Problém zneužití zranitelností nultého dne a možnosti jeho řešení nástroji mezinárodního práva veřejného

Jan Strakoš*

Abstrakt: **Tento článek se v podstatě zaměřuje na možnosti mezinárodní spolupráce v oblasti kybernetické bezpečnosti při řešení problému zneužití zranitelností nultého dne. Jeho prvních několik částí uvede čtenáře do některých klíčových kybernetických pojmů, přičemž vysvětlují především, co znamená kybernetická exploatace a zneužívání zranitelných míst v informačních systémech, které jsou často využívány ke kybernetickému teroru. Zohledněn je také fenomén umělé inteligence, která automatizuje mechanismy reakce a zlepšuje kybernetickou odolnost, ale zároveň je využívána hackery k vyhledávání chyb v informačních systémech a vytváření nových strategií útoků v reálném čase. Třetí část článku s názvem „Základní problém při řešení zneužití zranitelností nultého dne" popisuje minulé i aktuální přístupy mezinárodního společenství k řešení kybernetických hrozeb obecně a zkoumá otázku, zda mezinárodní spolupráce či nástroje mezinárodního práva veřejného umožňují efektivní potírání tohoto problému. V závěru jsou navrženy možné přístupy, které by mezinárodní společenství mohlo přijmout (nebo již přijímá) k zamezení zneužívání zranitelností nultého dne.**

Klíčová slova: **mezinárodní právo veřejné, kybernetická bezpečnost, kybernetická špionáž, kybernetická hrozba, zneužití zranitelností nultého dne**

Úvod

Dnešní dobu si bez vymožeností současné informatiky prakticky nelze představit. Společnost je globálně propojená a závislá na softwaru, který se stal téměř její existenční otázkou. Moderní technologie ovládané tímto softwarem přinášejí soukromému i veřejnému sektoru příjmy, mezinárodní prestiž, konkurenční výhody, ale bohužel také závažná bezpečnostní rizika. V této souvislosti se často hovoří o kybernetických bezpečnostních hrozbách, kybernetické kriminalitě a strategiích jednotlivých států či mezinárodního společenství odrážejících snahy tyto problémy řešit pomocí nástrojů kybernetické bezpečnosti.[1] Avšak překvapivě jen málokdy se zaměřuje pozornost na nejdůležitější problém, jímž je definování kybernetické exploatace v rámci mezinárodního práva a řešení zneužití zranitelností tzv. nultého dne, pod kterým si mnozí lidé nedokážou nic konkrétního, natož právního představit. Přitom právě tento problém byl pravděpodobně příčinou největší loupeže v historii kryptoměn, ke které došlo 21. února 2025, kdy severokorejští hackeři, zřejmě ze skupiny Lazarus,[2] obešli zlatý standard kryptografického zabezpečení, tzv. cold

* Ing. Mgr. Jan Strakoš, LL.M., Ministerstvo průmyslu a obchodu České republiky. E-mail: strakos.jan@centrum.cz. ORCID: https://orcid.org/0009-0007-9133-5904.

1 Třebaže podle některých teoretiků „kybernetická bezpečnost", tím spíše „mezinárodní kybernetická bezpečnost" v podstatě neexistuje, respektive je jen zbožným přáním. S tímto názorem, že něco jako kybernetická bezpečnost vlastně neexistuje, se lze setkat např. v právní monografii *Právo informačních technologií*, která se stala velmi cenným průvodcem při koncepci tohoto příspěvku, a která „provokuje" i tím, uvádí-li se v ní, že problémem zdaleka nemusí být vymezení kybernetické bezpečnosti jako již toho, co všechno si máme představit pod pojmem „bezpečnost" (viz POLČÁK, Radim a kol. *Právo informačních technologií*. Praha: Wolters Kluwer ČR, 2018, s. 587).

2 Viz Lazarus Group. *MITRE ATT&CK and ATT&CK* [online] 2015–2024 [cit. 2025-03-15]. Dostupné z: https://attack.mitre.org/groups/G0032/.

peněženku,[3] a z dubajské kryptoměnové burzy *Bybit* odcizili 1,5 miliard dolarů.[4] Jelikož i tato skutečnost podtrhuje potřebu mezinárodně právně řešit otázky kybernetické bezpečnosti, tento článek si klade za cíl objasnit podstatu zneužití zranitelností nultého dne, které představují významnou hrozbu pro současnou kybernetickou bezpečnost. Hrozbu velmi silně přítomnou. Cílem je analyzovat, jak státy řeší tento problém na mezinárodní úrovni a zda mezinárodní právo veřejné nabízí vhodné nástroje k jeho potírání. Zaměříme se proto na definování hlavních otázek současné mezinárodní spolupráce, ale i na možné budoucí přístupy, kterými by se mohla mezinárodní scéna ubírat při hledání efektivního řešení tohoto problému a naplnění jeho cíle, jímž je posílení veřejného dobra v mezinárodním kyberprostoru, spočívající v náležitém objasnění kybernetických incidentů a spravedlivém potrestání viníků. Za tím účelem budou v článku reflektovány historické i dosavadní postoje OSN, jakož i některých států, pokud jde o formování mezinárodní spolupráce v této oblasti a názory na kybernetickou exploataci. Dále bude zohledněna historicky první Zpráva o stavu kybernetické bezpečnosti v Unii (EU),[5] kterou v roce 2024 přijala agentura ENISA[6] ve spolupráci se skupinou pro spolupráci v oblasti bezpečnosti sítí a informací a Evropskou komisí v souladu s článkem 18 směrnice (EU) 2022/2555[7] (dále též „NIS 2"), vybraná evropská legislativa a příležitostně i text nedávno přijaté Úmluvy OSN proti kyberkriminalitě.[8]

1. Kybernetická exploatace jako kybernetický problém číslo jedna

Pro pořádek je třeba poukázat na to, že v současném mezinárodním slovníku se setkáme s řadou kybernetických pojmů, jako je „kybernetický prostor" (*cyber space*), „kybernetická bezpečnost" (*cyber security*), „kybernetická hrozba" (*cyber threat*), ale také „kybernetický útok" (*cyber attack*), jenž je právě někdy nesprávně, či dokonce účelově zaměňován s „kybernetickým průzkumem" (*cyber reconnaissance*). Bohužel v právních předpisech

---

3 Cold peněženka (nebo *cold wallet*) je typ kryptoměnové peněženky, která není připojena k internetu. Slouží k bezpečnému uložení kryptoměn mimo dosah online útoků, což ji činí odolnější vůči hackům. Tyto peněženky jsou většinou hardwarové zařízení (např. USB disk) nebo papírové peněženky, kde se private key (privátní klíč) uchovává offline. Cold wallet může být zároveň *Multisig* či *Multi-Signature wallet*, pokud je navržena tak, že k podepsání transakce je potřeba více klíčů, přičemž tyto klíče jsou uložené offline. Podrobněji např. viz Multi-Signature Wallets: Definition and Use Cases. *Investopedia* [online]. [cit. 2025-03-15]. Dostupné z: https://www.investopedia.com/multi-signature-wallets-definition-5271193.

4 SIGALOS, MacKenzie. Hackers steal $1.5 billion from exchange Bybit in biggest-ever crypto heist. *CNBC* [online]. 2025 [cit. 2025-03-15]. Dostupné z: https://www.cnbc.com/2025/02/21/hackers-steal-1point5-billion-from-exchange-bybit-biggest-crypto-heist.html.

5 Publikovaná dne 3. 12. 2024 a dostupná v pdf verzi z webových stránek ENISA. *2024 Report On The State of The Cybersecurity In The Union* [online]. [cit. 2025-03-15]. Dostupné z: https://www.enisa.europa.eu/publications/2024-report-on-the-state-of-the-cybersecurity-in-the-union#contentList.

6 Agentura Evropské unie pro kybernetickou bezpečnost – *European Union Agency For Network and Information Security*.

7 Směrnice Evropského parlamentu a Rady (EU) 2022/2555 ze dne 14. prosince 2022 o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii a o změně nařízení (EU) č. 910/2014 a směrnice (EU) 2018/1972 a o zrušení směrnice (EU) 2016/1148 (směrnice NIS 2).

8 Tu schválilo Valné shromáždění OSN konsenzem dne 24. 12. 2024 v podobě, v jaké byla schválena *ad hoc* mezivládním výborem expertů k tomu ustavenému usnesením Valného shromáždění OSN 74/247 ze dne 27. 12. 2019, s jedinou výjimkou – návrhem Vietnamu, že úmluva bude otevřena k podpisu v Hanoji v roce 2025. Poté bude úmluva otevřena k podpisu též v sídle OSN v New Yorku a to do 31. 12. 2026. Text úmluvy dostupný z: https://documents.un.org/doc/undoc/gen/n24/426/74/pdf/n2442674.pdf.

jednotlivých států není výjimkou, že jeden a týž pojem, který je stejně vnímán i ostatními státy (což je ten lepší případ), je jinak označen.[9] Tato okolnost pochopitelně nepřispívá k právní jistotě ani bezchybné mezinárodní spolupráci v oblasti kybernetické bezpečnosti. Horší však je, pokud není určitý problém vůbec definován. To je pro právníky doslova noční můra, protože předvídání účinnosti jednotlivých nástrojů mezinárodního práva je v takovém případě velmi obtížné. Proto je záhodno čtenáře nejprve uvést do kontextu a vysvětlit mu, co se rozumí kyberprostorem, kybernetickou bezpečností a kybernetickou exploatací, než přistoupíme k definování zneužívání zranitelností nultého dne.

Kyberprostorem standardně rozumíme *„globálně propojený prostor, který se skládá z Internetu a dalších počítačových sítí, digitálních zařízení, systémů, služeb a procesů na nich“*.[10] Tedy jedná se o prostor, pro který jsou, např. podle Doucka, charakteristické minimálně tyto znaky:

a) anonymita jeho uživatelů (ta pochopitelně ztěžuje jakékoliv vyšetřování; navíc podíl na kybernetických incidentech lze poměrně snadno popřít);

---

9 Tak např. Francie dává na místo pojmu „kritická infrastruktura“ přednost pojmu „provozovatelé kritického významu“ *(Opérateur d'importance vitale)*. Naproti tomu české právo používá pro identickou záležitost pojem „kritická infrastruktura“ – tou zákon č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon), ve znění pozdějších předpisů, rozumí *prvek kritické infrastruktury nebo systém prvků kritické infrastruktury, narušení jehož funkce by mělo závažný dopad na bezpečnost státu, zabezpečení základních životních potřeb obyvatelstva, zdraví osob nebo ekonomiku státu*. Co je však zajímavé, tak to je, že zatímco již zmiňovaná kritická infrastruktura je (i přes její rozdílné pojmenování) z velké části jednotně definována Francií, Rakouskem, Estonskem, Německem či třeba Tureckem, to samé se již nedá říci o „kritické informační infrastruktuře“, kde naopak definice ve vnitrostátním právu (s výjimkou České republiky, Lotyšska či např. Itálie) spíše chybí (KASKA, Kadri – TRINBERG, Lorena. *Regulating Cross-Border Dependencies of Critical Information Infrastructure*. Tallinn: CCDCOE, 2015, s. 10. [online]. [cit. 2025-03-15]. Dostupné z: https://ccdcoe.org/uploads/2018/10/CII_dependencies_2015.pdf), [v České republice jde o § 2 písm. b) zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů, v platném znění].

10 Definice *kyberprostoru* dle mezinárodně uznaného technického standardu, normy ISO/IEC 27100, byla zvolena záměrně, protože, jak potvrzuje čl. 2 bodu 19 aktu o kybernetické bezpečnosti (k tomuto nařízení viz dále), je uznávaná i předpisy komunitárního práva, jež mají supranacionální charakter (normy ISO tedy hrají významnou roli také v jednotlivých státech EU). Aktem o kybernetické bezpečnosti zde rozumíme nařízení Evropského parlamentu a Rady (EU) 2019/881 ze dne 17. 4. 2019 o agentuře ENISA, o certifikaci kybernetické bezpečnosti informačních a komunikačních technologií a o zrušení nařízení (EU) č. 526/2013, které nabylo účinnosti dne 27. 6. 2019. Předmětný článek 2 bodu 19 „normou“ rozumí normu ve smyslu čl. 2 bodu 1 nařízení Evropského parlamentu a Rady (EU) č. 1025/2012 o evropské normalizaci, a tou se podle právě zmíněného nařízení rozumí *technická specifikace přijatá uznávaným normalizačním orgánem* (mj. ISO – International Organization for Standardization, nebo IEC – International Electrotechnical Commission) *k opakovanému nebo trvalému použití, jejíž dodržování není povinné* a která patří do jedné z kategorií stanovených tímto nařízením (právě do kategorie mezinárodních norem). Obdobně viz čl. 16 odst. 1 písm. e) dnes již zrušené směrnice Evropského parlametu a Rady (EU) 2016/1148 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii (tzv. „směrnice NIS 1“), podle něhož: *„Členské státy zajistí, aby poskytovatelé digitálních služeb určili a přijali vhodná a přiměřená technická a organizační opatření k řízení bezpečnostních rizik, jimž jsou vystaveny sítě a informační systémy, které využívají v souvislosti s nabízením služeb uvedených v příloze III v rámci Unie. S ohledem na nejnovější technický vývoj tato opatření musí zajišťovat úroveň bezpečnosti sítí a informačních systémů odpovídající existující míře rizika, přičemž* (mj.) *zohledňují soulad s mezinárodními normami.“* Aktuálně podle čl. 21 odst. 1 směrnice NIS 2: *„Členské státy zajistí, aby základní a důležité subjekty přijaly vhodná a přiměřená technická, provozní a organizační opatření k řízení bezpečnostních rizik, jimž čelí sítě a informační systémy, jež tyto subjekty používají pro svůj provoz nebo poskytování svých služeb, a k předcházení incidentům nebo minimalizaci jejich dopadů na příjemce jejich služeb a na další služby. S ohledem na nejnovější technický vývoj a případně na příslušné evropské a mezinárodní normy a na náklady na provádění musí opatření uvedená v prvním pododstavci zajišťovat úroveň bezpečnosti sítí a informačních systémů odpovídající existující míře rizika. Při posuzování přiměřenosti těchto opatření je třeba náležitě zohlednit míru vystavení subjektu rizikům, jeho velikost a pravděpodobnost výskytu incidentů, jejich závažnost a společenský a ekonomický dopad.“* (Poznámka – v době sepisování tohoto příspěvku, tj. v letech 2021 až polovina března 2025, probíhaly legislativní práce na zcela novém zákoně o kybernetické bezpečnosti s ohledem na NIS 2).

b) asymetričnost jednotlivých procesů, které se v něm uskutečňují nezávisle na důvěryhodnosti výchozího zdroje;

c) virtuální teritorialita, tj. problém delokalizace (tím, že se kriminální činy mohou projevit na území jakéhokoliv státu, jenž je zrovna *on-line*, může být obtížné identifikovat místo, odkud přesně kybernetický útok pochází; jedná-li se o kybernetický útok ať už v podobě poškození webových stránek, odepření určité služby, nebo zničení konkrétní infrastruktury);

d) okamžitost akcí s mezinárodními dopady a volný vstup do něj i výstup a schopnost maximálně ovlivňovat ostatní.[11]

Kybernetickou bezpečnost, kterou je třeba odlišovat od informační bezpečnosti[12] (v rámci informační bezpečnosti totiž neřešíme kybernetické bezpečnostní incidenty[13]), definuje např. akt o kybernetické bezpečnosti následujícím způsobem. Podle jeho čl. 2 bodu 1) se jí rozumí *„činnosti nezbytné k ochraně sítí a informačních systémů, jejich uživatelů a dalších osob dotčených kybernetickými hrozbami"*. Naproti tomu z pohledu českého vnitrostátního práva je kybernetická bezpečnost neurčitým právním pojmem spadajícím pod tzv. nedistributivní práva k informacím.[14] Sice zde existuje český zákon o kybernetické bezpečnosti, ten však zmíněný pojem (oproti kyberprostoru) nijak nevysvětluje.[15] Český zákon upravuje *„pouze práva a povinnosti osob, působnost a pravomoci orgánů veřejné moci v oblasti kybernetické bezpečnosti, zpracovává příslušné právní předpisy EU a upravuje zajišťování bezpečnosti sítí elektronických komunikací a informačních systémů"* (§ 1 odst. 1 a 2 cit. zákona). Co je však dále podstatné, je skutečnost, že zákon v této souvislosti v § 7 rozlišuje mezi kybernetickou bezpečnostní událostí (odst. 1) a kybernetickým bezpečnostním incidentem (odst. 2). Zatímco *kybernetickou bezpečnostní událostí* rozumí *„událost, která může způsobit narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací"* (v tomto případě jde tedy o událost využívající zranitelnosti informačního systému, aniž by ještě došlo ke škodnému následku[16]), *kybernetickým bezpečnostním incidentem* rozumí již faktický negativní následek v podobě narušení bezpečnosti informací, respektive informačního systému.[17] V zásadě se shodným členěním se lze setkat i na poli

---

11 Klasifikace použita dle DOUCEK, Petr – KONEČNÝ, Martin – NOVÁK, Luděk. *Řízení kybernetické bezpečnosti a bezpečnosti informací*. Praha: Professional Publishing s.r.o., 2019, s. 18–19.

12 Tu má standardně u instituce na starosti manažer informační bezpečnosti (*Chief Information Security Officer* neboli zkráceně *CISO*).

13 DOUCEK, Petr – KONEČNÝ, Martin – NOVÁK, Luděk. *Řízení kybernetické bezpečnosti a bezpečnosti informací*, s. 27.

14 O distributivních a nedistributivních právech k informacím a faktické důležitosti nedistributivních práv k informacím, kam náleží i kybernetická bezpečnost, a problému jejich upozaďování hovoří např. prof. Polčák: POLČÁK, Radim. *Internet a proměny práva*. Praha: Auditorium, 2012, s. 343.

15 Tak je tomu mnohdy i v případě národních zákonů jiných států (např. v Německu či Belgii), které kybernetickou bezpečnost (značně fragmentarizovanou na konkrétní oblasti; např. oblast financí, telekomunikací či ochrany osobních údajů) často také nesoustředí jen do jednoho zákona, ale do několika zákonů. V tomto směru proto zdůrazněme, že směrnice NIS 2 apeluje na horizontální přístup ke kybernetické bezpečnosti.

16 Lze zmínit např. někdejší skandály čínských firem Huawei nebo Zhenhua Data Technology ze Šen-čenu, k nimž Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB) před několika lety, konkrétně dne 17. 12. 2018 vydal tzv. varování. Dostupné v pdf verzi z úřední desky NÚKIB: Úřední deska. *NÚKIB* [online]. [cit. 2025-03-15]. Dostupné z: https://nukib.cz/cs/uredni-deska/.

17 Za připomenutí stojí např. událost, která se odehrála v září roku 2020 v Německu. Tehdy totiž došlo zřejmě k historicky prvnímu oficiálně zaznamenanému kybernetickému útoku, jehož důsledkem byla smrt člověka. Šlo o pacientku

mezinárodním. Ostatně jak uvádí např. komentář k zákonu o kybernetické bezpečnosti: *„Cizojazyčný pojem ‚incident' byl použit z důvodu zachování souladu zákonného pojmového aparátu s mezinárodní technickou terminologií."*[18]

Nyní se dostáváme k hrozbě *mezinárodní špionáže* uskutečňované státními i nestátními aktéry v kyberprostoru, která je, jak potvrzuje např. Zpráva o stavu kybernetické bezpečnosti v Unii, jevem nepřetržitým a navzdory omezenému informování veřejnosti zůstává trvalou a vážnou hrozbou.[19] Do výčtu kybernetických útoků se v obecném slova smyslu totiž někdy řadí i tzv. „kybernetická exploatace" (*cyber exploitations*), zahrnující „kybernetické vykořisťování" nebo „kybernetickou (počítačovou) špionáž" (*cyber espionage*), pro kterou se užívá zkratka „APT" (*Advanced Persistent Threat* – pokročilá a trvalá hrozba).[20] Podle převažujícího mínění odborníků, např. dle Lina,[21] je však toto tvrzení nepřesné, neboť na rozdíl od kybernetických útoků tyto kybernetické operace zpravidla nepředstavují žádné narušení počítačové sítě, ale omezují se pouze na dlouhodobé monitorování, kopírování dat a špionáž pomocí počítačového systému.[22] Tento názor potvrzují i mezinárodní normy, které uvedené vnímají jako kybernetickou hrozbu (událost) a jakkoliv za ní obvykle stojí nějaký státní aktér (APT totiž vyžaduje vysokou úroveň znalostí a dostatek kapitálu), nedefinují ji jako formu kybernetického útoku, respektive kybernetický incident. Proto je i doktrína obecně názoru, že nejde o destruktivní užití síly (*use of force*), respektive o „ozbrojený útok" na cizím území, o kterém hovoří čl. 51 Charty OSN, který jinak umožňuje aktivovat právo na individuální nebo kolektivní sebeobranu.[23] Ostatně i Tallinnský manuál o mezinárodním právu použitelném na kybernetickou válku nechápe kybernetickou špionáž jako ozbrojený konflikt, ale jako *„jakýkoli čin, provedený*

Fakultní nemocnice v Düsseldorfu, která musela být z důvodu napadení nemocnice ransomwarem (hackeři zneužili chybu zabezpečení ve verzi softwaru Citrix VPN) a selhání nemocničních IT systémů převezena do jiné nemocnice, přičemž při převozu zemřela. K tomu lze odkázat na článek German hospital hacked, patient taken to another city dies. *AP News*. [online]. 17. 9. 2020 [cit. 2025-03-15]. Dostupné z: https://apnews.com/article/technology-hacking-europe-cf8f8eee1adcec69bcc864f2c4308c94.

18 Viz MAISNER, Martin – VLACHOVÁ, Barbora. *Zákon o kybernetické bezpečnosti: Komentář*. Praha: Wolters Kluwer, stav k 1. 2. 2020, pramen ASPI KO181_2014CZ.

19 Viz str. 14 Zprávy o stavu kybernetické bezpečnosti v Unii / *2024 Report On The State of The Cybersecurity In The Union* [online]. ENISA [cit. 2025-03-15]. Dostupné z: https://www.enisa.europa.eu/sites/default/files/2024-11/2024%20Report%20on%20the%20State%20of%20the%20Cybersecurity%20in%20the%20Union.pdf.

20 O APT jako o dlouhodobé formě systematického kybernetického útoku hovoří např. Kolouch: KOLOUCH, Jan. *Cyber Crime*. Praha: nakladatelství Milan Hodek, 2016, s. 320–322. Viz dále např. v médiích „probírána" jedna z nejnebezpečnějších hackerských skupin na světě ruská APT28, známá jako *Forest Blizzard*, *Fancy Bear* či *Sofacy Group*; k tomu dále viz např. Upozornění na kompromitaci routerů Ubiquity Edge OS aktérem sponzorovaným ruským státem. *NÚKIB* [online]. [cit. 2025-03-15]. Dostupné z: https://nukib.gov.cz/cs/infoservis/hrozby/2083-upozorneni-na-kompromitaci-routeru-ubiquity-edge-os-akterem-sponzorovanym-ruskym-statem/.

21 *" 'Cyberexploitation' refers to the use of actions and operations – perhaps over an extended period of time – to obtain information that would otherwise be kept confidential and is resident on or transiting through an adversary's computer systems or networks."* In: LIN, Herbert. Offensive Cyber Operations and the Use of Force. *Journal of National Security Law & Policy* [online]. 2010, Vol. 4, No. 63, s. 63 [cit. 2025-03-15]. Dostupné z: https://jnslp.com/wp-content/uploads/2010/08/06_Lin.pdf.

22 MRÁZEK, Josef. Mezinárodní právo v kybernetickém prostoru. *Právník*. 2014, roč. 153, č. 7, s. 542–543.

23 Podle čl. 51 Charty OSN: *„Žádné ustanovení této Charty neomezuje, v případě ozbrojeného útoku na některého člena Organizace spojených národů, přirozené právo na individuální nebo kolektivní sebeobranu, dokud Rada bezpečnosti neučiní opatření k udržení mezinárodního míru a bezpečnosti. Opatření učiněná členy při výkonu tohoto práva sebeobrany oznámí se ihned Radě bezpečnosti; nedotýkají se nikterak pravomoci a odpovědnosti Rady bezpečnosti, pokud jde o to, aby kdykoli podle této Charty podnikla takovou akci, jakou považuje za nutnou k udržení nebo obnovení mezinárodního míru a bezpečnosti."*

tajně nebo pod falešnou záminkou, který využívá kybernetické schopnosti ke shromažďování (nebo pokusu o shromažďování) informací s úmyslem sdělit je protistraně konfliktu".[24]

To ovšem neznamená, že jde o činnost, která by nebyla protiprávní, potažmo že by nemohla zakládat odpovědnost za veřejnoprávní, mezinárodněprávní delikt. Vzhledem k tomu, že špión (*threat agent*) využívá veřejnosti dosud neznámého zranitelného místa v operačním systému k vlastnímu prospěchu (typicky krade data, nejčastěji duševní vlastnictví, v horším případě citlivé vojenské informace, což každý stát samozřejmě popře; podle toho také můžeme někdy rozlišovat mezi průmyslovou, vojenskou či politickou špionáží), dopouští se kybernetického zločinu, přičemž není vyloučeno, že předmětné zranitelnosti nevyužije i k uskutečnění rozsáhlého kybernetického útoku majícího znaky kybernetického bezpečnostního incidentu. Pokud by tedy kybernetická špionáž zahrnovala i jiné než výše uvedené činnosti (monitoring, shromažďování údajů[25]), o formu kybernetického útoku (incidentu) by se jednat mohlo.[26]

Máme zde tedy co do činění s řadou zločineckých uskupení mnohdy podporovaných státy, která se obvykle formují za účelem zneužití zranitelností nultého dne a která často vystupují pod velmi originálními názvy. Zmiňme alespoň některé. Např. *The Shadow Brokers* označuje hackerskou skupinu, která se poprvé objevila v létě roku 2016. Tato skupina zveřejnila několik *zero-day exploitů*, které údajně pocházely od „Equation Group", jež je považována za součást Národní bezpečnostní agentury USA (*National Security Agency*[27]). Naproti tomu *Dark Caracal* je hrozivá skupina připisována libanonskému Generálnímu ředitelství pro všeobecnou bezpečnost a působí nejméně od roku 2012. Skupina je známá útoky, které zahrnují sledování obětí prostřednictvím sociálních médií, jako jsou Facebook a WhatsApp, pořizování snímků obrazovky pomocí malwaru pro Windows a další špionážní aktivity. *Indigo Zebra* je čínská kyberšpionážní skupina, která se zaměřuje na středoasijské vlády nejméně od roku 2014. Skupina využívá různé techniky sociálního inženýrství a malwaru k získání přístupu k citlivým informacím. *Bronze Butler*, také známá jako *Tick*, je kyberšpionážní skupina s pravděpodobným čínským původem, která je aktivní nejméně od roku 2008. Skupina se primárně zaměřuje na japonské organizace, zejména ve státní

---

24 Viz SCHMITT, Michael N. *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge University Press, 2013, s. 193.

25 Vzpomeňme v této souvislosti např. špionážní software izraelské společnosti NSO Group, známý jako *Pegasus*. Tento spyware, údajně vyvinutý pro vlády a bezpečnostní složky za účelem odhalování terorismu a boje proti organizovanému zločinu, byl totiž zneužit i ke sledování novinářů a politických oponentů po celém světě, od Mexika přes Saúdskou Arábii až po Indii, přičemž spočíval v tom, že nepozorovaně infikoval mobilní telefony (iPhone i Android) skrze zranitelná místa v jejich operačních systémech a umožňoval sledovat stisky kláves, odposlouchávání telefonních hovorů, sledování polohy v reálném čase či skryté používání mikrofonu a fotoaparátu mobilního telefonu bez vědomí jeho uživatele.

26 V obecné rovině mohou kybernetické útoky nabývat různé podoby, např. i takové, jakou jsme mohli v případě České republiky zaznamenat na konci roku 2019 či počátku roku 2020; ať už je řeč o vyděračském viru, který napadl nemocnici v Benešově, o napadení OKD, které muselo kvůli útoku hackerů pozastavit provoz v dolech na Karvinsku anebo o napadení psychiatrické nemocnice v Kosmonosech. Ze zahraniční kazuistiky je pak možno zmínit např. kybernetický útok ze dne 19. 3. 2019 na servery a počítače norské společnosti NORSK HYDRO, zabývající se výrobou hliníkových produktů. Malware, který útočníci použili, byl ransomware s názvem „LockerGoga". Důsledkem napadení bylo, že část tavících pecí, které nebyly izolovány a byly tak zasaženy, musely být dočasně odpojeny od výrobních systémů. Z důvodu omezení výroby byla škoda vyčíslena na x milionů eur. Za pomocí KUBOŠ, Petr. *Kybernetická bezpečnost v kritických infrastrukturách společností* [přednáška]. Praha: IT Security Workshop, 26. 3. 2019.

27 Zatímco NSA spadá pod americké Ministerstvo obrany a zaměřuje se mj. na kyberšpionáž, signální zpravodajství a vojenskou kybernetickou bezpečnost, tzv. CISA *(Cybersecurity and Infrastructure Security Agency)* spadá pod americké Ministerstvo vnitra a zaměřuje se na ochranu kritické infrastruktury a kybernetickou bezpečnost v civilním sektoru. CISA však nemá pravomoc provádět kybernetické útoky nebo špionáž.

správě, biotechnologii, výrobě elektroniky a průmyslové chemii. Bronze Butler využívá různé zranitelnosti v softwaru, včetně těch v produktech Microsoft Office, k provádění svých útoků. Skupina *Andariel* je severokorejská státem sponzorovaná skupina, která je aktivní nejméně od roku 2009. Skupina se zaměřuje na různé cíle, včetně finančních institucí a obranných průmyslových odvětví, a je známá využíváním různých zranitelností k provádění svých útoků. *Sandworm Team* je destruktivní skupina, která je připisována vojenské jednotce Hlavního střediska pro speciální technologie (GTsST) Hlavního ředitelství generálního štábu ozbrojených sil Ruské federace (GRU). Skupina je aktivní nejméně od roku 2009 a je spojována s několika významnými kybernetickými útoky, včetně útoků na ukrajinskou energetickou infrastrukturu a šíření malwaru NotPetya.

S mnoha dalšími skupinami se lze podrobněji seznámit na internetu – např. na webových stránkách GitHub;[28] anebo na adrese společnosti Kaspersky Lab,[29] kde najdeme nejen jejich přehledný výčet, ale i specifikaci oblastí zájmů, na které tyto „syndikáty" cílí. Z vůbec nejslavnějších je pak možno zmínit čínskou skupinu APT1 (*Comment Panda*) nebo ruskou špiónážní skupinu APT28 (*Fancy Bear*), která, opomeneme-li skutečnost, že údajně v roce 2016 zkompromitovala volební kampaň Hillary Clintonové, stála v uplynulých deseti letech také za většinou útoků na české státní instituce.[30]

2. Zneužití zranitelností tzv. nultého dne aneb nejlépe slouží ten, kdo neví, že slouží

Chceme-li pochopit mechanismus kybernetických hrozeb a těmto účinně čelit, zvláště v tomto století se v právu neobejdeme bez znalostí výpočetní techniky. Následující přiblížení problému bude proto poněkud technicistního rázu.

Zero-Day nebo-li nultý den označuje časovou periodu, během níž je uživatel softwaru ohrožen pro chyby, které se v softwaru skrývají a o kterých neví ani jeho výrobce či programátor. Tyto chyby – zpravidla označované identifikátorem „CVE"[31] – mohou být způsobeny vadným nastavením softwaru anebo třeba jeho včasnou neaktualizací, a protože představují v operačním systému zranitelná místa, která mohou vést k neautorizovanému přístupu ke zdrojovým systémům,[32] mohou být zneužity prostřednictvím jednoduchého kódu, kterému říkáme *exploit*, např. k již zmiňované průmyslové, vojenské či politické špionáži. Společným znakem mezinárodní špionáže totiž je, že vždy těží ze zranitelnosti systému (*vulnerabillity*), kterou může představovat i nedostatečné povědomí člověka o riziku, kterého hacker, přesněji cracker, využije. Způsob, jakým je systém zneužit, pak nazýváme *vektorem útoku*. V této souvislosti hovoříme o problému zneužití nultého dne,

28 Dostupné z: https://github.com/cybershujin/Threat-Actors-use-of-Artifical-Intelligence.

29 Dostupné z: https://apt.securelist.com.

30 Viz ČTK. Hackerům APT28 se připisují útoky na politiky, instituce či NATO. *ITBIZ.CZ*. [online]. 6. 5. 2024 [cit. 2025-03-15]. Dostupné z: https://www.itbiz.cz/zpravicky/hackerum-apt28-se-pripisuji-utoky-na-politiky-instituce-ci-nato/.

31 Dle organizace The National Vulnerability Database (NVD). *NVD* [online], [cit. 2025-03-15]. Dostupné z: https://nvd.nist.gov.

32 DOUCEK, Petr – KONEČNÝ, Martin – NOVÁK, Luděk. *Řízení kybernetické bezpečnosti a bezpečnosti informací*, s. 25. Jednu z nejméně prozkoumaných oblastí zranitelnosti představuje závislost na přeshraniční kritické informační infrastruktuře (např. v oblasti bankovnictví nebo telekomunikací), jak potvrzuje i např. velmi hezky zpracovaná studie Kooperativního centra kybernetické obrany NATO (CCDCOE – Cooperative Cyber Defence Centre of Excellence (Kooperativní centrum NATO kybernetické obrany se sídlem v Tallinnu) z roku 2015. Dostupné z: https://ccdcoe.org/uploads/2018/10/CII_dependencies_2015.pdf.

tedy o problému využití dlouho neviděného slabého místa uvnitř operačního systému ke sběru informací o nějakém subjektu.[33] Tento proces zpravidla zahrnuje tyto fáze:[34]

1. fázi, kdy je systém zranitelný pro existenci skryté chyby v něm;
2. fázi, kdy je předmětná zranitelnost využita útočníkem a systém je prolomen – tato fáze tedy zahrnuje přípravu útoku a průnik do systému za pomocí *exploitu* využívajícího konkrétní zranitelnosti (předmětný *exploit* je nebezpečný do doby, dokud není zranitelné místo v softwaru odstraněno bezpečnostní záplatou, které říkáme *patch*);
3. konečně útočnou fázi, během níž dojde ke kompromitaci systému škodlivým kódem, jímž může být např. Adware, Worm, Ransomware, Spyware či jiné známé signatury malweru, a nechtěné činnosti vyvinuté útočníkem, který z ní má nějaký užitek; popř. tato fáze zahrnuje i tzv. *clean-up*, jehož účelem je vymazat důkazy o útoku.

Lze přitom dodat, že se zapojením nástrojů umělé inteligence do on-line procesů nabývá celý problém na mnohem větší intenzitě nebezpečnosti a tím pádem i globálním významu. Umělá inteligence totiž nerozumí morálce. Nejenže umožňuje nalézat slabiny v informačních systémech dříve, než je bezpečnostní týmy stihnou opravit, ale také přizpůsobuje techniky útoku na základě živých bezpečnostních reakcí a umožňuje tak jejich autonomní provádění včetně úprav, aby je nebylo možné odhalit.[35]

3. Základní problém při řešení zneužití zranitelností nultého dne

Základní problém, který znesnadňuje účinné potírání zneužití zranitelností nultého dne, jednoduše představují samy státy a jejich přístup k mezinárodní spolupráci, obrazně řečeno: rozeklaný ve dví.

Mezinárodní spolupráce v oblasti kybernetické bezpečnosti je bezesporu základním předpokladem pro existenci bezpečnější informační společnosti. Může být proto překvapením, že tato spolupráce příliš nefunguje. Důvody nespočívají jen v absenci komplexní mezinárodní úmluvy zabývající se tímto problémem a z toho vyplývajícími otázkami právní odpovědnosti a donucení,[36] hlavním problémem je především politická polarizace jednotlivých států a z toho pramenící problém neochoty domluvit se na řešení řady palčivých otázek. Ostatně jak již v září roku 2019 potvrdila debata Otevřené pracovní skupiny k problematice informačních a telekomunikačních technologií při OSN (zkr. OEWG[37]),

---

33 Viz např. zneužití nultého dne v aplikaci Adobe Flash díky chybě v zabezpečení CVE-2015-3043 či CVE-2015-1701. In Threat Research FIREEYE LABS. Operation RussianDoll: Adobe & Windows Zero-Day Exploits Likely Leveraged by Russia's APT28 in Highly-Targeted Attack. *FireEye* [online]. 2020 [cit. 2025-03-15]. Dostupné z: https://www.fireeye.com/blog/threat-research/2015/04/probable_apt28_useo.html.

34 Obdobně např. CHOWDHURY, Tamal Dutta. Using Artificial Intelligence To Counter Zero-Day Cyber Attacks: A Security Imperative During The COVID-19 Global Crisis. *LinkedIn Corporation* [online]. 2020 [cit. 2025-03-15]. Dostupné z: https://www.linkedin.com/pulse/using-artificial-intelligence-counter-zero-day-cyber-dutta-chowdhury/?articleId=6646779218049011712.

35 Obdobně DAVIS, Steve. Sweden's AI Governance & Cybersecurity: Safeguarding Data, Digital, Energy, and AI Systems. *LinkedIn Corporation* [online]. 6. 2. 2025 [cit. 2025-03-15]. Dostupné z: https://www.linkedin.com/pulse/swedens-ai-governance-cybersecurity-safeguarding-data-steve-davis-maiwf/?trackingId=XgVlJ8Tm67KaKTWry2PAWg%3D%3D.

36 Srov. MRÁZEK, Josef. *Mezinárodní právo v kybernetickém prostoru*, s. 539. K tomu obdobně dále viz SMEJKAL, Vladimír. *Kybernetická kriminalita*. 2. vyd. Plzeň: Aleš Čeněk, 2018, s. 764. Profesor Smejkal je názoru, že by měla být uzavřena Úmluva o internetu a to se všemi státy světa, aby nevznikaly *oázy kyberterorismu*.

37 Open-ended working group on developments in the field of information and telecommunications in the context of international security.

názory jednotlivých států na povahu hrozeb v kyberprostoru se diametrálně rozcházejí. Zatímco západní státy v čele s USA a EU obvykle spatřují největší hrozbu v sofistikovaných kybernetických útocích některých agresorů, zejména Číny a Ruska na kritické informační infrastruktury jiných států a dále se v případě těchto „agresorů" obávají, že ve jménu národní bezpečnosti budou pokračovat v omezování komunikační svobody a svobody přístupu k informacím na internetu – ať už jeho fragmentarizováním, či zaváděním cenzury, naopak východní státy spatřují hlavní problém rozmachu kybernetického terorismu a kyberkriminality v nedostatečné kontrole západních států nad kyberprostorem.[38] Zatímco západní státy včetně České republiky[39] jsou povětšinou utkvělého názoru, že aktuálně platné prostředky mezinárodního práva veřejného jsou víceméně dostačujícím nástrojem, který jen musíme umět správně používat, respektive vykládat (jakkoli je zároveň paradoxem, že např. USA neuznávají ani statut Mezinárodního trestního soudu, což americká administrativa pod vedením staronového prezidenta Donalda Trumpa jen akcentuje), východní státy stejný názor nesdílí.[40] Naopak se dlouhodobě snaží v mezinárodní debatě prosadit pojetí kyberprostoru jako prostoru stojícího „mimo právo", který vyžaduje speciální mezinárodněprávní úpravu, pokud možno zdůrazňující suverénní práva států na úkor základních lidských práv a svobod. Nejčastějším argumentem světových lídrů, proč se tedy nelze v zásadě domluvit, tak nakonec bývá celkem tradiční a dosti výmluvný argument, že národ, který zastupují, definují prostě jiné potřeby. I když je platnost onoho argumentu přinejmenším sporná, žijeme-li současně v éře internetu a sociálních sítí, díky nimž se národy stávají exteritoriálními jednotkami sdíleného jazyka a kultury,[41] složitost celého problému umocňuje fakt, že státy samy masivně podporují systematické pronikání do kyberprostoru těch „druhých", a to nikoliv jen z bohulibých důvodů. Je to takový souboj věčně chtěné neviditelnosti[42] a farizejství, který nespočívá v ničem jiném než v cílené kybernetické špionáži sousedů. Současnou situaci, která je výsledkem selhání minulých jednání na mezinárodní úrovni, tak do jisté míry vystihuje, co již v roce 1990 napsal W. Hays Parks, a to že OSN doposud nepřišla s žádným seriózním návrhem, který by ono mezinárodní

38 KADLČÁK, Richard. *Problémy kybernetické bezpečnosti v kontextu mezinárodních vztahů* [přednáška]. Praha: Workshop AV ČR. 27. 11. 2019.

39 Viz Czechia has published a Position Paper on the Application of International Law in Cyberspace. *Ministerstvo zahraničních věcí ČR* [online]. 27. 2. 2024 [cit. 2025-03-15]. Dostupné z: https://mzv.gov.cz/jnp/en/foreign_relations/international_law/news/czechia_has_published_a_position_paper.html.

40 Připomeňme však, že pro země východního bloku je již tradičně příznačná mnohem větší míra nedůvěry v nové věci a zároveň tendence mít všechno pod kontrolou. Proto se také nelze divit tomu, že Rusko ještě před vypuknutím válečného konfliktu na Ukrajině přistoupilo k vytvoření vlastního, tj. na jakémkoliv jiném státě nezávislého internetu *(RusNet)* či že čínský prezident Si Ťin-pching na summitu skupiny zemí G20 dne 21. 11. 2020 navrhl v souvislosti s pandemií Covid-19, aby každému člověku cestujícímu do zahraničí byl přidělen QR kód a mohl být tak mezinárodně za pomocí informačních a komunikačních technologií sledován jeho pohyb (vzpomeňme i na jiné úvahy o zavádění plošných „trasovačů" též v jiných zemích) – viz YEUNG, Karen. Coronavirus: Chinese President Xi Jinping proposes global QR code system to help free up travel. *South China Morning Post* [online]. 2020 [cit. 2025-03-15]. Dostupné z: https://www.scmp.com/news/china/diplomacy/article/3110871/coronavirus-chinese-president-xi-jinping-proposes-global-qr.

41 BAUMAN, Zygmunt – DONSKIS, Leonidas. *Morální slepota – ztráta citlivosti v tekuté modernitě*. Praha: Pulchra, 2023, s. 79.

42 Jakkoli se některé státy dokonce neštítí onen neviditelný plášť někdy i odhodit a přiznat se k tomu; např. v březnu roku 2025 USA v souvislosti se snahou sjednat příměří mezi Ukrajinou a Ruskem a zejména obnovením diplomatických vztahů s Ruskem zcela otevřeně veřejně přiznaly, že proti Rusku prováděly řadu kybernetických operací, když prohlásily, že tyto pozastavují. Viz např. článek Spojené státy nařídily zastavení kybernetických operací proti Rusku. Je to riskantní krok, píšou média. *iRozhlas* [online]. 3. 3. 2025 [cit. 2025-03-15]. Dostupné z: https://www.irozhlas.cz/zpravy-svet/spojene-staty-naridily-zastaveni-kybernetickych-operaci-proti-rusku-je-riskantni_2503031236_kvr.

„špiclování“ (Parks mluví o tichém shromažďování zpravodajských informací o „protivníkovi“) jasně označil za porušení mezinárodního práva.[43] Právě OSN by přitom měla mít vedoucí roli při podpoře dialogu mezi státy ke všem tématům, včetně uplatňování mezinárodního práva v kyberprostoru. V tomto směru je proto přínosem, že Valné shromáždění OSN v roce 2018 ustavilo k řešení těchto některých problémů alespoň dva poradní orgány: OEWG,[44] přístupnou všem členským státům OSN (viz rezoluce A/RES/73/27[45]), a dále Skupinu vládních expertů k prosazování zodpovědného chování v kyberprostoru v kontextu mezinárodní bezpečnosti (dále jen „GGE“[46]), s členstvím 25 států (mezi nimi např. Mexiko, Nizozemsko, Norsko, Francie, Rusko, ale i Čína), přičemž smyslem této skupiny vládních odborníků z jednotlivých zemí, která dne 14. července 2021 vydala „závěrečnou“ zprávu,[47] byla rovněž konzultace s regionálními organizacemi, jakými jsou Africká unie, EU, Organizace amerických států, Organizace pro bezpečnost a spolupráci v Evropě (OBSE)[48] a Regionální fórum Sdružení národů jihovýchodní Asie (viz odstavec 3 rezoluce A/RES/73/266[49]). Posláním obou uskupení bylo přispět ke stabilizaci kybernetického prostoru skrze dosažení konsensu v pěti klíčových tématických oblastech:

1) současné a budoucí hrozby v kyberprostoru;
2) aplikace mezinárodního práva na informační a komunikační technologie;
3) další rozvoj pravidel, norem a principů chování obsažených ve zprávě Skupiny vládních odborníků Valného shromáždění OSN pro vývoj v oblasti informací a telekomunikací v kontextu mezinárodní bezpečnosti (tj. předchůdkyně GGE) z roku 2015;
4) opatření k budování důvěry (tzv. CBMs – confidence-building measures);
5) budování kapacit a odolnosti v oblasti kybernetické bezpečnosti.[50]

---

43 PARKS, W. Hays. The International Law of Intelligence Collection. In: MOORE, John Norton et al. eds. *National security law 433*. 1990, s. 433–434; LIN, Herbert. Offensive Cyber Operations and the Use of Force. *Journal of National Security Law & Policy* [online]. 2010, Vol. 4, No. 63, s. 72 [cit. 2025-03-15]. Dostupné z: https://jnslp.com/wp-content/uploads/2010/08/06_Lin.pdf.

44 Dne 31. prosince 2020 přijalo Valné shromáždění OSN rezoluci A/RES/75/240, kterou zřídilo „novou“ Otevřenou pracovní skupinu pro bezpečnost informačních a komunikačních technologií a jejich využívání (Open-ended Working Group on security of and in the use of information and communications technologies) na období 2021–2025. Úkolem této „nové“ pětileté OEWG je pokračovat v pravidelném institucionálním dialogu s širokou účastí států na pravidelných zasedáních v New Yorku.

45 Dostupné z: https://undocs.org/A/RES/73/27.

46 Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security. Skupina uspořádala čtyři formální zasedání: první od 9. do 13. 12. 2019 v sídle OSN, druhé od 24. do 28. 2. 2020 v Ženevě, třetí ve virtuálním formátu od 5. do 9. 4. 2021 a čtvrté ve virtuálním formátu od 24. do 28. 5. 2021. Třetí zasedání skupiny bylo odloženo na základě rozhodnutí Valného shromáždění OSN 75/551 kvůli pandemii covid-19.

47 Dostupné z: https://dig.watch/wp-content/uploads/2022/08/UN-GGE-Report-2021.pdf.

48 V roce 2012 byla také zřízena neformální pracovní skupina OBSE pro kybernetickou bezpečnost (OSCE Informal Working Group on Cyber Security, IWG) skládající se ze států OBSE, jejímž úkolem bylo vypracovat soubor CBMs. Celkem šestnáct opatření si dává za cíl posílit mezinárodní spolupráci, zvýšit transparentnost, předvídatelnost, stabilitu a zároveň snížit riziko nedorozumění a konfliktů spojených s využíváním informačních a komunikačních technologií. Ačkoli tato opatření nejsou právně závazná, všech 57 států OBSE se politicky zavázalo je dodržovat. CBMs v rámci OBSE: 1. Threat information sharing; 2. Cross-border cooperation; 3. Hold consultations; 4. Open, interoperable, secure, and reliable Internet; 5. Capacity building platform; 6. Legislation to facilitate cooperation; 7. National strategies, policies and programs; 8. Points of contact; 9. ICT terminologies; 10. OSCE platforms for Exchange; 11. Regular IWG meetings; 12. Act jointly to reduce tensions; 13. Effective communication channels; 14. Public-private Partnerships. (PPPs); 15. Critical infrastructure protection; 16. Sharing vulnerability information.

49 Dostupné z: https://undocs.org/en/A/RES/73/266.

50 KADLČÁK, Richard. *Problémy kybernetické bezpečnosti v kontextu mezinárodních vztahů*.

Rovněž je v současné době nesporně vítaným krokem sjednání Úmluvy o kyberkriminalitě při OSN. Tato úmluva totiž kriminalizuje neoprávněný přístup k celému systému informačních a komunikačních technologií nebo k jeho části (viz čl. 7 odst. 1) i odposlech neveřejných přenosů elektronických údajů do informačního a komunikačního technologického systému, z něj nebo v jeho rámci, včetně elektromagnetických emisí ze systému informačních a komunikačních technologií, který tyto elektronické údaje přenáší (viz čl. 8). Otázkou však zůstává, do jaké míry může úmluva reálně dopadat na samotné aktéry mezinárodní špionáže. Je iluzorní si myslet, že státy ze dne na den přestanou s cíleným „špiclováním". Ostatně, jak někteří uvádějí, již historicky např. Paul Maxwell,[51] jde o činnost v dnešní době široce praktikovanou a v mezích také tolerovanou a v současném geopoliticky a ekonomicky napjatém světě navíc dramaticky se rozvíjející především díky využívání různých bezpečnostních chyb v běžně používaném softwaru, kupříkladu typu Microsoft Outlook, respektive jeho slabých, zranitelných místech, o nichž neví jeho výrobce.

Zneužití zranitelností nultého dne je tak příčinou kybernetických útoků některých států, potažmo jimi řízených a sponzorovaných skupin na kritickou informační infrastrukturu jiného státu. A ačkoliv jsou některé z těchto útoků následně i samotnými státy ospravedlňovány, protože mají být údajně „legálně" páchány v jakési sebeobraně, např. z důvodů zamezení teroristického útoku,[52] je nezpochybnitelným faktem, že v převážné míře případů představují konflikt vojenský, kvůli němuž jsou na životech ohroženi sami civilisté. S dynamickým rozvojem umělé inteligence a na ní založených technologiích, jak již ostatně bylo naznačeno, navíc získávají nový rozměr.[53] Na mezinárodní scéně se tak objevují nová rizika pro společnost i jednotlivce,[54] která mohou mít vliv na politickou soutěž, společenské narativy či stabilitu mezinárodního míru. Snad právě proto by měly být precizně nastaveny normy mezinárodního práva veřejného, jejichž účelem je ochraňovat veřejný zájem, jakým je i bezpečnost, a všechny, nikoliv jen některé činnosti uskutečňované v kybernetickém prostoru, by měly být s nimi v souladu.[55] Je proto zcela na místě, pokud státy

---

51 Viz MAXWELL, Paul. Stockpiling Zero-Day Exploits: The Next International Weapons Taboo. In: *12th International Conference on Cyber Warfare and Security*. Dayton, Ohio, USA, s. 237. [online]. March 2017 [cit. 2025-03-15]. Dostupné z: https://1url.cz/6riTs.

52 K jednomu z historicky nejznámějších kybernetických útoků, údajně realizovaných v zájmu posílení mezinárodní bezpečnosti, došlo např. v r. 2010. Šlo o útok na íránskou jadernou elektrárnu Búšehr, respektive na její závod k obohacování uranu. Útočníci, patrně tajné služby USA a Izraele, tehdy využili chyby v operačním systému Microsoft Windows, červa *Stuxnet*, k tomu, aby vyřadili z provozu jaderné centrifugy.

53 Jakkoli nelze v současné době nevnímat snahy některých států, unií či mezinárodních institucí přijímat právní nástroje k regulaci systémů využívajících AI. Zmiňme např. *Principy Organizace pro hospodářskou spolupráci a rozvoj* (OECD) z roku 2019, jež představují vůbec první mezivládní standard pro AI, respektive soubor etických pokynů pro užívání AI, na něž navazuje nejen nařízení Evropského parlamentu a Rady (EU) 2024/1689 ze dne 13. června 2024, kterým se stanoví harmonizovaná pravidla pro umělou inteligenci a mění nařízení (ES) č. 300/2008, (EU) č. 167/2013, (EU) č. 168/2013, (EU) 2018/858, (EU) 2018/1139 a (EU) 2019/2144 a směrnice 2014/90/EU, (EU) 2016/797 a (EU) 2020/1828 (akt o umělé inteligenci), schválené Evropským parlamentem dne 13. března 2024, Radou EU pak dne 21. 5. 2024, ale také globální rezoluce OSN k AI, kterou Valné shromáždění OSN přijalo na svém zasedání dne 21. 3. 2024. Z dalších je pak možno uvést např. tzv. *Bletchleyskou deklaraci* neboli *Pokyny pro bezpečný vývoj systémů AI*, které byly přijaty na mezinárodním summitu ke kybernetické politice pořádaném Velkou Británií v Bletchley v listopadu 2023 (dostupné z: https://www.ncsc.gov.uk/files/Guidelines-for-secure-AI-system-development.pdf).

54 Např. panenka *Cayla* je zářným příkladem toho, jak může být hackry zneužita dětská hračka. Viz NERAD, Filip. Zamíří ‚šmírující' panenka Cayla i na české pulty? Záleží na obchodní inspekci, vzkazuje Jourová. *iRozhlas* [online]. 21. 2. 2017 [cit. 2025-03-15]. Dostupné z: https://www.irozhlas.cz/zpravy-domov/zamiri-smirujici-panenka-cayla-i-na-ceske-pulty-zalezi-na-obchodni-inspekci-vzkazuje-jourova_201702210640_dbernardy.

55 Viz MRÁZEK, Josef. *Mezinárodní právo v kybernetickém prostoru*, s. 537.

přijímají úmluvy o kyberkriminalitě, jakkoli praktickou otázkou zůstává jejich vymahatelnost. Podporují pořádání různých summitů či konferencí na téma kybernetické bezpečnosti[56] a realizují diskuse o globální správě umělé inteligence v rámci Globálního digitálního paktu a také o vojenském využití umělé inteligence, respektive o legálních autonomních zbraňových systémech, které formují způsob vývoje a využití AI. To je mimochodem nanejvýše žádoucí, reflektujeme-li možná nebezpečí v obranném průmyslu spojovaná t. č. zejména s americkými společnostmi *Anduril Industries*[57] či *Palantir Technologies*,[58] a zvláště pak vezmeme-li v úvahu poněkud temné závěry vyplývající např. ze Zprávy o stavu kybernetické bezpečnosti v Unii,[59] které v jádru vyznívají v tom smyslu, že umělá inteligence oportunisticky proces vyhledávání zranitelných míst softwaru výrazně urychluje, čímž posiluje i pravděpodobnost vzniku nových kybernetických útoků.

Na druhou stranu, pokud do dnešních dnů nejsou mezinárodní nástroje patřičně nastaveny (ve smyslu možnosti jejich rychlého použití), třebaže se o to paradoxně od počátku devadesátých let snažilo do jisté míry i Rusko,[60] má smysl tak zásadní věc, jakou je problém „zneužití nultého dne" řešit cestou standardních mezinárodních úmluv? I když bychom totiž křísili mnohé nástroje mezinárodního práva veřejného z pomyslné narkózy, nezůstalo by jejich aktivování nadále nesmírně komplikované? Žijeme přeci v éře, kterou definuje rychlost informací, a tedy i snaha o nalezení rychlého způsobu řešení problému, který, jak se shodují i státy v rámci OEWG, umělá inteligence a kvantová výpočetní technika zásadně zrychlují. Jak tedy tento problém správně právně uchopit a jak se mu bránit, když je sporná již ta otázka, zda se vůbec dá subsumovat pod kybernetický incident?

---

56 Např. konference typu britské CYBERUK – podrobněji viz CYBERUK [online]. [cit. 2025-03-15], dostupné z: https://www.ncsc.gov.uk/section/keep-up-to-date/cyberuk či americké RSAConference – podrobněji viz RSAConference [online]. [cit. 2025-03-15]. Dostupné z: https://www.rsaconference.com/usa. Z pohledu EU jde pak především o zasedání Rady EU, na kterých jsou k problematice kybernetické bezpečnosti prezentovány pozice Evropské komise, Agentury ENISA, EUROPOLu, Evropského centra kompetencí pro kybernetickou bezpečnost (ECCC), Skupiny pro spolupráci NIS, CSIRTs Network či Evropské sítě styčných organizací pro řešení kybernetických krizí, tzv. EU-CyCLONe, jíž předcházel plán Evropské komise z roku 2017, označovaný jako „kybernetický blueprint" [dle čl. 16 směrnice Evropského parlamentu a Rady (EU) 2022/2555 ze dne 14. 12. 2022 o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii a o změně nařízení (EU) č. 910/2014 a směrnice (EU) 2018/1972 a o zrušení směrnice (EU) 2016/1148 (dále jen „směrnice NIS 2")]. Velmi příhodným místem pro tuto debatu jsou pak dále akce pořádané Otevřenou pracovní skupinou pro bezpečnost informačních a komunikačních technologií a jejich využívání při OSN ve spolupráci s EU, Ústavem EU pro studium bezpečnosti (EUISS), Globálním fórem pro kybernetickou expertízu (GFCE) a Institutem OSN pro výzkum odzbrojení (UNIDIR).

57 Ke jmenované společnosti více na webových stránkách https://www.anduril.com.

58 Ke jmenované společnosti více na webových stránkách https://www.palantir.com.

59 V ní se totiž na str. 14 výslovně uvádí.: *"Furthermore, the systems of EU MSs as well as Union entities continue to be exposed to the exploitation of known and unknown vulnerabilities. In light of the observations and findings concerning the cyber threat landscape, the cyber threat level to the EU during the reporting period was assessed as substantial, meaning that it is likely entities are being directly targeted by threat actors or could be exposed to breaches using recent discovered vulnerabilities, while serious disruptions of essential and important entities or EUIBAs is considered a realistic possibility. The substantial severity of the threat is also based on the intent and capability of the threat actors. While the threat actors we tracked demonstrated the intent to generate high-scale cybersecurity incidents in Europe, only some of them had previously displayed the capabilities needed to cause them."* Dále také viz str. 19: *"Finally, while multiple state-nexus threat groups reportedly continue to exploit zero-day vulnerabilities in the context of targeted espionage, unpatched vulnerabilities (N-day vulnerabilities) remain a greater risk due to their impact on a wide array of organisations."*

60 To již totiž v roce 1998 v rámci mezinárodního jednání o omezení kybernetického konfliktu probíhajícího na půdě OSN navrhovalo *dohodu o kontrole zbraní*, která by zakazovala užití kyberprostoru pro vojenské účely, což západní státy v čele s USA odmítaly. Bohužel to samé Rusko dnes porušuje klíčové principy a závazky Charty OSN a řadu dalších smluv.

4. Možnosti řešení zneužití zranitelností nultého dne mezinárodními nástroji

V této části článku se upíná pozornost k základním přístupům a strategiím, které mohou být (či pozvolna již jsou) implementovány na mezinárodní úrovni za účelem prevence a mitigace dopadů zneužití zranitelností nultého dne, a v jádru k základní otázce, zda mezinárodní právo veřejné je vůbec vhodným prostředkem k řešení tohoto problému.

4.1 Zveřejnění chyb jako prevence a aplikace čl. 39 Charty OSN?

Odborníci se neshodují zcela v názoru, zda mají být zranitelná místa v jednotlivých systémech po jejich odhalení průběžně zveřejňována, a pokud ano, do jaké míry. Opomeneme-li totiž světlou stránku jejich zveřejnění, díky kterému společnost disponuje povědomím o existenci určitých problémů v softwaru, pročež z toho důvodu se na ně lépe může připravit (např. zabezpečením kritických dat), ozývají se též hlasy, že s větší informovaností roste riziko častějších, sofistikovanějších útoků. V kontextu hrozeb, které přináší umělá inteligence, se těmto obavám rozhodně nelze divit. Někteří jsou proto názoru opačného, tedy že udržováním předmětných informací v tajnosti se může vznik nových kybernetických útoků omezit.[61]

Tedy v principu se zde profilují dva možné přístupy: kladný, prosazující zveřejňování zranitelných míst (což je vlastní i většině členských států EU, respektive evropské regulaci – NIS 2, CRA,[62] NCCS[63] a EUIBA[64] totiž obsahují povinné nebo dobrovolné hlášení zranitelnosti[65]), a záporný jako jeho přímý protiklad. Nutno přitom poznamenat, že na tom kladném se zpočátku velkou měrou podíleli též etičtí hackeři, kteří věřili, že svými činy vykonávají pro společnost dobré skutky. Aktuálně jsou spíše zmiňovány tzv. *Bug Bounty* programy, které představují výzvy různých společností, typu Google nebo Microsoft, motivující IT specialisty k objevování chyb a jejich zveřejňování pod příslibem zajímavých finančních odměn. Za nalezení programátorských chyb jsou ovšem ochotni zaplatit velice dobře nejen samotní výrobci softwarů, ale i jednotlivé státy. Tu se rýsuje onen pomyslný kámen úrazu. Právě ona finanční motivace bývá příčinou, proč se s objevenými informacemi vyplatí spíše obchodovat jako s velmi lukrativními komoditami za miliony dolarů ilegálně. Prostě zisk má přednost před etikou. Pokud se navíc státy samy zapojují do tohoto byznysu ve snaze sbírat údaje o zranitelných místech a využívat je pak třeba k zastrašování protivníka, čímž *de facto* podporují bujení černého trhu s nimi (dá se říci, že v průběhu let vznikla doslova celá ekonomika *Zero-Day Exploits*), pak jak zcela správně

---

61 MAXWELL, Paul. *Stockpiling Zero-Day Exploits: The Next International Weapons Taboo*, s. 237. Dostupné z: https://1url.cz/6riTs.

62 *The European Cyber Resilience Act (CRA)*, tj. nařízení Evropského parlamentu a Rady (EU) 2024/2847 ze dne 23. října 2024 o horizontálních požadavcích na kybernetickou bezpečnost produktů s digitálními prvky a o změně nařízení (EU) č. 168/2013 a (EU) 2019/1020 a směrnice (EU) 2020/1828 (akt o kybernetické odolnosti).

63 Viz nařízení Evropského parlamentu a Rady (EU) 2021/887 ze dne 20. 5. 2021, kterým se zřizuje Evropské průmyslové, technologické a výzkumné centrum kompetencí pro kybernetickou bezpečnost a síť národních koordinačních center.

64 Nařízení Evropského parlamentu a Rady (EU, Euratom) 2023/2841 ze dne 13. 12. 2023, kterým se stanoví opatření k zajištění vysoké společné úrovně kybernetické bezpečnosti v orgánech, institucích a jiných subjektech Unie.

65 Viz ENISA. *2024 Report On The State of The Cybersecurity In The Union*, s. 55 [online]. 2024 [cit. 2025-03-15]. Dostupné z: https://www.enisa.europa.eu/sites/default/files/2024-11/2024%20Report%20on%20the%20State%20of%20the%20Cybersecurity%20in%20the%20Union.pdf.

uvádí Maxwell, vedlejším efektem tohoto kolotoče je, že státy samy zásadně přispívají k nejistotě našeho už tak zasíťovaného světa, místo toho, aby zlepšovaly kybernetickou bezpečnost.[66]

Záporný přístup, preferující utajování informací, pak toto prostředí nejenže posiluje, ale vytváří i z jednotlivých států v závislosti na jejich informovanosti, státy s mocnými zpravodajskými službami a státy, jež jsou v podstatě v pozici „obětních beránků". Jde tedy o jistou primitivnost ovládanou ziskem a mocí mít informační převahu nad ostatními. Neshoda na jednom společném přístupu v mezinárodním kontextu je konečně příčinou toho, proč dodneška nemáme účinný právní prostředek, jak problém zneužití nultého dne řešit. Podle Maxwella by však šlo skoncovat s tímto černým trhem rázně. Stačilo by, pokud by jediná mocnost všechny informace o zranitelných místech prostě nakoupila a vyzradila je, což je ovšem utopie. Pokud by navíc měli všichni stejné informace, vedlo by to skutečně k nalezení kýžené rovnováhy?[67]

Pomineme-li evropský recept, jenž spočívá ve vytváření úložišť zranitelností, která mohou být využita ke zlepšení situačního povědomí (pokud jde o subjekty spadající pod NIS 2, „řešení a zveřejňování zranitelnosti" je jedním z povinných opatření pro řízení rizik v oblasti kybernetické bezpečnosti, která se musí uplatňovat[68]), možná by nakonec mohla být řešením nová globální úmluva, která by nezaváděla jen mezinárodní sankce, o jejichž účinnosti lze někdy vésti polemiku, ale která by zaručovala všem signatářům určité ekonomické, bezpečnostní nebo reputační výhody. Mohlo by se jednat o úmluvu o zákazu obchodování se softwarovými chybami s tím, že státy, které by se k takovéto úmluvě připojily, by se automaticky těšily lepší pověsti na mezinárodním trhu; např. by mohly získat preferenční přístup k různým technologickým inovacím. To by vedlo ke zvýšení jejich celkové kredibility a posilování jejich kybernetického štítu.[69] Firmy a instituce z těchto států by mohly snadněji získat přístup k mezinárodním investicím a dotacím na projekty kybernetické bezpečnosti, čímž by se zlepšila jejich konkurenceschopnost a statut na globální úrovni. Celkově by tak nová úmluva mohla přispět nejen ke zvýšení bezpečnosti, ale i k ekonomickému růstu a posílení postavení signatářských států v diplomatických jednáních na světové scéně. To by koneckonců mohlo přivábit do veřejné služby i kvalifikované odborníky v oblasti kybernetické bezpečnosti, v důsledku čehož by došlo k eliminaci přetrvávajícího problému jejich nedostatku (*skills gap*). Současně by OSN mohla vést mezinárodní registr států a organizací, z něhož by bylo zjistitelné, kdo podporuje obchodování se softwarovými chybami či tyto nezveřejňuje.

---

66 MAXWELL, Paul. *Stockpiling Zero-Day Exploits: The Next International Weapons Taboo*, s. 237. Dostupné z: https://1url.cz/6riTs.

67 Ibidem.

68 Viz ENISA. *2024 Report On The State of The Cybersecurity In The Union*, s. 55. Dostupné z: https://www.enisa.europa.eu/sites/default/files/2024-11/2024%20Report%20on%20the%20State%20of%20the%20Cybersecurity%20in%20the%20Union.pdf.

69 I když jsou kybernetické útoky bezpochyby nebezpečné pro jakýkoliv stát a jeho obyvatele, pravděpodobnější verzí je, že většímu počtu útoků budou zpravidla čelit ty státy, které jsou např. ekonomicky vyspělejší, notabene jsou významnější. Lze tak např. očekávat, že častější obětí útoku mohou být USA oproti malému africkému státu. Schopnost překonat kybernetický štít USA bude ovšem mnohem složitějším úkolem pro útočníka. Na uvedeném příkladu se tedy krásně ilustruje skutečnost, že rozdíly v kybernetické ochraně (obraně), co se týče její úrovně, se značně odvíjejí též od celkové povědomosti té dané země o existenci kybernetických hrozeb. Tedy stát, který čelí většímu množství útoků, má logicky více zkušeností a může být také mnohem lépe připraven.

Teoreticky bychom mohli uvažovat i o tom, zda by se „nezveřejňování" údajů o zranitelných místech a kupčení s nimi nemělo pro nebezpečí, které jejich uchovávání v tajnosti představuje, subsumovat pod „ohrožení" mezinárodního míru. Pokud by tato myšlenka totiž průchozí byla, Rada bezpečnosti by podle čl. 40 Charty OSN mohla přinutit stát, o který jde, aby splnil zatímní opatření, jež považuje za nutná nebo žádoucí (těmi by mohlo být zveřejnění shromážděných údajů o zranitelných místech) s tím, že taková zatímní opatření nesmí být na újmu práv, nároků nebo postavení stran konfliktu, o které jde. Řešením by také mohlo být obrácení důkazního břemene, tedy „nejít" vyloženě po útočníkovi, ale po subjektu, který měl kybernetickou bezpečnost na starost. Posílit by se pak měla také role Mezinárodního soudního dvora, který t. č. není povolán k tomu, aby posuzoval vhodnost opatření Rady bezpečnosti, zejména pokud tato opatření slouží k zachování světového míru; nabíledni je pak aktivace čl. 38 odst. 2 Statutu Mezinárodního soudního dvora, podle něhož může soudní dvůr rozhodovat i *ex aequo et bono*.[70] Popřípadě lze zmínit též článek 41 Charty OSN, který umožňuje Radě bezpečnosti v případě, kdy je ohrožen mezinárodní mír a bezpečnost, uvalení různých nevojenských opatření (ta mohou zahrnovat úplné nebo částečné přerušení hospodářských vztahů, železniční, námořní, letecké, poštovní, telegrafické, rádiové a jiné spojení a přerušení diplomatických styků) či článek 42, jenž povoluje použití ozbrojených sil, pokud nevojenská opatření nejsou dostatečná. Je však otázkou, zda případná opatření proti zneužití zranitelností nultého dne lze připodobňovat sankcím proti Jihoafrické republice[71] nebo proti bývalé Jugoslávii.

4.2 Kybernetická bezpečnost jako veřejný statek

S názory, že kybernetická bezpečnost má být považována za veřejný statek anebo, přesněji řečeno dle Rosenzweiga, na sdílení informací o hrozbách, včetně zranitelných míst v softwaru, se má pohlížet jako na veřejný statek,[72] lze jen souznít. Řeč je o „koncepci kybernetické bezpečnosti jako veřejném statku", o které podrobně pojednává také Maxwell. Pozitivem celé této koncepce je, že by se na uvedený problém narušení kybernetické bezpečnosti nahlíželo jako na porušení něčeho, co je obecně každému právem garantováno. Tak jako lidé mají právo na život, svobodu a osobní bezpečnost dle čl. 3 Všeobecné deklarace lidských práv OSN, na svobodu pohybu, právo na informace, jež jsou součástí jejich práva svobodně se projevovat, právo využívat nejzákladnější produkty přírody, mělo by být lidem zaručeno také právo na nerušené užívání kyberprostoru a jejich bezpečnost v něm s možností se účinně dovolat porušení tohoto práva, pokud někdo kybernetické prostředí úmyslně zneužije, a to nejen sběrem údajů o nich, ale i o chybách v systémech, jež v konečném důsledku použije proti nim; např. v podobě znemožnění přístupu ke zdravotní péči v důsledku dlouhodobého výpadku informačního systému nemocnice způso-

70 SEIDL-HOHENVELDERN, Ignaz. *Mezinárodní právo veřejné*. 3. vyd. Praha: Wolters Kluwer, 2001, s. 328.

71 V roce 1963 Rada bezpečnosti přijala rezoluci č. 181, která uvalila dobrovolné zbrojní embargo na Jihoafrickou republiku kvůli její politice apartheidu. V roce 1977 byla přijata rezoluce č. 418, která zbrojní embargo rozšířila a učinila ho povinným.

72 Rosenzweig uvádí, že kybernetická bezpečnost není v současné době veřejným statkem. Tím je dle jeho názoru sdílení informací o hrozbách, včetně zranitelných míst v softwaru. ROSENZWEIG, P. *Cybersecurity, the Public/Private "Partnership," and Public Goods*. Hoover National Security and Law Task Force. 2011, s. 29. Dostupné z: http://ssrn.com/abstract=1923869; MAXWELL, Paul. *Stockpiling Zero-Day Exploits: The Next International Weapons Taboo*, s. 238. Dostupné z: https://1url.cz/6riTs.

beného kybernetickým útokem hackra, jenž využil skryté zranitelnosti systému. Veřejné statky založené veřejným právem k zabezpečení těchto obecných potřeb primárně slouží. V podstatě tu jde o vytváření univerzální hodnoty a potřeby ji vymáhat srovnatelným způsobem jako třeba porušení lidského práva na veřejné zdraví[73] (čl. 29 odst. 2 Všeobecné deklarace lidských práv OSN). Ani v Evropě se totiž nesetkáme s tím, že by někdo dodržování kybernetické bezpečnosti v této podobě vymáhal. Konstrukce kybernetické bezpečnosti jako veřejného statku by však umožňovala vytvoření patřičných právních záruk a mohla by alternativně (při příměru k právu na veřejné zdraví) vést k vytvoření obdobné instituce typu Světové zdravotnické organizace (*World Health Organization*), která by podporovala nejen účinnou mezinárodní spolupráci na vládní i akademické úrovni, ale i ohlašování incidentů v mezinárodním kyberprostoru, včetně povinného zveřejňování zranitelných míst. Mohlo by jít o Globální digitální bezpečnostní radu OSN a po sankční stránce o Mezinárodní kybernetický tribunál. Tím by se, jak příhodně uvádí Kadlčák, mohl „posílit" i běžný výkon trestního práva. Tedy pokud by např. nejmenovaná státní mocnost toto právo nezabezpečila, mohla by být potrestána obdobně, jako kdyby schvalovala nebo nečinně přehlížela „týrání lidí". V podstatě uplatňování mezinárodního humanitárního práva ve vztahu k řešenému tématu se také jeví jako skvělá myšlenka, naráží však na jeden zcela zásadní problém. Tuto koncepci naprosto odmítá Čína. Jejím argumentem totiž je, že uznáním aplikovatelnosti mezinárodního humanitárního práva by *de facto* došlo k militarizaci informačních a komunikačních technologií i možnosti války v kyberprostoru.[74]

4.3 Mezinárodněprávní princip náležité péče a kybernetická diplomacie

Princip náležité péče (*due diligence*) představuje velmi důležitou zásadu mezinárodního práva, která zavazuje státy přijímat vhodná a dostatečná opatření k zajištění, že jejich území není využíváno k aktivitám v rozporu s mezinárodním právem. Tento princip nachází uplatnění v nejrůznějších oblastech, jako je ochrana životního prostředí nebo mezinárodní bezpečnost. Další možností, jak k předmětnému problému přistupovat, proto může být prosazování povinnosti náležité péče a povinnosti států zjednat nápravu, pokud je jejich území využíváno k aktivitám v rozporu s mezinárodním právem i v oblasti kybernetické bezpečnosti. Zde je však dlouhodobým problémem, že ne všechny státy přijímají náležitou péči za závazné pravidlo. Jednou za to může skutečnost, že ne všechny státy mají dostatečné technologické zdroje a odborné znalosti k monitorování a regulaci kybernetických aktivit na svém území, podruhé fakt že některé státy nemají celé své území pod kontrolou (pokud je například část území ovládána povstaleckými skupinami nebo jinými nestátními aktéry, může být obtížné zajistit, aby tyto oblasti nebyly využívány k nezákonným kybernetickým aktivitám). V kontextu kyberprostoru tak vyvstává otázka, jak princip náležité péče vlastně aplikovat v praxi, když hrozby s přeshraničním dopadem narůstají (což potvrzuje i studie agentury ENISA *Foresight 2030 Threats*[75])? A Kadlčák v této sou-

73 MAXWELL, Paul. *Stockpiling Zero-Day Exploits: The Next International Weapons Taboo*, s. 238, [online], [cit. 2025-02-15]. Dostupné z: https://1url.cz/6riTs.

74 KADLČÁK, Richard. *Problémy kybernetické bezpečnosti v kontextu mezinárodních vztahů*.

75 Dostupná z: https://www.enisa.europa.eu/sites/default/files/2024-11/Foresight%20Cybersecurity%20Threats%20For%202030%20Update%202024_0.pdf.

vislosti pokládá zcela relevantní otázky: Je třetí země např. zodpovědná za kybernetické aktivity vedené z jejího území v případě, kdy nekontroluje část území, ze kterého kybernetické útoky pocházejí? Je třetí země povinna zjednat nápravu i v případě, kdy nedisponuje dostatečnými technologickými kapacitami ke zjednání nápravy? Zde se rozchází názory rozvojových a rozvinutých zemí na míru a způsob uplatnění povinnosti náležité péče.[76] Tyto rozdíly je však třeba překonat a vytvořit efektivní mezinárodní rámec, který by umožnil koordinovanou a účinnou reakci na kybernetické hrozby. Snad nebudeme daleko od pravdy, když k tomu dodáme, že zásadní by v tomto směru měl být především rozvoj nástrojů kybernetické diplomacie. Ta sice je na unijní úrovni předmětem mnohých diskusí (viz *Cyber Diplomacy Toolbox*,[77] tzv. *Cyber Posture* a *Cyber Defence Policy*) a odráží se také v NIS 2, ovšem její dosavadní rétorika, tím méně celosvětově, problém zneužití nultého dne ze všech již v tomto článku dříve uvedených důvodů neřeší efektivně. Svým způsobem se tak některé dosavadní formy kyberdiplomacie na mezinárodní scéně mohou vyznačovat i jistou primitivností maskovanou pod nánosem všelijakých proklamací ohledně odhodlání prosazovat změny, respektive být akceschopní. V tomto směru by mohlo být nabíledni vytvoření nezávislého orgánu, jako je mezinárodní ombudsman, který by dohlížel na výkon principu náležité péče v oblasti kybernetické bezpečnosti. Takový ombudsman by mohl fungovat bez vlivu jednotlivých států, dohlížet na dodržování principu náležité péče, koordinovat mezinárodní úsilí v oblasti kybernetické bezpečnosti a výměnu informací, respektive mohl by poskytovat technickou a finanční podporu rozvojovým zemím, které nemají dostatečné kapacity k implementaci principu náležité péče (povahově by tedy jeho činnost mohla vycházet z cílů evropského projektu *CyberVAC*[78]) a sloužit jako platforma pro řešení sporů mezi státy týkajících se kybernetických aktivit.

4.4 A co umělá inteligence?

Mimo tradiční rámec mezinárodního práva, jakož i nástrojů *soft law*, by však významnou roli v pozitivním slova smyslu mohla sehrát i samotná umělá inteligence, jež by veřejnost mohla automatizovaně upozorňovat na zranitelná místa v systémech. Ať už by se jednalo o vytvoření globální sítě OSN (např. na principu evropské *CyberNet*), která by za pomocí nástrojů hlubokého strojového učení nepřetržitě monitorovala kybernetické aktivity a identifikovala státem podporované útoky či spravovala mezinárodní decentralizovaný[79] registr zranitelností, tedy jakýsi blockchainový registr exploitů, který by umožnoval sledovat, zda určitá zranitelnost byla opravena anebo s ní bylo manipulováno.

---

76 KADLČÁK, Richard. *Problémy kybernetické bezpečnosti v kontextu mezinárodních vztahů*.

77 *Cyber Diplomacy Toolbox* je rámec vytvořený EU pro společnou diplomatickou reakci na škodlivé kybernetické aktivity. Byl zaveden na základě závěrů Rady EU ze dne 19. 6. 2017 a jeho cílem je posílit schopnost EU předcházet, odrazovat a reagovat na kybernetické hrozby, které mohou ohrozit její vnější bezpečnost.

78 *CyberVac* je označení pro evropský projekt, který vychází z Cílů udržitelného rozvoje OSN 2030, zejména z cíle č. 9 c) „Zvýšit přístup k informačním a komunikačním technologiím", a je zaměřen na sdílení informací a osvědčených postupů v oblasti kybernetické bezpečnosti v zemích Latinské Ameriky. Tento projekt je financován i Českou republikou.

79 Proč decentralizovaný? Neboť jak uvádí i Patrick Zandl: *„decentralizovaný prvek je blíže měnícím se podmínkám, a může se proto pružněji rozhodovat. […] Decentralizace má vyšší nároky na vnitřní komunikaci, ale snižuje vliv vlastního organizačního úpadku na inovace. Jednotlivé součásti lze inovovat i v případě, že celek zrovna není v dobré kondici."* ZANDL, Patrick. *Mýty a naděje digitálního světa – Vše, co potřebujete vědět o kryptoměnách, umělé inteligenci a dalších převratných technologiích*. Praha: Jan Melvil Publishing, 2022, s. 47–48.

5. Shrnutí poznatků

Obecný determinant obsahu pojmu „kybernetické bezpečnosti" lze v případě národních úprav vysledovat ze smyslu a účelu právního předpisu o kybernetické bezpečnosti jako celku. Tak je tomu i v případě dosud platné a účinné české právní úpravy. Co jednotlivé předpisy spojuje např. s evropskou normou, je skutečnost, že si kladou za cíl poskytovat ochranu veřejnému kyberprostoru souborem činností, jež mají chránit společnost před kybernetickými zásahy. Tato ochrana je vytvářena stanovením souboru určitých povinností, které mají subjekty vstupující do kyberprostoru dodržovat s tím, že stát anebo mezinárodní společenství může s ohledem na nadindividuální zájmy ospravedlnit zásah do jejich práv.

Ač je toto pojetí v zásadě společné všem státům, jejich politika a předpisy se rozcházejí v názoru, jakým způsobem problém kybernetické bezpečnosti řešit. Zatímco jedny usilují o zjištění identifikace subjektu, který způsobil kybernetický bezpečnostní incident (přístup vlastní např. USA), pro druhé není až tak podstatná otázka zjištění totožnosti útočníka jako spíše obecná ochrana prostředí (přístup vlastní EU).[80] Zatímco jedny země usilují o posilování kontrolních a donucovacích mechanismů, jiné po této potřebě přizpůsobovat mezinárodní normy novým kybernetickým výzvám příliš nevolají, neboť mají za to, že jsou nastaveny dostatečně. Insuficience některých, byť zažitých pojmů pak v právní terminilogii nepřispívá k právní jistotě. Má-li být tedy kybernetická bezpečnost předmětem úspěšné mezinárodní spolupráce, je třeba souhlasit se závěrem, že případné nástroje této spolupráce – typicky mezinárodní smlouvy – musejí být stavěny na identické teleologii.[81] Zde však vzhledem k poměrně agilnímu vývoji softwaru, progresivnímu růstu jednotlivých kybernetických hrozeb,[82] různým zájmům jednotlivých států, a tedy i různému přístupu, jak kybernetickou bezpečnost řešit (např. prolomením soukromí), narážíme na zásadní problém. Tento problém primárně spočívá v neochotě diskutovat na téma možného omezení národní suverenity ve prospěch prosazování jakéhosi všeobecného blaha. Posláním kybernetické bezpečnosti je přitom předcházet kyberkriminalitě; zejména pak té, jíž se subjekty dopouštějí na kritické informační infrastruktuře. A třebaže drtivá většina kybernetických útoků není cílená a obecně míří hlavně na běžné uživatele,[83] právě kybernetickým útokům některých státních aktérů, zejména Číny, Ruska nebo Severní Korey, respektive zločineckých skupin operujících ve službách těchto aktérů, je třeba věnovat nejvyšší pozornost.

---

80 POLČÁK, Radim a kol. *Právo informačních technologií*. Praha: Wolters Kluwer ČR, 2018, s. 590–591.

81 Ibidem, s. 588. Vhodno poznamenat, že např. Společné výzkumné středisko Komise aktivně přispívá ke kybernetické bezpečnosti v EU tím, že vyvinulo taxonomii kybernetické bezpečnosti. Tím sjednocuje terminologii používanou v oblasti kybernetické bezpečnosti. Viz dostupné z: https://ec.europa.eu/digital-single-market/en/cyber-security.

82 K pojmenování výzev pro kybernetickou bezpečnost z pohledu mezinárodního práva lze využít Zprávu o globálních rizicích (*Global Risk Report*), kterou každoročně vydává Světové ekonomické forum ve švýcarském Davosu. Např. již ve zprávě za rok 2019 je jako hrozba označeno ovlivňování emocí prostřednictvím umělé inteligence, syntetické biologie, ztráta soukromí, kybernetické útoky nebo třeba *deep fakes*. Dostupné z: https://www.weforum.org/reports.

83 Běžný uživatel si při užívání IT systému totiž zpravidla nejenže volí nejmenší cestu odporu (taková cesta však nemusí být tou cestou nejbezpečnější), ale také až slepě důvěřuje třeba svému zaměstnavateli nebo vládě, že jeho data a systémy, které používá, jimi budou ochráněna. Krásným příkladem tu budiž velice časté nedostatečné zabezpečení účtu triválním heslem. I americký prezident Donald Trump by mohl vyprávět. Viz RYŠÁNEK, Adam. Hacker prolomil Trumpův Twitter. Heslo bylo „maga2020". *Seznam Zprávy* [online]. 22. 10. 2020 [cit. 2025-03-15]. Dostupné z: https://www.seznamzpravy.cz/clanek/hacker-prolomil-trumpuv-twitter-heslo-bylo-maga2020-125668.

Stěžejní problém je možno spatřovat v tom, že kybernetické vykořisťování ani kybernetická špionáž nejsou vnímány jako kybernetický útok, na který by bylo možné vztáhnout platné mezinárodní normy. To je příčinou, proč se jim nebývale daří. Zneužití zranitelností nultého dne pak představuje kybernetickou hrozbu, jež předchází kybernetické exploataci. Závažnost této hrozby podtrhuje fakt, že většina zranitelných míst v operačních systémech zůstává dlouho nezjištěna s tím, že pokud místa zjištěna jsou, údaje o nich jsou drženy v tajnosti a je s nimi čile obchodováno na černém trhu. Tato tajemná absurdita samozřejmě nahrává potenciálním útočníkům a růstu kyberkriminality.[84] Státy financované kybernetické útoky jsou tak na vzestupu. Již z toho důvodu je nutno se v rámci vytváření jednotlivých koncepcí kybernetické bezpečnosti zaměřit na hledání způsobů řešení tohoto problému, tj. nikoliv jen na bezpečnost jednotlivců, ale na celkovou bezpečnost.

V tomto článku byly zmíněny některé možnosti řešení problému. Nejde o výčet taxativní ani zmapovaný do sebemenších detailů, jeho nástin však postačuje pro závěr, že pokud kyberprostor představuje jakési virtuální veřejné prostranství, má být i jeho ochrana, respektive ochrana jeho uživatelů jednoznačně veřejným statkem. V zájmu zajištění jeho ochrany je proto nezbytné upozadit otázku, „zda" mají být zranitelná místa zveřejňována, na úkor otázky základního významu, „kdy" mají být zveřejněna, aby mohlo být včas předejito kybernetickým incidentům, které v nejhorších případech vedou i ke ztrátě na lidských životech.[85] Odpovědné státy přitom často beztrestně unikají kvůli obtížím při přičítání kybernetických útoků jejich zdroji, třebaže by na ně OSN mohlo uvalit, při špetce chtění, digitální embargo.

Závěr

Lze uzavřít, že nás stále více obklopuje technologická realita. Z našeho běžného života se stává život digitální. Pokud ten má dobře fungovat, je nezbytné budovat všeobecnou důvěru v kybernetickou bezpečnost a instituce, které ji ztělesňují. Jak má být ovšem tato důvěra v kyberprostor budována, nejsou-li státy samy schopny domluvit se na klíčových prioritách a problémech, které by mohly přispět k účelnému prosazování kybernetické ochrany? Jakkoliv byla v tomto článku označena za pomyslné „zlo" především kybernetická špionáž, prováděná státními aktéry, k té by jistě nedocházelo v tak masivní míře, pokud by státy řešily již problém zneužití zranitelností nultého dne a uměly spolu komunikovat. Ten by šlo přitom vyřešit rázně, např. tím, že by se do mezinárodní úmluvy zakotvila povinnost každého státu a jeho obyvatel zranitelná místa povinně zveřejňovat. Ať už jsou argumenty proti tomuto názoru jakékoliv, právě jejich držení v tajnosti vrhá na využitelnost informačních a komunikačních technologií stíny, díky nimž jsou lidské myšlenky v globálním měřítku zneužívány a proti svobodné vůli lidstva je ohrožena jeho mezinárodní bezpečnost. Proto lze pokládat za zcela správné uvažovat o ochraně této hodnoty. Pokud pak bylo

---

84 *„Podle oficiálních odhadů Europolu (kybernetičtí) zločinci projevují stále větší odhodlání využívat nové technologie k dosažení svých nezákonných účelů. S exponenciálně rostoucí digitalizací naší společnosti existuje mnoho příležitostí: Sociální média, DarkNet, internet věcí (IoT) a další technologie lze také využít jako nástroje k provádění nebo usnadňování trestných činů. Kromě toho se hranice mezi různými druhy trestných činů ztenčují a těžko rozlišují: terorismus, organizovaný zločin a počítačový zločin se často prolínají…"* In: Prevision Concept. *Prevision* [online]. [cit. 2025-03-15]. Dostupné z: http://www.prevision-h2020.eu/?page_id=979.

85 Obdobně viz MAXWELL, Paul. *Stockpiling Zero-Day Exploits: The Next International Weapons Taboo*, s. 242. Dostupné z: https://1url.cz/6riTs.

v tomto článku řečeno, že kyberprostor je místem neustálých změn, pak je třeba říci, že změnám samozřejmě podléhá i reálný svět, avšak v porovnání s kybernetickým světem, je reálný svět relativně statický, proto v něm právo dokáže lépe sehrát svou roli. Agilní vývoj informačních a komunikačních technologií je pro právo a zvláště pro právo mezinárodní naopak noční můrou. Obecně proto stojíme před otázkou, zda může být právo vtělené do předpisu, tím spíše do mezinárodního předpisu, spolehlivým prostředkem k naplňování požadavků na obsah kybernetické bezpečnosti? Lze snad vyjádřit naději, že v této záležitosti dosud může sehrát rozhodující roli. Zda však k tomu opravdu dojde, notabene zda v zájmu posílení právní jistoty a bezpečnosti v mezinárodním kyberprostoru dojde k uzavření „dějinotvorné" úmluvy, která přinutí státy k plné, nikoliv částečné zodpovědnosti, lze jen obtížně predikovat.

The Issue of Zero-Day Vulnerability Abuse and Its Resolution through Instruments of Public International Law

Jan Strakoš (https://orcid.org/0009-0007-9133-5904)

Abstract: This article primarily focuses on the possibilities of international cooperation in the field of cybersecurity to address the problem of exploiting zero-day vulnerabilities. The first parts of the article introduce the reader to some key cyber concepts, explaining what cyber exploitation means and how vulnerabilities in information systems, often used for this cyber-terrorism, are exploited. The phenomenon of artificial intelligence, which automates response mechanisms and improves cyber resilience, is also considered. However, it is also used by hackers to find bugs in information systems and create new strategies for real-time attacks. The third part of the article describes past and current approaches of the international community and individual states to address cyber threats in general, and examines whether international cooperation or its tools can truly enable effective solutions to this problem. In conclusion, possible approaches are proposed that the international community could adopt (or is already adopting) to prevent the abuse of zero-day vulnerabilities.

Keywords: public international law, cyber security, cyber espionage, cyber threat, exploiting the vulnerability of the zero day