Daniela Gavurová, Andrej Lipták

Digitálny prenos informácií a systém kryptoaktív ako nástroje hybridného konfliktu

Anotácia: V tomto príspevku sa autori zaoberajú problematikou digitálneho prenosu informácií a využitia systémov kryptoaktív ako nástrojov hybridného konfliktu. V príspevku sa prvkami kvantitatívno-kvalitatívneho skúmania rozoberá systém kryptoaktív a prenos informácií v digitálnom prostredí, ich vplyv na potenciálne narušenie demokratického zriadenia, rozvrat hospodárskej stability a potenciálnu podprahovú manipuláciu obyvateľstva. Predmetom skúmania príspevku je vzťah systému kryptoaktív v zmysle technológie umožňujúcej alternatívny digitálny prenos informácií vrátane oceniteľných hodnôt, a vzťah informácií nepresného, neúplného, alternatívneho charakteru k hybridným hrozbám. Cieľom príspevku je poskytnúť štruktúrovaný, logicky usporiadaný rámec, ktorý približuje možnosti zneužitia novodobých technológií v ére digitalizácie z pohľadu nekonvenčného hybridného konfliktu.

Kľúčové slová: digitálny prenos, dezinformácie, kryptoaktíva, obchádzanie sankcií, hybridné hrozby.

Úvod

Autori sa v článku s využitím prvkov kvantitatívno-kvalitatívneho skúmania venujú problematike vybraných nástrojov hybridného konfliktu. Objektom je vzťah digitálneho prenosu informácii a vzťah systému kryptoaktív k hybridným hrozbám, možnostiam ich zneužitia v konvenčnom a nekonvenčnom hybridnom konflikte. Efektivita boja proti hybridným hrozbám, ktorých riziká nemožno podceňovať ani ignorovať, je podmienená poznaním jednotlivých nástrojov hybridného konfliktu s následným prijímaním správnych a včasných preventívnych, profylaktických alebo represívnych opatrení. Zásahy do kritickej infraštruktúry, mediálnych subjektov, akademického, politického, športového, právneho, kultúrneho, hospodárskeho a ekonomického sektora ovplyvňujú budúcnosť krajiny, štátnu identitu, demokratické piliere, občiansku spolupatričnosť a prvky právneho štátu. Propaganda, informácie nepresného charakteru vedome podsúvané obyvateľom krajiny, nenávistné, radikálne, extrémistické prejavy predstavujú len malý súhrn nástrojov, ktorými agresor môže zasahovať do právnych a morálnych, spoločenských hodnôt štátu a jeho obyvateľov, a ovplyvňovať tak chod štátneho zriadenia a verejnej mienky neželaným spôsobom. Predmetom článku je teda charakteristika, analýza vybraných nástrojov hybridného konfliktu, ktoré považujeme za jedinečné a ich skúmanie za hodné osobitého zreteľa. Potenciál digitálneho prenosu dát a systému kryptoaktív ako nástrojov hybridného konfliktu možno považovať za významný a fundamentálny pre stanovenie úspechu alebo neúspechu v boji proti hybridným hrozbám, resp. v samotnom hybridnom konflikte. Cieľom príspevku je priblíženie spôsobov zneužitia digitálneho prenosu informácii a systému kryptoaktív pre neželanú destabilizáciu hodnotovo-názorového systému obyvateľstva, princípov demokracie, slobody a euroatlantického smerovania ako prvkov hybridného konfliktu, analýza znakov, procesov, postupov a spôsobov zneužitia týchto vybraných systémov a vyvodenie odporúčaní, ktorých účelom je zefektívnenie a podpora boja proti hybridným hrozbám, resp. aktívneho hybridného konfliktu. Uvedené sledujeme dosiahnuť kvalitatívnym analyticko-syntaktickým skúmaním podporeným kvantitatívnymi výsledkami vykonanej externej prieskumnej činnosti. Čiastkové závery prezentujeme na modelovaných a praktických príkladoch

Hybridné hrozby

Hybridné hrozby narúšajú celistvosť demokratického zriadenia, systému orgánov verejnej moci, stabilnú verejnú mienku, hospodárske a ekonomické prostredie štátu, a to atypickým spôsobom. Šírenie dezinformácií, poskytovanie nepresných údajov pri dôležitých strategických rozhodnutiach oprávnených orgánov, podprahové informácie cieliace na vyvolanie nespokojnosti u obyvateľstva, poskytovanie neracionálnych možností, posúvanie hranice morálky, všetky tieto aspekty pracujú v takzvanej šedej zóne. Svojím charakterom nie sú ľahko detekovateľné, pretože operujú na hranici zakázaného, resp. dovoleného, skrývajú sa za princípy a prvky demokracie, slobody, alternatívneho rozmýšľania. Ich snahou je minimalizovať jasne stanovené štruktúry vojny, vojenského konfliktu, označujú agresora, páchateľa, osobu narušujúcu morálku ako nepochopenú inú stranu, ktorá vo svojej podstate nemusí byť zlá.

Nástroje hybridného konfliktu sú nebezpečné aj kvôli svojej mnohotvárnosti. Ovplyvňovanie verejnej mienky, oslabovanie hospodárskej stability, kybernetické útoky, znefunkčňovanie strategických objektov, systémov, biologické a chemické ohrozovanie, destabilizácia sociálneho systému sú len počiatkom pri tej početnej variabilite nástrojov hybridného konfliktu. V podstate sa dá povedať, že vzhľadom na dynamický rozvoj v oblasti vedy a výskumu, ktorý aktuálne zažívame najmä na úrovni umelej inteligencie, nie je možné vymenovať všetky nástroje hybridného konfliktu. Nástroje hybridného konfliktu sú veľmi diverzifikované a čo nebolo zneužité na vojenské účely dnes, môže byť použité zajtra a *vice versa.*

Nástrojmi hybridného konfliktu môžu byť výsledky technologického pokroku, ktoré sú samé o sebe neutrálne, dokonca si dovolíme tvrdiť, že technologický rozvoj je vo väčšine prípadov podmienený pozitívnou motiváciou. Nemení to však nič na skutočnosti, že takýto technologický aspekt môže byť zneužitý na účely hybridného konfliktu. Obmedzenie vývoja a výskumu nie je na mieste, pretože úmysel agresora absentovaním nástroja zmenený nebude, agresor si zväčša nájde inú sofistikovanejšiu cestu. Ako príklad môžeme uviesť drony, ktoré sú v hybridnom konflikte, jeho konvenčnej časti, využívané po prvýkrát. Zákazom alebo obmedzením dronovej techniky by však nedošlo k obmedzeniu sledovania vojensky relevantného priestoru a osôb, hliadkovania na hraniciach vojensky relevantných obvodov, resp. k vzdušným útokom, ale iba k výmene nástroja, teda dronu, za napr. malé lietadlá alebo inú vojenskú techniku. Na mieste je teda vhodná regulácia a s ňou spojené poznanie a detekcia nástrojov hybridného konfliktu, ktoré sú viac podmienené účelom než ich samotnou podstatou.

Kryptoaktíva ako nástroj hybridného konfliktu

Kryptoaktíva sú novodobou technológiou. Predstavujú alternatívu k finančnému systému. Ich podstatu možno prirovnať k medzinárodným bankovým prevodom, resp. ku globálnej sieti, ktorá zabezpečuje prevod oceniteľných hodnôt alebo vo svojej najväčšej podstate presun informácií medzi subjektami. Systém kryptoaktív nepotrebuje pre svoju funkčnosť centrálnu autoritu, ako je to napríklad pri systémoch SWIFT alebo SEPA alebo ACH. Práve táto decentralizácia systému kryptoaktív zabezpečuje stabilitu presunu informácií z pohľadu ich nezameniteľnosti. Veď ako si môže byť ktokoľvek istý, že presun informácií skrz pôvodne vojensky relevantnú sieť Tor nebol ovplyvnený neoprávnenou osobou, ktorá nezanechala digitálne stopy? Alebo, ako si v priestore internetu môže byť niekto istý, že odoslaná informácia z jedného uzla siete je tá istá, neovplyvnená než prijatá informácia iným uzlom siete? Určitým spôsobom uvedené rieši asymetrická kryptografia a pre ňu typický

systém privátnych a verejných kľúčov. Ak však je potrebné informácie zdieľať s viacerými strategickými entitami, bezpečnosť informácií je negatívne ovplyvnená počtom entít.

Uvedené kryptoaktíva riešia transparentnosťou blockchainu, ktorú si však netreba mýliť s dostupnosťou dát. Systém kryptoaktív zabezpečuje, aby si každý uzol siete mohol s istotou overiť pravdivosť informácie. Tieto pravidlá a použité technológie však nie sú v systéme kryptoaktív unifikované. Relevantný je však napríklad systém Zero-Knowledge proof[1], ktorý zabezpečuje overenie validity informácii bez toho, aby bola informácia zverejnená buď jemu, alebo inej entite v sieti. Ďalšou skutočnosťou, ktorú zaisťuje systém kryptoaktív, je celistvosť informácií. To znamená, že akákoľvek informácia umiestnená do distribuovanej databázy transakcií systému kryptoaktív ostáva nezmeniteľná vzhľadom na výpočtovú náročnosť, ktorú by neoprávnený útočník musel vynaložiť na jej zmenu. Medzinárodný prevod finančných prostriedkov, resp. presun informácií prostredníctvom centralizovane zabezpečených sietí nevytvára také možnosti pre dynamický rozvoj ako systém kryptoaktív. Ak hovoríme o presune informácií a o ich celistvosti a nezmeniteľnosti v rámci systému kryptoaktív, prečo neumiestniť do distribuovanej databázy transakcií určitý program, ktorý vzhľadom na znaky systému kryptoaktív bude realizovať činnosti bez toho, aby ho bolo možné ovplyvniť? Smart kontrakty alebo programy bežiace v rámci systému kryptoaktív[2] existujú, no ich funkčnosť je podmienená ich stupňom vývoja. Protokoly, na základe ktorých sú vytvárané smart kontrakty, sú na počiatku svojho vývoja, aktuálne obsahujú množstvo chýb využiteľných agresorom vo svoj prospech.

Za dôležité však považujeme poukázať na potenciál systému kryptoaktív aj v tejto oblasti. Vytvorenie decentralizovaných bánk, zmenární, úschov, systémy na určovanie vlastníctva a iných finančných inštitúcií ako programov bez centrálnej autority, bez možnosti ich absolútneho zákazu spojením s bezpečným presunom informácií, ktorý môže mať charakter prevodu oceniteľných hodnôt založených na dôvere (ako tomu je aj v aktuálnom finančnom systéme), vykazuje znaky značného technologického pokroku. Na jednej strane systém kryptoaktív môže priniesť množstvo pozitív, akými sú reštartovanie finančného systému zbankrotovanej krajiny v priebehu niekoľkých dní s minimálnymi nákladmi, no na druhej strane môže takýto systém pôsobiť ako nástroj hybridného konfliktu.[3]

Rusko ako nespochybniteľný iniciátor aktuálneho rusko-ukrajinského konfliktu bolo za svoje počínanie ohodnotené rôznymi sankciami. Sankcie Európskej únie[4] alebo americkej finančnej spravodajskej jednotky OFAC sú reštriktívnymi opatreniami, ktoré sú reakciou na ruské konanie narúšajúce zvrchovanosť a nezávislosť Ukrajiny. Odpojenie vybraných ruských bánk už zo spomínaného systému SWIFT a obmedzenie medzinárodného obchodu okrem iného zapríčinilo hospodársky úpadok Ruska, oslabenie ruskej meny a nutnej orientácie ruského hospodárstva smerom k autoritatívnym a diktátorským režimom. Kryptoaktíva v tomto ponímaní môžu byť vzhľadom na svoj fundament spolu s kybernetickými útokmi priamym nástrojom hybridného konfliktu alebo nástrojom na obchádzanie uvalených sankcií. Vedeckovýskumný inštitút v USA, Congressional Research Service vo svojich výstupoch poukazuje na metódy a techniky, akým spôsobom môžu byť kryptoaktíva použité najmä na obchádzanie sankcií. Vylúčenie Ruska ako hospodárskeho partnera znamená prerušenie

---

[1] *Awesome zero knowledge proofs*. [online]. [cit. 7.októbra 2023]. Dostupné na internete: https://github.com/matter-labs/awesome-zero-knowledge-proofs.

[2] *Introduction to smart contracts*. [online]. [cit. 7.októbra 2023]. Dostupné na internete: https://ethereum.org/en/smart-contracts/.

[3] ŠANTA, J. a I. ŠANTA, 2023. *Virtuálne meny - trestnoprávne a niektoré analyticko-ekonomické aspekty,* s. 15 –20.

[4] *EU restrictive measures against Russia over Ukraine (since 2014).* [online]. [cit. 7.októbra 2023]. Dostupné na internete:https://www.consilium.europa.eu/en/policies/sanctions/restrictive-measures-against-russia-over-ukraine/.

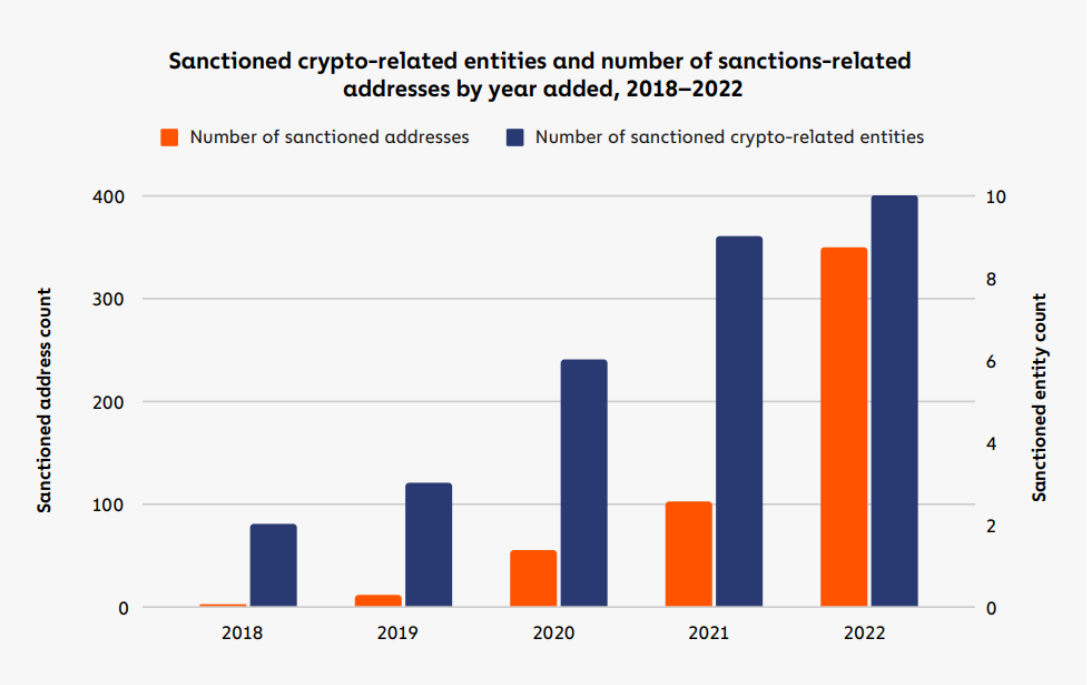
transakčného toku medzi Ruskom a ostatnými krajinami. Najmä v prípade SWIFT, celosvetovo používanej transakčnej siete, ktorej funkčnosť zaisťuje centrálny orgán so sídlom v Belgicku, možno hovoriť o úspešnom obmedzení transakčného toku Ruska. Kryptoaktíva však nie sú riadené centrálnym orgánom, a preto predstavujú jednu z potenciálnych možností, ako môže Rusko obísť takéto obmedzenie transakčného toku.[5]

Transparentnosť systému kryptoaktív však dáva oprávneným orgánom do rúk moc pozorovať všetky transakcie vykonané jednotlivými uzlami siete kryptoaktív. To znamená, že aj keď je systém kryptoaktív a jeho transakčný tok neovplyvniteľný, možno tento transakčný tok kryptoaktív pozorovať, odhaľovať pokusy o zneužitie tohto transakčného toku a na základe uvedeného sankcionovať jednotlivé entity. Týmito entitami môžu byť poskytovatelia služieb kryptoaktív reprezentovaní verejnými adresami prijímajúcimi a odosielajúcimi kryptoaktíva, resp. môže byť uvalený zákaz prijímania alebo odosielania kryptoaktív v súvislosti so zakázanými verejnými adresami. V tomto ponímaní poukazujeme na finančnú spravodajskú jednotku OFAC a jej sankčný list, v ktorom sú uvedené aj odhalené verejné adresy sankcionovaných entít, ktoré boli použité alebo mali byť použité na obchádzanie sankcií alebo na realizáciu inej trestnej činnosti, najčastejšie legalizovania výnosov z trestnej činnosti. Za zmienku stojí napríklad sankcionovaná entita TASK FORCE RUSICH (program RUSSIA-EO14024) a identifikované a priradené sankcionované verejné adresy kryptoaktíva Bitcoin bc1q2lpgjntr348pfvxhfy33ehmdzy3gmx8w4052z6, bc1ql7dlyh8xz6tpqk92vztrhqh88dmjvcwrmsemrm, kryptoaktíva Ethereum 0x3AD9dB589d201A710Ed237c829c7860Ba86510Fc, 0xc2a3829F459B3Edd87791c74cD45402BA0a20Be3 alebo verejné adresy kryptoaktíva USDT, ktoré kopíruje hodnotu amerického dolára TX5GV4DyfxNB3rPkzZJhmqZ1efVmL4rEqG, prípadne poskytovateľ služby kryptoaktív aktívny v Rusku GARANTEX EUROPE OU, známy zapojením do legalizácie výnosov z trestnej činnosti rôznych hackerských skupín, ako je napríklad severokórejská skupina Lazarus Group a jej sankcionované verejné adresy kryptoaktíva Bitcoin 3Lpoy53K625zVeE47ZasiG5jGkAxJ27kh1, alebo kryptoaktíva Ethereum 0x7FF9cFad3877F21d41Da833E2F775dB0569eE3D9.[6] Identifikácia verejných adries a ich priradenie nie je jednoduchý proces, na jeho realizáciu však možno použiť metódy analýzy distribuovanej databázy transakcií, trasovania a vykonávania prvkov súčinnosti a spolupráce s poskytovateľmi služby kryptoaktív a finančnými spravodajskými jednotkami jednotlivých štátov.

[5] *Potential Sanctions Evasion with Cryptocurrency*. [online]. [cit. 7.októbra 2023]. Dostupné na internete: https://crsreports.congress.gov/product/pdf/IN/IN11920.

[6] *OFAC sanction list search.* [online]. [cit. 7.októbra 2023]. Dostupné na internete: https://sanctionssearch.ofac.treas.gov/.

Kvantitatívne tieto skutočnosti potvrdzujú aj výsledky výskumnej činnosti spoločností, ktoré realizujú skúmanie systému kryptoaktív. Od začiatku rusko-ukrajinského hybridného konfliktu len do marca 2022 bolo vykonaných množstvo transakcií kryptoaktív v hodnote prevyšujúcej 62 miliónov amerických dolárov z identifikovaných ruských verejných adries. Väčšina týchto transakcií bola určená vysoko rizikovým pôvodcom a prostredníctvom formy OTC obchodov. Forma OTC transakcií je rizikovejšou formou než je forma nákupu alebo predaja kryptoaktíva priamo s poskytovateľom služby kryptoaktív. Ten vie určiť pôvod svojich kryptoaktív. Avšak pri OTC transakciách dochádza zo strany poskytovateľa služby kryptoaktív len k sprostredkovaniu transakcie medzi jednotlivými subjektmi s neznámym pôvodom kryptoaktív. Niektorí autori subsumujú pod OTC formu obchodu aj P2P formu obchodu alebo tzv. „vexl kryptoaktív“. Podľa indexu Cambridge Bitcoin Elecricity Consumption, ktorý hodnotí koľko elektrickej energie sa globálne využíva na zabezpečenie funkčnosti systému kryptoaktíva Bitcoin, sa Rusko koncom augusta 2021 umiestnilo na treťom mieste v míňaní množstva elektrickej energie na zabezpečovanie funkčnosti kryptoaktíva Bitcoin. Táto skutočnosť bezpochyby súvisí so snahou o prílev kapitálu do krajiny, čo je opäť forma, ako sa vyhnúť sankciám, keďže presun hodnoty medzinárodného obchodu bol Rusku obmedzený prostredníctvom zablokovania prístupu do medzinárodného transakčného toku SWIFT. Prísun kapitálu do krajiny si Rusko v súvislosti s kryptoaktívami zaisťuje aj činnosťou hackerských skupín využívajúcich metódy hackerských útokov na autonómne aplikácie, smart kontrakty decentralizovaných financií, iné smart kontrakty alebo využívajúcich metód hackerských útokov známych ako ransomware útoky, resp. prostredníctvom poskytovania služieb výmeny kryptoaktív, pri ktorých nie sú dodržiavané AML opatrenia.[7] Uvedené potvrdzuje aj činnosť analytickej spoločnosti Chainalysis, ktorá realizuje induktívno-deduktívnu analýzu transakcií viacerých distribuovaných databáz transakcií kryptoaktív. Od roku 2018 až do roku 2022 dochádzalo k plynulému nárastu



Obrázok 1 Sankcionované verejné adresy a iné entity kryptoaktív

[7] ŠANTA, J.a I. ŠANTA, 2023. K najaktuálnejšej počítačovej a inej kriminalite súvisiacej s virtuálnymi menami In: *Justičná revue. – Roč. 75, Vydanie 5/2023*, s. 640 – 643.

sankcionovaných verejných adries a súvisiacich entít americkou finančnou spravodajskou jednotkou OFAC. Z obrázku 1 vyplýva, že v roku 2022 bolo sankcionovaných viac ako 300 verejných adries kryptoaktív v prípade viac ako ôsmich poskytovateľov služieb kryptoaktív. Oprávnene sa možno domnievať, že existuje omnoho viac entít vykonávajúcich obdobné aktivity a tie entity, ktoré boli sankcionované, predstavujú len malý výber z fakticky stále pôsobiacich entít. Väčšina sankcionovaných entít preukázateľne vykonáva svoje aktivity na území Ruska, resp. na účel posilnenia Ruskej federácie. Tieto skutočnosti úzko súvisia s posilňovaním hospodárskeho a ekonomického rastu, čo negatívne vplýva na krajiny, ktoré sa ocitajú v hybridnom konflikte s Ruskou federáciou. [8] Kryptoaktíva v tomto ponímaní slúžia ako nástroj na priame obchádzanie reštriktívnych opatrení uvalenými nielen ostatnými krajinami, ale aj inými subjektmi medzinárodného práva voči Ruskej federácii. Kryptoaktíva sú vďaka svojej decentralizácii a nezávislosti ideálnym prostriedkom na zvyšovanie hospodárskej stability, a to vďaka prílevu kapitálu do krajiny, ktorého podstata nie je vždy v súlade s princípmi demokracie. Účel sankcií, ktorým je oslabenie a obmedzenie činností agresora hybridného konfliktu a prostredníka hybridných hrozieb, nie je možné napĺňať efektívne. Z uvedeného vyplýva, že kryptoaktíva nepriamo ovplyvňujú vznik rôznorodých hybridných hrozieb, a to najmä protredníctvom ich využitia ako alternatívneho transakčného mechanizmu pre agresorov hybridných konfliktov, ktorým sa obchádzajú sankčné opatrenia hospodárskeho a ekonomického charakteru.

Vzhľadom na svoju nezmeniteľnosť a transparentnosť kryptoaktíva okrem toho ponúkajú jedinečný systém výmeny informácií medzi jednotlivými subjektmi vykonávajúcim úkony hybridného konfliktu. Ak sa na distribuovanú databázu transakcií pozrieme z jej fundamentálneho hľadisk, zistíme, že tá funguje na princípe výmeny dát, teda informácií prostredníctvom sieťovej elektronickej komunikácie medzi jednotlivými uzlami siete. Tieto uzly siete možno chápať ako zariadenia schopné komunikácie na základe pravidiel, ktoré sú určené sieťou; v tomto prípade vyplývajú zo zdrojového kódu daného kryptoaktíva spolu s dodržiavaním ostatných technologických aspektov umožňujúcich takúto elektronickú komunikáciu. Vzhľadom na decentralizáciu a bezpečnosť distribuovanej databázy transakcií kryptoaktív je možné zároveň tvrdiť, že neexistuje úplná možnosť cenzúry participovania v tejto sieti, ktorá by mohla byť prítomná najmä v totalitných režimoch. Distribuovaná databáza transakcií určitého kryptoaktíva je teda nezmeniteľný, relatívne bezpečný súbor informácií transparentný pre všetkých účastníkov siete. Zápis informácií do tejto databázy je podmienený transakčným mechanizmom, ktorý však umožňuje účastníkom siete zapísať do databázy aj informácie, ktoré nemajú ekonomický charakter, teda nemajú bežnú formu transakcie. Transakcia, pri ktorej sa predpokladá jej zápis do distribuovanej databázy transakcií kryptoaktív iniciovaná určitým uzlom siete teda neobsahuje informácie o pôvodcovi kryptoaktív, sume odosielaných kryptoaktív, prijímateľovi kryptoaktív, časovom zázname atď., ale obsahuje iný druh informácií. Pojem transakcia kryptoaktív sa teda prirodzene rozširuje a už ho viac nemožno chápať iba v ekonomickom zmysle. Pod transakciou kryptoaktív teda rozumieme každú ucelenú informáciu, ktorá prešla mechanizmom overovania až po jej zápis do distribuovanej databázy transakcií. [9]

V prípade distribuovanej databázy transakcií kryptoaktíva Bitcoin je takýto odklon možné realizovať napr. prostredníctvom vytvárania podmienok, ktorých splnenie je potrebné uskutočniť ešte pred samotným utratením kryptoaktíva. Takýto odklon je v sieti kryptoaktíva Bitcoin používaný najmä na zvýšenie bezpečnosti pri odosielaní transakcií, a to tým

[8] *The 2023 Crypto Crime Report*. [online]. [cit. 7.októbra 2023]. Dostupné na internete: https://go.chainalysis.com/2023-crypto-crime-report.html.
[9] ŠANTA, J. a I. ŠANTA, 2023. *Virtuálne meny - trestnoprávne a niektoré analyticko-ekonomické aspekty*, s.15 – 23.

spôsobom, že sa určia počet a detaily verejných kľúčov oprávnených na odoslanie vybraných transakcií. Takéto podmieňovanie môže byť určené jednému alebo viacerým verejným kľúčom, a to buď samostatne súbežne. Z uvedeného vyplýva, že do klasickej transakcie je možné uložiť aj také údaje nad rámec, ktoré majú charakter podmienky. Skriptovací jazyk v prípade Bitcoinu však umožňuje aj samostatný zápis informácii neplatobného charakteru do distribuovanej databázy transakcií prostredníctvom technológie OP_RETURN. Pri iniciovaní transakcie kryptoaktíva Bitcoin je možné túto funkciu aplikovať samostatne na úrovni zdrojového programovateľného kódu skriptovaním. Na realizáciu uvedeného je však potrebné disponovať erudíciou v oblasti programovania, ktorú však môžu suplovať aplikácie a iné softvérové rozhrania poskytovateľov služieb peňaženky kryptoaktív. Či už samostatne, alebo sprostredkovane, funkcia OP_RETURN umožňuje iniciovanie takej transakcie kryptoaktíva Bitcoin, ktorá obsahuje akékoľvek dáta zadané pôvodcom transakcie. Transakcia je následne za dodržania všetkých princípov zápisu transakcií do distribuovanej databázy transakcií Bitcoin potvrdená sieťou a považuje sa za validnú. V tomto momente sa takáto transakcia stáva transparentnou pre všetkých používateľov siete. Uvedené rozširuje využitie a pole pôsobnosti kryptoaktíva Bitcoin. Funkcia OP_RETURN, teda zápis dát neplatobného charakteru do distribuovanej databázy transakcií kryptoaktíva Bitcoin aktuálne slúži najmä na účely kvázi notárskej zápisnice, určovania originality dokumentov, uchovávania dát odkazujúcich na externé úložiská alebo ako potvrdenie pre poskytovateľov výmeny virtuálnych mien medzi jednotlivými distribuovanými databázami transakcií. Kryptoaktívum Bitcoin teda môže slúžiť ako ďalší stupeň ochrany, napr. pri kontrole originality dôležitých dokumentov, utajovaných skutočností alebo iných vojensky relevantných údajov. [10]

Distribuovaná databáza transakcií kryptoaktíva Bitcoin teda v tomto ponímaní môže slúžiť agresorovi hybridného konfliktu ako spôsob komunikácie medzi jednotlivými podriadenými subjektmi zabezpečujúcimi koordinovanú politickú virtuálnu aktivitu s cieľom destabilizovať politický systém v cieľovej krajine, resp. na koordinovanú aktivitu s cieľom destabilizovať demokraciu v cieľovej krajine entitami vykonávajúcim úlohy na úseku narúšania politického systému krajiny, podkopávania dôvery k zákonným predstaviteľom cieľovej krajiny, deštrukcie ekonomickej a hospodárskej sily cieľovej krajiny, prípadne osobami vykonávajúcimi koordinovanú dezinformačnú kampaň.[11] Aj výsledky induktívneho skúmania spravodajských služieb Slovenskej republiky dokazujú, že pôsobenie týchto jednotlivcov, skupín, subjektov alebo entít je rizikom pre bezpečnosť Slovenskej republiky a že takéto činnosti je možné subsumovať pod hybridné hrozby.[12] Komunikácia medzi agresorom a jeho podriadenými entitami situovanými zväčša v krajine, ktorú z pohľadu aplikácie konvenčných a nekonvenčných nástrojov hybridného konfliktu možno považovať za cieľovú, musí byť zabezpečená a utajená. Odhalenie týchto kanálov je determinantom pre následné represívne alebo iné proaktívne opatrenia. Narušenie a ovplyvnenie komunikačného toku je významným prostriedkom v boji proti hybridným hrozbám, preto je nesmierne dôležité poznanie rôznorodosti spôsobov komunikácie v tejto oblasti. Využitie kryptoaktív ako nástroja hybridného konfliktu na úrovni zabezpečenia komunikácie medzi agresorom a vykonávateľom operácií hybridného konfliktu preto nemožno opomenúť. Agresor v tomto prípade môže využiť kryptoaktíva priamo na zapisovanie informácií do distribuovanej databázy transakcií pre svojho podriadeného vykonávateľa. Tieto informácie môžu mať formu

[10] *Dominating OP Returns: The Impact of Omni and Veriblock on Bitcoin*. [online]. [cit. 7.októbra 2023]. Dostupné na internete: https://link.springer.com/article/10.1007/s10723-020-09537-9.

[11] KORAUŠ, A. a M. GOMBÁR, 2023. Vnímanie frekvencie výskytu hybridných hrozieb z pohľadu študentov vybraných vysokých škôl na Slovensku. In: *Zborník príspevkov z vedeckej konferencie s medzinárodnou účasťou Bezpečnosť elektronickej komunikácie 2023*, s. 57- 68.

[12] *Hybridné hrozby a formy ich pôsobenia*. [online]. [cit. 2.septembra 2023].Dostupné na internete: https://www.sis.gov.sk/pre-vas/sprava-o-cinnosti.html#hrozby.

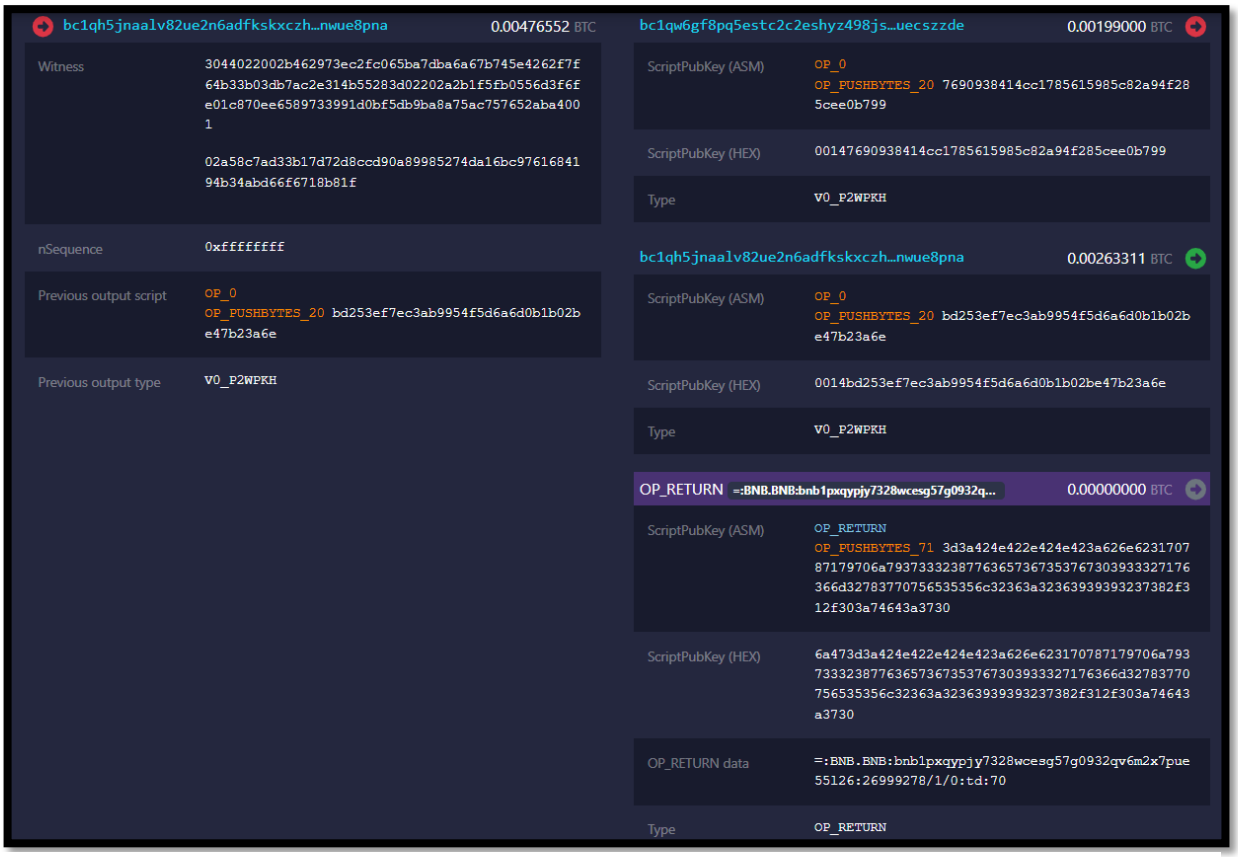
strategických, operatívnych alebo funkčných pokynov, administratívnych, personálnych zmien, údajov o miestach stretnutia a ďalších relevantných údajov pre výkon opatrení hybridného konfliktu. Distribuovaná databáza transakcii kryptoaktíva však môže mať podpornú funkciu na overenie originality správy, ktorá bola zaslaná prostredníctvom neznámeho komunikačného kanála, resp. komunikačného kanála s doposiaľ neprelomeným šifrovaním. Podobne môže distribuovaná databáza transakcií slúžiť agresorovi na overenie celistvosti a funkčnosti utajeného dátového toku. V prípade, ak by sa na takýto odhalený pôvodne utajovaný komunikačný tok medzi agresorom a vykonávateľom aplikovali opatrenia na odchytávanie a úpravu dát prostredníctvom artefaktu, resp. tokenu originality uloženého v distribuovanej databáze transakcii, mohlo by dôjsť k prezradeniu aplikovaných opatrení a známy komunikačný kanál by agresorovi nepozorovane mohol slúžiť na kvázi kontrašpionážne ovplyvňovanie pozorovateľa dátového toku.

Uvedené ilustrujeme na modelovanom príklade:

Agresor hybridného konfliktu – krajina A (ďalej „agresor“ alebo „krajina A“), má záujem na vyhlásení referenda o samostatnosti v krajine B. Uvedené sa snaží dosiahnuť ovplyvnením volieb a dosadením politických elít podporujúcich referendum. Agresor disponuje roztrieštenou dezinformačnou scénou reprezentovanou tromi vplyvnými alternatívnymi médiami v krajine B. Pred voľbami chce agresor okrem iných opatrení hybridného konfliktu iniciovať koordinovaný mediálny tlak na obyvateľstvo krajiny B. Starostlivo vypracovaný plán mediálneho tlaku, ktorého obsahom sú pokyny pre jednotlivých vykonávateľov, spôsoby a metódy ovplyvňovania verejnej mienky, návrhy mediálnych výstupov, dátumy zhromaždení a okruh zodpovedných osôb, je potrebné odoslať všetkým trom alternatívnym médiám z krajiny A do krajiny B. Agresor nedbá na skutočnosť odhalenia vypracovaného plánu, dôležitým aspektom je pre neho tá skutočnosť, aby sa tento plán dostal do dispozície alternatívnych médií neporušený a celistvý. Tento plán vo forme elektronického dokumentu je prostredníctvom kryptografických algoritmov a funkcii konvertovaný do jedinečného číselno-znakového kódu, ktorý je agresorom prostredníctvom transakcie kryptoaktíva Bitcoin s využitím skriptu OP_RETURN zapísaný do distribuovanej databázy transakcií. Následne dokument vo svojej plnej verzii odoslal prostredníctvom vlastného šifrovaného komunikačného kanála všetkým trom alternatívnym médiám. Po prijatí dokumentu, ktorým je plán mediálneho tlaku jednotlivými predstaviteľmi alternatívnych médií pôsobiacich v krajine B, si títo predstavitelia môžu overiť originalitu prijatého dokumentu a to tak, že dokument konvertujú prostredníctvom rovnakých kryptografických algoritmov. Výsledkom je číselno-znakový reťazec, ktorý porovnajú s údajmi v OP_RETURN transakcií uloženej v distribuovanej databáze transakcií Bitcoin. V prípade totožnosti týchto číselno-znakových reťazcov možno s istotou usúdiť, že je tento dokument originálny a nezmenený. Ak by bol číselno-znakový reťazec iný, agresor a vykonávatelia (alternatívne média) usúdia, že ich vlastný šifrovaný kanál bol prezradený a bol doň realizovaný zásah, čo pre nich znamená zmenu šifrovaného komunikačného kanálu.

Kryptoaktívum Bitcoin a jeho distribuovaná databáza transakcií môže slúžiť ako nástroj hybridného konfliktu, pretože zabezpečuje celistvosť a nezmeniteľnosť ukladaných dát, ktoré sú transparentne pozorovateľné pre každého účastníka siete bez potreby významnej erudície alebo hardvérovo-softvérového vybavenia. Uvedené prezentujeme na výsledkoch jednoduchého skúmania realizovaného analýzou distribuovanej databázy transakcií kryptoaktíva Bitcoin spolu s využitím pozorovania údajov voľne dostupných na indexovanom internete.

Na výkon uvedených činností bolo použité softvérovo-hardvérové vybavenie, ktoré je určené pre bežnú kancelársku a administratívnu činnosť. Na samotnú analýzu distribuovanej databázy transakcií Bitcoin bol využitý voľne dostupný nástroj na prehliadanie transakcií „www.mempool.space“. V náhodne vybratom bloku transakcií (blok č. 829 559), ktorý obsahoval 1 544 transakcií kryptoaktíva Bitcoin, bol vykonaný rešerš, ktorý pozostával v nájdení skriptu OP_RETURN vo všetkých týchto transakciách. Uvedené je možné realizovať buď priamo, pozorovaním, alebo sprostredkovane prostredníctvom využitia jednoduchých analytických metód a techník až po zložitejšie softvérové rozhrania. Tým, že sú všetky transakcie zapísané do distribuovanej databázy transakcií transparentne dostupné, nepovažujeme za problém prehľadávanie obsahu transakcií. Vykonaná rešerš preukázala niekoľko zhôd pri vyhľadávaní skriptu OP_RETURN. Náhodne bola vybraná zhoda reprezentovaná transakciou



Obrázok 2 Detaily náhodne vybranej transakcie kryptoaktíva Bitcoin s poukazom na OP_RETURN skript

„28ed6d8155de18da2f5c533f421ce1ea9e23555b56a4f8293dfeb642c0a01213“. Po detailnej analýze obsahu transakcie, ako vyplýva z obrázka 2, bolo zistené, že verejná adresa „bc1qh5jnaalv82ue2n6adfkskxczhermywnwue8pna“ odoslala 0,00199000 BTC verejnej adrese „bc1qw6gf8pq5estc2c2eshyz498jsh8wpduecszzde“ a zároveň, že bolo použitých niekoľko skriptov vrátane skriptu OP_RETURN, ktorého hodnota znie: „=:BNB.BNB:bnb1pxqypjy7328wcesg57g0932qv6m2x7pue55l26:26999278/1/0:td:70“.
Analýzou tohto číselno-znakového reťazca môžeme okrem iného pozorovať aj prítomnosť verejnej adresy, ktorá je typická pre kryptoaktívum Binance Coin BNB, a teda „bnb1pxqypjy7328wcesg57g0932qv6m2x7pue55l26“. V tomto prípade do OP_RETURN bola uvedená informácia o verejnej adrese inej distribuovanej databázy transakcií. Na analýzu tejto verejnej adresy je potrebné použiť voľne dostupný prehliadač transakcií databázy transakcií Binance Coin – BNB , napr. „www.explorer.bnbchain.org“. Po analýze tejto

verejnej adresy sa zistilo, že tá približne v čase vykonania pôvodnej transakcie kryptoaktíva Bitcoin od inej verejnej adresy prijala kryptoaktíva BNB a následne tieto kryptoaktíva odoslala prostredníctvom transakcie typu BNB Smart Chain Delegate poskytovateľovi služby kryptoaktív Trust Wallet na účel ich uloženia do decentralizovaného programu, smart kontraktu, ktorého účelom je prijímanie likvidity nutnej na overovanie a potvrdzovanie transakcií kryptoaktíva BNB. Z uvedeného možno usúdiť, že OP_RETURN správa uložená v distribuovanej databáze transakcií Bitcoin odkazovala na transakciu realizovanú na inej distribuovanej databáze transakcií. Uvedené znaky teda naznačujú, že s najväčšou pravdepodobnosťou išlo o zámenu kryptoaktív medzi jednotlivými distribuovanými databázami transakcií, na účel využitia hodnoty vlastneného kryptoaktíva Bitcoin v smart kontraktoch kryptoaktíva Binance Coin.[13]

Takéto jednoduché skúmanie preukazuje skutočnosť variability používania OP_RETURN skriptu v transakciách kryptoaktíva Bitcoin. K podobnému skriptovaniu dochádza za podobných podmienok aj pri ostatných distribuovaných databázach transakcií iných kryptoaktív.

Systém kryptoaktív teda môže byť zneužitý ako akákoľvek digitálna technológia na účely hybridného konfliktu. Jeho zrušenie alebo *en bloc* zákaz neprichádza do úvahy. Je preto nevyhnutné byť erudovaný v tejto oblasti, pochopiť systém kryptoaktív a využívať dostupné metódy, akými sú analýza distribuovanej databázy transakcií, trasovanie kryptoaktív a identifikácia verejných adries na účel regulovania tejto technológie. Zvolenie efektívneho prístupu k tejto technológii bude mať za následok udržanie etického a morálneho rozvoja systému kryptoaktív.[14]

Digitálny prenos informácií ako hybridná hrozba

V súčasnej dobe žijeme vo svete, kde digitálny prenos informácií zohráva kľúčovú úlohu v našom každodennom živote. Internet, sociálne siete a elektronická komunikácia sa stali neodmysliteľnou súčasťou našej existencie. Zároveň sa však stáva zrejmým, že digitálny prenos informácií môže byť použitý ako nástroj na dosiahnutie rôznych cieľov vrátane nekalých. Hybridná hrozba spočíva v tom, že zahŕňa kombináciu tradičných a digitálnych techník na dosiahnutie politických, ekonomických alebo vojenských cieľov a predstavuje novú výzvu pre bezpečnosť a ochranu nášho spoločenstva.[15]

Digitálny prenos informácií ako nástroj hybridnej hrozby sa stáva čoraz viac sofistikovanejším. Často sa začína v online prostredí, v ktorom sa dezinformácie, propagandistické kampane a kybernetické útoky môžu ľahko šíriť. Tieto digitálne nástroje môžu slúžiť na rôzne ciele vrátane oslabenia dôvery verejnosti voči inštitúciám, destabilizácie politických systémov a dokonca vyvolania konfliktov.[16]

---

[13] *Transaction 28ed6d8155de18da2f5c533f421ce1ea9e23555b56a4f8293dfeb642c0a01213*. [online]. [cit. 2.septembra 2023].Dostupné na internete: https://mempool.space/tx/28ed6d8155de18da2f5c533f421ce1ea9e23555b56a4f8293dfeb642c0a01213#flow=&vout=2.

[14] *Cryptocurrency Brings Millions in Aid to Ukraine, But Could It Also Be Used For Russian Sanctions Evasion?* [online]. [cit. 7.októbra 2023]. Dostupné na internete: https://www.chainalysis.com/blog/cryptocurrency-ukraine-russia-sanctions.

[15] *Hybridné hrozby na SR*. [online]. [cit. 13.októbra 2023]. Dostupné na internete: https://www.globsec.org/sites/default/files/2018-01/Hybridne-hrozby-na-SR_6-tematickych-oblasti.pdf/.

[16] *Nástroje hybridných hrozieb*. [online]. [cit. 13.októbra 2023]. Dostupné na internete: https://www.hybridnehrozby.sk/1648/nastroje-hybridnych-hrozieb/.

Jedným z príkladov hybridnej hrozby, ktorá využíva digitálny prenos informácií, sú dezinformačné kampane. Agentúry alebo štátne inštitúcie môžu vytvoriť falošné správy, ktoré majú ovplyvniť verejnú mienku. Tieto správy sa následne môžu šíriť prostredníctvom sociálnych sietí a online médií, vďaka čomu sa dostanú k veľkému množstvu ľudí. Týmto spôsobom môže byť verejná mienka zmanipulovaná, a to bez použitia vojenských síl.

Dezinformácie ako hybridné hrozby

V oblasti spoločenských vied nachádzame poznatky o mnohých faktoroch, ktoré sú úzko prepojené s vierou v pravdivosť dezinformácií. Môžeme hovoriť o faktoroch, ktoré sa dotýkajú napríklad osobnosti človeka, spôsobu akým zvykne uvažovať nad vecami vo svojom okolí, ale aj toho, z akého prostredia pochádza.[17] Vzhľadom na to, koľko dezinformácií sa dnes vyskytuje v našom okolí, je takmer nemožné, aby ktokoľvek z nás nikdy žiadnej „nenaletel". Dezinformácie sú vo svojej podstate vytvorené tak, aby boli pre ľudí prirodzene pútavé, pritiahli ich pozornosť a aby intuitívne dávali zmysel a nútili ľudí pýtať sa, či všetko náhodou nie je úplne inak, ako sme si doposiaľ mysleli. V súčasnosti existujú tri najznámejšie psychologické mechanizmy, ktoré sú spojené s vyššou náchylnosťou na rôzne typy dezinformácií.[18]

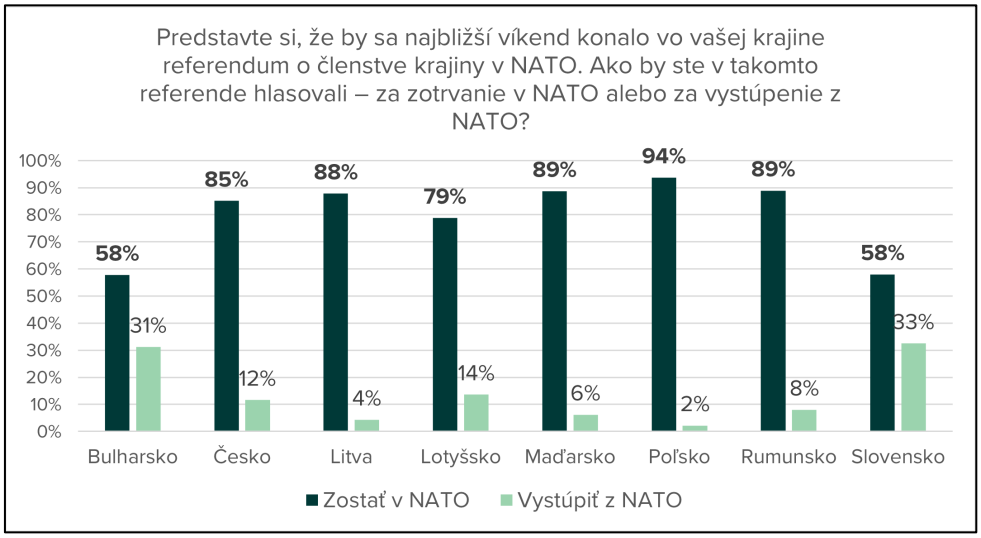
Prvý mechanizmus súvisí s prínosom kvanta informácií, ktoré na jedinca pôsobia zo všetkých strán. Je prirodzené, že nie všetky informácie dokáže človek správne vyhodnotiť. V mnohých prípadoch sa stáva, že napríklad v časovej tiesni, pod váhou emócií alebo pod vplyvom názorov ľudí z blízkeho okolia človek podľahne skratkovitému uvažovaniu a uverí aj niečomu, čomu by bežne neuveril. Dôležitou súčasťou skratkovitého uvažovania je to, že človek si automaticky predstavuje súvislosti aj medzi úplne náhodnými udalosťami. Veľmi dobrým príkladom v tejto oblasti boli dezinformácie šírené s ochorením COVID-19. Ľudia si v súvislosti s týmto ochorením často spájali rôzne iné nesúvisiace informácie. Napríklad, ak človek zomrel na uvedenú chorobu, zaujímali sa, či bol zaočkovaný alebo nie, koľko mal očkovacích dávok a pod. Takéto vzájomné prepájanie udalostí je veľmi bežnou súčasťou skratkovitého uvažovania. V mnohých prípadoch sa stáva, že človek v rýchlosti vyvodí nejaký mylný záver a až následne, keď sa nad ním hlbšie zamyslí, zistí, že existuje aj iné, jednoduchšie a pravdepodobnejšie vysvetlenie. Takéto skratkovité uvažovanie v značnej miere pomáha šíriteľom dezinformácií, ktorí sa často snažia ľudí k niečomu dotlačiť, napr. „zdieľajte, kým to nezmažú". Vyvolávanie pocitu u človeka, že musí konať rýchlo, ho navedie na to, že zdieľa alebo dokonca aj uverí takým tvrdeniam, nad ktorými sa poriadne nezamyslí.[19]

Druhým častým prvkom pri šírení dezinformácií je náznak ohrozenia, ktorý vplýva na myšlienkovú a aj emocionálnu stránku jedinca. Pod váhou emócií človek dokáže ľahšie podľahnúť skratkovitému uvažovaniu. Niektoré pocity dokážu byť natoľko nepríjemné, že sa ich človek snaží najskôr vytlačiť preč. Preto ľahšie uverí takým tvrdeniam, ktoré napomáhajú pocitu úzkosti či bezmocnosti dostať tieto tvrdenia pod kontrolu bez toho, aby sa človek dokázal lepšie zamyslieť nad ich pravdivosťou. Mnoho ľudí počas pandémie COVID-19 na Slovensku uverilo dezinformácii, že ochorenie COVID-19 v skutočnosti neexistuje a celá pandémia je iba tzv. „hoax". Ak zvážime koľko rôznych politikov, lekárov či vedcov by sa muselo po celom svete tajne dohodnúť, aby vzbudili dojem celosvetovej pandémie, zrejme si uvedomíme, že tento názor je vysoko nepravdepodobný. Aj napriek tomu, mnohí ľudia tejto možnosti aspoň na istý čas uverili. Takéto presvedčenie im mohlo dočasne pomôcť zbaviť sa

[17] BROTHERTON, R., 2015.*Suspicious minds: Why we believe conspiracy theories*,
[18] USCINSKI, J. E., 2018. *Conspiracy theories and the people who believe them.*
[19] RISEN, J. L, 2016.Believing what we do not believe: Acquiescence to superstitious beliefs and other powerful intuitions. In: *Psychological Review, 123(2*), s. 182.

veľkého náporu strachu o seba a svojich blízkych. Vyvolávanie pocitu ohrozenia a takisto prípadné poskytovanie úniku pred strachom sú účinnými mechanizmami využívanými pri šírení dezinformácií.

S vyvolaním strachu a nenávisti súvisí aj tretí prvok šírenia dezinformácií, ktorý vyvoláva pocit strachu z niečoho alebo pocit nenávisti voči vonkajšiemu nepriateľovi, ktorý zdanlivo ohrozuje našu vlastnú skupinu. V tomto prípade nemusí ísť o skutočnú hrozbu, môže hrozba môže byť aj domnelá. Typickým príkladom pre tento prvok bola migračná kríza v Európe, pri ktorej sa niektorým skupinám ľudí podarilo vyvolať na Slovensku obrovský strach z prichádzajúcich migrantov. Takéto vyvolávanie strachu a nenávisti z údajných

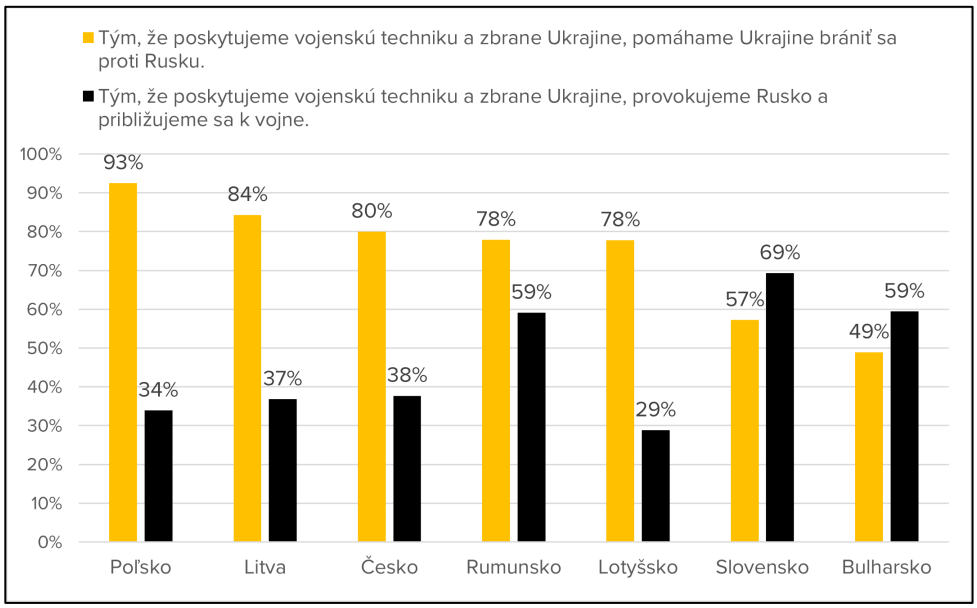


Obrázok 3 Prieskum verejnosti o referende za zotrvanie alebo vystúpenie z NATO

vonkajších nepriateľov je známou taktikou na odpútanie pozornosti ľudí od iných, skutočných a závažnejších problémov.

Z prieskumov GLOBSEC, mimovládnej organizácie, dlhodobo vyplýva, že Slovensko v „hoaxových“ rebríčkoch dlhodobo obsadzuje nelichotivé miesta. Aj keď sú „hoaxy“ považované za celosvetový problém, napriek tomu v tejto oblasti existujú regionálne rozdiely. Výsledky uvedených prieskumov poukazujú na to, že Slováci sú najviac náchylní uveriť konšpiračným teóriám z krajín Vyšehradskej štvorky, tzv. „V4“. Či už ide o dezinformácie o pandémii COVID-19, migračnej kríze či vojne na Ukrajine, mnohé rezonujú medzi tretinou až polovicou obyvateľov, a to bez ohľadu na ich vzdelanie, vekovú skupinu či bydlisko. Napriek všeobecne vysokej popularite dezinformácií vieme v krajine definovať typy, ktoré sú náchylnejšie veriť manipulatívnym informáciám. Sú to prevažne starší ľudia, ľudia s nižším vzdelaním a tí, ktorí neveria médiám a nie sú spokojní s demokraciou. Najnovší prieskum verejnej mienky, ktorý GLOBSEC uskutočnil v ôsmich krajinách strednej a východnej Európy (Bulharsko, Česko, Maďarsko, Lotyšsko, Litva, Poľsko, Rumunsko a Slovensko), skúma postoje regiónu ku kľúčovým naratívom – pravdivým aj manipulatívnym.

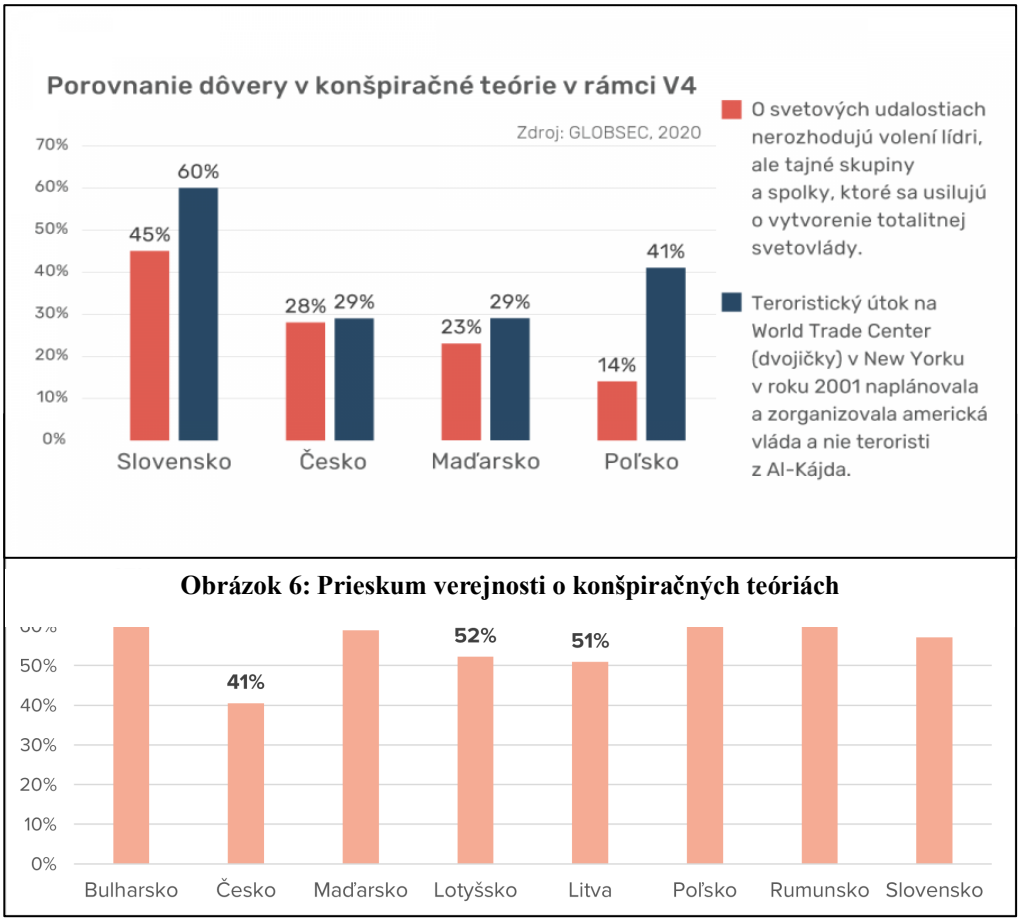
Priemerná podpora členstva v NATO v regióne je 79 %, ale údaje sa v jednotlivých krajinách výrazne líšia. Na jednej strane členstvo podporuje 94 % Poliakov a na druhej strane 58 % Slovákov a Bulharov. Podobne v priemere 74 % respondentov uznáva, že vojenská podpora Ukrajine jej pomáha brániť sa proti Rusku, ale na Slovensku a v Bulharsku si viac ľudí myslí, že vojenská pomoc Ukrajine provokuje Rusko a približuje ich krajiny k vojne.



Obrázok 4 Prieskum verejnosti o vojenskej podpore Ukrajiny

„Slovensko je príkladom toho, čo sa môže stať, keď skombinujeme nedôveru v inštitúcie a spoločnosť s náchylnosťou veriť dezinformáciám a silným politickým aktérom, ktorí vedia využiť frustrácie a obavy spoločnosti vo svoj prospech. Sme poznačení politickým chaosom a zmätkami spôsobenými vládnucou koalíciou v rokoch 2020 až 2023. Aktuálne máme na Slovensku historicky najnižšiu mieru dôvery v inštitúcie, keď vláde dôveruje len 18 % respondentov. Tento nedostatok dôvery vytvoril živnú pôdu pre časť opozičných strán na kampaň obviňujúcu Západ z vojny a podkopávanie podpory Ukrajine, ktorá našla odozvu u značnej časti obyvateľstva,“ vysvetlila Katarína Klingová, senior analytička GLOBSECu.

GLOBSEC Trends tento rok poukazuje aj na to, ako vplyv dezinformácií týkajúcich sa zdravia, ktoré sa šírili počas pandémie COVID-19, prispel k nedôvere voči farmaceutickým spoločnostiam, zdravotníckym organizáciám a očkovaniu. Približne 37 % obyvateľov regiónu



Obrázok 6: Prieskum verejnosti o konšpiračných teóriách

Obrázok 5 Prieskum verejnosti o farmaceutických spoločnostiach

strednej a východnej Európy sa domnieva, že vakcíny proti COVID-19 zvyšujú riziko predčasných úmrtí, a 56 % podozrieva farmaceutické spoločnosti, že z dôvodu zisku zatajujú účinné spôsoby liečby chorôb, akými sú COVID-19 a rakovina. „Tieto nálady rezonujú aj v spoločnostiach, ktoré vykazujú väčšiu odolnosť voči geopolitickým dezinformáciám, napríklad Česko a Poľsko. Ak chceme byť lepšie pripravení na budúce zdravotné krízy, túto nedôveru by sme mali riešiť teraz, keď zdravie nie je témou číslo jedna politickej agendy," dodala D. Hajdu.[20]

Dezinformačné šírenie rôznymi aktérmi na Slovensku, od politikov cez širokú spleť webstránok a facebookových skupín v online priestore, vytvára rôzne názorové bubliny, ktoré dokážu utvrdiť každého v jeho vlastných domnienkach, a tým zatvárajú prístup do svetov iných. Početné množstvo ľudí sa uchyľuje ku konšpiračným teóriám s cieľom zjednodušiť si odôvodnenie vecí, ktorým dnes nie ľahké porozumieť. Svet sa rýchlo mení a je plný zložitých javov, preto uveriť konšpiračným teóriám predstavuje spôsob, ako si v živote nájsť nové

[20] *Nový prieskum GLOBSEC-u*. [online]. [cit. 13.októbra 2023]. Dostupné na internete: https://www.globsec.org/what-we-do/press-releases/novy-prieskum-globsec-u-slovensko-zaznamenalo-vyrazny-prepad-v/.

istoty. Takýmto konaním môže človek pocítiť výnimočnosť, že patrí k „vyvolenej“ skupine, ktorá pozná „ozajstnú pravdu“.[21]

Kritické myslenie a mediálna gramotnosť

Kritické myslenie a mediálna gramotnosť patria medzi základné prvky, ktoré sú nevyhnutné na analýzu a následnú interpretáciu moderných informácií. Rýchle šírenie chybných informácií a dezinformácií v posledných rokoch práve vďaka rozvoju a zvyšovaniu dostupnosti internetu sa stalo masovým fenoménom. Dezinformácie využívajú klamstvá a podvody s cieľom zmanipulovať jedinca spôsobom vyhovujúcim ich tvorcom. Občas tvorcovia dezinformácií dokonca využívajú pravdivé, faktami podložené informácie, ktoré prekrútia vytrhnutím z kontextu alebo zmenou rámca. Za najefektívnejšie dezinformácie môžeme považovať tie, ktoré sú akousi zmesou pravdivých a nepravdivých informácií. [22]

Najúčinnejším spôsobom, ako bojovať proti dezinformáciám, je využitie analytických schopností, ktorých pomocou dokážeme preskúmať to, čo čítame, sledujeme či počujeme, a to racionálnym, logickým a nezaujatým spôsobom. Tento spôsob umožňuje lepšie identifikovať jednotlivé faktami podložené informácie a odlíšiť ich od nepravdivých a klamlivých informácií. Pri analýze je z hľadiska dôveryhodnosti užitočné zaoberať sa napríklad týmito otázkami: „Kto je autorom – šíriteľom danej informácie?“; „Aký jazyk a gramatiku príspevok používa a aké pocity vyvoláva?“; „Z ktorého obdobia informácia pochádza?“; „Sú používané údaje stále relevantné?“[23]

Vedomosť, kto je autorom a distribútorom konkrétnej informácie, môže pomôcť pri odpovedi na otázku, či ide o spoľahlivé spravodajstvo. Tento údaj môže byť užitočným ukazovateľom práve toho, kedy treba byť opatrný. Ak chce človek zistiť, kto je producentom konkrétneho média, zväčša stačí len jednoduché vyhľadanie na internete. Zároveň je potrebné overiť si vierohodnosť daného zdroja informácií aj prostredníctvom rôznych webstránok overovačov faktov tzv. „fact-checkers“. V prípade slovenských zdrojov je nápomocný portál konšpirátori.sk, ktorý zverejňuje zoznam konšpiračných teórii, dezinformačných médií či webov. V prípade jazyka a gramatiky je hovorový, vulgárny alebo emotívny jazyk varovným signálom, že to, čo si človek prezerá alebo číta, môže byť dezinformácia. Samotné dezinformácie svojou povahou manipulujú, a preto sú presýtené emotívnym jazykom a obrazmi. Kvalitné médiá len zriedkavo využívajú veľké písmená na zdôraznenie svojho názoru. Titulky plné veľkých písmen a výkričníkov spravidla znamenajú, že ide o šírenie možnej dezinformácie. Dezinformácie sa šíria aj formou „klikacích“ návodov. tzv. „clickbaitových článkov“, ktoré využívajú práve tento typ jazyka s prvkami dôverného a hovorového tónu. V mnohých prípadoch sa stáva, že články, videá alebo obrázky sú „recyklované“. Dezinformačné kampane využívajú aj niekoľko rokov staré obrázky a videá práve pre aktuálne príbehy. Cieľom je použiť emocionálne šokujúce alebo násilné obrázky na vyvolanie strachu. Účinnými nástrojmi v boji proti dezinformáciám, ktoré pomôžu nestratiť sa v kvante informácií môžu. byť aj stránky: Hoaxy a podvody – Polícia S“, Hoax.sk, Demagog.sk, Pouzimerozum.sk, či Argumentuj.sk.[24]

---

[21] *Slováci veria hoaxom viac ako iné národy, prečo je to tak*. [online]. [cit. 13.októbra 2023]. Dostupné na internete: https://vedanadosah.cvtisr.sk/ludia/sociologia/slovaci-veria-hoaxom-viac-ako-ine-narody-preco-je-to-tak/.

[22] STENGEL, R., 2019. *Information Wars*, str. 290.

[23] CILLIZZA, C.. 2019. *Why our politics can‘t handle Jussie Smollett*. [online]. [cit. 13.októbra 2023]. Dostupné na internete: https://edition.cnn.com/2019/02/18/politics/jussie-smollett-politics/index.html/.

[24] Každý druhý Slovák verí konšpiráciám. [online]. [cit. 13.októbra 2023]. Dostupné na internete: https://eduworld.sk/cd/janka-horniakova/8510/kazdy-druhy-slovak-veri-konspiraciam/.

Vyvolanie pocitu dôvery a začlenenia sa do spoločnosti predstavujú kľúčovú rolu pre fungujúcu demokraciu. Boj s korupciou a klientelizmom, ktoré bránia uprednostňovaniu určitých skupín obyvateľstva pred inými, ako aj reforma vzdelávania, v ktorej sa bude práve poukazovať na dôležitosť kritického myslenia a vysvetlenie fungovania demokracie i života v nej, sú primárnymi prvkami štrukturálnych zmien, ktoré sa v spoločnosti musia odohrať.
V individuálnej rovine sa síce môže každý snažiť filtrovať čas strávený na sociálnych sieťach, ktoré sú dnes hlavným ohniskom konšpiračných teórií a dezinformácií, ale je dôležité byť aktívnejším používateľom namiesto pasívneho konzumovania a komunikovať viac mimo virtuálnej reality. Ak sa človek už rozhodne zapájať do konverzácií nie len v offline, ale aj v online priestore, je dôležité dbať na slušnú komunikáciu a overiť si informácie predtým, ako sa ich rozhodne zdieľať v informačnom priestore.[25]

Záver

Príspevok analyzuje hybridné hrozby v kontexte narušania demokratických štruktúr a orgánov verejnej moci. V hybridných konfliktoch sa ich aktéri pohybujú v tzv. „šedej zóne“, ovplyvňujúc napr. verejnú mienku alebo hospodárstvo štátu. Riziká spojené s kryptoaktívami, ako je obchádzanie sankcií, sú diskutované a rozoberané na pozadí aktuálne prebiehajúceho rusko-ukrajinského konfliktu. Uvádzajú sa príklady sankcionovaných entít a ich verejných adries s návrhom monitorovania transakcií kryptoaktív ako možného opatrenia na minimalizovanie vzniku hybridných hrozieb v tejto oblasti. Príspevok zdôrazňuje, že zákaz kryptoaktív nie je optimálnym riešením a namiesto toho sa odporúča vzdelávanie a regulácia tohto sektora. V oblasti dezinformácií a psychologických mechanizmov sa v príspevku analyzuje význam kritického myslenia, mediálnej gramotnosti a dôveryhodných informačných zdrojov. Dezinformačné kampane v online prostredí sú identifikované ako ďalšie hybridné hrozby, v ktorých sú zdôraznené jednotlivé psychologické taktiky a dôležitosť kritického myslenia. Kritické myslenie a mediálna gramotnosť sú kľúčovými faktormi v boji proti dezinformáciám, a teda aj v boji proti hybridným hrozbám tohto charakteru.

Literatúra

ŠANTA, J. a I. ŠANTA, 2023. K najaktuálnejšej počítačovej a inej kriminalite súvisiacej s virtuálnymi menami. In: *Justičná revue*. Roč. 75, Vydanie 5/2023, s. 636 – 650.

ŠANTA, J. a I.ŠANTA, 2023. *Virtuálne meny - trestnoprávne a niektoré analyticko-ekonomické aspekty*. Praha: Leges. 199 strán. ISBN: 978-80-7502-668-2.

KORAUŠ, A a M. GOMBÁR, 2023. Vnímanie frekvencie výskytu hybridných hrozieb z pohľadu študentov vybraných vysokých škôl na Slovensku. In: *Zborník príspevkov z vedeckej konferencie s medzinárodnou účasťou Bezpečnosť elektronickej komunikácie 2023*. Bratislava: Akadémia Policajného zboru v Bratislave. s 57–68. ISBN 978–808054–997–8.

Awesome zero knowledge proofs. [online]. [cit. 7. októbra 2023]. Dostupné na internete: https://github.com/matter-labs/awesome-zero-knowledge-proofs.

Introduction to smart contracts. [online]. [cit. 7. októbra 2023]. Dostupné na internete: https://ethereum.org/en/smart-contracts/.

Posilňovanie odolnosti voči hybridným hrozbám. [online]. [cit. 7. októbra 2023]. Dostupné na internete:https://www.mzv.sk/diplomacia/bezpecnostna-politika/hybridne-hrozby.

[25] Slováci veria hoaxom viac ako iné národy. [online]. [cit. 13.októbra 2023]. Dostupné na internete: https://vedanadosah.cvtisr.sk/ludia/sociologia/slovaci-veria-hoaxom-viac-ako-ine-narody-preco-je-to-tak/.

Cryptocurrency Brings Millions in Aid to Ukraine, But Could It Also Be Used For Russian Sanctions Evasion? [online]. [cit. 7. októbra 2023]. Dostupné na internete: https://www.chainalysis.com/blog/cryptocurrency-ukraine-russia-sanctions/.

EU restrictive measures against Russia over Ukraine (since 2014). [online]. [cit. 7. októbra 2023]. Dostupné na internete: https://www.consilium.europa.eu/en/policies/sanctions/restrictive-measures-against-russia-over-ukraine/.

OFAC sanction list search. [online]. [cit. 7. októbra 2023]. Dostupné na internete: https://sanctionssearch.ofac.treas.gov/.

The 2023 Crypto Crime Report. [online]. [cit. 8. februára 2024]. Dostupné na internete: https://go.chainalysis.com/2023-crypto-crime-report.html.

Potential Sanctions Evasion with Cryptocurrency. [online]. [cit. 7. októbra 2023]. Dostupné na internete: https://crsreports.congress.gov/product/pdf/IN/IN11920/.

Hybridné hrozby na SR. [online]. [cit. 13. októbra 2023]. Dostupné na internete: https://www.globsec.org/sites/default/files/2018-01/Hybridne-hrozby-na-SR_6-tematickych-oblasti.pdf/.

Nástroje hybridných hrozieb. [online]. [cit. 13. októbra 2023]. Dostupné na internete: https://www.hybridnehrozby.sk/1648/nastroje-hybridnych-hrozieb/.

BROTHERTON R., 2015. *Suspicious minds: Why we believe conspiracy theories*. Bloomsbury Publishing. 298 s. ISBN 978-1-4729-1564-1.

USCINSKI, J. E., 2018. *Conspiracy theories and the people who believe them*. Oxford University Press. 560 s. ISBN 978-0-1908-4408-0.

RISEN, J. L., 2016. Believing what we do not believe: Acquiescence to superstitious beliefs and other powerful intuitions. In: *Psychological Review*, 123(2). s.182 – 207.

Hybridné hrozby na SR. [online]. [cit. 13. októbra 2023]. Dostupné na internete: https://www.globsec.org/sites/default/files/2018-01/Hybridne-hrozby-na-SR_6-tematickych-oblasti.pdf/>.

Nástroje hybridných hrozieb. [online]. [cit. 13. októbra 2023]. Dostupné na internete: https://www.hybridnehrozby.sk/1648/nastroje-hybridnych-hrozieb/.

STENGEL, R., 2019. *Information Wars*. New York: Atlantic Monthly Press, 384 s. ISBN 978-0-8021-4799-8.

CILLIZA, C., 2019. *Why our politics can't handle Jussie Smollett*. CNN Politics. [online]. [cit. 13. októbra 2023]. Dostupné na internete: https://edition.cnn.com/2019/02/18/politics/jussie-smollett-politics/index.html/.

Každý druhý Slovák verí konšpiráciám. [online]. [cit. 13. októbra 2023]. Dostupné na internete: https://eduworld.sk/cd/janka-horniakova/8510/kazdy-druhy-slovak-veri-konspiraciam/.

Slováci veria hoaxom viac ako iné národy. [online]. [cit. 13. októbra 2023]. Dostupné na internete: https://vedanadosah.cvtisr.sk/ludia/sociologia/slovaci-veria-hoaxom-viac-ako-ine-narody-preco-je-to-tak/.

Keywords: digital transmission of data, disinformation, crypto-assets, sanctions evasion, hybrid threats

Summary

The scientific article analyses hybrid threats in the context of disrupting democratic structures and public authorities. In hybrid conflicts, their actors operate in the so-called grey zone, influencing, for instance, public opinion or the state's economy. Risks associated with crypto-assets, such as sanctions evasion, are discussed against the backdrop of the ongoing Russia-Ukraine conflict. Examples of sanctioned entities and their public addresses are provided, along with a proposal to monitor crypto-asset transactions as a possible measure to minimise the emergence of hybrid threats in this area. This article emphasises that a ban on crypto-assets is not an optimal solution, instead, it recommends education and regulation in this sector. In the realm of disinformation and psychological mechanisms, the article analyses the importance of critical thinking, media literacy, and trustworthy information sources. Disinformation campaigns in the online environment are identified as additional hybrid threats, highlighting specific psychological tactics, and the importance of critical thinking. Critical thinking and media literacy are key factors in combating disinformation and, consequently, hybrid threats of this nature.

por. Mgr. Daniela Gavurová
odbor Bratislava
Národná kriminálna agentúra Prezídia PZ
Pribinova 2, 812 72 Bratislava
e-mail: daniela.gavurova@minv.sk

Andrej Lipták
odbor finančného vyšetrovania
Národná centrála osobitných druhov kriminality PPZ
Pribinova 2, 812 72 Bratislava
e-mail: andrej.liptak@minv.sk

Recenzent: doc. JUDr. Ján Šanta, PhD., LL.M., MBA, MSc.