BACKGROUND REPORT

Kybernetická bezpečnost

Marie Šmejkalová
marie.smejkalova@amo.cz

#SUMMIT26

PRAŽSKÝ STUDENTSKÝ SUMMIT

AMO.CZ

1 JAK ČÍST BACKGROUND?

Tento background report vznikl pro účely simulovaného jednání Výboru pro odzbrojení a mezinárodní bezpečnost OSN na Pražském studentském summitu. Má zejména pomoci delegátům se sepsáním stanoviska jimi zastupovaného státu a slouží jako základní zdroj informací k dané problematice. Background se zaměřuje na hlavní aspekty kybernetické bezpečnosti jako například na kybernetickou diplomacii. Dále se věnuje i historickému vývoji kybernetické bezpečnosti a současnému světovému trendu v této oblasti. Byl napsán v červenci roku 2020 a z tohoto důvodu mohou některá obsažená data nebýt aktuální.

2 ÚVOD

V době enormního rozmachu internetového připojení všude ve světě je otázka zabezpečení kyberprostoru důležitější než kdy dříve. Státům, a to zejména rozvojovým, chybí prostředky a schopnosti na to, aby zvládly zaručit bezpečnost svých občanů online. Toto se netýká jen uživatelského přístupu k internetu, ale i finančního či bezpečnostního sektoru. OSN v současné době usiluje o vytvoření jednotného postupu členských států v otázce kybernetické obrany a o prohloubení spolupráce mezi jednotlivými státy.[1]

Pro začátek je zcela zásadní vymezit termín kyberprostor. Podle Výzkumného institutu OSN pro otázky odzbrojení (UNIDIR) se jedná o téměř vše od osobních počítačů až po internetové sítě, satelity, telefony či dokonce televize. Obecně by se dalo definovat, že se jedná o technologie a sítě, které je spojují a propojují. Častou chybou je označovat kyberprostor pouze jako internet, ten je totiž jen jednou z jeho částí.[2]

Dalším důležitým termínem, jehož definici je třeba představit, je kybernetická bezpečnost. Podle Mezinárodní telekomunikační unie (ITU) se jedná o shromažďování nástrojů, bezpečnostních konceptů a záruk a přístupů k řešení rizik. Hlavním cílem kybernetické bezpečnosti je tak snaha o dosažení a hlavně udržení bezpečnosti uživatelů komunikačních technologií a potírání největších bezpečnostních rizik v kyberprostoru.[3]

Termínem, který s kybernetickou bezpečností úzce souvisí, je státní suverenita. Nejedná se výhradně o politický, právní, či strategický koncept, ale v praxi spíše o kombinaci všeho výše zmíněného. Obecně určuje, že každý ze států je autonomní a žádný z jiných států nemá právo intervenovat za svými hranicemi. Toto pojetí suverenity vzniklo již kolem roku 1648 s podepsáním Vestfálského míru. Některé ze států – například Rusko, Čína, Saudská Arábie či Francie – souhlasí s tím, aby se i ke kyberprostoru přistupovalo jako k fyzickému teritoriu, a odmítají tak cizí vměšování.[4]

V běžné praxi jde totiž o to, že vládní i nevládní organizace daného státu umožňují, ale zároveň i kontrolují pohyb informací, osob či kapitálu přes hranice. Zde ale v případě kyberprostoru nastává další problém – je velmi těžké, pokud ne nemožné, uhlídat veškerá data a informace.[5]

Kdyby došlo k pokusu o velmi striktní jurisdikci ve vestfálském stylu, internet a kyberprostor samotný by se musel velmi omezit a limitovat pouze na národní užití. Veškeré servery by musely být umístěny jen v daných zemích a veškerý software by bylo nutno certifikovat pro jednotlivé země. V současnosti je struktura internetu silně globalizovaná a cesta zpět by byla velmi náročná.[6]

3 PRVNÍ VÝBOR A KYBERNETICKÁ BEZPEČNOST

Jelikož se jedná o téma velmi rozsáhlé a komplikované, Výbor pro odzbrojení a mezinárodní bezpečnost (DISEC) není ani zdaleka jedinou institucí, která se touto problematikou zabývá. Kromě Rady bezpečnosti, která se specializuje spíše na zneužitelnost internetu teroristickými organizacemi, se kybernetickou bezpečností zabývá i Hospodářský a finanční výbor, jehož hlavní agendou je udržitelný rozvoj, či případně Sociální, humanitární a kulturní výbor, který se zase specializuje spíše na lidskoprávní aspekt či prevenci internetového zločinu.[7]

DISEC se v řešení tohoto problému angažuje dvěma různými způsoby. Tím nejvýraznějším je vytvoření takzvaných skupin vládních expertů (GGEs), které existují již od roku 2003. Druhým přístupem, který DISEC aplikuje, je každoroční přijetí návrhu rezoluce pro Valné shromáždění „Developments in the Field of Information and Telecommunications in the Context of International Security" (Nejnovější vývoj v oblasti informací a telekomunikací v kontextu mezinárodní bezpečnosti).[8]

3.1 Skupiny vládních expertů (Groups of Governmental Experts)

Hlavní snahou DISEC je ale zajištění mezinárodní bezpečnosti, což v tomto konkrétním případě zajišťují i takzvané GGEs, neboli Groups of Governmental Experts (skupiny vládních expertů). Již v roce 2003 rezoluce Prvního výboru volala po vytvoření skupin odborníků, které se budou problematice kyberprostoru věnovat. Tito experti se měli věnovat výzkumu potenciálních rizik (zejména napadení kyberprostoru či ohrožení bezpečnosti jednotlivých států) v této sféře a doporučovat kroky k jejich vyřešení.[9] Počet expertů se s každou skupinou (k dnešnímu dni je skupin pět) zvyšuje a nyní jich je již dvacet pět. To nasvědčuje faktu, že GGEs se s postupem času přisuzovala větší a větší důležitost, a ač jsou jejich zprávy pouze doporučujícího charakteru, berou se velmi vážně, protože mají napomoci k vybudování stabilnějšího kyberprostoru.[10] V roce 2015 mezi závěry zprávy patřilo zejména zdůraznění nutnosti mezistátní kooperace. Zpráva sice říká, že každý stát by se měl snažit zabezpečit svůj vlastní kyberprostor, ale zároveň

poukazuje na to, že mezinárodní spolupráce může v mnoha ohledech pomoci.[11]

3. 1. 1 Druhá skupina

První skupina byla ustanovena již na začátku 21. století, v roce 2004. Nicméně odborníci nebyli schopni dojít žádného konsenzu, a proto mezi roky 2009 a 2010 vznikla skupina druhá, složená z expertů z Běloruska, Brazílie, Číny, Estonska, Francie, Německa, Indie, Izraele, Itálie, Kataru, Korejské republiky, Spojeného království a Spojených států. Tato skupina se sešla čtyřikrát a během každého setkání řešila poslední vývoj v kybernetické oblasti. Dokument, který z těchto setkání vzešel, konstatoval, že kyberprostor se stal prakticky „arénou" pro nelegální, či alespoň šedé aktivity. Podle expertů se jednalo o ilegální činnost v různých oblastech, kdy nejzávažnější z nich byly krádeže peněz. Zároveň dokument poukazoval na to, že hrozby mohou představovat nejen státy samotné, ale i nelegální organizace a potenciálně i teroristé. Nicméně, protože se jedná o zprávu z doby před deseti lety, teroristická aktivita v kyberprostoru ještě nebyla tak výrazná. Dnes, když má přístup na internet většina lidí na světě (v březnu 2020 se počet aktivních uživatelů internetu pohyboval kolem 4,8 miliardy, což představuje přibližně 62 % světové populace[12]), je pro teroristické organizace (jedná se například o Islámský stát) mnohem jednodušší šířit svou ideologii, rozšiřovat své řady a radikalizovat touto cestou osoby prakticky všude na světě.[13]

Jedna z velmi zásadních věcí, které zpráva zdůraznila, je fakt, že státy kyberprostor využívají jako další místo pro vedení válek a pro politickou agitaci.[14] Svým způsobem by se dalo říct, že v kyberprostoru probíhá nový vesmírný závod. Pouze se tentokrát nejedná o to, kdo se dříve dostane do kosmického prostoru, ale o to, kdo bude mít pokročilejší a lépe zabezpečený kyberprostor. Zabezpečení kyberprostoru je samozřejmě velmi zásadní, ale přesto pro mezinárodní společenství není nový závod zcela žádoucí. Aby se novému závodu zabránilo, zpráva zejména zdůrazňuje nutnost kooperace na mezistátní úrovni.[15]

3. 1. 2 Třetí skupina

Řádný právní a politický přesah měla ale až skupina třetí, která fungovala mezi lety 2012 a 2013. Experti dospěli k rozhodnutí, že současné mezinárodní právo platí i v kybernetickém prostoru. Hlavní dokument, na který se odvolávali, je Charta OSN, jejíž zásady mají platit i v tomto případě.[16]

Vcelku zásadní koncept, o kterém zpráva hovoří, je problematika suverenity, která zde již byla zmíněna. Jelikož kyberprostor je velmi fluidní a fyzické státní hranice neplatí, bylo třeba vymezit i toto. Státy by se tak měly vyvarovat zasahování do záležitostí kybernetické bezpečnosti cizích států. Zároveň je však nezbytná kooperace mezi státy, a to z úplně stejného důvodu – kyberprostor není fyzicky ohraničen.[17]

Mezistátní spolupráce je jedním z hlavních pilířů celé zprávy, která podtrhává zejména nutnost předávání informací o zabezpečení kyberprostoru a důležitost dalšího vylepšování spolupráce. Kromě již existujících komunikačních kanálů by tak měly vzniknout kanály nové, jimiž by se daly opět šířit nejnovější přístupy ke kybernetické bezpečnosti, o nichž by se dále mohlo v mezinárodním prostředí hovořit[18]

Vzhledem k tomu, že v této době došlo k odhalení několika narušení kyberprostoru ze strany států, byly výsledky zprávy více než žádané. Nebylo výjimkou, že státy prováděly hospodářskou či politickou špionáž právě v prostředí kyberprostoru. Jelikož vzájemná špionáž jen prohlubovala nedůvěru mezi státy na bilaterální úrovni, návrhy na určitou politickou spolupráci byly napříč mezinárodním společenstvím jen vítány.[19]

3. 1. 3 Čtvrtá GGE

Možná trochu neočekávaně je státem, který se v této oblasti nejvíce angažuje, Ruská federace. Vytvoření čtvrté skupiny mezi lety 2014 a 2015 pocházelo hlavně z její iniciativy. Tentokrát už se počet expertů navýšil a nově jich bylo celkem dvacet. Skupinu od začátku provázela nedůvěra ze strany členských států OSN, kterou vzbudily další intervence států (a to včetně členů Rady bezpečnosti) do kyberprostorů jiných států (např. intervence Ruské federace v ukrajinských prezidentských volbách roku 2014 atd.).[20] Jedním ze zdůrazňovaných bodů zprávy je tak zákaz intervence mimo vlastní teritorium, aby se zabránilo narušení suverenity.[21]

Zpráva dále konstatuje, že například rozvojové státy nemohou být schopny zajistit si takovou kybernetickou bezpečnost jako státy ostatní a nelze tak po nich (v současné chvíli) vyžadovat to stejné, co po státech, které mají dostatečnou finanční kapacitu.[22]

Poslední skupina se sešla mezi roky 2016 a 2017. Bohužel, během této doby nebylo dosaženo žádného konsensu. Nejčastější spory se týkaly aplikace mezinárodního práva či přístupu k suverenitě.[23]

3.2 Nejnovější vývoj v oblasti informací a telekomunikací v kontextu mezinárodní bezpečnosti

Rezoluce, které DISEC již od roku 1998 každoročně přijímá, se věnují nejnovějšímu vývoji na poli mezinárodní bezpečnosti. Obsah rezolucí se za posledních 22 let samozřejmě změnil. V roce 1998 rezoluce pouze hovořila o významném vývoji na poli kybernetiky, zároveň ale zdůrazňovala obavu, která spočívala ve strachu ze zneužitelnosti nových technologií. Už tehdy ale volala po spolupráci mezi jednotlivými státy. Na multilaterální úrovni se měly státy dělit o své znalosti a vědomosti, které se potenciálních hro-

zeb týkaly.[24] O rok později již rezoluce hovořila i o potenciální zneužitelnosti teroristickými organizacemi a dále volala po mezistátní spolupráci.[25]

V roce 2000 pak již rezoluce otevřeně hovořila o strachu, který přinášelo hlavně možné zapojení informačních a komunikačních technologií do ilegálních aktivit. Ohrožení světové bezpečnosti a vliv na bezpečnost jak státních, tak soukromých aktérů se stalo jedním z primárních témat Prvního výboru.[26]

Jak již bylo zmíněno výše, rezoluce z roku 2003 přinesla asi nejvýraznější posun. Díky této rezoluci byla založena první, i když neúspěšná, skupina vládních expertů.[27] Následující vývoj v oblasti kybernetické bezpečnosti pak byl do jisté míry ovlivněn právě těmito skupinami.

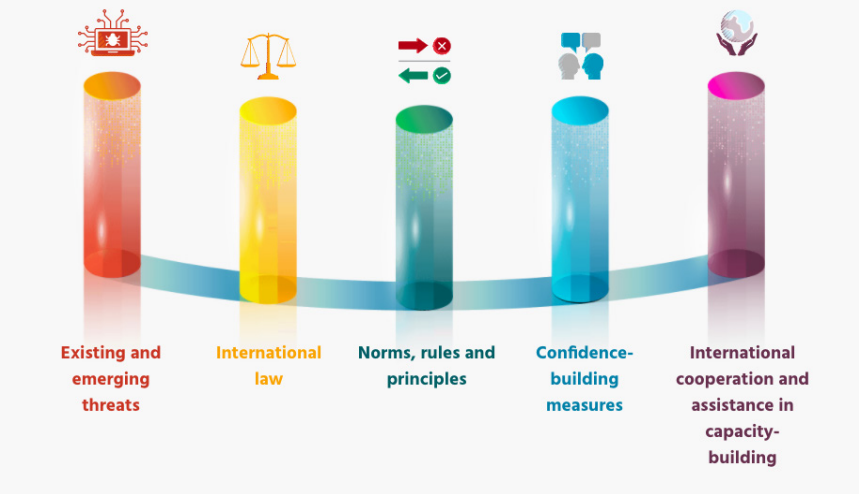
Novější rezoluce, včetně té poslední z prosince 2019, se už problémem zabývají mnohem konkrétněji. Důraz je přednostně kladen na využití informačních technologií pro mírové účely a také na to, aby se zabránilo konfliktům majícím kořeny právě v kyberprostoru. Mnohem větší důraz se teď klade i na samotnou OSN, která má být mediátorem pro všechny státy. Opět má docházet k podpoře dialogu, aby i méně vyspělé státy měly šanci na stejné pochopení kyberprostoru jako státy, které jsou v této oblasti pokročilejší.[28]

V posledních dvou letech vznikla ještě jedna rezoluce, která se tentokrát věnovala podpoře zodpovědného chování států v kybernetickém prostoru (Advancing Responsible State Behaviour in Cyberspace in the Context of International Security). Jak už název napovídá, rezoluce se specificky zabývá přístupem jednotlivých států, avšak upozorňuje i na důležitost mezistátní kooperace. Velmi často se v ní skloňují doporučení skupin vládních expertů, podle kterých se mají jednotlivé členské státy řídit.[29]

4 KYBERNETICKÁ DIPLOMACIE

Jednou z neodmyslitelných částí mezinárodní kooperace je i kybernetická diplomacie. Jedná se o relativně nový koncept, který začal být častěji využíván až s masivnějším nástupem internetu na počátku 21. století.[30]

Samotná definice kybernetické diplomacie je velmi složitá, protože se stále jedná o relativně neprobádanou oblast, ale obvykle se popisuje jako využití diplomatických schopností v kybernetickém prostoru. Toto by mělo pomoci dosáhnout zájmů jednotlivých států stejně jako diplomacie běžná. Nejčastěji jsou vyzdvihována témata jako kybernetická bezpečnost, kybernetický zločin, svoboda internetu a vláda nad internetem.[31]



Obr. 1: Pět pilířů kybernetické diplomacie[35].

Kybernetickou diplomacii lze už tak dnes pozorovat jak na bilaterální úrovni (například dialog mezi Čínou a Spojenými státy v roce 2015, kdy bylo dosaženo spolupráce mezi oběma zeměmi po mnoha letech vzájemného obviňování z kybernetické špionáže), tak na multilaterální úrovni – v poslední době se téma čím dál častěji objevuje na plénu Valného shromáždění OSN. Zároveň se ale nesmí zapomínat na důležitost komunikace s nestátními aktéry, kteří jsou v této oblasti také důležitými hráči (jako například Facebook).[32]

Celá oblast kyberprostoru je i po několika desetiletích velmi neprobádaná. Totéž platí i o kybernetické diplomacii. Stále panují spory o tom, jakým způsobem by měla probíhat a nakolik by se měla lišit od diplomacie běžné.[33] Organizace spojených národů ale v této oblasti již učinila určité kroky. UNODA poskytuje výukové materiály, které se týkají právě kybernetické diplomacie a mají prohloubit stupeň mírového využití informačních a komunikačních technologií. Podobně jako kybernetická bezpečnost, i kybernetická diplomacie podle UNODA stojí na pěti pilířích, kterým se ve svých výukových materiálech věnují.[34]

5 SHRNUTÍ

Kybernetická bezpečnost je s rozmachem internetu stále palčivějším tématem. Navzdory tomu ale stále panují neshody o tom, do jaké míry by státy měly intervenovat například mimo své fyzické hranice. Suverenita, která je již od Vestfálské smlouvy jedním ze základních stavebních kamenů uspořádání světa, je v této oblasti dosud předmětem sporů. Mezi státy nepanuje shoda, zdali by kyberprostor měl, či neměl podléhat vestfálskému uspořádání.

Dlouhodobé snahy o regulaci kyberprostoru spočívají zejména v podpoře vytvoření právního rámce, jenž se bude problematice dostatečně věnovat a ustanoví všeobecné podmínky využívání kyberprostoru. Dalším stěžejním stavebním kamenem kybernetické bezpečnosti je bilaterální i multilaterální spolupráce mezi jednotlivými státy a také spolupráce mezi státy a nestátními aktéry, kteří se ve sféře pohybují.

Na plénu Organizace spojených národů panuje všeobecná shoda, že by se mělo zabránit možným teroristickým aktivitám v kyberprostoru, ale tato agenda spadá zejména do jurisdikce Rady bezpečnosti. Výbor pro odzbrojení a mezinárodní bezpečnost klade největší důraz na mezistátní kooperaci a předávání relevantních informací, které se týkají zabezpečení kyberprostoru.

V průběhu posledních dvou dekád vzniklo několik hlavních pilířů kybernetické diplomacie, které jednak za pomoci edukace, jednak za podpory vzdělanosti zvyšují obranyschopnost světového kyberprostoru. Otázkou tak zůstává, jestli budou státy ochotny sdílet své obranné strategie se státy ostatními a zda se nebudou příliš obávat, že by mohly právě tímto sdílením odhalit své vlastní slabiny a vystavit se možnému kybernetickému útoku ze strany jiných státních i nestátních aktérů.

6 OTÁZKY PRO JEDNÁNÍ

1. Jak se váš stát zapojuje do ITU Global Cybersecurity Agenda?
2. Je váš stát ochoten sdílet své obranné mechanismy se státy ostatními?
3. Jak váš stát chápe suverenitu v rámci kyberprostoru?
4. Potýká se váš stát s častými kybernetickými útoky?
5. Jaká je současná strategie kybernetického zabezpečení vašeho státu?
6. Podporuje váš stát další práci skupin vládních expertů?

7 DOPORUČENÉ A ROZŠIŘUJÍCÍ ZDROJE

» SCHJOLBERG, Stein a Solange GHERNAOUTI-HELIE. *A Global Treaty on Cybersecurity and Cybercrime.* 2. Oslo: AiTOslo, 2011. ISBN 978-82-997274-3-3.

» *INTERNATIONAL STRATEGY FOR CYBERSPACE: Prosperity, Security, and Openness in a Networked World* [online]. Washington, 2011 [cit. 2020-07-31]. Dostupné z: https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf

» *Global Cybersecurity Agenda (GCA)* [online]. [cit. 2020-07-31]. Dostupné z: https://www.itu.int/en/action/cybersecurity/Pages/gca.aspx

» *Cyberdiplomacy* [online]. [cit. 2020-07-31]. Dostupné z: https://cyberdiplomacy.disarmamenteducation.org/home/

» *Cybersecurity* [online]. [cit. 2020-07-31]. Dostupné z: https://www.un.org/counterterrorism/cybersecurity

» *Developments in the field of information and telecommunications in the context of international security* [online]. [cit. 2020-07-31]. Dostupné z: https://www.un.org/disarmament/ict-security/

8 SEZNAM POUŽITÝCH ZDROJŮ

1 Cyber Risk [online]. [cit. 2020-08-19]. Dostupné z: https://unite.un.org/digitalbluehelmets/cyberrisk

2 KAVANAGH, Camino. The United Nations, Cyberspace and International Peace and Security [online]. 2017 [cit. 2020-07-29]. Dostupné z: https://www.unidir.org/files/publications/pdfs/the-united-nations-cyberspace-and-international-peace-and-security-en-691.pdf, s. 7.

3 Definition of cybersecurity [online]. [cit. 2020-08-19]. Dostupné z: https://www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx

4 AYERS, Cynthia E. RETHINKING SOVEREIGNTY IN THE CONTEXT OF CYBERSPACE [online]. In:. Pennsylvania, USA: U.S. ARMY WAR COLLEGE, 2016 [cit. 2020-08-03]. Dostupné z: http://www.csl.army.mil/AllPublications.aspx, s. 67.

5 Tamtéž, s. 68.

6 Tamtéž, s. 72.

7 KAVANAGH, Camino. The United Nations, Cyberspace and International Peace and Security [online]. 2017 [cit. 2020-07-29]. Dostupné z: https://www.unidir.org/files/publications/pdfs/the-united-nations-cyberspace-and-international-peace-and-security-en-691.pdf, s. 13.

8 KUMAR, Sheetal. UN FIRST COMMITTEE PROCESSES ON RESPONSIBLE STATE BEHAVIOUR IN CYBERSPACE: AN EXPLAINER [online]. 2019 [cit. 2020-08-18]. Dostupné z: https://www.gp-digital.org/un-first-committee-processes-on-responsible-state-behaviour-in-cyberspace-a-briefing/

9 Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security: Note by the Secretary-General [online]. 2010 [cit. 2020-07-29]. Dostupné z: https://undocs.org/en/A/65/201, s. 4.

10 KAVANAGH, Camino. The United Nations, Cyberspace and International Peace and Security [online]. 2017 [cit. 2020-07-29]. Dostupné z: https://www.unidir.org/files/publications/pdfs/the-united-nations-cyberspace-and-international-peace-and-security-en-691.pdf, s. 16.

11 Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (2015). United Nations General Assembly [online]. New York. 1998. [cit. 2020-08-31]

12 INTERNET USAGE STATISTICS The Internet Big Picture World Internet Users and 2020 Population Stats [online]. 2020 [cit. 2020-08-18]. Dostupné z: https://www.internetworldstats.com/stats.htm

13 Tamtéž, s. 16.

14 Tamtéž, s. 7.

15 Tamtéž, s. 8.

16 Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security: Note by the Secretary-General [online]. 2013 [cit. 2020-07-29]. Dostupné z: https://undocs.org/en/A/68/98, s. 8.

17 Tamtéž, s. 8.

18 Tamtéž, s. 10.

19 KAVANAGH, Camino. The United Nations, Cyberspace and International Peace and Security [online]. 2017 [cit. 2020-07-29]. Dostupné z: https://www.unidir.org/files/publications/pdfs/the-united-nations-cyberspace-and-international-peace-and-security-en-691.pdf, s. 18.

20 Tamtéž, s. 19.

21 Tamtéž, s. 21.

22 Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security: Note by the Secretary-General [online]. 2015 [cit. 2020-07-29]. Dostupné z: https://undocs.org/en/A/70/174, s. 8.

23 KAVANAGH, Camino. The United Nations, Cyberspace and International Peace and Security [online]. 2017 [cit. 2020-07-29]. Dostupné z: https://www.unidir.org/files/publications/pdfs/the-united-nations-cyberspace-and-international-peace-and-security-en-691.pdf, s. 24.

24 Resolution 5370 (1998). United Nations General Assembly [online]. New York. 1998. [cit. 2020-07-29]

25 Resolution 5449 (1999). United Nations General Assembly [online]. New York. 1999. [cit. 2020-07-29]

26 Resolution 5528 (2000). United Nations General Assembly [online]. New York. 2000. [cit. 2020-07-29]

27 Resolution 5832 (2003). United Nations General Assembly [online]. New York. 2003. [cit. 2020-07-29]

28 Resolution 7429 (2019). United Nations General Assembly [online]. New York. 2019. [cit. 2020-07-29]

29 Resolution 7428 (2019). United Nations General Assembly [online]. New York. 2019. [cit. 2020-07-29]

30 BARRINHA, André a Thomas RENARD. Cyber-diplomacy: the making of an international society in the digital age. Global Affairs [online]. 2018, 3(4-5), 353-364 [cit. 2020-07-25]. DOI: 10.1080/23340460.2017.1414924. ISSN 2334-0460. Dostupné z: https://www.tandfonline.com/doi/full/10.1080/23340460.2017.1414924, s. 356.

31 Tamtéž, s. 355.

32 Tamtéž, s. 355.

33 Tamtéž, s. 361.

34 CYBERDIPLOMACY: Furthering the peaceful use of ICTs [online]. [cit. 2020-07-31]. Dostupné z: https://cyberdiplomacy.disarmamenteducation.org/home/

35 Five pillars of work. In: Cyberdiplomacy.disarmamenteducation.org [online]. New York: OSN, 2020 [cit. 2020-10-17]. Dostupné z: https://cyberdiplomacy.disarmamenteducation.org/home/

Pražský studentský summit

Pražský studentský summit je unikátní vzdělávací projekt existující od roku 1995. Každoročně vzdělává přes 300 studentů středních i vysokých škol o současných globálních tématech, a to především prostřednictvím simulace jednání tří klíčových mezinárodních organizací – OSN, NATO a EU.

studentsummit.cz
summit@amo.cz
facebook.com/studentsummit
instagram.com/praguestudentsummit
twitter.com/studentsummit
youtube.com/studentsummit

Asociace pro mezinárodní otázky (AMO)

AMO je nevládní nezisková organizace založená v roce 1997 za účelem výzkumu avzdělávání v oblasti mezinárodních vztahů. Tento přední český zahraničně politický think-tank není spjat s žádnou politickou stranou ani ideologií. Svou činností podporuje aktivní přístup k zahraniční politice, poskytuje nestrannou analýzu mezinárodního dění a otevírá prostor k fundované diskusi.

Marie Šmejkalová

Autorka je spolupracovnicí Asociace pro mezinárodní otázky a členkou přípravného týmu Pražského studentského summitu.

POŘADATEL

AMO.CZ

GENERÁLNÍ PARTNER

The Kellner Family Foundation

TOP PARTNEŘI

Ministerstvo zahraničních věcí České republiky

Evropská komise
Zastoupení v České republice

Ministerstvo školství, mládeže a tělovýchovy

Praha Prague Praga Prag

Vysoká škola ekonomická v Praze

KB

PARTNEŘI

Univerzita Karlova v Praze

US embassy

Embassy of Canada
Ambassade du Canada

SCIO

Auto Zrucký Dealer Nissan

United Nations
Informační centrum OSN v Praze

Informační centrum o NATO
NATO Information Center

Městská část Praha 6

T

ČSU

Program mladých delegátů ČR do OSN

MEDIÁLNÍ PARTNER

RESPEKT

#SUMMIT26

Autor: Marie Šmejkalová
Imprimatur: Jiří Rajtr, Radek Mazuch, Petr Boháček
Jazyková úprava: Barbora Novotná, Štěpán Komárek, Anna Zadražilová
Sazba: Tereza Ondráčková
Grafická úprava: Lucie Vodvářková

Vydala Asociace pro mezinárodní otázky (AMO) pro potřeby XXVI. ročníku Pražského studentského summitu.

Asociace pro mezinárodní otázky (AMO)
Žitná 27, 110 00 Praha 1
Tel.: +420 224 813 460, e-mail: summit@amo.cz
IČ : 65 99 95 33

www.amo.cz
www.studentsummit.cz