VÝZNAM MEZINÁRODNÍ SPOLUPRÁCE

Lucie Kadlecová, M.A.
NCKB / Institut mezinárodních studií,
Fakulta sociálních věd, Univerzita Karlova

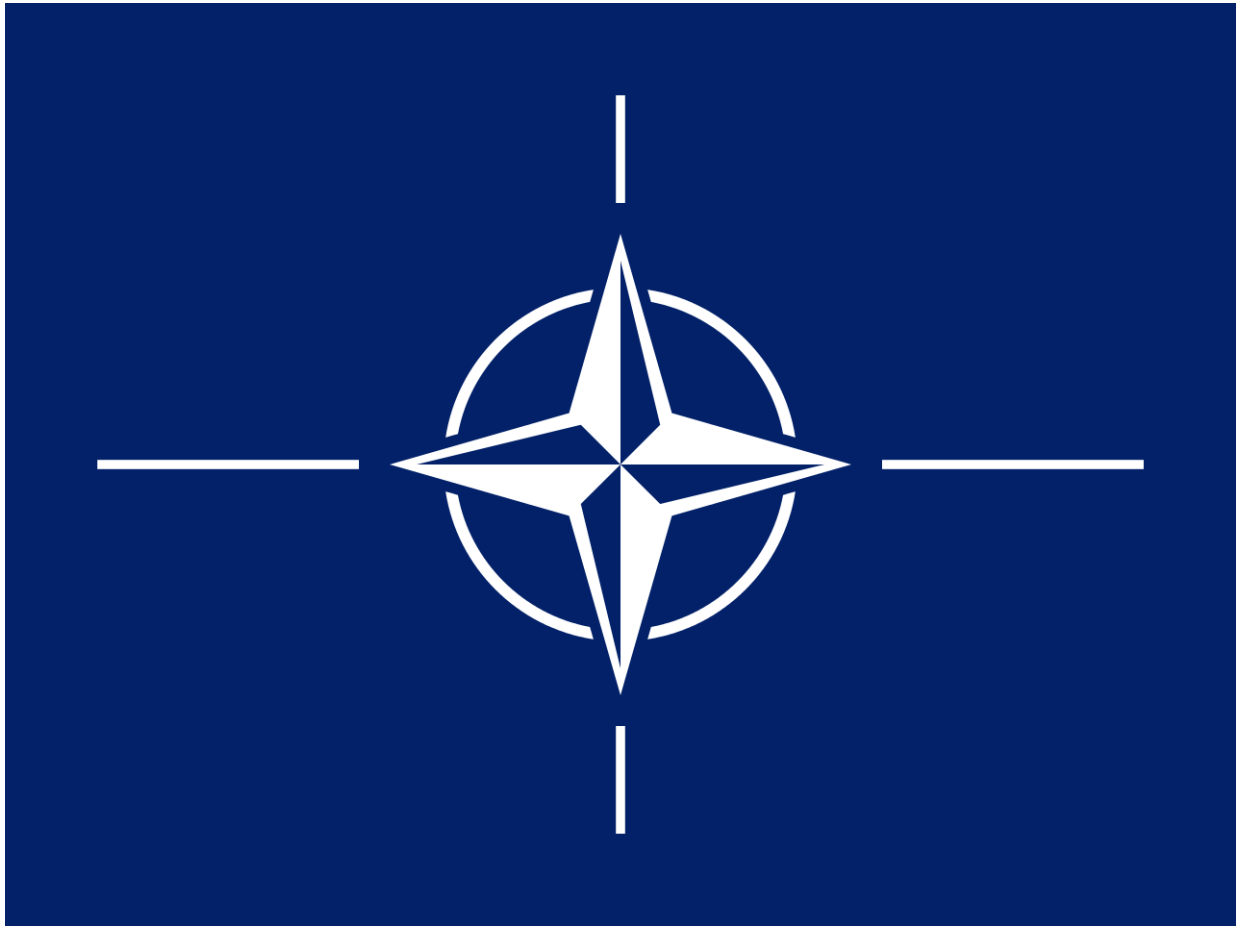
Národní centrum kybernetické bezpečnosti

Obsah

- Bilaterální úroveň
- Multilaterální úroveň:
  - NATO
  - EU
  - OBSE
  - OSN

Bilaterální spolupráce

- **ČR a druhý stát**
  - Např. Memorandum of Understanding mezi ČR a Izraelem (1/2015)
- **ČR a mezinárodní organizace**
  - Např. Memorandum of Understanding mezi ČR a NATO (10/2015)



NATO – obecný přehled

- **Historie**:
  - NATO summit v Praze (2002) – KB poprvé součástí politické agendy
  - 1/2008 – první Policy on Cyber Defence (reakce na Estonsko 2007)
  - 6/2011 – druhá Policy on Cyber Defence
  - NATO summit v Walesu (2014) – třetí, Enhanced Policy on Cyber Defence
  - 10/2015 – podpis CZE-NATO Memorandum of Understanding
  - NATO summit ve Varšavě (2016) - ?
- **Základní principy**:
  - KO nedílnou součástí kolektivní obrany NATO
  - NATO je odpovědné pouze za ochranu svých vlastních komunikačních sítí → jako prostředek pasivní kybernetická obrana (resilience-based CD)
  - Členské státy jsou zodpovědné za bezpečnost svých vlastních komunikačních sítí
  - Aktuální důraz na: zintenzivnění spolupráce s průmyslem, vzdělávání, trénink a výcvik/cvičení

NATO Enhanced Policy on Cyber Defence

- **Mezinárodní právo** aplikovatelné v kybernetickém prostoru
- **Art 5 Washingtonské smlouvy** v případě kybernetického útoku dosahujícího srovnatelných efektů jako konvenční útok
- **Spolupráce s průmyslem** (NICP)
- **Asistence spojencům** při zajištění potřebné úrovně KO na národních KII
- **Rozvoj schopností a kapacit NATO** v kybernetickém prostoru:
  - Smart Defence projekty
  - Vzdělávání (CCDCoE, NATO CISS, NATO School Oberammergau…)
  - Cvičení (Cyber Coalition, Locked Shields ...)
- **Spolupráce s partnery**:
  - Mezinárodní organizace (EU, OSN, OBSE…)
  - Bilaterálně (Science for Peace and Security projekt s Jordánskem, …)

NATO Cooperative Cyber Defence Centre of Excellence

- Mezinárodní vojenská organizace, založena 2008 v Talinu
- **Cíl**: pozvednout schopnosti, spolupráci a sdílení informací v rámci NATO a mezi členskými zeměmi a partnery na poli KO skrze E&T, R&D, konzultace a lessons learned
- **Co nabízí**:
  - **Talinský manuál** 1.0 a 2.0
  - Conference on Cyber Conflict (**CyCon**)
  - Interaktivní databáze **INCYDER**
  - **Cvičení**
  - **Výzkum** (technický, policy, právo)
  - **Kurzy** (technické/netechnické)

NATO CD Stakeholders

Box 4. NATO Cyber Defense Stakeholders

NATO HQ Emerging Security Challenges Division
Deals with the growing range of nontraditional risks and security challenges such as terrorism, the proliferation of WMD, nuclear policy, cyber defense, and energy security.

NATO Communication and Information Agency (NCIA)
Through NCIRC Technical Center, it assumes the Alliance's cyber defense and provides analysis and concept development through experimentation and capability development in cyber defense. NC3A was merged into NCIA in July 2012.

NATO C3 Board
Multinational policy body in the consultation, command, and control area.

Allied Command Transformation
Responsible for doctrine development, scientific research, experimentation, and technological development. Assesses the viability and value of new operational concepts. NATO coordinates the work of CCD COE via ACT.

Cooperative Cyber Defense Center of Excellence
Enhances the capability, cooperation, and information sharing in cyber defense through education, research, development, lessons learned, and consultation.

Formal Governance

North Atlantic Council
Principal political decision-making authority for policy and operational questions requiring collective decisions in the cyber defense area.

↕

Cyber Defense Committee
The lead committee for political governance and cyber defence policy in general, providing oversight and advice to allied nations on NATO's cyber defense efforts at the expert level.

↕

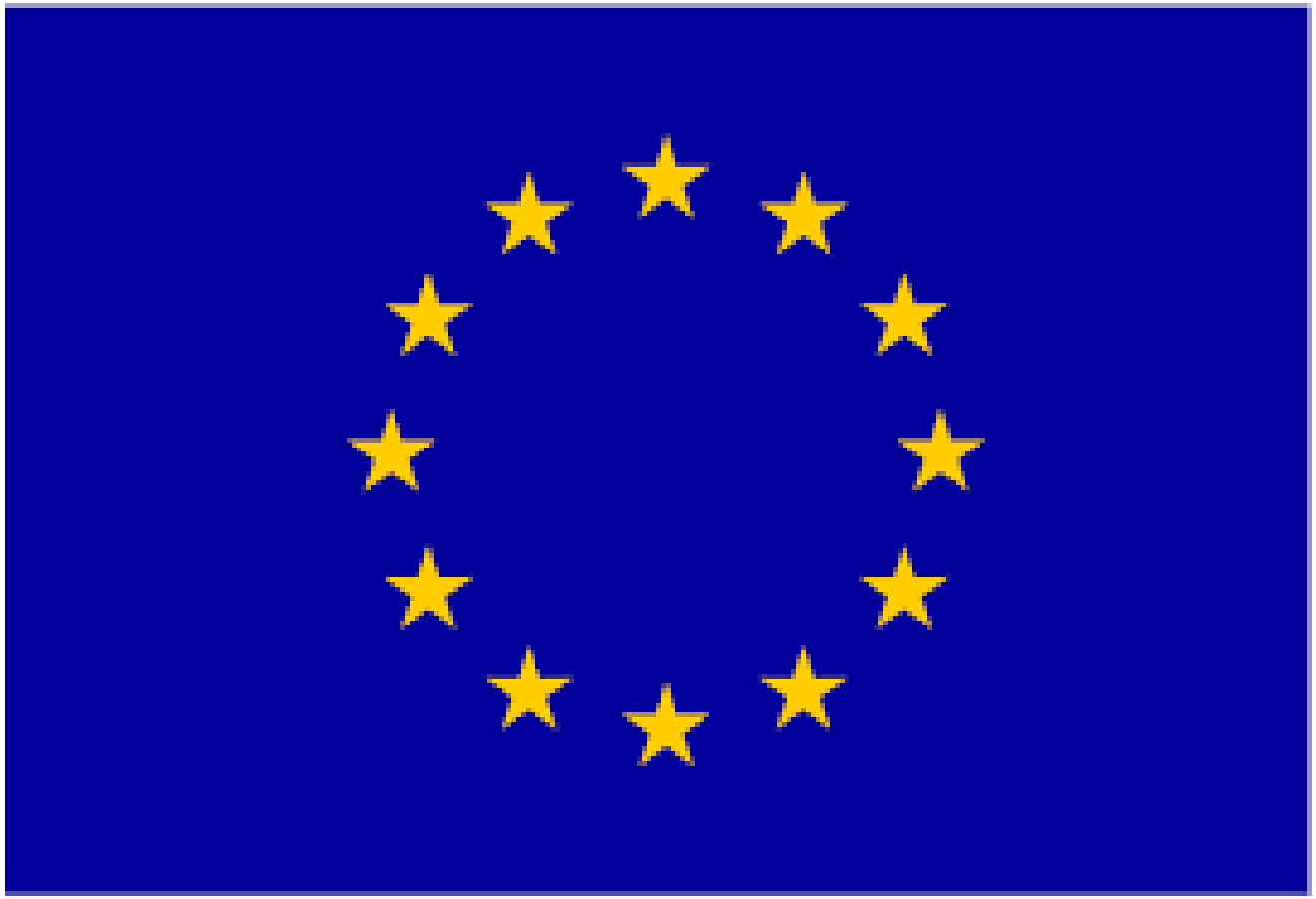
Cyber Defense Management Board
Assembles leaders of NATO political, military, operational, and technical staffs with responsibilities for cyber defense. The board coordinates cyber defense throughout NATO civilian and military bodies. Operates under auspices of HQ NATO ESCD.

↕

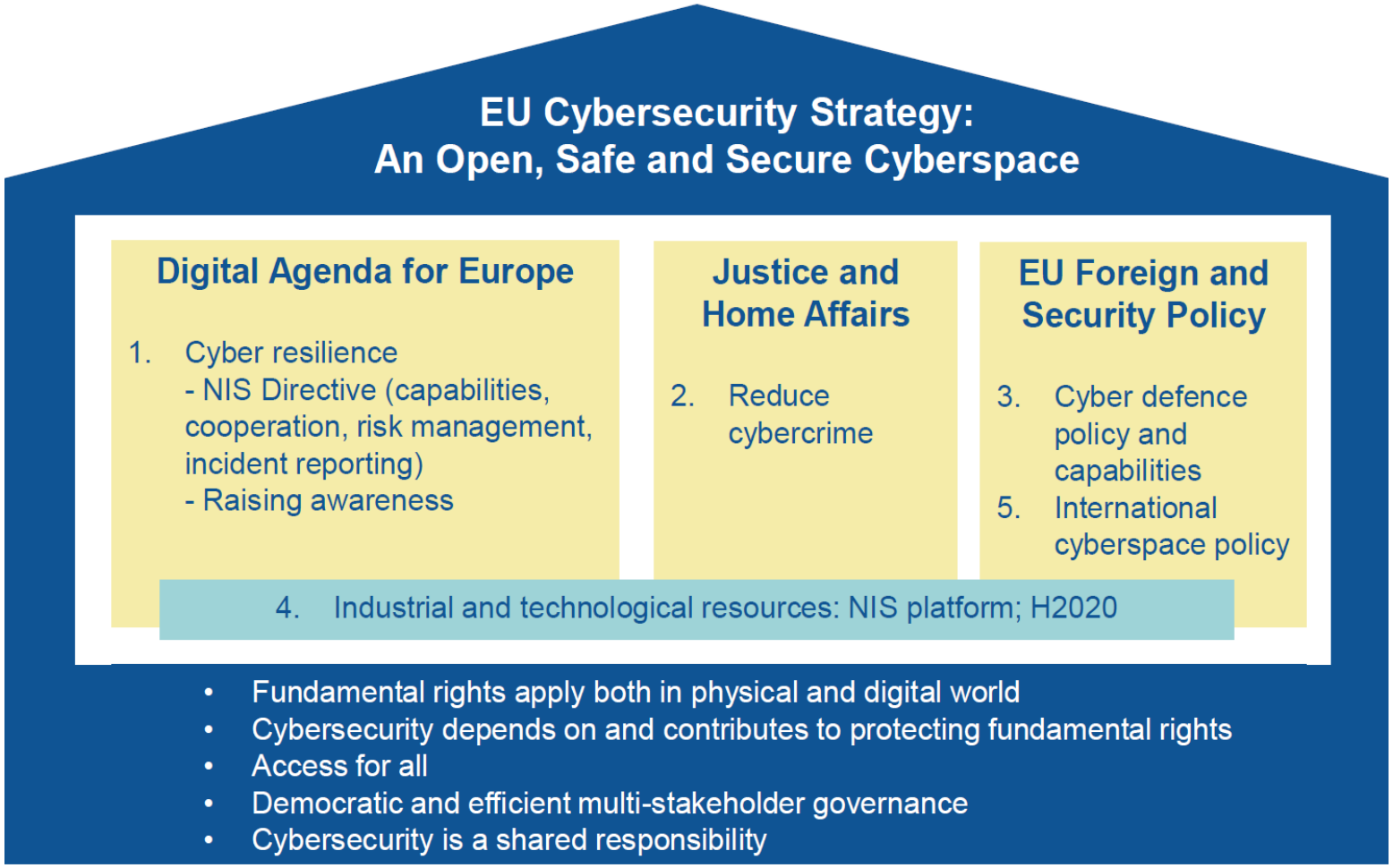
NATO Computer Incident Response Capability (NCIRC)
Provides centralized protection and round the clock cyber defence support to NATO static and deployed HQs, agencies, and national networks.

Source: Various official NATO and NATO PA websites.

Zdroj: *NATO's Cyber Capabilities* by Jason Healey and Klara Tothova Jordan (Atlantic Council, 2014)



EU Cybersecurity Strategy



Evropská agentura pro informační a síťovou bezpečnost (ENISA)

- Založena 2004, sídlo v Heraklionu (Kréta)
- Hlavní zaměření na technický element
- **Cíl: dosáhnout vysoké úrovně informační a síťové bezpečnosti v rámci EU** → napomáhá EU a členským státům posilovat obranyschopnost proti kybernetickým hrozbám

  \+ ENISA jako „hub“ pro výměnu informací a best practices
- **3 hlavní oblasti činnosti**:
  - **Poradenství** a asistence EK a členským státům na téma KB
  - **Sběr a analýza dat** o bezpečnostních incidentech v Evropě
  - **Podpora obecného povědomí** a vzájemné spolupráce mezi relevantními subjekty (EU instituce, členské státy, business) – např. semináře, školení, guidelines, EU cvičení Cyber Europe

European Cybercrime Centre (EC3)

- Součástí **EUROPOLu**
- **Cíl**: boj proti kybernetické kriminalitě
- **3 hlavní oblasti zájmu**:
  - Kyberzločin spáchaný organizovanými skupinami
  - Kyberzločin způsobující značnou škodu oběti
  - Kyberzločin, jež má vliv na KI a informační systémy EU
- **Aktivity**:
  - „hub“ pro sdílení informací
  - Podpora vyšetřování v členských státech (např. digitální forensní analýza)
  - Analýzy na strategické úrovni
  - Spojovací článek pro relevantní subjekty (soukromý sektor, akademie, law enforcement atd.) → reprezentace evropské komunity law enforcementu
  - …

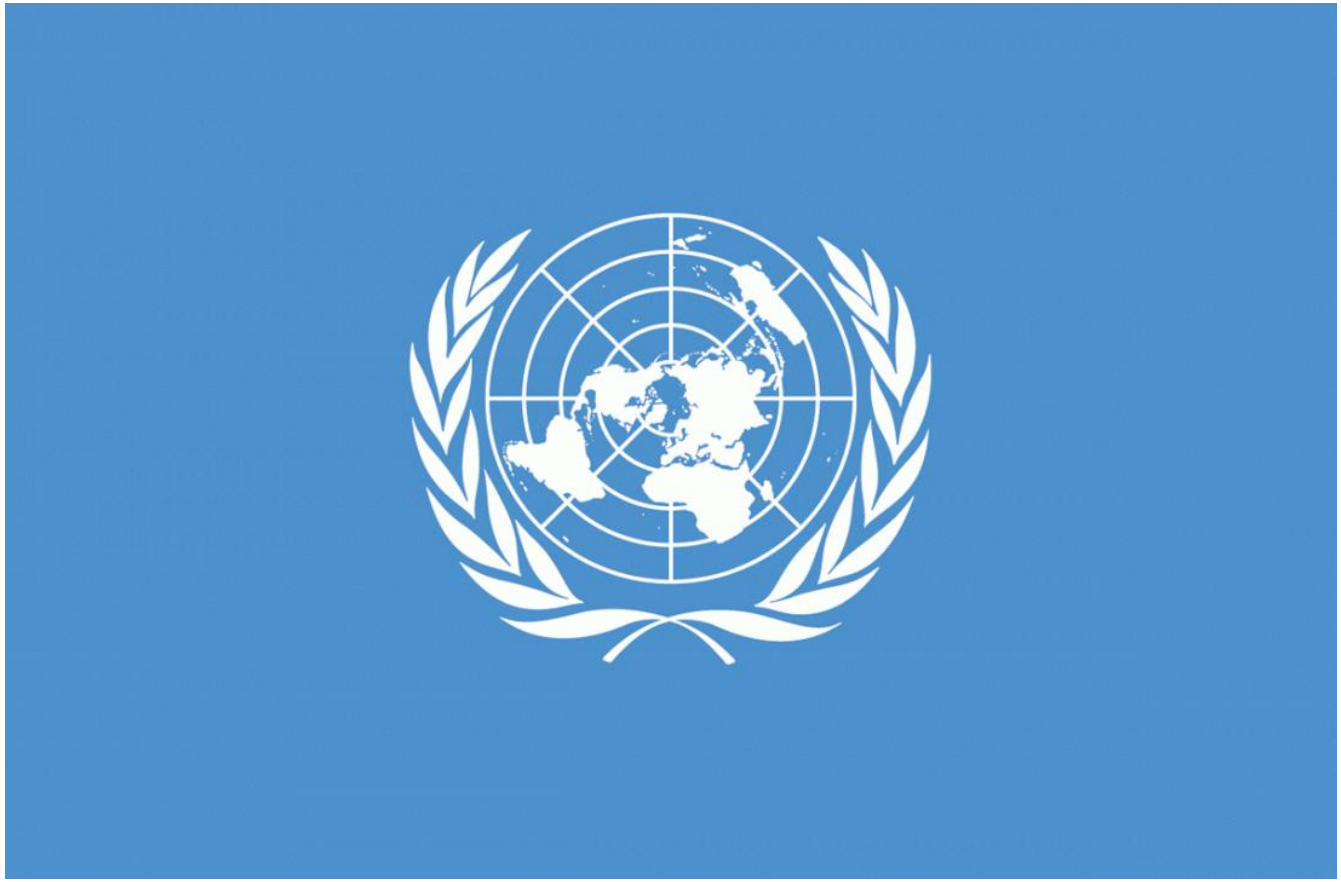
CERT-EU

- **Computer Emergency Response Team pro EU instituce**, agentury a ostatní jednotky
- Založen 2012 na základě *Digital Agenda for Europe*
- IT experti z hlavních EU institucí (EK, Rada, EP, Výbor regionů, ENISA…)
- **Hlavní úkoly**:
  - Spolupráce s CERTy členských států a specializovanými IT bezpečnostními firmami
  - Efektivní a rychlá reakce na kybernetické incidenty a hrozby → 24/7


osce

OBSE

- **3 oblasti zájmu:**
  - **Counter-terrorism**
  - **Kybernetický zločin**
  - **Confidence-building measures (CBMs) for cyber space**
    - Inciativa z 12/2013
    - Cílem potlačení konfliktů, jejichž existence nebo vývoj pramení z používání informačních a komunikačních technologií
    - Zahrnuje např.: výměnu informací o kybernetických hrozbách, zajištění otevřeného a bezpečného internetu, výměnu POCs, využití OBSE jako platformy pro dialog



OSN

- Silně **fragmentované** aktivity
- Dosud žádná rezoluce RB, **pouze rezoluce VS**:
  - Economic and Financial Committee
  - Social, Humanitarian and Cultural Committee
  - Disarmament and International Security Committee
    - Od 1998 Rusko každý rok předkládá draft **„Developments in the field of information and telecommunication in the context of Security“** → základ pro **Group of Government Experts** (2001)
- Stále neexistuje konsensus ohledně aplikace mezinárodního práva do kybernetického prostoru
  - Viz 2011 a 2015 Shanghai Cooperation Organisation a návrh **International Code of Conduct for Information Security**

Group of Governmental Experts (GGE)

- **1. GGE (2004)**
  - Bez konsensu
- **2. GGE (2009)**
  - Shoda na potřebě pokračovat v diskuzi o normách řešících hrozby v kybernetickém prostoru
- **3. GGE (2012-3)**
  - Potvrzena aplikovatelnost mezinárodního práva do kybernetického prostoru
- **4. GGE (2015)**
  - Návrh norem pro responsible behaviour
  - Komentář k aplikovatelnosti mezinárodního práva do cyber
  - Speficikace normativního rámce pro použití cyber capabilities státy
  - Doporučený seznam dobrovolných CBMs
- **5. GGE (2016?)**

International Telecommunication Union (ITU)

- **Specializovaná agentura OSN** pro informační a telekomunikační technologie
- 193 členů OSN + 700 zástupců telekomunikačního sektoru
- **Cíle** (mimo jiné):
  - Shoda na globálních technických telekomunikačních standardech
  - Alokace radio frekvencí
  - Zlepšení telekomunikační infrastruktury
- **World Conference on International Telecommunications** (2012, Dubaj)
  - **Revize International Telecommunication Regulations** (původně z 1988)
  - Výsledek: **neshoda vzhledem k rozdílným názorům na internet governance a kontrolu obsahu** → smlouva podepsána pouze 89 členy, přičemž v opozici zejména USA a EU

Děkuji za pozornost

Lucie Kadlecová, M.A.

Lucie.Kadlecova@nbu.cz