Název dokumentu:

Ročenka evropské bezpečnosti pro rok 2021

Odkazy:

https://www.iss.europa.eu/content/yearbook-european-security-2021

https://www.iss.europa.eu/sites/default/files/EUISSFiles/YES_2021.pdf

Autor:

Institut Evropské unie pro bezpečnostní studia (European Union Institut for Security Studies - EUISS)

(11. října 2021)

Typ dokumentu:

Pravidelná ročenka obsahující komplexní informace na dané téma za rok 2020.

K vybraným částem dokumentu:

I. Hybridní hrozby.

Pandemie představovala zvláštní výzvu v roce 2020 s nárůstem dezinformací souvisejících s Covid-19. Po počátečním šoku způsobeném pandemií však došlo k výraznému poklesu dezinformací a pozornost se obrátila ke konspiracím a falešným zprávám o vakcínách. června 2020 Společné sdělení o Covid-19 a dezinformacích zdůraznilo rostoucí rizika záplavy informací o viru a falešných a nepřesných zpráv, které se rychle šíří po sociálních sítích. Společné sdělení upozornilo zejména na rostoucí výzvu, že nepřátelské zahraniční vlády využívají pandemie k využívání společenských obav a k vytváření rozporů mezi členskými státy EU a občany. Zvláště škodlivé jsou konspirační teorie, jako jsou instalace 5G, které jsou zodpovědné za šíření viru. Komise a vysoká představitelka vyzvala k posílení strategické komunikace uvnitř i vně EU, posílení stávajícího systému rychlého varování pro dezinformace, s mezinárodními partnery a zvýšení transparentnosti online platforem při ohlašování dezinformací a ovlivňování operací.

Zvláštní zpráva European External Action Service o dezinformacích za období od května do listopadu 2020 se navíc konkrétně zmiňovala o nárůstu „očkovací diplomacie“ ze strany Číny a Ruska s mobilizací jejich příslušných diplomatických kanálů a sdělovacích prostředků k podpoře pozitivního obrazu jejich příběhů a zprávy. Zejména prokremelská média během roku zaměřila svou pozornost na zlehčování hrozby viru a zesilování konspirací. V závěrech Rady zveřejněných dne 15. prosince EU uznala rostoucí riziko, které během pandemie představují dezinformace. Nepřátelští státní a nestátní aktéři nasazovali nekonvenční nástroje k narušení demokratických institucí a rozdělení obyvatelstva. Pandemie učinila členské státy a orgány EU zranitelnějšími vůči hybridním hrozbám a Rada znovu připomněla důležitost buňky hybridní fúze Střediska EU pro informace a situaci jako ústředního bodu úsilí Unie o boj proti hybridním hrozbám.

V září 2020 provedla Evropská komise posouzení kodexu o dezinformacích. Kodex, vyvinutý v roce 2018, se snaží poskytnout rámec pro strukturovaný dialog s online společnostmi sociálních médií a dalšími zúčastněnými stranami. Tento kodex zásadně omezuje prostor pro škodlivé reklamní praktiky, zvyšuje transparentnost politické reklamy, podporuje zveřejňování informací o škodlivých a manipulativních akcích a technikách, vytváří prvky pro důvěryhodné informace a zapojuje ověřovače faktů a výzkumné komunity, které se potýkají s dezinformacemi. Evropská komise ve svém každoročním hodnocení kodexu uvedla, že je potřeba více společných definic a přesnějších závazků společností. Hodnocení rovněž lituje nedostatečného přístupu k údajům pro nezávislé hodnocení nově se objevujících trendů a hrozeb, které představují dezinformace online. Komise v hodnocení uvedla, že je stále příliš obtížné přesně rozeznat konkrétní kroky podniknuté sociálními médii a online společnostmi.

Na konci roku zveřejnila Evropská komise akční plán pro evropskou demokracii, který zdůraznil význam demokracie, právního státu a základních práv jako základů Evropské unie. Akční plán zdůraznil, že demokracii nelze považovat za samozřejmost a že nepřátelští vnitřní a vnější aktéři se snaží podkopat EU a její členské státy. Akční plán poznamenal, že demokratické systémy a instituce jsou dnes vystaveny většímu tlaku a útokům než v minulosti a že integrita

voleb je ohrožena, zatímco se šíří nepravdivé a zavádějící informace. Evropská komise také poznamenala, že větší digitalizace by vyvolala obavy o demokracii a vytvořila by příležitosti. V tomto ohledu akční plán vyzval k posílení rámce politiky EU na podporu svobodných a spravedlivých voleb a silné demokratické účasti, podporu svobodných a nezávislých médií a boj proti dezinformacím. Konkrétněji akční plán zdůraznil výzvu hybridních hrozeb pro demokracie, přičemž se zaměřil zejména na dezinformace, dezinformace, operace ovlivňující informace a cizí zásahy do informačního prostoru. Za tímto účelem Evropská komise vyzvala:

- posílení strategických komunikačních činností a pracovních skupin ESVČ;
- vytvoření společného rámce a metodiky pro shromažďování systematických důkazů o zahraničním vměšování do demokracií a v době voleb;
- podpoře vnitrostátních orgánů při posilování nezávislých sdělovacích prostředků a občanské společnosti jako způsobu odhalování dezinformací a operací zahraničního vlivu a reakce na ně.

Akční plán pro evropskou demokracii také zdůraznil důležitou roli online platforem a společností globálních sociálních médií, zejména pokud jde o správu osobních údajů, šíření online nenávisti a radikalizace. Kromě toho Evropská komise poukázala na potřebu celospolečenského přístupu k posílení mediální gramotnosti a poskytnutí společných pokynů pro učitele a pedagogické pracovníky pro digitální gramotnost a boj proti dezinformacím. Taková opatření by byla nutná k zajištění spravedlivých a svobodných voleb v EU, což je bod posílen na začátku roku zpráva Komise ze dne 19. června 2020 o volbách do Evropského parlamentu v roce 2019.

II. Kybernetická bezpečnost.

V souvislosti s cílenějšími kybernetickými útoky během pandemie byla dne 16. prosince 2020 Evropskou komisí a vysokou představitelkou představena společná strategie EU v oblasti kybernetické bezpečnosti. Vzhledem k rozsahu kybernetických útoků na demokratické instituce, jako jsou francouzské volby v roce 2017, nebo útok na německý Spolkový sněm v roce 2015, a nemluvě o útoku WannaCry z roku 2017, reaguje nová strategie EU v oblasti kybernetické bezpečnosti na čtyři hlavní bezpečnostní problémy. **Za prvé**, rostoucí propojenost zařízení, sítí a informačních systémů a zranitelnosti, které to může znamenat. **Za druhé**, měnící se prostředí hrozeb a geopolitické napětí, kde jsou páchány útoky na demokratické instituce a internet je využíván pro hybridní hrozby a ideologické a politické důvody. **Za třetí**, zacílení na kritickou informační infrastrukturu poznamenanou narušením a odmítnutím klíčových služeb. **Za čtvrté**, počítačová kriminalita a škodlivé aktivity určené k podvodnému získávání osobních údajů a finančních zdrojů.

V boji proti takovému škodlivému chování nová strategie navrhuje 20 konkrétních návrhů navržených tak, aby:

1. utvářely kyberprostor posílením mezinárodního práva a opatřeními na budování důvěry;
2. rozvíjely kybernetické dialogy s klíčovými partnery a mezinárodními fóry;
3. pomáhaly budovat externí kybernetické kapacity;
4. předcházely kybernetickým hrozbám vůči EU ze strany státních a nestátních aktérů, odrazovat od nich a reagovaly na ně; a
5. posílily spolupráci v oblasti kybernetické obrany mezi členskými státy EU prostřednictvím PESCO a EDF.

Strategii EU v oblasti kybernetické bezpečnosti doprovázel legislativní návrh Komise ze dne 16. prosince 2020 na zrušení směrnice o sítích a informačních systémech (NIS 1) a její nahrazení rozšířenou směrnicí (NIS 2). Cílem je lépe reagovat na rostoucí digitalizaci společností v EU a vyšší úrovně stále sofistikovanějších kybernetických útoků v EU i mimo ni. Stalo se tak po posouzení NIS 1 Komisí se závěrem, že je třeba řešit nízkou úroveň kybernetické odolnosti podniků působících v EU, nejednotnou odolnost členských států a nízkou úroveň situačního povědomí a nedostatek společné reakce na krize. Celkově byl NIS 1 považován za příliš omezený, pokud jde o odvětví, na která se vztahuje, a nebyl členskými státy řádně prováděn. S NIS 2 doufáme, že by mohly být zavedeny přísnější mechanismy dohledu, mohly by být uplatňovány správní sankce za porušení směrnice, mohla by být vytvořena evropská síť styčných organizací pro kybernetické krize, mohly by být rozšířeny zjednodušené povinnosti hlášení incidentů a další.

Dny před vydáním nové strategie kybernetické bezpečnosti EU dne 2. prosince se Rada EU zabývala otázkou propojení zařízení a kybernetické bezpečnosti. Rada ve svých závěrech zdůraznila, že digitální suverenita a strategická autonomie EU vyžaduje schopnost zajistit bezpečnost připojených zařízení, včetně strojů, senzorů a sítí. Rada EU uznala, že připojení zařízení bude hrát klíčovou roli při utváření digitální budoucnosti Unie a vyhlídky na technologie 5G, AI, kvantové počítače, cloud computing a distribuované účetní knihy, jako je blockchain, ještě více nutnost zajistit kybernetický -zabezpečte připojená zařízení. Za tímto účelem Rada vyzvala Evropskou komisi, aby vyvinula další systémy technické certifikace a normalizace, začlenila kybernetickou bezpečnost do příslušných budoucích právních předpisů, vybudovala důvěru v produkty, služby a procesy v oblasti informačních komunikačních technologií (ICT) a podpořila iniciativy na úrovni EU jako jsou společná kritéria EU pro navrhovaná schémata cloudových služeb.

Během roku byly navrženy dvě iniciativy, které měly zajistit odolnost kritických subjektů a sítí. Za prvé, dne 29. ledna 2020 Komise schválila společný soubor nástrojů pro zmírnění rizik plynoucích ze zavádění 5G. Soubor nástrojů se bude opírat o společné hodnocení rizik EU služeb 5G a zajistí, že podniky a občané EU budou moci používat 5G bezpečným způsobem. Sada nástrojů 5G by umožnila zejména zabezpečení infrastruktury a dodavatelského řetězce. Zadruhé, dne 16. prosince Evropská komise navrhla novou směrnici na zvýšení odolnosti kritických subjektů poskytujících základní služby v EU. Navrhovaná směrnice by zavazovala členské státy k tomu, aby měly zavedenou strategii pro odolnost kritických subjektů, a od těchto

subjektů by se vyžadovalo, aby prováděly hodnocení rizik svých vlastních opatření a hlásily rušivé incidenty. Směrnice by také viděla vytvoření skupiny pro odolnost kritických subjektů, která by usnadnila přeshraniční spolupráci.

Na kyberdiplomacii se v roce 2020 zaměřila i Rada EU. Ve svých červnových závěrech Rada zdůraznila, že je důležité, aby bylo možné „předcházet škodlivým kybernetickým aktivitám, odrazovat od nich a reagovat na ně“ prostřednictvím rámce pro společnou diplomatickou reakci EU škodlivých kybernetických aktivit (dále jen „soubor nástrojů EU pro kybernetickou diplomacii“). Dne 14. května 2020 se Rada EU rozhodla prodloužit režim kybernetických sankcí do 18. května 2021, aby Unii lépe připravila na odrazování od škodlivých kybernetických aktivit ze strany vnějších aktérů a na reakci na ně. EU uvalila své vůbec první kybernetické sankce dne 30. července 2020 proti jednotlivcům a subjektům odpovědným za pokus o útok na OPCW a za útoky nazvané WannaCry, NotPetya a Operation Cloud Hopper. Dne 22. října 2020 Rada rovněž uvalila kybernetické sankce na dvě osoby a jeden subjekt, který byl v roce 2015 odpovědný za hacking německého spolkového parlamentu. ze škodlivých činností a zajistit, aby byly kybernetické aspekty plněji integrovány do struktur a misí a operací EU pro řešení krizí. Jen několik měsíců po pandemii Covid-19 HR/VP varoval, že škodlivé kybernetické aktivity jsou na vzestupu a zdravotnický sektor byl zvláště zranitelný vzhledem k tlakům na systém způsobeným zvýšenou lékařskou péčí.

III. EU a předcházení konfliktům v kyberprostoru.

Šíření informačních a komunikačních technologií (ICT), jak rozšíření používání, tak i zvýšená dostupnost škodlivých prostředků, přineslo nové způsoby projekce energie. Politická a ekonomická soutěž mezi státy nyní zahrnuje cílené kybernetické útoky proti utilitám, finančním sítím, volební infrastruktuře a systémům správy jiných zemí. Kybernetické útoky – záměrné použití škodlivého softwaru ke zneužití nebo pozměnění počítačového kódu, dat nebo logiky za účelem způsobení škody – nabízejí nové metody cílení na internetovou infrastrukturu, telekomunikační sítě, informační systémy a také počítače a počítačové systémy. Takové aktivity mohou mít za cíl zničit nebo ovlivnit řádné fungování těchto systémů s nepříznivými dopady na jejich uživatele – ať už státy, společnosti, poskytovatele veřejných služeb nebo jednotlivce. Výsledkem je, že projekce energie nemusí zahrnovat tanky nebo rakety; ani nemusí mít za následek přímou smrt a zničení srovnatelné s ozbrojeným konfliktem. Konfrontace je však konstantou ambicí, postojů a schopností států a stírá hranici mezi válkou a mírem.

IV. Správa hranic, kriminalita a terorismus.

Boj proti terorismu zůstal v agendě EU v roce 2020 i nadále na prvním místě. Na začátku roku EU aktualizovala a obnovila svůj seznam teroristických osob a organizací, na které se vztahují sankce - teroristické útoky ve Francii v říjnu 2020 a v Rakousku v listopadu 2020 sloužily jako připomínkou potřeby zvýšit úsilí v otázkách, jako je radikalizace a násilný extremismus. Dne 24. července 2020 zveřejnila Evropská komise svou novou strategii bezpečnostní unie EU na období 2020–2025, akční plán EU pro obchodování se střelnými zbraněmi, a provedla přezkum směrnice 2016/681 o používání jmenné evidence cestujících. údaje pro prevenci, odhalování, vyšetřování a stíhání teroristických trestných činů a závažné trestné činnosti. Cílem akčního plánu proti obchodování s lidmi na období 2020–2025 bylo zvýšit tlak na zločinecké sítě

posílením zpravodajského obrazu Unie o nedovoleném obchodování s lidmi. Přezkum směrnice 2016/681 odhalil, že dva roky jejího uplatňování byly celkově pozitivní, ale že by se směrnice mohla v budoucnu vztahovat i na lety uvnitř EU, a nikoli pouze na lety přilétající ze zemí mimo Unii. Rada EU v polovině října obnovila sankce proti Daesh a Al-Káidě do 31. října 2021.

Nová strategie bezpečnostní unie se zaměřuje na boj proti terorismu a organizovanému zločinu, předcházení hybridním hrozbám a ochranu kritické ochranné infrastruktury a také na posílení kybernetické bezpečnosti. Nová strategie stanoví řadu klíčových strategických priorit pro EU na nadcházejících 5 let, včetně: zajištění odolnosti klíčové infrastruktury, posílení spolupráce veřejného a soukromého sektoru při ochraně veřejných prostranství před terorismem, dokončení revize směrnice NIS, boj proti identitě krádeží, zlepšení digitálního vyšetřování trestné činnosti, rozvoj základních znalostí o bezpečnostních hrozbách, posílení spolupráce s Europolem, Eurojustem a Interpolem, boj proti obchodování se střelnými zbraněmi a pašování migrantů a další. První zpráva o pokroku nové strategie bezpečnostní unie byla zveřejněna 9. prosince 2020 s plánem provádění, který dokumentoval řadu politických opatření, která mají být provedena v období 2020–2021.

V červnu 2020 zveřejnila Rada EU závěry o vnějších rozměrech prevence a boje proti terorismu a násilnému extremismu. Rada vyzvala EU, aby využila svých diplomatických, rozvojových, bezpečnostních a humanitárních nástrojů ke stabilizaci sousedství EU a k boji proti terorismu. Rada vzala na vědomí, že vývoj teroristické hrozby pro Unii je znepokojivý a útoky ze strany Daeš a al-Káidy a jejich přidružených členů jsou i přes úspěšnou kampaň na omezení těchto skupin v Sýrii a Iráku stále vysoké. V tomto ohledu Rada uvedla, že existuje riziko, že teroristické skupiny budou více využívat online platformy k propagaci islamistických ideologií a k využívání politického vakua v nestabilních zemích, zejména v Sahelu, západní Africe a oblasti Čadského jezera. Rovněž zopakovala potřebu reagovat na terorismus v Africkém rohu a Střední Asii a zastavit jeho šíření v jihovýchodní Asii a na západním Balkáně. Rada rovněž uznala, že

Rada dále vyzvala EU, aby účinněji reagovala na zahraniční teroristické bojovníky tím, že posílí sdílení informací mezi členskými státy, Europolem, INTCEN, Eurojustem a Interpolem. Zde Rada rovněž zdůraznila význam zajištění uchovávání a předávání elektronických důkazů během přeshraničních trestních vyšetřování a stíhání. Rada EU rovněž vyzvala k častějším a hlubším dialogům se třetími zeměmi a partnery s cílem zastavit šíření extremistických a násilných ideologií. V tomto ohledu Rada zdůraznila rostoucí význam dialogů s globálními technologickými společnostmi s cílem vypořádat se s projevy nenávisti, šířením radikalizace a extremistické propagandy a zároveň chránit svobodu projevu. Rada nakonec uznala, že nové technologie, jako je umělá inteligence, drony, robotika, krypto technologie a aditivní výroba, představují hlavní výzvu v boji proti teroristickým strategiím a že je třeba maximalizovat výhody používání bezpečnostních služeb a současně omezit nezákonné zneužívání tyto technologie.

V polovině května Evropská komise zveřejnila Akční plán pro komplexní unijní politiku k předcházení praní špinavých peněz a financování terorismu. Akční plán zdůraznil nulovou toleranci EU vůči nezákonným penězům v Unii a potřebu reagovat na nedávný nárůst trestné

činnosti v souvislosti s pandemií Covid-19. Komise použila akční plán k nastínění plánu opatření proti praní peněz, který zahrnoval opatření, jako jsou: nadnárodní posouzení rizik, doporučení pro jednotlivé země v rámci evropského semestru, společná metodika rizik a mechanismus výměny informací atd. V listopadu 2020 Rada EU zdůraznila potřebu zaměřit se na boj proti praní špinavých peněz jako způsob, jak zastavit financování terorismu. V závěrech Rada vyzvala Evropskou komisi, aby vytvořila jednotný soubor pravidel EU a mechanismus dohledu a koordinace na úrovni EU pro boj proti praní peněz a terorismu. Ačkoli vnitrostátní orgány dohledu zůstávají ústředním bodem pro boj proti praní peněz, Rada zdůraznila hodnocení Komise, že ve vnitrostátních orgánech přetrvávají nedostatky v dohledu. Rada EU navíc vyzvala Komisi, aby se zaměřila na jednotný standard pro hloubkovou kontrolu a ověřování klienta v celé EU. Nakonec Rada vyzvala k vyjasnění toho, jak sladit úsilí v oblasti boje proti praní špinavých peněz s právními předpisy na ochranu údajů, a vyzvala Evropskou komisi, aby posoudila potřebu budoucích změn příslušných právních předpisů EU.

Dne 9. prosince 2020 zveřejnila Evropská komise sdělení o agendě EU pro boj proti terorismu. Vzhledem k nedávným teroristickým útokům na evropské půdě v roce 2020 a pokračujícímu stavu vysoké úrovně teroristické pohotovosti v Unii vyzvala Komise EU, aby se připravila na další džihádistické útoky. Ve sdělení se uvádí, že hlavním důvodem k obavám jsou hrozby ze strany nových a vznikajících technologií a zlomyslné používání dronů, umělé inteligence a CBRN materiálu, stejně jako šíření radikálních ideologií a online propagandy. Navrhovaný program boje proti terorismu se snažil vytvořit jednotnější přístup k boji proti terorismu a podporovat celospolečenský přístup, který zahrnuje občany, komunity, náboženské skupiny a soukromé subjekty. Za tímto účelem program vyzval k větší výměně informací mezi členskými státy o vznikajících a stávajících hrozbách, většímu úsilí předcházet terorismu prostřednictvím boje proti radikalizaci a extremistickým ideologiím, ochraně Evropanů účinnější správou údajů a hranic a reakci na teroristické útoky prostřednictvím agentur EU, jako je Europol a Eurojust.

V prosinci 2020 vydala Rada EU závěry o evropském zatýkacím rozkazu (EZR) a extradičním řízení. Aby se zlepšila reakce EU na přeshraniční trestnou činnost, Rada uznala, že je třeba zlepšit vnitrostátní provedení rámcového rozhodnutí o EZR; zabývající se hodnocením základních práv; vyřizování žádostí o vydání občanů EU do třetích zemí; a posílení postupů předávání EZR v době krize. Rada EU zejména uznala, že pandemie Covid-19 měla dramatický dopad na hranice, letecký provoz a sociální kontakty, což mělo následně významný dopad na justiční spolupráci v trestních věcech v EU, zejména pokud jde o ustanovení rámcového rozhodnutí o EZR. Podle Rady krize Covid-19 pouze zdůraznila potřebu zlepšit rychlou koordinaci a výměnu informací mezi orgány členských států. Konkrétněji Rada EU vyzvala k urychlené a komplexní digitalizaci přeshraniční justiční spolupráce ak investicím do bezpečných elektronických komunikačních kanálů mezi příslušnými orgány.

Ve stejném měsíci Evropská komise navrhla nařízení o Europolu a nakládání s osobními údaji během vyšetřování trestných činů a také o úloze agentury ve výzkumu a inovacích. S cílem držet krok s rostoucími procesy digitalizace a riziky, která pandemie přináší, se Komise snažila posílit úlohu Europolu-agentury, která je trvale zapojena do každého významného protiteroristického vyšetřování v EU. Jak uvedla Evropská komise, Europol by měl být posílen řadou opatření, včetně: posílení schopnosti Europolu spolupracovat se soukromými subjekty

(např. bankovnictví, dopravní služby) a donucovacími orgány, rozvojem opatření pro velké objemy dat pro zlepšení vyšetřovacích schopností Europolu, posílením parlamentního dohledu a odpovědnost agentury a zvyšování spolupráce s třetími zeměmi. Další legislativní návrh Komise ze dne 9. prosince 2020 usiloval o další posílení Europolu zdůrazněním důležitosti možnosti vkládat informace o zahraničních teroristických bojovnících ze zemí mimo EU do Schengenského informačního systému (SIS). Europol oznámil, že informace o 1 000 zahraničních bojovnících ze zemí mimo EU nelze vložit do SIS z důvodu mezer v právních předpisech na vnitrostátní úrovni a omezení sdílení údajů pocházejících ze třetích zemí.