu v podobě Cyber Threat Inteligence (CTI)**
- **Informační šetření**

# NUKIB

## Činnost oddělení výzkumu a inovací

**Národní plán výzkumu v kybernetické a informační bezpečnosti**

**Dva zdroje financování:**

- **Financováno z rozpočtu NÚKIB – vyčleněno na vědu a výzkum 20 mil. Kč – převážná většina v utajovaném režimu Tempest a krypto**
- **Bezpečnostní výzkum MV (řádově 500 mil Kč. pro všechny oblasti)**
  - **. Výzkumná potřeba státu – řešitelé jsou vybíráni veřejnou soutěží – řešení zůstává majetkem státu**
  - **. Nabídka tématu řešiteli – řešení zůstáva majetkem (příklad KYPO MU)**

**Pozn 1. možné financování přes TAČR - zatím se nevyužívá**

**Pozn 2. Bezpečnostní výzkum MV může být i v utajeném režimu.**

**Pozn 3. Existuje i obranný výzkum MO – zatím se nevyužívá**

# NUKIB

**NUKIB zajišťuje Národní koordinační centrum výzkumu a vývoje v oblasti kybernetické bezpečnosti (NCK) na základě nařízení EU 2021/887**

**NKC působí jako kontaktní místo PRO komunitu na národní úrovni, spolupracuje s CyberSecurity Hub (zapsaný ústav) – sdružení MU,VUT a ČVUT zabývající se kyberbezpečnostním výzkumem a je zároveň členem Digital Innovation Hun Network**

# NUKIB

## Odbor bezpečnosti informačních technologií

**Kryptografická ochrana**

- **Aplikovaný výzkum a vývoj kryptografických prostředků**
- **Analýza a hodnocení šifrových systémů a kryptografických algoritmů určených k ochraně utajovaných informací**
- **Vývoj nových technologií  a výrobních klíčových materiálů a kryptografických prostředků a vývoj v oblasti jejich zabezpečení proti neoprávněné manipulaci při převozu**

# NUKIB

## Odbor bezpečnosti informačních technologií

**Certifikace informačních a komunikačních systémů**

- **Certifikace systémů – 100 z toho 700 aktivních, 90% státní správa, z toho PT a T 15%, D-50%, V-35%**
- **Schvaluje změny v certifikovaných IS cirka 1000 ročně**
- **Tvorba standartů  a metodik ochrany UI v IS**
- **Akreditace IS EU a NATO**

# NUKIB

## Odbor bezpečnosti informačních technologií

**TEMPEST(Telecommunications Electronics Materials Protected from Emanating Spurious Transmissions)**

- **Národní středisko pro měření kompromitujícího elektromagnetického vyzařování (KV) cca 200/rok**
- **Návrh metod a postupů hodnocení el. Zařízení, zabezpečené oblasti nebo objektu proti úniku UI prostřednictvím KV**
- **Certifikace stínících komor cca 20/r**
- **Kontroly jednacích místností k nepovolenému použití technických prostředků určených k získávání informací nebo KV**
- **Určování standardů v oblasti TEMPEST**

**Pozn. V současnosti se zvýšilo riziko laserového odposlechu jak akustického tak obrazového.**

# NUKIB

## Odbor bezpečnosti informačních technologií

**Šifrová služba**

- **Výroba kryptografického materiálu KM) pro provoz kryptografických prostředků (KP)**
- **Evidence KM, pracovníků kryptografické ochrany včetně evidense kompromitace a ničení KM**
- **Národní středisko pro distribuci KM (NDA)**
- **Servis a údržba KP**

**Nová výzva postkvantová kryptografie!!!!!!!!**

# Spolupráce se zpravodajskými službami

- **Problémem jsou částečně společné a částečně odlišné zájmy.**
- **Společný zájem NÚKIBU a kontrarozvědek je ochrana před špionáži a další. (např. ochrana ministerstva zahraničí)**
- **Odlišné zájmy mají zpravodajské služby, které využívají zranitelností pro získávání informací technickými prostředky.**
- **Zájem NÚKIB je získávat informace o zranitelnostech a informovat o tom.**

# Spolupráce se zpravodajskými službami

**Získávání informací o o hrozbách i rizicích a vzájemné poskytování informací.**

- **NÚKIB získává informace ze sítě CERT/CSIRT na základě důvěry, že nebudou zneužity a využijí se k ochraně před kybernetickými útoky.**
- **Zpravodajské služby získávají informace od partnerských služeb a svojí zpravodajskou činností.**
- **Vzájemné poskytování informací díky tomu je složité.**

# Spolupráce s Policií ČR

- **Spolupráce na počátku byla velmi složitá – NÚKIB není vnímán jako partner, ale jako zdroj informací (totéž platí pro i u ZS)**
- **Činnost policie je, že když se dozví o podezření ze spáchání trestného činu, tak zajišťuje důkazy a hledá pachatele.**
- **Činnost a zájem  NÚKIBu v případě kybernetického útoku je zjištění co se stalo, jak se to stalo, proč se to stalo, zamezení dalších škod, co nejrychlejší uvedení IS do bezpečného provozu a varování dalších možných obětí.**
- **Pachatelé jsou převážně v zahraničí a jejich vypátrání a zejména potrestání je prakticky nemožné a mnohdy to jsou státní nebo polostátní aktéři.**
- **Policie o kybernetickém útoku informace vede v trestním spise, ke kterému má přístup kromě ní pouze státní zástupce.**
- **Pokud se dozvíte o podezření z trestném činu, jste povinen informovat policii – problém hlášení GovCERTU.**

# Spolupráce s ostatními orgány státní správy

- **Spolupráce v rámci ZKB.**
- **Spolupráce s MV – v rámci Cloudové vyhlášky a E-govermentu. (DIA)**
- **Spolupráce s Českým statistický úřadem**
- **Spolupráce se Státním úřadem pro jadernou bezpečnost**
- **Spolupráce s řízením letového provozu**
- **Spolupráce s prevencí a vzděláváním**
- **Další**

# Mezinárodní spolupráce

- Spolupráce v GOVCERu v rámci CERT/CSIRT komunity

- Členství v

  FIRST

  TF-CSIRT

  CSIRT NETWORK

# Mezinárodní spolupráce

**Spolupráce NÚKIB**

- **Strategičtí partneři –**

  **USA – FBI,DHS, Ministerstvo obrany, NSA**

  **Jižní Korea – NIS**

  **Izrael - MalMab, National Cyber Burea**

- **Cyber ataché – Washington D.C.,Brusel, Tel Aviv, v přípravě Austrálie**

- **Kapacity NÚKIB v oblasti kybernetické bezpečnosti nástrojem zahraniční politiky ČR**

# Mezinárodní spolupráce

- **NATO**

  **zastupování v pracovních skupinách**

  **připomínkování bezpečnostních standartů**

  **účast na cvičeních**

  **zastoupení v CCD COE v Talinu**

- **EU** **zastupování v pracovních skupinách**

  **spolupráce na evropské legislativě (NIS I. NIS II.)**

  **spolupráce na certifikačních schématech**

  **ENISA – členství managment border**

  **kybernetická bezpečnost – téma Českého předsednictví**

# Mezinárodní spolupráce

**Spolupráce s U.S. společnostmi**

- **BotNet Feed (exkluzivní spolupráce s Microsoft)**
- **Shadowserver (Cisco – výměna dat a informací ohledně malware, botnet aktivit, podvodného jednání, apod**

# Mezinárodní spolupráce

- **Spolu z MZV zastupování v**

  **OSN**

  **OBSE**

  **ITU a další**

- **Organizacování Pražských konferencí Pražské návrhy**

  **2019 - 5G sítě**

  **2020 - 5G sítě – budování sítí**

  **2021 - bezpečnost přelomových technologií**

  **2022 - bezpečnost dodavatelských řetězců**

# „Varování Huawei“

**17. prosince 2018 NUKIB vydal na základě § 18 ZKB Varování před používáním SW a HW společností Huawei Technologies a ZTE Corporation – používání technických a programových prostředků představuje hrozbu v oblasti kybernetické bezpečnosti**.

**Proč bylo vydáno?**

- **Hrozba spočívá zejména v tom, že uvedené společnosti jsou srozuměny upřednostnit zájmy ČLR (KSČ) před zájmy uživatelů jejich technologií (zákazníků), s reálnou možností narušit bezpečnost dat.**
- **Politické a právní prostředí ČLR dává povinnost právnickým a fyzickým osobám podílet se na zpravodajské činnosti státu a napomáhat v prosazování jeho zájmu.**
- **Technologie uvedených společností jsou nebo se mohou nacházet se mohou nacházet v IS a KS strategického významu, přičemž jejich vliv na úroveň bezpečnosti těchto systémů je či může být značný mnohdy zásadní.**
- **Zjištění českých zpravodajských služeb o zpravodajských aktivitách ČLR vlivového a špionážního charakteru.**

# „Varování Huawei“

**Co to znamená?**

- **Prostřednictvím varování NUKIB upozornil na existenci hrozby v oblasti kybernetické bezpečnosti, na kterou je nutno bezprostředně reagovat.**
- **Subjekty, které spadají pod ZKB jsou povinny se touto hrozbou zabývat a zohlednit ji v analýze rizik, kterou jsou v souladu se ZKB a příslušné vyhlášky, které jsou povinny pravidelně provádět.**
- **Varování neznamená bezpodmínečný zákaz používání daných technických a programových prostředků, ale nutnost zvážit případné bezpečnostní riziko související s jeho používáním.**
- **Dovolí-li to výsledky analýzy rizik, uvedené technické nebo programové prostředky je možno i nadále používat.**
- **Orgánům a osobám, kterým ZKB neukládá povinnost zavést a provádět bezpečnostní opatření, stejně jako široké veřejnosti, nezakládá varování žádnou povinnost.**

# „Varování Huawei“

**Co tedy dotčené subjekty měly udělat?**

- **Na základě vydaného varování tedy musí povinné osoby v rámci zavedeného řízení rizik povézt (novou analýzu rizik), ve kterém zohlední hrozbu a následně na riziko reagovat přijetím bezpečnostního opatření, které musí být v souladu s nastavenými metrikami pro akceptovatelnost rizika a hodnotou daného rizika.**

- **Hrozba uvedená ve varování je definována jako velmi pravděpodobná až víceméně jistá. (stupeň 4 ze 4).**

- **Metodika k varováni vydána 4.1. 2018 – konkretizuje možné přístupy správců či provozatelů IS a KS v reakci na vydané varování.**

- **Pokud z analýzy rizik vyplyne riziko, které je neakceptovatelné dle ZKB a vyhlášky, je nutné přistoupit ke konkrétním opatřením.  Může být například postupná náhrada daných technologických prvků a vyloučení společností týká z výběrových řízení.**

# „Varování Huawei“

- **Dvě poznámky:**
- **V analýze rizik dochází k definování hodnoty hrozby, zranitelnosti a dopadu narušení aktiva. Díky výsledné hodnotě rizika organizace identifikuje, zda je nutné pro analyzované aktivum ( to co chceme chránit, např. server, stanici , síťové prvky) zavádět opatření (tedy je více chránit) nebo, zda je riziko akceptovatelné (tedy není třeba potřeba opatření zavádět.**

- **Vztah varování k zákonu o zadávání veřejných zakázek (ZZVZ)- Zadavatel podle ZVZZ nesmí vytvářet při stanovování zadávacích podmínek „bezdůvodné překážky hospodářské soutěže“. Pokud je oprávněnou autoritou tj. NÚKIBem , vydáno varování dle ZKB, nelze pak přijetí vhodných bezpečnostních, kterými může být i vyloučení daných technologií, považováno za vytváření bezdůvodné překážky hospodářské soutěže.**

# „Varování Huawei“

- **Proč bylo varování bylo vydáno „za pět minut dvanáct?**
- **V polovině roku ČTU měl vypsat výběrové řízení na provozování mobilních sítí 5.generace (5G)**
- **Pokud má ČR udržet si konkurenceschopnost a ekonomickou výkonnost budou 5G sítě tvořit páteř její ekonomiky.**
- **V případě, výrobce komponentů sítě 5G umožní přístup k zařízení třetí straně, získá tento aktér schopnost způsobit společnosti a ekonomice ČR masívní škody. I pouhé vědomí (či dokonce odůvodněné podezření) existence takové možnosti může mít dopad na svobodné a suverénní postavení ČR, jak v domácí tak zahraniční politice.**
- **Narušení bezpečnosti sítí 5G bude mít celospolečenské dopady v rovině ekonomické, společenské, strategické a vojenské. Takový efekt je v současné době srovnat snad je s výpadkem elektrické energie.**
- **Pokud bude mít cizí státní či nestátní aktér přístup k páteřním komponentům, může dojít i k manipulaci a pozměňování dat**

# „Varování Huawei“

**Reakce Číny**

- **Návštěva premiéra v sídle HUAWAY – dopis ze stížností**
- **Aktivizace lobistů, včetně na nejvyšších mistech státu**
- **Strašení lobistů, že varování bude mít  nedozírné následky pro ČR**
- **Setkání premiéra s čínským velvyslancem v Průhonicích**
- **Tisková zpráva velvyslance o setkání**
- **Pokusy o mediální kampaň**
- **Výhružný dopis vládě – vyhrožování arbitráží a škodou 40 miliard korun**

  ***(západní ambasadoři pečlivě sledovali so se bude dít)***

**NIC se NESTALO!**

# „Varování Huawei“

- **V podmínkách výběrového řízení na provozování mobilních sítí 5G byla věta: „Mobilní sítě 5G budou s vysokou pravděpodobností Kritickou informační infrastrukturou a bude se na ně vztahovat Zákon o kybernetické bezpečnosti.**

- **Doporučení pro hodnocení důvěryhodnosti dodavatelů technologií do 5G sítí v České republice – společný materiál NÚKIB,MO,MZV,BIS,ˇUZSI a VZ**

- **Připravuje se nové řešení uvedeného problému. NÚKIB dostal úkol vlády připravit Zákon o dodavatelských řetězcích. - Je součástí nZKB**

# „Varování Huawei“

## Mezinárodní souvislosti:

**S nástupem technologií došlo  k zásadnímu obratu v geopolitickém uvažování – rozhodujícím faktorem již není konkrétní území a vliv na něj, ale kontrola infrastruktury. S přechodem k digitalizované společnosti není potřeba kontrolovat území a politické prostředí formou vlády jedné strany či represemi pomocí fyzického útlaku. Celé státy je možné si podmanit kontrolou infrastruktury, která je digitalizovaná. Státní celky a společnost jsou zcela závislé na přenosu informací v době míru, ale především v době politických rozhodnutí a konfliktu. Toto si globální hráči (Rusko ?) uvědomili a měly by si to uvědomiti i menší státy, které jsou předmětem snah ČLR.**

# „Varování Huawei“

## Mezinárodní souvislosti:

**„ Spojence jsme“ ,podle George Masona, státního contractora pro obast čínského vlivu (USA), „Varováním zcela zaskočili a překvapili. Když bylo Varování vydáno, způsobilo jemně řečeno poprask v komunitě bezpečnostních složek a vlády, neboť měli za to, že ČR je jež ve sféře politického vlivu ČLR.“**

**Dle tvrzení Huawai zprávu o Varování četlo na světě 750 mil. lidí.**

**Američany a spojence překvapili principem  Varování, který označili za novátorský a univerzální. V podstatě šlo o ukázku nejlepšího postupu (best practise). V té době se hodně hovořilo o technických důkazech. Varování primárně nepotřebovalo technické důkazy. Šlo cestou analýzy strategického zájmu a právního prostředí ve kterém se firmy pohybují. Technické důkazy byly pouze podpůrné.**

# „Varování Huawei“

- **Mezinárodní souvislosti:**
- **Před Varováním:**
- **Austrálie opatrně nejmenovitě nepřímo vyřadilo čínské firmy z 5G sítí.**
- **Francie v tichosti problém měla vyřešen zákonem o odposleších.**
- **USA – řada dílčích opatření**

- **Varování rozproudilo na „Západě“ intenzivní diskuzi, „došlo k prolomení ledu“.**
- **Názory se postupně se v jednotlivých státech postupně měnily. Intenzivní boj mezi „bezpečáky“ a „ekonomy“. Např. UK a Německo)**
- **USA – prezidentské dekrety**
- **Diskuze v Komisi EU**

# „Varování Huawei“

## Mezinárodní souvislosti:

**Pražská konference o bezpečnosti sítí 5G – květen 2019 – doporučení nazvané „Prague Proposals“ (vymahatelnost práva, otevřenost, monitorovatelný dodavatelský řetězec, omezení státní podpory a podobně) vytvořilo další prostor pro debaty v rámci EU, NATO a OSN.**

**26.9.2019 – Doporučení Komise EU (5G toolbox):**

- **Posoudit bezpečnostní rizika ovlivňující 5G sítě**
- **Určit nejzranitelnější prvky**
- **Přezkoumat bezpečnostní požadavky a bezpečnostní hrozby**
- **Vzít v potaz technické i netechnické aspekty včetně politického rámce**

# Evropská komise

Evropská komise vydala v roce 2023 dokument, který mapuje pokrok členských zemí při adopci tzv. „5G Toolboxu“ – souboru pravidel a opatření, jak se vypořádat s rizikovými dodavateli infrastruktury do operátorských 5G sítí. Zpráva uvádí, že 24 členských států přijalo nebo připravuje legislativní opatření, která vnitrostátním orgánům udělují pravomoc provádět posuzování dodavatelů a zavádět omezení. Z těchto 24 států již 10 omezení zavedlo a 3 v současné době připravují provedení vlastních předpisů v této oblasti (sem patří i Česká republika).

Komise ve svém sdělení zdůrazňuje, že je velmi znepokojena riziky, která pro bezpečnost Unie představují někteří dodavatelé komunikačních zařízení mobilních sítí a poprvé otevřeně jmenuje čínské společnosti Huawei a ZTE. Vzhledem k významu infrastruktury pro konektivitu digitální ekonomiky a k závislosti mnoha kritických služeb na sítích 5G by členské státy měly všechna opatření ze souboru neprodleně zrealizovat.

Pozn. Ochota některých operátorů v ČR nahradit potenciálně rizikové technologie v jejich sítích je nízká. Prostřednictvím vlastní asociace APMS operátoři poukázali, že kompletní náhrada technologií Huawei (včetně radiové přístupové části sítě – vysílačů) v jejich sítích by si vyžádala 18 miliard korun. Asociace preferuje vyloučení Huawei pouze z jádra sítí, nikoli z vysílačů, což by znamenalo údajně pouze desetinu uvedených nákladů. S kompletním nahrazením čínských technologií aktuálně z českých operátorů počítá pouze O2, resp. sesterská společnost CETIN, která postupně do své mobilní sítě instaluje výhradně zařízení od švédského Ericssonu.

*„V rekordním čase jsme byli schopni snížit nebo odstranit naši závislost v jiných odvětvích, například v energetice, ačkoli se mnozí domnívali, že to není možné. Situace v případě sítí 5G by se neměla být jiná: kritickou závislost v tomto ohledu si nemůžeme dovolit, jelikož by se mohla obrátit proti nám. Pro naši společnou bezpečnost by to bylo kvůli zvýšené zranitelnosti příliš vážné riziko. Vyzývám proto všechny členské státy a telekomunikační operátory, aby neprodleně přijali nezbytná opatření.“*

**Thierry Breton, komisař pro vnitřní trh**

# Další varování NÚKIB

- **Varování před hrozbou kybernetických útoků na strategické organizace v České republice**
- **Varování před použitím chytrých elektroměrů ze zemí s nedůvěryhodným právním prostředím**
- **Varování v souvislosti s ekonomickými sankcemi spojenými s Ruskou federací**
- **Varování v souvislosti s aplikací TikTok**

# Dotazy?
# Diskuze!