Riziká hybridného pôsobenia cudzej moci prostredníctvom MNO: Prípadová štúdia českých prezidentských volieb v roku 2023

Autor: Viliam Kaliňák

Názov výstupu: Riziká hybridného pôsobenia cudzej moci prostredníctvom MNO: Prípadová štúdia českých prezidentských volieb v roku 2023
Názov výstupu z opisu: **Zhodnocovanie prínosov a rizík MNO pre novobudovaný systém pokrývania hybridných hrozieb**
Zadávateľ: Úrad splnomocnenca vlády SR pre rozvoj občianskej spoločnosti
Národný projekt: PODPORA PARTNERSTVA A DIALÓGU V OBLASTI PARTICIPATÍVNEJ TVORBY VEREJNÝCH POLITÍK II.
ITMS kód projektu: 314011CQM9
Operačný program: Efektívna verejná správa
Obdobie vyhotovenia /spracovania: apríl – jún 2023

Tento projekt je podporený z Európskeho sociálneho fondu.

Zhrnutie

Česká republika sa nachádza v neprehľadnom, nepredvídateľnom a čoraz konfliktnejšom medzinárodnom prostredí, v ktorom snahou jednotlivých globálnych aj regionálnych aktérov je presadenie svojich vlastných sfér vplyvu a ambícií na preskupenie mocenského rozloženia síl vo svete. Títo aktéri na to využívajú množstvo prostriedkov vrátane dezinformácií, propagandy, špionáže, kybernetických útokov či podvratných aktivít, interagujúc pritom s ďalším množstvom rôznych aktérov od politikov, akademikov, novinárov až po zástupcov občianskeho sektora.

Takéto hybridné pôsobenie cudzej moci bolo možné po skúsenostiach s voľbami do poslaneckej snemovne parlamentu ČR v roku 2021 pozorovať aj počas prezidentských volieb začiatkom roka 2023, kedy bolo zjavnou snahou viacerých domácich, zahraničných, štátnych aj neštátnych aktérov ovplyvniť ich výsledok cielenou diskreditáciou a útokmi voči niektorým kandidátom. Spomedzi 22 českých dezinformačných a konšpiračných webstránok, ktorých blokáciu si z dôvodu ospravedlňovania ruskej agresie na Ukrajine vyžiadalo Vojenské spravodajstvo, bol jeden prevádzkovaný mimovládnou neziskovou organizáciou, ktorá sa po obnove činnosti svojho webu podieľala aj na diskreditačnej kampani voči konkrétnemu kandidátovi v čase volieb. Tento jej vplyv a vplyv ďalších predstaviteľov domácej dezinformačnej a proruskej scény bol naviac v čase volieb podporený nielen vypustením dezinformácie do českého informačného priestoru zo strany spravodajskej agentúry cudzieho štátu, ale tiež kybernetickými útokmi na odopretie prístupu k webstránkam českých štátnych orgánov, kandidátov na prezidenta a mimovládnych organizácií, ktoré mohli šírené poplašné správy potenciálne vyvrátiť.

Odpozorovaný vzorec medzi šírením dezinformácií a naratívov, a následnými kybernetickými útokmi, predovšetkým krátko pred druhým kolom volieb, značí snahu amplifikovať vplyv subjektov podporujúcich cudziu moc na voliča tým, že mu budú v krátkom čase poskytnuté nepravdivé a zmanipulované informácie a súčasne odopretý prístup k faktom. Mimovládne neziskové organizácie pôsobiace v informačnej doméne tak môžu zohrať v snahe získať operatívnu informačnú a kognitívnu prevahu pre prospech cudzích záujmov ako rolu amplifikátora vplyvu, tak rolu obete.

Tento projekt je podporený z Európskeho sociálneho fondu.

Úvod

Česká republika sa nachádza v neprehľadnom, nepredvídateľnom a čoraz konfliktnejšom prostredí meniaceho sa medzinárodného systému, v ktorom snahou jednotlivých globálnych aj regionálnych aktérov je presadenie svojich vlastných sfér vplyvu a ambícií na preskupenie mocenského rozloženia síl vo svete.[1] Hodnoty, prístupy a riešenia Západu sú spochybňované až odmietané, veľmi často založené na výhradne ideových a ideologických východiskách, a nie na odôvodnených argumentoch a znalostiach reálneho prostredia.[2]

K stupňovaniu tohto súperenia mocností prispela pandemická kríza v rokoch 2020 a 2021, počas ktorej došlo k masívnemu prechodu z osobnej na elektronickú komunikáciu a inštrumentalizácii faktov, poloprávd a klamstiev na ovplyvňovanie postojov, rozhodnutí a podpory ľudstva, vrátane politických predstaviteľov, v globálnom meradle.[3] V prípade samotného ochorenia COVID-19 zasahovali dezinformácie do vnútornej bezpečnosti ČR predovšetkým tým, že spochybňovali závažnosť ochorenia, testovanie a vakcíny, odrádzali od dodržiavania protipandemických opatrení, útočili na legitimitu štátu a vyzývali na protesty a občiansku neposlušnosť.[4] Ďalšie útoky dezinformátorov pokračovali v roku 2021 proti štátnym inštitúciám po odhalení zapojenia príslušníkov ruskej tajnej služby do výbuchu v muničnom sklade vo Vrběticiach z roku 2014 a proti politickým stranám kandidujúcim vo voľbách do poslaneckej snemovne parlamentu ČR.[5]

Najčastejšími šíriteľmi týchto dezinformačných správ sú osoby silne sympatizujúce s autoritárskymi režimami a/alebo motivované vlastným ekonomickým prospechom, ktoré takouto činnosťou vedome aj nevedomky prispievajú k presadzovaniu záujmov cudzej moci na úkor bezpečnostných záujmov ČR.[6] Záujem o kontakty s nimi prejavujú najmä ruské spravodajské služby, ktorým sa aj napriek vyhosteniu niekoľkých dôstojníkov s diplomatickým krytím v roku 2021 darilo udržiavať a rozširovať sieť proruských aktivistov, novinárov a sprostredkovateľov kontaktov na niektorých politikov za účelom šírenia ruskej propagandy.[7] Naopak čínske spravodajské služby sa na rozdiel od ruského masívneho ovplyvňovania verejnej mienky snažia v Česku budovať úzke kontakty na akademické prostredie a politickú scénu za účelom získavania expertného know-how a presadzovania čínskej zahraničnej politiky.[8] V neposlednom rade Irán sa v Česku zameriava na odporcov režimu v exile združených okolo Rádia Fardá v rámci Rádia Slobodná Európa/Rádia Sloboda so sídlom v Prahe.[9]

Medzi dlhodobo najzávažnejšie hrozby pre ČR patria tiež aktivity štátnych a/alebo štátom podporovaných skupín v kybernetickom priestore,[10] za ktorými stoja zväčša ruskí a čínski aktéri útočiaci na prvky kritickej infraštruktúry, vrátane štátnych inštitúcií, ďalej na politické strany, výskumné organizácie a mimovládne neziskové organizácie.[11]

[1] Vojenské zpravodajství, *Výroční zpráva 2021*, 6.
[2] Ibid.
[3] Vojenské zpravodajství, *Výroční zpráva 2020*, 4.
[4] Ministerstvo vnitra ČR, *Zpráva o situaci v oblasti vnitřní bezpečnosti 2020*, 63.
[5] Ministerstvo vnitra ČR, *Zpráva o situaci v oblasti vnitřní bezpečnosti 2021*, 114.
[6] Bezpečnostní informační služba, *Výroční zpráva 2020*, 11.
[7] Bezpečnostní informační služba, *Výroční zpráva 2021*, 11.
[8] Ibid, 11-12.
[9] Bezpečnostní informační služba, *Výroční zpráva 2020*, 16.
[10] Národní úřad pro kybernetickou a informační bezpečnost, *Zpráva o stavu kybernetické bezpečnosti 2020*, 15.
[11] Bezpečnostní informační služba, *Výroční zpráva 2021*, 13.

Tento projekt je podporený z Európskeho sociálneho fondu.

Vzhľadom na rôzne prejavy a aktérov hybridného pôsobenia cudzích mocí v ČR za posledné roky je cieľom tejto štúdie zistiť rolu, akú zohrávajú MNO v rámci hybridného pôsobenia cudzej moci, a riziká, ktoré sa na ňu viažu. Konkrétne nás bude zaujímať, aká je rola MNO v rámci hybridného pôsobenia, akými rôznymi spôsobmi interagujú aktéri hrozby s MNO pri zasahovaní do situácie v krajine a aké následky má táto interakcia.

Priebeh hybridného pôsobenia

Prípravná fáza

Predvojom snáh o zasiahnutie do priebehu českých prezidentských volieb v roku 2023 boli aktivity viacerých domácich a zahraničných neštátnych aktérov v informačnej a kybernetickej doméne, ktoré eskalovali po vypuknutí ozbrojeného konfliktu na Ukrajine vo februári 2022. Ich cieľom bolo vyvinúť tlak na vládu ČR pri zvládaní vzniknutej situácie prostredníctvom zasievania animozít, polarizáciou spoločnosti a útokov na informačné systémy.

Hlavnými aktérmi hybridného pôsobenia v informačnej doméne boli neštátne subjekty z českej kvázi-mediálnej a prokremeľskej scény,[12] ktoré šírili naratívy, dezinformácie a konšpiračné teórie na podporu ruskej zahraničnej politiky a záujmov.[13,14] Operovali na dezinformačných weboch, sociálnych sieťach a prostredníctvom reťazových e-mailov, cez ktoré šírili správy o genocíde na Ukrajine, ktorej mali ruské mierové sily zamedziť,[15] správy o vojenskej podpore fašistov na Ukrajine, ktorou vláda ČR zaťahovala krajinu do vojny,[16] správy o finančnej a materiálnej podpore utečencov z Ukrajiny na úkor Čechov[17] alebo správy o formovaní nového svetového poriadku, v ktorom bol prezident Ukrajiny vykreslený len ako bábka v zástupnej vojne medzi Ruskom a USA.[18] Spomedzi 22 dezinformačných webov, ktorých blokáciu si na jar 2022 vyžiadalo české Vojenské spravodajstvo práve z dôvodu ospravedlňovania a schvaľovania ruskej agresie na Ukrajine,[19] bol jeden prevádzkovaný rovnomennou mimovládnou neziskovou organizáciou – spolkom Nová republika.

Spolok vznikol v roku 2013 ako politická iniciatíva psychiatra a bývalého ministra zdravotníctva, ktorého víziou bolo prekonať „kleptokratický" a „perverzný neoliberalizmus" vytvorením „radikálne nového konceptu spoločenského zriadenia" inšpirovaného „radikálne ľavicovým programom" zo západnej Európy, Južnej Ameriky či Škandinávie.[20] Na rozdiel od deklarovaného združovania odborníkov z humanitných a technických odborov schopných analyzovať spoločenské a hospodárske problémy a navrhovať riešenia[21] však nadpolovičnú väčšinu obsahu dnes tvoria prebrané články z ruských zdrojov o politike a postupoch Ruska proti Ukrajine a Západu[22] doplnené o články kohokoľvek

[12] Kvázi-mediálnu a prokremeľskú scénu tvoria subjekty, ktoré v politicky a spoločensky citlivých alebo kontroverzných témach prezentujú odlišný pohľad od mainstreamovej scény, a to spôsobom, ktorý zodpovedá oficiálnemu kultúrnemu alebo politickému pohľadu a interpretácii ruskej vlády.

[13] Ministerstvo vnitra ČR, „Jak kvazi-mediální scéna reflektovala invazi vojsk Ruské federace na Ukrajinu".

[14] Ministerstvo vnitra ČR, „Konspirační rámování ruské agrese vůči Ukrajině".

[15] Smejkal a Zadražil, „Velká předjarní očista Ukrajiny".

[16] Netík, „X.Dolezal".

[17] Záhumenská, „Milion migrantů a ukrajinská zdravotní turistika".

[18] Protiproud, „Ve stínu hrozby 3. světové války".

[19] Cibulka, ‚Hybridně působí ve prospěch Ruska'.

[20] David, „Projev Ivana Davida".

[21] Nová republika, „Manifest a stanovy".

[22] Ministerstvo vnitra ČR, „Jak česká kvazi-mediální scéna přebírá kremelské oficiální propagandistické i dezinformační narativy".

s proruským a ľavicovým cítením – od politikov, cez dokumentaristov, až po nespokojných občanov, blogerov. Web spolku dnes po zablokovaní jeho domény .cz v marci 2023 funguje na novej doméne .online.[23]

Aktérmi v kybernetickej doméne boli naopak ruskojazyčné hacktivistické skupiny, ktoré na protest proti konkrétnym krokom vlády ČR viedli útoky na informačné a komunikačné systémy rôznych subjektov v ČR.

V prvom prípade z apríla 2022 podnikla skupina Killnet DDoS útoky proti webovým sídlam českých ministerstiev a Národného úradu pre kybernetickú a informačnú bezpečnosť v bezprostrednej reakcii na oznámenie opráv ukrajinskej ťažkej vojenskej techniky v ČR.[24] Rovnaký typ útokov podnikla neskôr v októbri 2022 skupina Anonymous Russia proti webovým sídlam vládnych inštitúcií, médií, bánk, letiska a i.[25] len dva dni po tom, čo Ministerstvo zahraničných vecí ČR neuznalo a odsúdilo anexiu Doneckej, Luhanskej, Záporožskej a Chersonskej oblasti Ruskou federáciou.[26]

Obe tieto zoskupenia boli do jari 2023 súčasťou jednej platformy proruských hacktivistov, ktorých združil práve Killnet.[27] Podľa zakladateľa skupiny však jednotliví jej členovia, jednotky, naďalej operovali nezávislé od seba a ku koordinácii ich útokov dochádzalo len ak bolo treba zabezpečiť „nepretržitý cyklus práce".[28] Na druhej strane, podľa amerického ministerstva zdravotníctva sa Killnet okrem kybernetických útokov podieľal tiež na šírení kremeľskej propagandy a dezinformácií v rozhovoroch pre médiá,[29] a preto deklarovaný modus operandi nemusí byť pravdivý.

Destabilizačná fáza

Destabilizačná fáza hybridného pôsobenia na priebeh českých prezidentských volieb v roku 2023 začala najneskôr dva mesiace pred ich prvým kolom, kedy zaangažovaní aktéri nadviazali na dezinformačné a kybernetické aktivity z predchádzajúcich mesiacov a naďalej zneužívali kontext vojny na Ukrajine v zjavnej snahe zdiskreditovať nevyhovujúcich kandidátov.

V období pred zverejnením finálneho zoznamu kandidátov dňa 25. novembra 2022 a prvým kolom prezidentských volieb dni 13. a 14. januára 2023 dominovali kvázi-mediálnemu priestoru tri témy. Prvou bolo spochybňovanie legitimity volieb, podľa ktorého malo Ministerstvo vnútra ČR zámerne vyradiť nepohodlných kandidátov pri ich registrácii. V ostatných dvoch prípadoch išlo o útoky proti, resp. o podporu vybraným kandidátom.[30]

Najdiskutovanejšími kandidátmi na mainstreamovej aj kvázi-mediálnej scéne boli v tomto období bývalý premiér a predseda hnutia ANO Andrej Babiš, bývalý predseda vojenského výboru NATO Petr Pavel, rektorka Mendelovej univerzity v Brne Danuše Nerudová a poslanec za hnutie SPD Jaroslav Bašta. Zatiaľ čo mainstreamová scéna písala o týchto kandidátoch prevažne v neutrálnych sentimentoch, kvázi-mediálna scéna bola značne kritická voči Petrovi Pavlovi. Vykresľovala ho ako agenta USA, ktorý vtiahne krajinu do vojny na Ukrajine a ktorý by rovnako ako Danuše Nerudová v

[23] Ibid.
[24] Národní úřad pro kybernetickou a informační bezpečnost, *Kybernetické incidenty pohledem NÚKIB – DUBEN 2022*.
[25] Národní úřad pro kybernetickou a informační bezpečnost, *Kybernetické incidenty pohledem NÚKIB – ŘÍJEN 2022*.
[26] Ministerstvo zahraničních věcí ČR, „Prohlášení MZV k anexi ukrajinských území".
[27] Flashpoint, „Killnet Ostracizes Leader of Anonymous Russia".
[28] Galeev, „«Не надо было угрожать моей стране»".
[29] Health sector cybersecurity coordination center. *HC3 Analyst Note*.
[30] Ministerstvo vnitra ČR, „Souhrn poznatků k českým prezidentským volbám 2023".

prípade svojho zvolenia do úradu vyhlásil mobilizáciu.[31] Zvyšným dvom kandidátom vyjadrila kvázi-mediálna scéna podporu, pričom postupne prešla od výhradnej podpory Jaroslavovi Baštovi k vykresľovaniu Andreja Babiša ako „menšieho zla".[32]

Deň pred voľbami a v oba dni volieb boli nezávislé od verbálnych útokov zaznamenané tiež kybernetické útoky proti webom kandidáta Tomáša Zimu, Ministerstva zahraničných vecí ČR, Českého štatistického úradu a dvom mimovládnym organizáciám Hlídač státu a Programy do voleb,[33] ktoré zhromažďovali informácie o politikoch a volebnej kampani.

Autorom týchto útokov bola ruskojazyčná skupina NoName057(16), ktorá v priebehu celého mesiaca napadla viac ako desiatku štátnych a súkromných subjektov.[34] Špecifikami tejto skupiny, ktoré ju odlišujú od dvoch vyššie spomenutých, je jednak vlastný projekt DDosia, ktorý láka dobrovoľníkov na zapojenie sa do kybernetických útokov za finančnú odmenu, a jednak samostatnosť a explicitný dištanc od iných proruských hacktivistov.[35,36]

Pred druhým kolom volieb, ktoré sa uskutočnilo 27. a 28. januára 2023, sa začali dezinformačné a kybernetické aktivity stupňovať. Najprv sa dňa 18. januára 2023 začala na sociálnych sieťach šíriť poplašná správa o údajnej SMS správe, ktorá v mene Petra Pavla vyzývala na mobilizáciu.[37] Na jej šírenie upozornil ešte v ten istý deň samotný Petr Pavel.[38] V priebehu nasledujúcich 48 hodín nasledovali DDoS útoky proti Ministerstvu obrany ČR, Ministerstvu financií ČR, Ministerstvu dopravy ČR, Ministerstvu priemyslu a obchodu ČR a Českej agentúre na podporu obchodu,[39] teda proti subjektom systémov mobilizácie ozbrojených síl a hospodárskej mobilizácie. To, že išlo o hoax a nikto SMS správu v skutočnosti nedostal, potvrdila Polícia ČR až 23. januára 2023.[40] Pôvodným šíriteľom bola zrejme žena zo Sliezska, ktorá mala na príspevok s fotografiou SMS správy naraziť na Facebooku.[41]

Dňa 21. januára 2023 sa sociálnymi sieťami začala šíriť ďalšia dezinformácia vo forme manipulatívne zostrihaného videa, na ktorom Petr Pavel údajne vyhlásil, že ČR musí vstúpiť do vojny s Ruskom.[42] Na video upozornil a jeho odkaz vyvrátil Petr Pavel o deň neskôr zverejnením pôvodného videa.[43] Za touto dezinformáciou stál podľa českého Centra proti hybridným hrozbám nový účet ruského štátneho propagandistického média Sputnik, ktorý sa takýmto spôsobom snažil poškodiť kandidáta.[44] Podobne ako v predchádzajúcom prípade, DDoS útok nasledoval do 24 hodín od zverejnenia dezinformácie, pričom jediným cieľom bolo Ministerstvo obrany ČR.[45]

Deň pred druhým kolom prezidentských volieb boli následne rozoslané reťazové e-maily informujúce o údajnej smrti Petra Pavla – jeden s odkazom na podvrhnutú volebnú webstránku kandidáta, druhý s

[31] Tkáčová a Šefčíková, *České prezidentské volby v online prostoru (1. kolo)*.
[32] Ministerstvo vnitra ČR, „Souhrn poznatků k českým prezidentským volbám 2023".
[33] Havlík, „Kyberútoky proti České republice".
[34] Národní úřad pro kybernetickou a informační bezpečnost, *Kybernetické incidenty pohledem NÚKIB – LEDEN 2023*.
[35] Radware, *Hacktivism Unveiled*.
[36] NoName057(16), „Друзья, вы что-то попутали…".
[37] Gričová, „Přicházejí falešné SMS".
[38] Pavel, „Vůbec mě nepřekvapuje…".
[39] Havlík, „Kyberútoky proti České republice".
[40] Mubeenová, „Policie prověřila falešnou SMS…".
[41] Ibid.
[42] Bidrmanová, „Sítěmi se valí lživé video…".
[43] Pavel, „Na internetu koluje falešné video…".
[44] Ministerstvo vnitra ČR, „Souhrn poznatků k českým prezidentským volbám 2023".
[45] Havlík, „Kyberútoky proti České republice".

fiktívnym odvolaním sa na jeho hovorkyňu Markétu Řehákovou.[46] Petr Pavel vyvrátil dezinformáciu o svojej smrti ešte v ten istý deň.[47] Napriek tomu DDoS útoky nasledovali do 48 hodín, a to proti webom Ministerstva zahraničných vecí ČR, Českého štatistického úradu a dvom mimovládnym organizáciám Hlídač státu a Pro bezpečnou budoucnost.[48] Práve druhý menovaný spolok je prevádzkovateľom napadnutého, originálneho volebného webu Petra Pavla,[49] ktorý je zároveň predsedom tohto spolku.[50]

Analýza rizík

MNO zohrali v prípade hybridného pôsobenia cudzej moci na prezidentské voľby v roku 2023 dve protichodné role. Na jednej strane spolok Nová republika prevádzkuje konšpiračný web, ktorý od vypuknutia vojny na Ukrajine šíril proruské naratívy neskôr použité počas volebnej kampane v diskreditačných článkoch namiereným proti kandidátovi Petrovi Pavlovi. Príkladom je jeden autorský a dva prevzaté články publikované pred druhým kolom prezidentských volieb, podľa ktorých sa Pavel „vyvinul od veľmi aktívneho stúpenca komunistických ideí (...) v aktívneho stúpenca opačnej strany (...) v dobe jeho všeobecného úpadku a z toho prameniacej rastúcej agresivity",[51] ďalej sa „horlivo hlási k celej pokleslej progresivistickej agende, ku klimatickému šialenstvu a rinčaniu zbraní"[52] a jeho voľba za prezidenta nielen „prispeje k predlžovaniu vojny, k väčším vojnovým škodám a väčšiemu počtu mŕtvych",[53] ale „vzrastie tiež riziko, že vojenské akcie prebehnú priamo na území ČR".[54]

Vzhľadom na to, že spolok nemá povinnosť zverejňovať informácie o zdrojoch svojho financovania, nemá zriadený účet na sociálnych sieťach a ani na svojom webe neinformuje o členoch spolku, partneroch či iných realizovaných aktivitách a podujatiach, túto svoju činnosť vykonával bez akejkoľvek zjavnej väzby, koordinácie alebo podpory zahraničného aktéra. V rámci hybridného pôsobenia preto zohráva skôr rolu „užitočného idiota".

Na strane druhej boli spolky Hlídač státu, Programy do voleb a Pro bezpečnou budoucnost, ktoré prevádzkujú weby zhromažďujúce objektívne a faktické informácie o kandidátoch na prezidenta, ich volebnom programe a samotných voľbách. Hlídač státu spravuje databázy s vyjadreniami politikov, transparentnými účtami či zmluvami súkromných firiem s väzbami na politikov. Programy do voleb naopak pri každých voľbách od roku 2018 informovali o mediálnych výstupoch kandidátov, výsledkoch prieskumov či plánovaných podujatiach. Oba tieto spolky si za svoju činnosť vyslúžili v roku 2022 nomináciu na cenu českého internetu Křišťálová Lupa v kategóriách „Veřejně prospěšná služba – cena České televize", resp. „Nástroje a služby".[55] Predsedom spolku Pro bezpečnou budoucnost bol zas samotný kandidát na prezidenta Petr Pavel.

Kybernetické útoky voči týmto organizáciám boli zaznamenané až v čase volieb tesne pred, resp. vo volebné dni oboch kôl. V rámci hybridného pôsobenia tak figurovali len ako ciele zahraničného proruského neštátneho aktéra – skupiny NoName057(16). Zatiaľ čo však pri spolku Pro bezpečnou budoucnost bol útok vedený proti volebnému webu kandidáta a nie proti organizácii samotnej, v prípade zvyšných dvoch spolkov mohli byť útoky proti ním namierené práve z dôvodu mediálnej

[46] Juna a Valášek, „Mail z Ruska tvrdí, že zemřel Petr Pavel…".
[47] Pavel, „ODMÍTNĚME ŠPINAVOSTI VE VOLBÁCH!...".
[48] Havlík, „Kyberútoky proti České republice".
[49] WHOIS, „Whois Record for GeneralPavel.cz".
[50] Spolu silnější, „Kontakty".
[51] David, „Generál Petr Pavel je plukovníkem Emanuelem Moravcem…"
[52] Hrabák, „Prohlášení iniciativy Zachraňme náš stát…"
[53] Hampl, „Hrdina, co se bojí postavit za vlastní vizi".
[54] Ibid.
[55] Křišťálová Lupa, „Výsledky".

pozornosti, ktorej sa im dostalo vďaka nominácii na cenu a mediálnemu pokrytiu jej odovzdávania verejnoprávnou Českou televíziou.[56] Ide totiž zrejme o jediné pojítko, ktoré ich spája a zároveň odlišuje od iných potenciálnych cieľov z mimovládneho sektora, ako napr. od spolku Manipulátoři.cz a Ústavu nezávislé žurnalistiky, ktoré prevádzkujú weby na odhaľovanie vplyvov cudzích mocí a vyvracanie dezinformácií.

Pri hľadaní odpovede na otázku s akými rizikami pre štát a spoločnosť sa takáto ambivalentná rola MNO pôsobiacich v informačnej doméne spája je treba prípady identifikovaných MNO posudzovať nie individuálne, ale prostredníctvom prizmy synergického efektu širšej vplyvovej kampane prebiehajúcej na dvoch úrovniach.

Na strategickej úrovni je spolok Nová republika súčasťou kvázi-mediálnej a dezinformačnej scény dlhodobo podporujúcej zahraničnú politiku Ruska, ktorá podľa českého Centra proti hybridným hrozbám nielenže posilňuje polarizáciu spoločnosti šírením ruskej propagandy a dezinformácií, ale môže ju tiež v niektorých prípadoch až radikalizovať.[57] Informačný vplyv tohto spolku je naviac po celý čas posilňovaný osobou jeho zakladateľa a aktívneho prispievateľa, ktorým je verejne známy politik dnes sediaci v Európskom parlamente za stranu SPD.[58]

Na operatívnej úrovni bola v priebehu prezidentských volieb zjavná snaha podporiť informačný vplyv tejto proruskej scény tiež zo strany zahraničných aktérov. Prinajmenšom pred druhým kolom volieb totiž aktivity oboch strán vykazovali istý vzorec správania – počas diskreditačnej a dezinformačnej kampane domácich proruských neštátnych aktérov a zahraničných štátnych aktérov boli najneskôr do 48 hodín od ich vypustenia zaznamenané kybernetické útoky zo strany zahraničného proruského neštátneho aktéra proti webstránkam českých štátnych inštitúcií a iných subjektov objektívne informujúcich o voľbách a kandidátoch, a schopných vyvrátiť šírené dezinformácie ako napr. o údajnej mobilizácii. Tento časový úsek sa prekrýva s časovým úsekom exekučnej fázy informačných operácií, ktoré od prvej publikácie vo forme tweetu, videa alebo článku až po poslednú zaznamenanú aktivitu amplifikácie jej dosahu prezdieľaním trvá podľa Európskej služby pre vonkajšiu činnosť približne 37 hodín.[59]

Takýto vzorec správania vykazuje znaky boja o informačnú a kognitívnu prevahu, ktorého cieľom je v relatívne krátkom čase znásobiť informačný vplyv jednej strany na voliča tým, že mu bude odoprený prístup k informáciám druhej strany. Podľa tohto scenára by teda aktéri podporujúci cudziu moc boli schopní v horizonte pár dní až týždňa pred voľbami zamedziť voličovi v prístupe k objektívnym a faktickým informáciám o kandidátovi a zároveň mu podsunúť dezinformácie, konšpirácie alebo inú formu diskreditácie na poškodenie ním zvažovaného, ale pre cudziu moc nevyhovujúceho kandidáta. V prípade českých prezidentských volieb je príkladom dezinformácia o údajnej smrti Petra Pavla deň pred druhým kolom volieb podporená podvrhnutým volebným webom a zablokovaním prístupu k tomu pôvodnému.

Otázkou je, nakoľko boli tieto aktivity koordinované a či bola vôbec nejaká centralizovaná forma riadenia potrebná na to, aby sa dostalo želaného efektu. Súčasné ruské strategické myslenie takúto priamu interakciu medzi domácimi a/alebo zahraničnými proruskými aktérmi, či už štátnymi alebo neštátnymi, nepovažuje za potrebnú. Koncepty reflexívnej kontroly[60] a samoorganizovaných

[56] Česká televize, „Křišťálová Lupa 2022".
[57] Ministerstvo vnitra ČR, „Jak česká kvazi-mediální scéna přebírá kremelské oficiální propagandistické i dezinformační narativy".
[58] Ibid.
[59] European external action service, *1st EEAS Report on FIMI Threats*.
[60] Vasara, *Theory of Reflexive Control*.

prostredí[61] totiž predpokladajú, že aktívne prvky združené v systéme zdieľaných hodnôt, princípov a funkcií budú vyvíjať iniciatívu z ich vlastného presvedčenia a pocitu spoločenskej zodpovednosti.[62] Podľa tejto logiky by tak proruskí neštátni aktéri nielenže dokázali samostatne a nezávisle prispievať do operácií na dosiahnutie ruských štátnych záujmov, ale oprostili by tiež Kremeľ od potreby priamej interakcie s nimi a poskytli mu tak možnosť hodnoverného poprenia akejkoľvek účasti na ich aktivitách.

Samotné proruské hackerské skupiny poukazujú na to, že nedochádza ku koordinácii so štátom[63] ani medzi nimi samými.[64] K takémuto výkladu o autonómii hackerov sa po dlhodobej viere v centralizovanejšiu formu koordinácie medzi vládou cudzej moci a neštátnymi aktérmi postupne obracajú tiež odborníci na kybernetickú bezpečnosť z Európy,[65] podľa ktorých v prípade Ruska prenášajú štátne orgány časť svojej zodpovednosti práve na hacktivistické a zločinecké skupiny.[66]

Nezodpovedaná zostáva otázka koordinácie medzi týmito hackerskými skupinami a domácimi a zahraničnými šíriteľmi propagandy a dezinformácií. Napriek tomu, že odpozorovaný vzorec správania nie je toho dôkazom, náhodnosť útokov je vylúčená deklarovaným záujmom hackerov zasiahnuť do priebehu prezidentských volieb. Buď teda sami museli sledovať dianie v Českej republike z externého prostredia a reagovať naň, alebo museli dostávať echo od miestneho kontaktu. O reálnosti druhej možnosti svedčí DDoS útok skupiny NoName057(16), ktorý bol ohlásený po skončení volieb dňa 2. februára 2023 o 13:15 hod. Bol namierený proti webstránke baru z centra Prahy, ktorý zmenil názov drinku „Biely Rus" na „Mŕtvy Rus".[67] O zmene názvu drinku informoval na Telegrame len štyri hodiny pred ohlásením útoku anonymný účet Selský rozum.[68] Podľa investigatívnych novinárov ide o účet šíriaci ruskú propagandu o dianí v Rusku a na Ukrajine v lámavej češtine, ktorý buďto využíva strojový preklad, alebo za ním stojí osoba, ktorej materinským jazykom nie je čeština.[69]

Vzhľadom na nízky počet subjektov napadnutých kybernetickými útokmi, krátkosť času zneprístupnenia ich webov a kontinuálny debunking zo strany poškodeného kandidáta na sociálnych sieťach bol výsledný efekt tohto pôsobenia na priebeh prezidentských volieb skôr zanedbateľný. Napriek tomu nie je možné vylúčiť možnosť, že išlo o testovaciu fázu mapovania cieľov, súčinnosti jednotlivých vplyvových aktérov a vyhodnocovania odozvy zacieleného prostredia, ktorá sa do budúcna pretaví vo väčšom meradle.

Záver

Lokálne MNO pôsobiace v informačnej doméne môže cudzia moc zneužiť dvojako. Na jednej strane môžu byť strategicky využívané ako „užitoční idioti" na šírenie naratívov a iných informačných vplyvov cudzej moci s cieľom polarizovať až radikalizovať spoločnosť v prospech jej zahraničnej politiky. Na strane druhej môžu byť proti ním podľa potreby vedené kybernetické útoky v rámci širšej destabilizačnej kampane, ktorej cieľom je zamedziť prístup k objektívnym a faktickým informáciám, a získať tak operatívnu informačnú a kognitívnu prevahu, napr. v čase volieb na ovplyvnenie rozhodnutia voliča.

[61] Lepskiy, „Reflexive Self-Organizing Decision Support Systems".
[62] Lepskiy, „Social responsibility in self-developing reflexive-active environments".
[63] Galeev, „«Не надо было угрожать моей стране»".
[64] NoName057(16), „Друзья, вы что-то попутали…".
[65] Národní úřad pro kybernetickou a informační bezpečnost, *Zpráva o stavu kybernetické bezpečnosti 2020*, 15.
[66] Grossman, *Workshop report*.
[67] Havlík, „Kyberútoky proti České republice".
[68] Selský rozum, „Nápojový lístek v jednom z pražských barů…".
[69] Šlerka, „Český Telegram jako ruský tlampač".

Zdroje

BEZPEČNOSTNÍ INFORMAČNÍ SLUŽBA. 2021. *Výroční zpráva 2020*. Dostupné z: https://bis.cz/public/site/bis.cz/content/vyrocni-zpravy/2020-vz-cz-2.pdf.

BEZPEČNOSTNÍ INFORMAČNÍ SLUŽBA. 2022. *Výroční zpráva 2021*. Dostupné z: https://bis.cz/public/site/bis.cz/content/vyrocni-zpravy/2021-vz-cz-2.pdf.

BIDRMANOVÁ, Markéta. 2023. „Sítěmi se valí lživé video o generálu Pavlovi. Je za ním proruský účet". *seznamzpravy.cz*. Dostupné z: https://seznamzpravy.cz/clanek/domaci-sitemi-se-vali-lzive-video-o-generalu-pavlovi-je-za-nim-prorusky-ucet-224034.

CIBULKA, Jan. 2022. „‚Hybridně působí ve prospěch Ruska.' Vojenští rozvědčíci zveřejnili dopis, proč žádali blokaci webů". *irozhlas.cz*. Dostupné z: https://irozhlas.cz/zpravy-domov/vz-rozvedka-armada-blokace-webu-cenzura-svoboda-projevu_2204050644_cib.

ČESKÁ TELEVIZE. 2022. „Křišťálová Lupa 2022". *ceskatelevize.cz*. Dostupné z: https://ceskatelevize.cz/porady/10000000219-kristalova-lupa/22225400054/.

DAVID, Ivan. 2013. „Projev Ivana Davida na Vratimovském semináři 2013". *novarepublika.online*. Dostupné z: https://novarepublika.online/2013/10/projev-ivana-davida-na-vratimovskem-seminari-2013.

DAVID, Ivan. 2023. „Generál Petr Pavel je plukovníkem Emanuelem Moravcem současného protektorátu". *novarepublika.online*. Dostupné z: https://novarepublika.online/2023/01/general-petr-pavel-je-plukovnikem-emanuelem-moravcem-soucasneho-protektoratu.

EUROPEAN EXTERNAL ACTION SERVICE. 2023. *1st EEAS Report on Foreign Information Manipulation and Interference Threats: Towards a framework for networked defence*. Dostupné z: https://euvsdisinfo.eu/uploads/2023/02/EEAS-ThreatReport-February2023-02.pdf.

FLASHPOINT. 2023. „Killnet Ostracizes Leader of Anonymous Russia, Adding New Chapter to Pro-Kremlin Hacktivist Drama". *flashpoint.io*. Dostupné z: https://flashpoint.io/blog/killnet-anonymous-russia-pro-kremlin-hacktivism/.

GALEEV, Artur. 2022. „«Не надо было угрожать моей стране» Хакеры Killnet защищают Россию, сражаясь с Anonymous и НАТО. Кто за ними стоит?". *lenta.ru*. Dostupné z: https://lenta.ru/articles/2022/04/15/killnet/.

GRIČOVÁ, Andrea. 2023. „Přicházejí falešné SMS jménem prezidentského kandidáta Petra Pavla. Případ šetří policie". *ceskatelevize.cz*. Dostupné z: https://ct24.ceskatelevize.cz/domaci/3558717-lidem-chodi-falesne-sms-zpravy-jmenem-prezidentskeho-kandidata-petra-pavla-pripad.

GROSSMAN, Taylor. 2023. *Workshop report — The Cyber Dimensions of the Russia-Ukraine War*. Dostupné z: https://eccri.eu/wp-content/uploads/2023/04/ECCRI_REPORT_The-Cyber-Dimensions-of-the-Russia-Ukraine-War-19042023.pdf.

HAMPL, Petr. 2023. „Hrdina, co se bojí postavit za vlastní vizi". *novarepublika.online*. Dostupné z: https://novarepublika.online/2023/01/hrdina-co-se-boji-postavit-za-vlastni-vizi.

HAVLÍK, David. 2023. „Kyberútoky proti České republice: Po stopách neznámého útočníka". Dostupné z: https://texty.hlidacstatu.cz/kyberutoky-proti-ceske-republice-po-stopach-neznameho-utocnika/.

HEALTH SECTOR CYBERSECURITY COORDINATION CENTER. *HC3 Analyst Note – KillNet's Targeting of the Health and Public Health Sector (December 2022 – March 2023)*. Dostupné z: https://hhs.gov/sites/default/files/202304051200-killnet-analyst-note-tlpwhite.pdf.

Tento projekt je podporený z Európskeho sociálneho fondu.

HRABÁK, Václav. 2023. „Prohlášení iniciativy Zachraňme náš stát k 2. kolu prezidentských voleb". *novarepublika.online*. Dostupné z: https://novarepublika.online/2023/01/prohlaseni-iniciativy-zachranme-nas-stat-k-2-kolu-prezidentskych-voleb.

JUNA, Petr a Lukáš Valášek. 2023. „Mail z Ruska tvrdí, že zemřel Petr Pavel. Případem se zabývá policie". *seznamzpravy.cz*. Dostupné z: https://seznamzpravy.cz/clanek/fakta-mail-z-ruska-tvrdi-ze-zemrel-petr-pavel-pripadem-se-zabyva-policie-224331.

KŘIŠŤÁLOVÁ LUPA. 2022. „Výsledky". *kristalova.lupa.cz*. Dostupné z: https://kristalova.lupa.cz/2022/vysledky/.

LEPSKIY, Vladimir. 2017. „Reflexive Self-Organizing Decision Support Systems for Development Governance". *International Journal of Engineering & Technology*, 7 (2.28). s. 255-258. Dostupné z: https://sciencepubco.com/index.php/ijet/article/view/12938/5172.

LEPSKIY, Vladimir. 2019. „Social responsibility in self-developing reflexive-active environments". In: *Conference Proceedings - Summaries of the 14th IRDO International Scientific & Business Conference on Social Responsibility and Current Challenges 2019*. Dostupné z: http://irdo.si/irdo2019/referati/a1-1-lepskiy.pdf.

MINISTERSTVO VNITRA ČR. 2021. *Zpráva o situaci v oblasti vnitřní bezpečnosti a veřejného pořádku na území ČR v roce 2020*. Dostupné z: https://mvcr.cz/soubor/zprava-o-situaci-v-oblasti-verejneho-poradku-a-vnitrni-bezpecnosti-na-uzemi-ceske-republiky-v-roce-2020.aspx.

MINISTERSTVO VNITRA ČR. 2022a. *Zpráva o situaci v oblasti vnitřní bezpečnosti a veřejného pořádku na území ČR v roce 2021*. Dostupné z: https://mvcr.cz/soubor/zprava-o-situaci-v-oblasti-verejneho-poradku-a-vnitrni-bezpecnosti-na-uzemi-ceske-republiky-v-roce-2021.aspx.

MINISTERSTVO VNITRA ČR. 2022b. *Jak kvazi-mediální scéna reflektovala invazi vojsk Ruské federace na Ukrajinu a šířila propagandu Kremlu v monitorovaném období od 24. února do 23. dubna*. Dostupné z: https://mvcr.cz/chh/clanek/jak-kvazi-medialni-scena-reflektovala-invazi-vojsk-ruske-federace-na-ukrajinu-a-sirila-propagandu-kremlu-v-monitorovanem-obdobi-od-24-unora-do-23-dubna.aspx.

MINISTERSTVO VNITRA ČR. 2022c. *Konspirační rámování ruské agrese vůči Ukrajině na české kvazi-mediální scéně*. Dostupné z: https://mvcr.cz/chh/clanek/konspiracni-ramovani-ruske-agrese-vuci-ukrajine-na-ceske-kvazi-medialni-scene.aspx.

MINISTERSTVO VNITRA ČR. 2022d. *Jak česká kvazi-mediální scéna přebírá kremelské oficiální propagandistické i dezinformační narativy – případ webu Nová republika*. Dostupné z: https://mvcr.cz/chh/clanek/jak-ceska-kvazi-medialni-scena-prebira-kremelske-oficialni-propagandisticke-i-dezinformacni-narativy-pripad-webu-nova-republika.aspx.

MINISTERSTVO VNITRA ČR. 2023. *Souhrn poznatků k českým prezidentským volbám 2023*. Dostupné z: https://www.mvcr.cz/chh/clanek/souhrn-poznatku-k-ceskym-prezidentskym-volbam-2023.aspx.

MINISTERSTVO ZAHRANIČNÍCH VĚCÍ ČR. 2022. *Prohlášení MZV k anexi ukrajinských území*. Dostupné z: https://mzv.cz/jnp/cz/udalosti_a_media/archiv_zprav/rok_2022/prohlaseni_mzv_k_anexi_ukrajinskych.html.

MUBEENOVÁ, Alžběta. 2023. "Policie prověřila falešnou SMS vyzývající jménem Petra Pavla k mobilizaci. Nikdo ji neobdržel". *ceskatelevize.cz*. Dostupné z: https://ct24.ceskatelevize.cz/domaci/3559836-policie-proverila-falesnou-sms-vyzyvajici-jmenem-petra-pavla-k-mobilizaci-nikdo-ji.

NÁRODNÍ ÚŘAD PRO KYBERNETICKOU A INFORMAČNÍ BEZPEČNOST. 2021. *Zpráva o stavu kybernetické bezpečnosti České republiky za rok 2020* . Dostupné z: https://nukib.cz/download/publikace/zpravy_o_stavu/Zprava_o_stavu_KB_2020.pdf.

NÁRODNÍ ÚŘAD PRO KYBERNETICKOU A INFORMAČNÍ BEZPEČNOST. 2022a. *Kybernetické incidenty pohledem NÚKIB – DUBEN 2022*. Dostupné z: https://nukib.cz/download/publikace/vyzkum/2022-04_Kyberneticke_incidenty.pdf.

NÁRODNÍ ÚŘAD PRO KYBERNETICKOU A INFORMAČNÍ BEZPEČNOST. 2022b. *Kybernetické incidenty pohledem NÚKIB – ŘÍJEN 2022*. Dostupné z: https://nukib.cz/download/publikace/vyzkum/2022-10.pdf.

NÁRODNÍ ÚŘAD PRO KYBERNETICKOU A INFORMAČNÍ BEZPEČNOST. 2023. *Kybernetické incidenty pohledem NÚKIB – LEDEN 2023*. Dostupné z: https://nukib.cz/download/publikace/vyzkum/2023-01_Kyberneticke_incidenty.pdf.

NETÍK, Jakub. 2022. „X.Dolezal". *facebook.com*. Dostupné z: https://facebook.com/jakub.netik.9/videos/488074036195350/.

NONAME057(16). 2022. „Друзья, вы что-то попутали…". *t.me*. Dostupné z: https://t.me/noname05716/934.

NOVÁ REPUBLIKA. 2023. „Manifest a stanovy". *novarepublika.online*. Dostupné z: https://www.novarepublika.online/manifest-a-stanovy.

PAVEL, Petr. 2023a. „Vůbec mě nepřekvapuje, že lež, kterou si Babiš dal na billboardy, následně někdo rozesílá lidem přes SMS a maily…". *twitter.com*. Dostupné z: https://twitter.com/prezidentpavel/status/1615731331610066946.

PAVEL, Petr. 2023b. „Na internetu koluje falešné video. Podívejte se na originál, jak jsem odpověděl jedné paní v Ostravě na její otázky…". *twitter.com*. Dostupné z: https://twitter.com/prezidentpavel/status/1617070375061393410.

PAVEL, Petr. 2023c. „ODMÍTNĚME ŠPINAVOSTI VE VOLBÁCH! Ano, žiju. Nikdy jsem nemyslel, že to budu muset napsat na sítě…". *twitter.com*. Dostupné z: https://twitter.com/prezidentpavel/status/1618553386198261760.

PROTIPROUD. 2022. „Ve stínu hrozby 3. světové války: Je čas jednat. Putin nebojuje s Ukrajinou, ale s elitami NWO. Rusko potvrdilo: Trump byl odstraněn podvodem. Zotročení Evropy. Biden nyní kryje kolosální kabalistické spiknutí. Vytvořme alianci za svobodu!". *protiproud.cz*. Dostupné z: https://protiproud.info/duchovni-svet/6398-ve-stinu-hrozby-3-svetove-valky-je-cas-jednat-putin-nebojuje-s-ukrajinou-ale-s-elitami-nwo-rusko-potvrdilo-trump-byl-odstranen-podvodem-zotroceni-evropy-biden-nyni-kryje-kolosalni-kabalisticke-spiknuti-vytvorme-alianci-za-svobodu.htm.

RADWARE. 2023. *Hacktivism Unveiled, April 2023 Insights Into the Footprints of Hacktivists*. Dostupné z: https://radware.com/security/threat-advisories-and-attack-reports/hacktivism-unveiled-april-2023/.

SELSKÝ ROZUM. 2023. „Nápojový lístek v jednom z pražských barů…". *t.me*. Dostupné z: https://t.me/selskyrozum/24676.

SMEJKAL, Eman a Jan Zadražil. 2022. „VELKÁ PŘEDJARNÍ OČISTA UKRAJINY PRÁVĚ TEĎ". *czechfreepress.cz*. Dostupné z: https://czechfreepress.cz/dalsi-blogy/velka-predjarni-ocista-ukrajiny-prave-ted.html.

SPOLU SILNĚJŠÍ. 2023. „Kontakty". *spolusilnejsi.cz*. Dostupné z: https://www.spolusilnejsi.cz/kontakty.

ŠLERKA, Josef. 2023. „Český Telegram jako ruský tlampač". *investigace.cz*. Dostupné z: https://investigace.cz/cesky-telegram-rusky-tlampac/?tztc=1.

TKÁČOVÁ, Natália a Kristína Šefčíková. 2023. *České prezidentské volby v online prostoru (1. kolo)*. Dostupné z: https://pssi.cz/download//docs/10201_ceske-volby-v-ere-dezinformaci-prezidentske-volby-1-kolo.pdf.

VASARA, Antti. *Theory of Reflexive Control.* Dostupné z: https://www.doria.fi/bitstream/handle/10024/176978/Vasara_FDS22_Theory%20of%20Reflexive%20Control%20%28web1%29-1.pdf.

VOJENSKÉ ZPRAVODAJSTVÍ. 2021. *Výroční zpráva Vojenského zpravodajství za rok 2020*. Dostupné z: https://vzcr.cz/uploads/41-Vyrocni-zprava-2020.pdf.

VOJENSKÉ ZPRAVODAJSTVÍ. 2022. *Výroční zpráva Vojenského zpravodajství za rok 2021*. Dostupné z: https://vzcr.cz/uploads/41-Vyrocni-zprava-2021.pdf.

WHOIS. 2023. *Whois Record for GeneralPavel.cz*. Dostupné z: https://whois.domaintools.com/generalpavel.cz.

ZÁHUMENSKÁ, Vendula. 2022. „Milion migrantů a ukrajinská zdravotní turistika". *novarepublika.online*. Dostupné z: https://novarepublika.online/2022/04/milion-migrantu-a-ukrajinska-zdravotni-turistika.