
IVANA KARÁSKOVÁ
NIKOLETA NEMEČKAYOVÁ
JAK NEHACKNOUT VOLBY
KARA NĚMEČKOVÁ
FILIP ŠEBOK
Foreign, Commonwealth & Development Office
AMO.CZ

Obsah

JAK (NE)HACKNOUT VOLBY
Duben 2024

Editorka – Ivana Karásková
Autoři – Ivana Karásková, Nikoleta Nemečkayová, Kara Němečková, Filip Šebok
Komiks – Kryštof Ulbert, Pavla Beránková (dialogy)

Citace – Ivana Karásková, Nikoleta Nemečkayová, Kara Němečková a Filip Šebok, *Jak (ne)hacknout volby*, (Praha, Asociace pro mezinárodní otázky (AMO), 2024).

Poznámka – Publikace vychází s podporou Foreign, Commonwealth & Development Office (FCDO).

Poděkování – Autoři publikace děkují účastníkům dvou uzavřených cvičení za jejich laskavé postřehy a nápady k prvním verzím scénářů s fiktivními politiky.

ASOCIACE PRO MEZINÁRODNÍ OTÁZKY (AMO)
Žitná 27/608
CZ 110 00 Praha 1
Tel.: +420 224 813 460
info@amo.cz
www.amo.cz

ISBN 978-80-88470-41-0 (tisk)
ISBN 978-80-88470-42-7 (pdf)

Předmluva

V době, kdy demokracie po celém světě čelí nečekaným výzvám, jsou volby víc než jen pravidelný rituál; jsou základním kamenem naší svobody a nezávislosti. Volby hrají v zastupitelské demokracii klíčovou roli, neboť nám – občanům – umožňují podílet se na chodu země prostřednictvím volených zástupců. Je proto důležité, aby probíhaly otevřeně, nebyly manipulované a každý občan volil na základě nezkreslených informací, které získá o kandidátech.

Vnější zásahy do volebních procesů mohou mít hluboký dopad na společnosti, v nichž se odehrávají. Takové zásahy narušují právo občanů vybrat si svobodně své zástupce, manipulují s veřejným míněním a mohou přispívat k nestabilitě a štěpení společnosti. Případy vměšování do voleb jsou přitom překvapivě časté. Jde o levný způsob s možným velkým dopadem, jak se ukázalo například u referenda o vystoupení Velké Británie z Evropské unie (tzv. brexit). Vměšování do voleb se díky tomu stalo poměrně oblíbeným nástrojem některých zahraničních aktérů, jejichž cílem je destabilizace západních společností. I neúspěšný případ vměšování do voleb totiž může podkopat důvěru veřejnosti ve férovost a smysl voleb a vést tak k cíli, který si útočník předsevzal.

Tyto aktivity s oblibou používají Rusko, Čína a Írán. Rusko je historicky v našem regionu známé snahou o štěpení společnosti a šíření dezinformací. Čína je v této oblasti spíše nováčkem, který se ale rychle učí. Snaží se zajistit si zejména pozitivní vnímání svého režimu v zahraničí a umlčet kritiky, kteří například poukazují na porušování lidských práv. Írán je velmi aktivní v oblasti kybernetického působení. Tyto země postupně rozvíjejí své strategie, učí se od sebe, vzájemně se inspirují a očekává se, že se budou výrazně snažit ovlivňovat volby v Evropě i v budoucnosti.

Je ale třeba říct, že útočit na volební procesy mohou i domácí aktéři. Například snahy o očernění kandidáta nebo kandidátky mohou využít političtí soupeři, kteří s prvotním útokem ze zahraničí nejsou přímo spojeni.

Tato publikace vychází u příležitosti nadcházejících voleb do Evropského parlamentu v červnu 2024. Volby do Evropského parlamentu jsou specifické tím, že současně probíhají ve 27 zemích, a představují tak velké lákadlo pro některé zahraniční aktéry. S ohledem na mnoho dříve popsaných případů vměšování do voleb je rozumné očekávat, že během volební kampaně nebo vlastních voleb proběhnou pokusy o jejich narušení. Proto se členské země Evropské unie, jejich vlády, ale i neziskový sektor a další na tuto možnost připravují – ať již kampaněmi, které mají za cíl informovat veřejnost, nebo monitorováním průběhu voleb, či spoluprací s firmami, které pomáhají odhalovat a potlačovat dezinformace a kybernetické útoky.

Publikace, kterou držíte v ruce, si klade za cíl seznámit českou veřejnost s tématem zahraničního vměšování do voleb interaktivní a přístupnou formou. Vychází z naší zkušenosti s tématem zahraničního vměšování, kterému se dlouhodobě věnujeme v Asociaci pro mezinárodní otázky (AMO), české nevládní neziskové organizaci, jež se od roku 1997 zaměřuje na vysvětlování zahraniční politiky veřejnosti. Čerpáme také z poznatků získaných ze dvou uzavřených cvičení, která jsme vedli v listopadu 2023 a lednu 2024 a jichž se zúčastnili pozvaní kandidáti do evropských voleb, jejich poradci, odborníci na strategickou komunikaci ze státní správy a akademických institucí a novináři.

Ve třech částech publikace se postupně věnujeme způsobům, jimiž může vměšování probíhat. Na konkrétních příkladech ukazujeme, jak mohou vypadat snahy cizích státních a nestátních aktérů ovlivnit volby – využitím finančních nástrojů (finanční podpora politických stran, kampaní nebo jednotlivých kandidátů), manipulací s informacemi (dezinformace, fake news) a kybernetickými nástroji (krádeže dat a následné zveřejnění informací s cílem očernit konkrétního kandidáta). Ačkoliv text pro větší přehlednost členíme do kapitol, skutečné případy vměšování často spojují různé prvky dohromady. Například dojde nejprve k napadení e-mailové komunikace kandidáta do voleb, získání citlivých informací, hesel k účtům na sociálních sítích apod., a poté ke zveřejnění upravených nebo zcela nepravdivých informací, jež mají kandidáta očernit.

V každé kapitole ukazujeme na příběhu zpracovaném komiksovou formou, jak může v praxi vměšování vypadat. Závěrem nabízíme sadu otázek, na které se můžete pokusit odpovědět. Přemýšlení o tom, co byste na místě našich vymyšlených politiků dělali vy, vám pomůže uvědomit si, jak je možné dosáhnout větší odolnosti proti zahraničnímu působení.

Kniha je určena široké veřejnosti. Doufáme, že text bude užitečný i pro učitele jako doplňkový materiál k výuce výchovy k občanství. Pokud byste se chtěli o tématu dozvědět více, nabízíme v závěru seznam další literatury.

Na následujících stránkách vás nejen seznamujeme s taktikami zahraničního vměšování, ale také vás vyzýváme, abyste se aktivně zapojili do ochrany naší demokracie. S poučenými a kriticky myslícími občany se nemanipuluje snadno. Společně můžeme vytvářet odolnější a informovanější společnost, připravenou čelit výzvám, které před nás staví současný svět.

Finanční nástroje

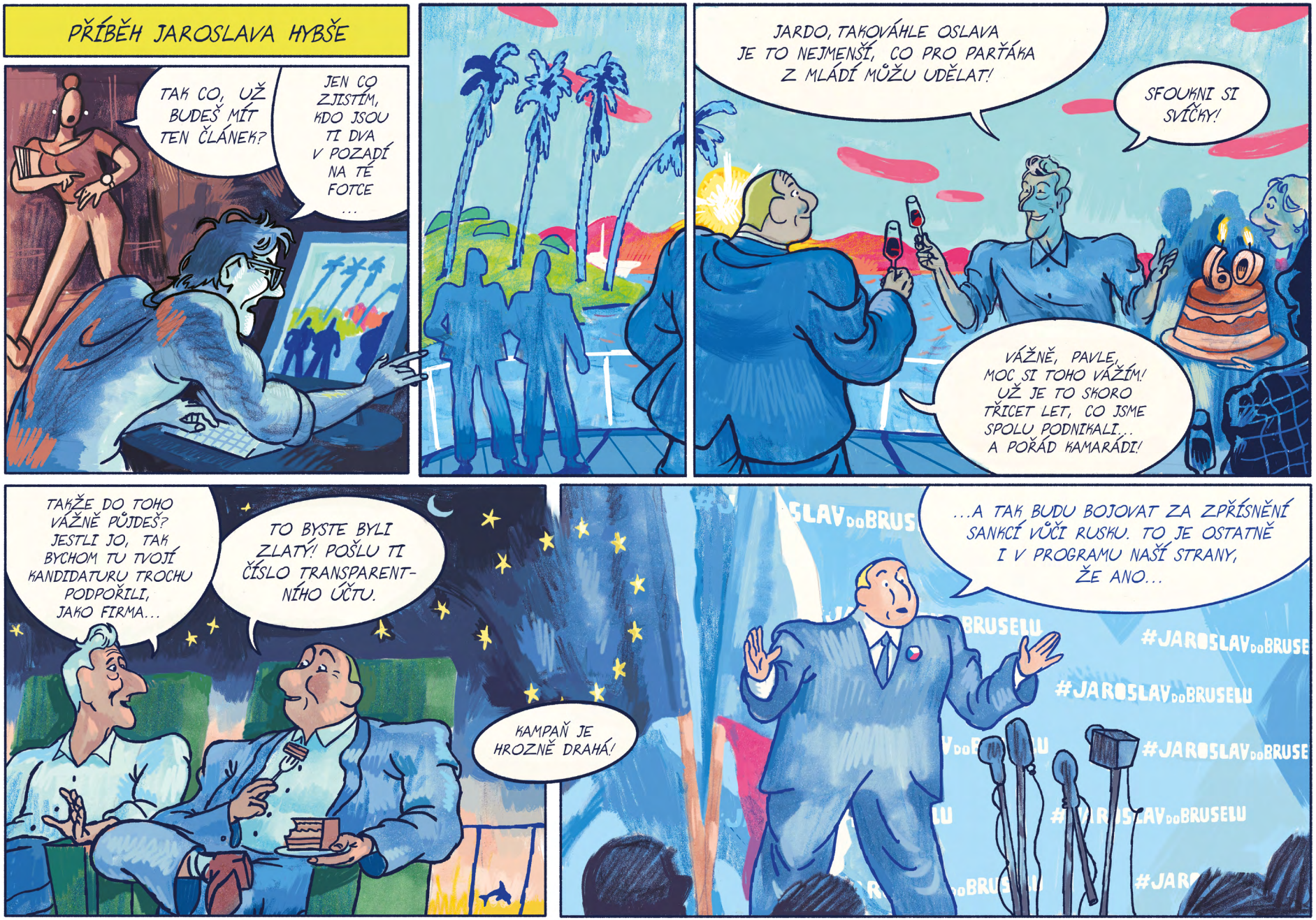
Poskytnutí finanční podpory kandidátovi nebo politické straně, případně financování politické kampaně na zvolení konkrétního politika, s sebou může nést očekávání, že se politik nebo strana budou chovat v souladu s cíli dárce. A to nejen v průběhu kampaně, ale – což je významnější – i po volbách.

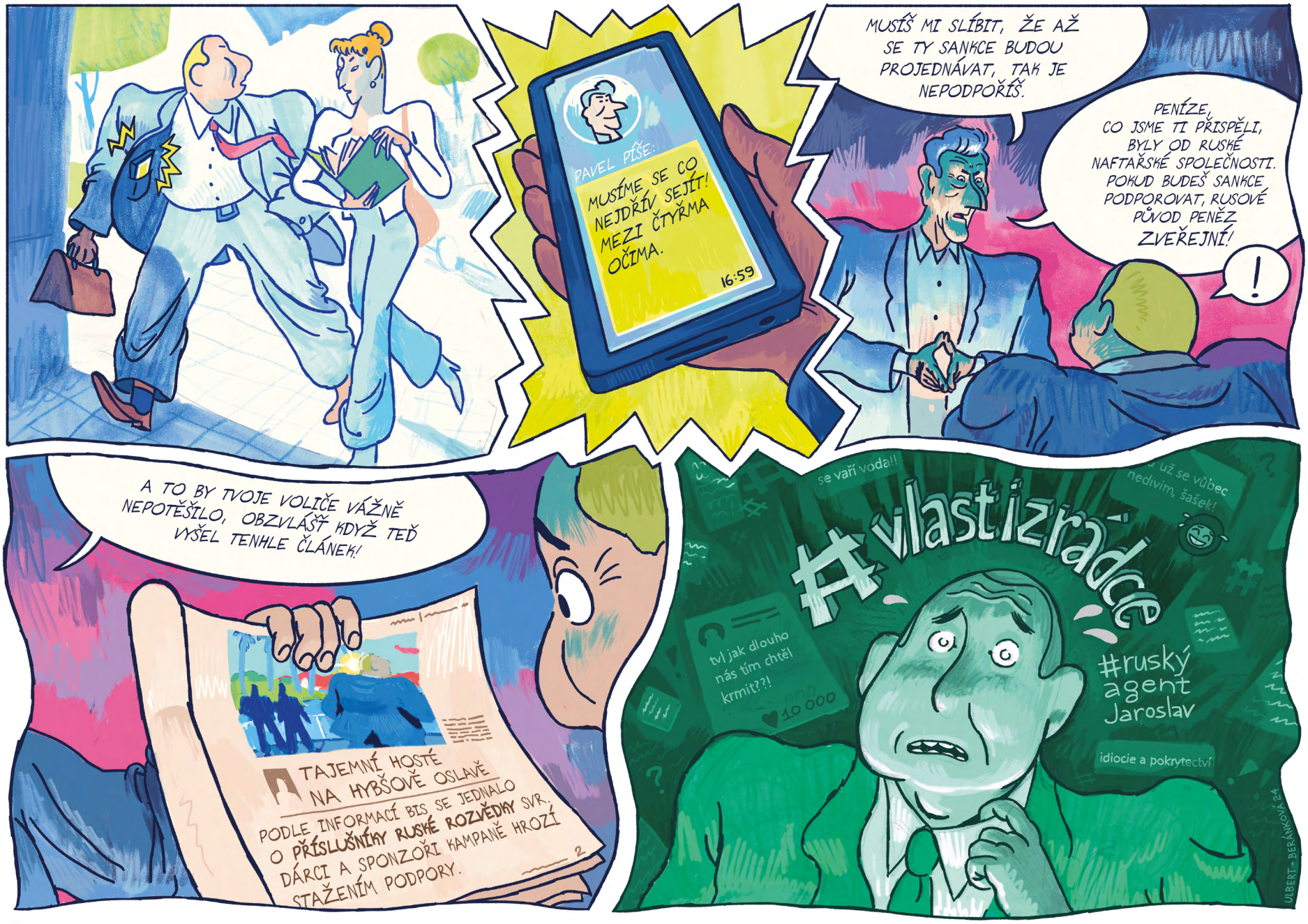
Přijímání finančních darů nebo nefinančních plnění (např. když třetí strana skoupí inzertní plochu nebo zaplatí článek v médiích pro propagaci kandidáta) přináší nejen etické otazníky, ale i bezpečnostní rizika. V extrémním případě totiž může vést k narušení schopnosti země vést vlastní politiku, vytvořit závislost na zahraničních dárcích a podněcovat korupci.

Vzhledem k vysokým nákladům spojeným s vedením volebních kampaní může poskytnutí finanční podpory znamenat i podstatnou výhodu pro podporovaného kandidáta. Taková pomoc může narušit férovost, kterou mají vytvořit domácí zákony o financování kampaní. Ty regulují a někdy omezují druhy a výši finanční podpory, kterou kandidáti dostávají. V důsledku toho zahraniční vměšování pomocí finančních nástrojů narušuje rovné podmínky ve volebním procesu.

Podpora politické straně nebo kandidátovi může mít podobu přímých darů, půjček nebo jiné finančně výhodné transakce. Může se odehrávat na celostátní, ale i komunální úrovni politiky, které věnují méně pozornosti analytici i veřejnost. Rusko například poskytlo značné finanční prostředky některým evropských politickým stranám – Národní frontě ve Francii, Hnutí pěti hvězd v Itálii a straně Syriza v Řecku. Čína se snažila ovlivnit komunální volby v Kanadě, v nichž finančně podporovala pročínské kandidáty. Čínská ambasáda také aktivně sháněla čínské studenty, aby těmto kandidátům pomáhali v jejich volebních kampaních.

V Evropské unii zatím chybí jednotná pravidla, která by zakazovala dary z mimoevropských zemí. Avšak i ve státech, které částečně nebo plně zakázaly dary politickým stranám, se najdou politici, kteří daná pravidla kreativně obcházejí. Kontakty mezi politickou stranou a dárcem někdy obstarávají prostředníci, a proto je přímých důkazů o financování konkrétních politiků ze třetích zemí relativně málo. Jedním z dobře popsaných případů je kauza senátora za labouristickou stranu v Novém Jižním Walesu Sama Dastyariho, která skončila jeho nuceným odstoupením. Dastyariho strana přijala dar od čínského milionáře Huang Xiangma během volební kampaně v roce 2016 s podmínkou, že Dastyari bude říkat, že sporné Jihočínské moře patří Číně.


PŘÍBĚH JAROSLAVA HYBŠE
TAK CO, UŽ BUDEŠ MÍT TEN ČLÁNEK?
JEN CO ZJISTÍM, KDO JSOU TI DVA V POZADÍ NA TÉ FOTCE ...
JARDO, TAKOVÁHLE OSLAVA JE TO NEJMENŠÍ, CO PRO PARŤÁKA Z MLÁDÍ MŮŽU UDĚLAT!
SFOUKNI SI SVÍČKY!
60
VÁŽNĚ, PAVLE, MOC SI TOHO VÁŽÍM! UŽ JE TO SKORO TŘICET LET, CO JSME SPOLU PODNIKALI... A POŘÁD KAMARÁDI!
TAKŽE DO TOHO VÁŽNĚ PŮJDEŠ? JESTLI JO, TAK BYCHOM TU TVOJÍ KANDIDATURU TROCHU PODPOŘILI, JAKO FIRMA...
TO BYSTE BYLI ZLATÝ! POŠLU TI ČÍSLO TRANSPARENTNÍHO ÚČTU.
KAMPAŇ JE HROZNĚ DRAHÁ!
...A TAK BUDU BOJOVAT ZA ZPŘÍSNĚNÍ SANKCÍ VŮČI RUSKU. TO JE OSTATNĚ I V PROGRAMU NAŠÍ STRANY, ŽE ANO...
#JAROSLAVdoBRUSELU


PAVEL PÍŠE:
MUSÍME SE CO NEJDŘÍV SEJÍT! MEZI ČTYŘMA OČIMA.
16:59
MUSÍŠ MI SLÍBIT, ŽE AŽ SE TY SANKCE BUDOU PROJEDNÁVAT, TAK JE NEPODPOŘÍŠ.
PENÍZE, CO JSME TI PŘISPĚLI, BYLY OD RUSKÉ NAFTAŘSKÉ SPOLEČNOSTI. POKUD BUDEŠ SANKCE PODPOROVAT, RUSOVÉ PŮVOD PENĚZ ZVEŘEJNÍ!
!
A TO BY TVOJE VOLIČE VÁŽNĚ NEPOTĚŠILO, OBZVLÁŠŤ KDYŽ TEĎ VYŠEL TENHLE ČLÁNEK!
TAJEMNÍ HOSTÉ NA HYBŠOVĚ OSLAVĚ
PODLE INFORMACÍ BIS SE JEDNALO O PŘÍSLUŠNÍKY RUSKÉ ROZVĚDKY SVR. DÁRCI A SPONZOŘI KAMPANĚ HROZÍ STAŽENÍM PODPORY.
2
se vaří voda!!
už se vůbec nedivím, šašek!
#vlastizrádce
tvl jak dlouho nás tím chtěl krmit??!
10 000
#ruský agent Jaroslav
idiocie a pokrytectví
ULBERT + BEŘÁNKOVÁ '24

Otázky k zamyšlení

Představte si, že jste členem volebního štábu Jaroslava Hybše. Vaším úkolem je vypořádat se s vývojem kauzy, v níž je zpochybňována nejen věrohodnost vašeho kandidáta, ale hrozí i ztráta významných podporovatelů a dárců. Vezměte v úvahu závažnost celé kauzy (příslušníci ruské rozvědky na jeho oslavě; skutečný původ peněz věnovaných na kampaň Hybšovým přítelem Pavlem; nátlak na to, aby Jaroslav Hybš po svém zvolení změnil postoj k sankcím uvaleným na Rusko, ačkoliv teď voličům slibuje, že sankce podpoří) a možné dopady.

Identifikujte klíčové body scénáře a pokuste se odpovědět na následující otázky:

1. **Proč přijal Jaroslav dar od Pavlovy firmy?**

2. **Udělal Jaroslav chybu? Nebo je chyba i jinde? (Můžete uvažovat o možném selhání jednotlivce, ale i o selhání systému.)**

3. **Kdyby se dal vrátit čas, co byste Jaroslavovi poradili předtím, než bude kandidovat ve volbách?**

4. **Co by měl Jaroslav udělat teď?**

Nebuďte jako Jarda

→ Politické kampaně jsou drahé a je běžné, že na ně prostřednictvím transparentního účtu (jehož zřízení je povinné) přispívají podporovatelé z řad podnikatelů i široké veřejnosti. Dělají to proto, že kandidát vyznává hodnoty a názory, které jsou podporovatelům blízké. Někdy ale také proto, že očekávají, že bude po svém zvolení podporovat zájmy těch, kteří dříve pomohli jemu.

→ Je třeba znát pravidla pro financování volebních kampaní. V České republice je upravují zákon o volbách do Parlamentu České republiky (zákon č. 247/1995 Sb.) a zákon o volbě prezidenta republiky (zákon č. 275/2012 Sb.). Na správnost financování volebních kampaní dohlíží Úřad pro dohled nad hospodařením politických stran a politických hnutí, na jehož webových stránkách jsou k dohledání úplné výroční finanční zprávy stran a hnutí.

→ Důkladné prověřování zdrojů podpory je nutnou podmínkou pro zajištění nezávislosti. U celostátních voleb často sledují a zveřejňují identitu dárců média. Není to ale vždy pravidlem. Férová politická soutěž je v zájmu všech, a proto je třeba očekávat, že se o původ peněz bude stále více zajímat i angažovaná veřejnost.

→ Dar je sice možné vrátit, je to však administrativně náročné. Může to s sebou nést negativní mediální pozornost a veřejnost může o kandidátovi začít pochybovat a váhat s další podporou. I proto je lepší důkladně prověřovat dárce (zejména u větších částek) ještě před přijetím finanční podpory.

Manipulace s informacemi

Informace, které se dostanou k voličům, jsou jedním z klíčových faktorů ovlivňujících jejich rozhodování, a tedy i výsledky voleb. Manipulace s informacemi je tak velmi účinným a díky digitálnímu věku i levným a snadným nástrojem k zasahování do volebních procesů.

Velmi častým způsobem manipulace s informacemi jsou kampaně v médiích a na sociálních sítích. V těchto kampaních se jejich tvůrci snaží využít polarizující témata a předsudky, které již v cílové společnosti existují (např. postoje k migraci nebo válce na Ukrajině). Zároveň se snaží, aby jejich pokusy vypadaly věrohodně. V minulosti bylo možné koordinované kampaně odhalit především díky gramatickým chybám a neobratným formulacím. V současné době jsou ale k dispozici různé nástroje umělé inteligence (artificial intelligence, AI), jako jsou DeepL, ChatGPT nebo Gemini. To dále komplikuje snahy takové kampaně odhalit a připsat je konkrétnímu pachateli. Na konci roku 2023 byla například odhalena koordinovaná kampaň nejméně 64 účtů, které využívaly obsah vytvořený pomocí ChatGPT k podkopávání podpory ruského opozičního politika Alexeje Navalného. Známou kampaní před nástupem AI bylo i zasahování Ruska do výsledků referenda o vystoupení Velké Británie z EU (tzv. brexit).

Další formou manipulace s informačním prostorem je vytváření překlepových webových stránek (typosquatting). V tomto případě útočník vytvoří doménu velmi podobnou skutečné webové stránce. Nová verze však obsahuje drobné překlepy, například zaměňuje nebo vynechává některá písmena z názvu. Její obsah pak na sociálních sítích pomáhají šířit účty vytvořené speciálně k tomuto účelu. Taková kampaň se objevila například ve Francii, kde kopie populárních médií, jako jsou deníky Le Monde a Le Figaro, šířily protiukrajinské narativy. V souvislosti s volbami může nastat podobná situace, kdy budou falešné stránky kopírovat oficiální weby kandidátů nebo institucí, které informují o průběhu a výsledcích hlasování.

Během voleb se objevují také manipulace s informacemi zaměřené přímo na kandidáty, například v podobě pomlouvačných kampaní. Jejich cílem je očernit nepohodlné kandidáty šířením nepravdivých nebo nelichotivých informací. K získání takových informací se využívají například hackerské útoky.

Kromě šíření obsahu, který jim pomáhá v dosahování cílů, se někteří aktéři také snaží potlačit obsah, který by je mohl poškodit. Dělají to prostřednictvím strategických žalob proti účasti veřejnosti (strategic lawsuits against public participation, SLAPPs). Tyto žaloby jsou stále častěji využívány k umlčení kritiků a ovlivňování veřejné debaty před volbami. Autoritářské vlády, včetně Ruska, Číny, Turecka a Venezuely, spoléhají na prostředníky (oligarchy nebo soukromé společnosti), kteří podávají žaloby na investigativní novináře, vydavatele, média, disidenty či exilové politiky, aby jim zabránili v šíření nepohodlných informací.


PŘÍBĚH MARIE PEŠIČKOVÉ
DĚKUJEME ZA VAŠI PODPORU.
STOP NUCENÝM STERILIZAC
TO JE SAMOZŘEJMOST. HLAVNĚ, ABY SE SITUACE UJGURŮ CO NEJDŘÍVE ZLEPŠILA.
MARIE, TOHLE BYSTE ASI MĚLA VIDĚT.
ANO?
...A JÁ MU ŘÍKÁM: NESTAČILO SEHNAT PÁR DĚTIČEK A VYFOTIT SE S NIMA? VŽDYŤ VÍŠ, ŽE TY MUSLIMY NEMŮŽU VYSTÁT.
CO SI SKUTEČNĚ MYSLÍ MARIE PEŠIČKOVÁ?
SMUTNÍK
...ALE TO NE, UJGURKY A TY JEJICH UTRÁPENÉ OBLIČEJE PRÝ NEJVÍC TÁHNOU.
TOHLE MÁM BÝT JAKO JÁ?!
KONFERENCE NA POPDORU
ŽE MI TO TAKHLE HODÍ KAŽDÝ PRAVDOLÁSKAŘ. I HAVLOID.
CHACHA!
NO TAK TEDA DOUFÁM, ŽE TA ŠARÁDA BUDE STÁT ZA TO...
0:00
3:24


NEMĚLI BYCHOM NA TO NĚJAK ZAREAGOVAT?
VŠAK JE TO ÚPLNĚ SMĚŠNÉ! KAŽDÝ PŘECE POZNÁ, ŽE TO NEJSEM JÁ. NESMÍME PŘISTOUPIT NA JEJICH HRU.
JEN BYCHOM PŘILÉVALI OLEJ DO OHNĚ!
VÁŽNĚ JSTE TAK NAIVNÍ A MYSLÍTE SI, ŽE TO VIDEO JE PODVRH?
PROČ TEDY PANÍ PEŠIČKOVÁ TAK DLOUHO MLČÍ? JÁ SE K PROBLÉMŮM STAVÍM ČELEM A OBČANÉ TO U VOLEB JISTĚ ZHODNOTÍ.
PROMIŇTE, K TOMU SE ALE VŮBEC NEHODLÁM VYJADŘOVAT!
SKANDÁL MARIE PEŠ... ODHALUJE DVOJÍ TVÁŘ PROTICÍNSKÝCH SIL!
OHÁNÍ SE LIDSKÝMI PRÁVY
PRÁZDNÁ SLOVA O HODNOTÁCH A DEMOKRACII
NĚJAKÉ JINÉ OTÁZKY NEMÁTE? PROTOŽE I DNES TOTO NECHÁM BEZ KOMENTÁŘE.
BEZ KOMENTÁŘE..?
VLBERT • BERÁNKOVÁ '24

Otázky k zamyšlení

Jste členové volebního štábu Marie Pešičkové a musíte vyřešit krizi, před kterou politička stojí. Zpochybňována je nejenom věrohodnost Mariiných politických názorů, ale i její osobní a hodnotová integrita. Právě díky své důvěryhodnosti si přitom Marie v minulosti získala přízeň voličů. Současná kauza tak může ohrozit nejen její současnou kandidaturu, ale i její budoucí politickou kariéru.

1. **Budete reagovat na zveřejněnou nahrávku?**

2. **Pokud se rozhodnete reagovat, jakým způsobem by bylo nejlepší se postavit k informacím, které se objevují na nahrávce?**

3. **Proč se nahrávka rychle šíří prostřednictvím médií? Proč na ni reagují představitelé jiných politických stran?**

4. **Jak se můžete připravit na podobné budoucí situace?**

Nereagujte jako Marie

→ Nevyjadřovat se k falešným informacím a nepodporovat jejich šíření se může zdát jako vhodná strategie. Jenže bez vyvracení se může stát, že informační prostředí ovládne právě nařčení. Není nutné vyvracet každou falešnou informaci, ale je třeba přijít s vlastním pozitivním příběhem.

→ Zapojte spojence. Mohou to být vaši blízcí, kteří se za vás mohou zaručit, nebo příznivci či média, která pomohou rozšířit reakci na falešné informace mezi širší skupinu lidí.

→ Snahy o očernění kandidáta nebo kandidátky mohou využít i lidé, kteří s útokem nejsou přímo spojení (např. političtí soupeři). V praxi bude obrana kandidáta spíše zaměřena právě proti těmto protivníkům než proti původci falešného tvrzení.

→ Je vhodné si dopředu připravit krizový plán. Ten může zahrnovat komunikační strategii, seznam potenciálních spojenců a osvědčená protiopatření. Kromě toho mohou kandidáti zvýšit svou odolnost školeními o práci s médii a sociálními sítěmi či kybernetické bezpečnosti. Lze využívat různé online nástroje (např. Brandwatch), které vám umožní sledovat zmínky o vašem jménu a reagovat na ně dříve, než se nějaká nepravdivá informace rozšíří. Je dobré zvýšit nejen svou vlastní odolnost, ale také odolnost svého publika a příznivců. Toho lze dosáhnout jejich poučením o hrozbě manipulací s informacemi a metodách jejich odhalování.

Kybernetické aktivity

Přestože se může zdát, že zranitelné vůči kybernetickým útokům jsou pouze země s pokročilými volebními technologiemi, ve skutečnosti je většina voleb závislá na informačních a komunikačních technologiích během celého volebního procesu.

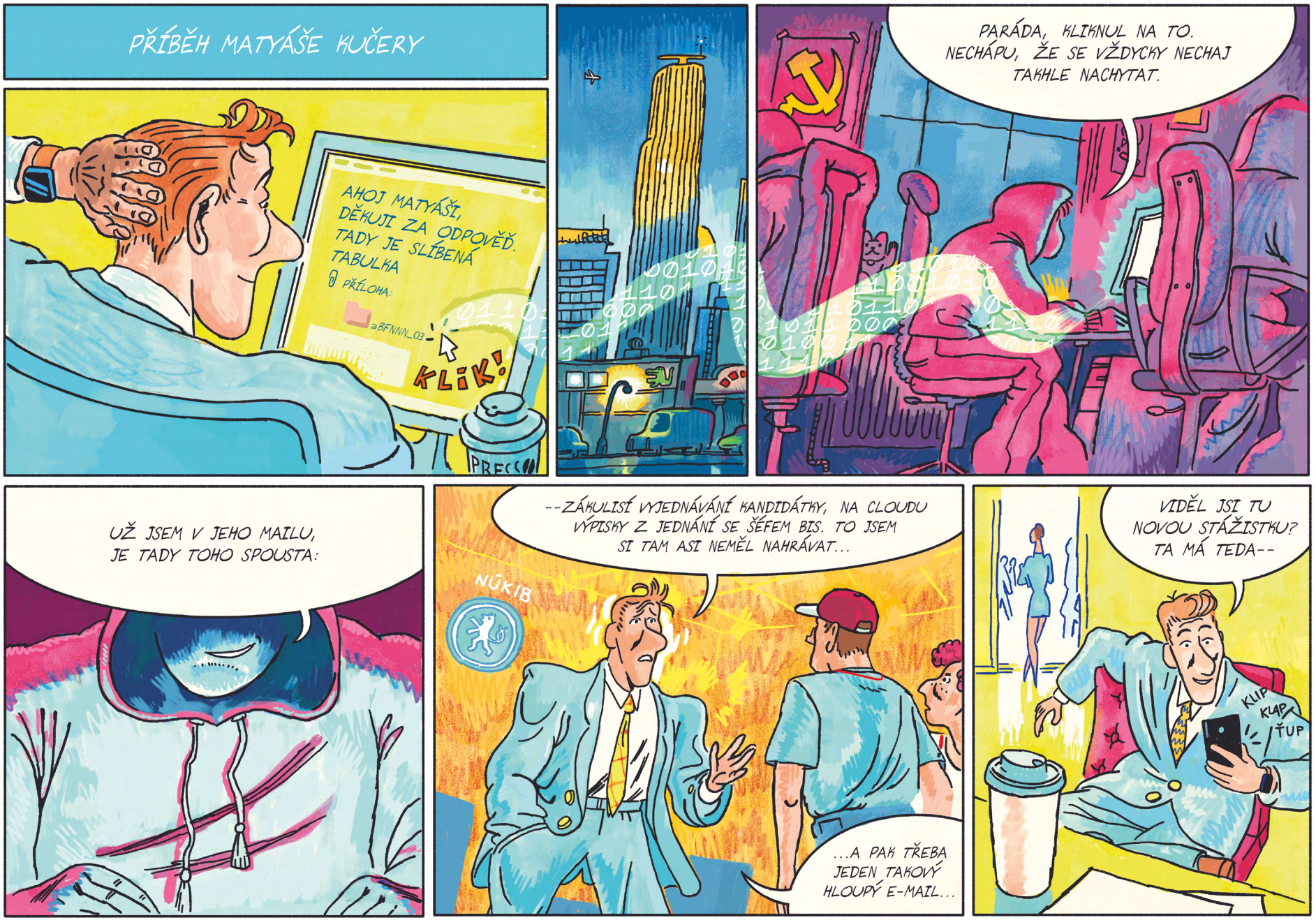
V posledních letech jsme byli svědky nárůstu kyberútoků a jiných nepřátelských aktivit v kyberprostoru vedených cizími státními a nestátními aktéry. Nejznámějším příkladem je ruské zasahování do amerických voleb v roce 2016, kdy hackeři napojení na Rusko zaútočili na několik cílů. Nabourali se například do počítačových sítí a účtů Demokratické strany nebo do databází se seznamy voličů ve dvou okrscích na Floridě. Tento incident vedl světové vlády k posílení kybernetické bezpečnosti a odolnosti.

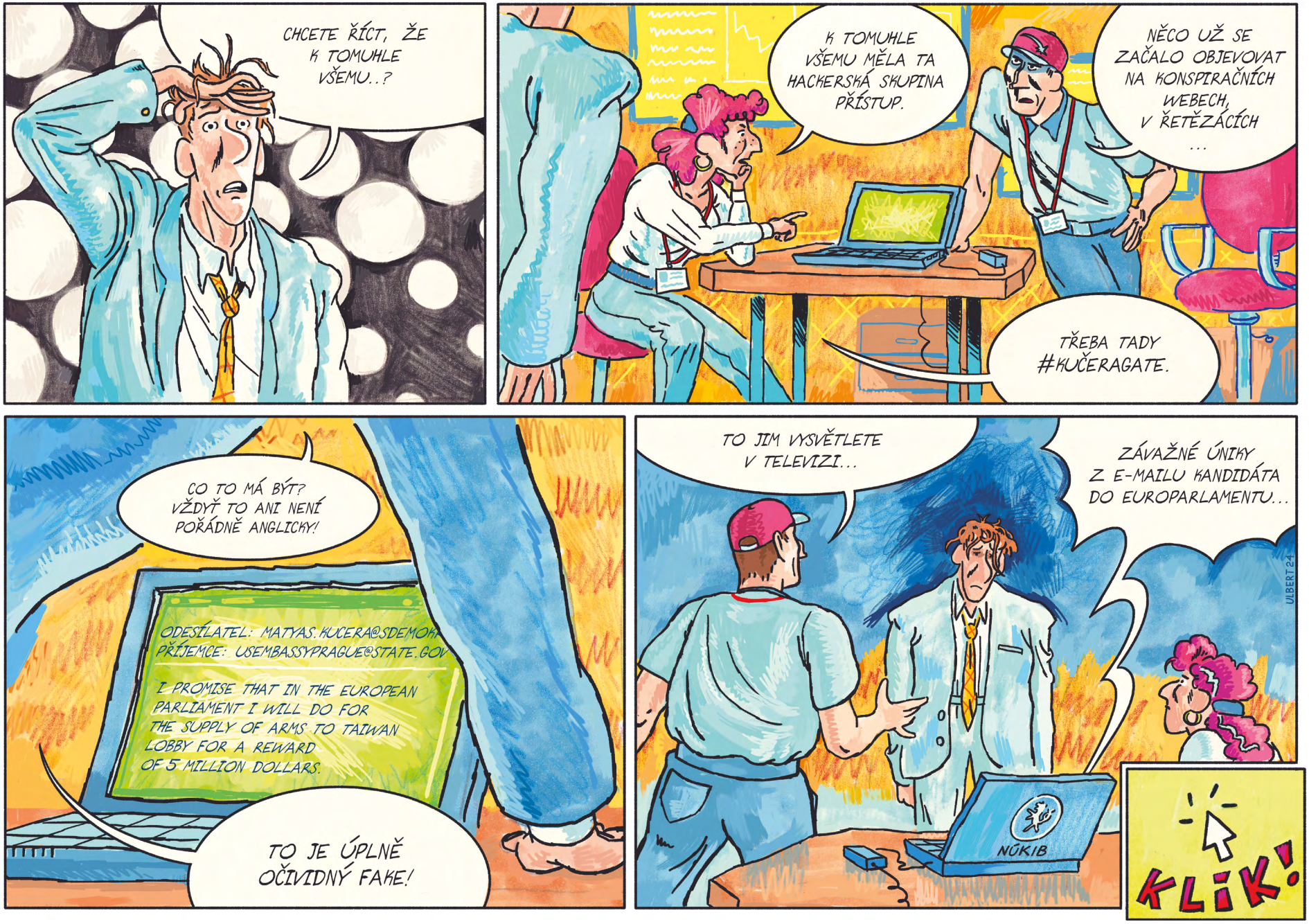
Jednou z často používaných metod je distribuované odmítnutí služby (Distributed Denial of Service, DDoS), což je technika útoku, při níž dochází k přehlcení internetových služeb nebo stránek požadavky, které vedou k jejich pádu nebo nefunkčnosti. Útok je koordinován mnoha útočníky a může způsobit nedostupnost volebních databází nebo informačních stránek o volbách. Například v roce 2017 došlo během voleb v České republice k výpadku prezentačních serverů Českého statistického úřadu kvůli rozsáhlému DDoS útoku. Přestože tyto útoky nemusí narušit samotné počítání hlasů, mohou snadno vytvořit dojem, že něco není v pořádku a že volby mohly být zmanipulované.

Další formou útoku je zkreslení webových stránek. Útočníci proniknou do webového serveru a nahradí obsah internetových stránek tím, který sami vytvořili. Tento typ útoku má za cíl získat mediální pozornost a může obsahovat zveřejnění ideologie nebo postojů útočníka.

Pokročilé a trvalé hrozby (Advanced Persistent Threats, APTs) jsou zacílenějším druhem útoku, který dlouhodobě a vytrvale infiltruje a zneužívá napadený systém. Tyto útoky často využívají techniky sociálního inženýrství, což je účelová manipulace s lidmi, která je má přimět k provedení určité akce nebo k vyzrazení důvěrné informace. Příkladem sociálního inženýrství je i tzv. phishing nebo spear phishing, kdy je cílem podvodné zprávy získat digitální identitu uživatele, jeho přihlašovací údaje, hesla, čísla bankovních karet nebo účtu pro jejich následné zneužití.

Hackeři také používají metodu zvanou hack-and-leak, kdy ukradnou citlivé informace, jako jsou e-maily politiků, a pak je zveřejní, aby ovlivnili volby. Obětí takového útoku byl například francouzský prezident Emmanuel Macron během voleb v roce 2017. Úniky informací jsou strategicky načasované. Často jsou zveřejněny těsně před volbami, kdy už nemají napadení čas reagovat. Útočníci pak ukradená data šíří přes sociální sítě. Někdy k nim přimíchávají i vymyšlené příběhy nebo falešné dokumenty, aby daného politika nebo političku co nejvíce očernili.


PŘÍBĚH MATYÁŠE KUČERY
AHOJ MATYÁŠI, DĚKUJI ZA ODPOVĚĎ. TADY JE SLÍBENÁ TABULKA
PŘÍLOHA:
aBFNNN_03
KLIK!
PARÁDA, KLIKNUL NA TO. NECHÁPU, ŽE SE VŽDYCKY NECHAJ TAKHLE NACHYTAT.
UŽ JSEM V JEHO MAILU, JE TADY TOHO SPOUSTA:
--ZÁKULISÍ VYJEDNÁVÁNÍ KANDIDÁTKY, NA CLOUDU VÝPISKY Z JEDNÁNÍ SE ŠÉFEM BIS. TO JSEM SI TAM ASI NEMĚL NAHRÁVAT...
NÚKIB
...A PAK TŘEBA JEDEN TAKOVÝ HLOUPÝ E-MAIL...
VIDĚL JSI TU NOVOU STÁŽISTKU? TA MÁ TEDA--
KLIP KLAP ŤUP


CHCETE ŘÍCT, ŽE K TOMUHLE VŠEMU..?
K TOMUHLE VŠEMU MĚLA TA HACKERSKÁ SKUPINA PŘÍSTUP.
NĚCO UŽ SE ZAČALO OBJEVOVAT NA KONSPIRAČNÍCH WEBECH, V ŘETĚZÁCÍCH ...
TŘEBA TADY #KUČERAGATE.
CO TO MÁ BÝT? VŽDYŤ TO ANI NENÍ POŘÁDNĚ ANGLICKY!
ODESÍLATEL: MATYAS.KUCERA@SDEMOK
PŘÍJEMCE: USEMBASSYPRAGUE@STATE.GOV
I PROMISE THAT IN THE EUROPEAN PARLIAMENT I WILL DO FOR THE SUPPLY OF ARMS TO TAIWAN LOBBY FOR A REWARD OF 5 MILLION DOLLARS.
TO JE ÚPLNĚ OČIVIDNÝ FAKE!
TO JIM VYSVĚTLETE V TELEVIZI...
ZÁVAŽNÉ ÚNIKY Z E-MAILU KANDIDÁTA DO EUROPARLAMENTU...
NÚKIB
KLIK!
ULBERT 24

Otázky k zamyšlení

Jste členové volebního štábu Matyáše Kučery a musíte vyřešit krizi, před kterou Kučera stojí. Kandidát čelí kritice na několika frontách: jeho voliči jej obviňují z ohrožení národní bezpečnosti, zatímco jiná část politického spektra nálepkuje Kučeru jako kolaboranta a agenta americké tajné služby CIA.

1. **Jaké kroky můžete podniknout, když ztratíte přístup ke svému e-mailovém účtu nebo účtům na sociálních sítích?**

2. **Koho a proč budete informovat o pravděpodobném hackerském útoku a možném úniku dat?**

3. **Jak přesvědčíte veřejnost, že dokumenty šířené na sociálních sítích jsou falešné?**

4. **Jak zabráníte dalšímu bezpečnostnímu narušení vašich dat a informačních systémů?**

Neklikejte jako Matyáš

→ Zabezpečení přístupu k oficiálním účtům je základním předpokladem kybernetické bezpečnosti. Přístup k těmto účtům musí být svěřen jen určeným jednotlivcům. K zabezpečení účtů musí existovat jasná pravidla jako jsou složitá a pravidelně měněná hesla nebo dvoufaktorové ověření.

→ Není radno zapomínat na dobrovolníky a externí spolupracovníky v kampani, kteří musí pravidla bezpečnosti také dodržovat. Jedním z klíčů k úspěchu je zajistit, aby všichni, kdo se podílejí na kampani, prošli školením na rozpoznávání phishingových e-mailů, nebezpečných příloh a podvodných webových stránek.

→ Aktivně vyhledávejte a udržujte spolupráci s vnějšími odborníky na kybernetickou bezpečnost a vládními agenturami, které vám mohou poskytnout další podporu a odborné znalosti.

→ Opatrnosti není nikdy dost. Buďte stále ostražití a reagujte okamžitě na jakékoli náznaky bezpečnostního narušení, a to i zdánlivě neškodné incidenty, které ale mohou signalizovat větší problémy v kybernetické bezpečnosti.

→ V případě hackerského útoku a úniku informací je vhodné zapojit policii a informovat ji o rozsahu a povaze úniku. Současně neváhejte přijmout právní kroky proti šiřitelům dezinformací, abyste omezili další škody. Za zvážení také stojí upozornění veřejnosti na útok a možné zkreslení informací kolujících po internetu.

Když chcete dělat víc

Ochrana demokracie a zajištění odolnosti volebních procesů představují společný cíl, který vyžaduje zapojení veřejnosti i institucí. Na jedné straně je nezbytné, aby občané znali rizika vměšování do voleb ze strany některých zahraničních aktérů a aktivně sledovali celý volební proces. Na druhé straně je klíčové, aby veřejnost nepropadala panice a měla důvěru v připravenost a schopnost státu čelit těmto rizikům. V ideálním případě by měly vlády vytvářet a prosazovat silné obranné strategie proti zahraničnímu vměšování do voleb, které podporuje informovaná a aktivní veřejnost.

Pokud se chcete více zapojit, informujte se o tom, jak můžete působit jako člen nebo členka volební komise. Zapojení veřejnosti do dohledu nad volbami může zvýšit transparentnost celého volebního procesu.

Politické strany a kandidáti by měli usilovat o transparentnost. Jako občané je můžete vyzývat, aby byli otevřenější v informování o svém financování. Můžete se také zapojit do kampaní, které vyžadují větší průhlednost ve financování politických aktivit. Zapojení veřejnosti pomáhá odhalovat možné odchylky od běžného volebního procesu a zvyšuje důvěru ve volby.

Můžete také aktivně pomáhat v boji proti dezinformacím tím, že se vzděláváte v rozpoznávání falešných zpráv a šíříte osvětu mezi svými vrstevníky, rodinou nebo přáteli. Podílejte se na vzdělávacích programech a seminářích a používejte sociální média k šíření ověřených informací.

V neposlední řadě mohou občané vyvíjet tlak na politické představitele a instituce, aby budovaly strategie pro ochranu voleb. Vytvářejte petice, účastněte se veřejných debat a zapojujte se do občanských iniciativ, které zvyšují odolnost voleb a tím i naší demokracie.

Když chcete vědět víc

- → Jeden svět na školách, **Fake news a dezinformace**, *https://www.jsns.cz/lekce/413754-fake-news-a-dezinformace.*
- → (Ne)bezpečně v síti, **Manuál rozvoje kritického myšlení v online prostoru**, 2022, *https://myslim.eu/wp-content/uploads/2022/02/Nebezpecne_v_siti_CZ.pdf.*
- → Centrum proti terorismu a hybridním hrozbám, Odbor komunikace britského úřadu vlády, **RESIST: příručka pro boj s dezinformacemi**, *https://www.mvcr.cz/chh/clanek/ke-stazeni-resist-prirucka-pro-boj-s-dezinformacemi.aspx.*
- → EDMO, **Disinformation narratives during the 2023 elections in Europe**, 2023, *https://edmo.eu/2023/12/13/disinformation-narratives-during-the-2023-elections-in-europe/.*
- → EUvsDisinfo, **Methods of Foreign Electoral Interference**, 2019, *https://euvsdisinfo.eu/methods-of-foreign-electoral-interference/.*
- → Evropský parlament, **Zpráva o zahraničním vměšování do všech demokratických procesů v Evropské unii, včetně dezinformací**, 2023, *https://www.europarl.europa.eu/doceo/document/A-9-2023-0187_CS.html.*
- → Ivana Karásková, Una Aleksandra Bērziņa-Čerenkova, Kara Němečková: **Foreign Electoral Interference Affecting EU Democratic Processes** (Brussels, Belgium: Authority for European Political Parties and European Political Foundations (APPF), 2023), *https://www.appf.europa.eu/cmsdata/277388/Foreign%20electoral%20interference%20affecting%20EU%20democratic%20processes.pdf.*
- → Veronika Krátká Špalková, Andrej Poleščuk, **Preventing election interference: Selected best practices and recommendations**, 2023, *https://www.hybridcoe.fi/publications/hybrid-coe-research-report-10-preventing-election-interference-selected-best-practices-and-recommendations/.*
- → Další materiály a informace o kurzech najdete například na stránkách organizace Zvol si info (*https://zvolsi.info/*) nebo projektu Fakescape! (*https://www.fakescape.cz/*).

O AMO

Asociace pro mezinárodní otázky (AMO) je nevládní nezisková organizace, která se věnuje výzkumu a vzdělávání v oblasti mezinárodních vztahů. Posláním AMO je zkoumat a vysvětlovat mezinárodní otázky, zkvalitňovat českou zahraniční politiku a přispívat k utváření světa, který ctí hodnoty svobody, demokracie a udržitelnosti.

ZŮSTAŇTE S NÁMI!

www.facebook.com/AMO.cz
www.twitter.com/AMO_cz
www.youtube.com/AMOcz
www.linkedin.com/company/AMOcz
www.instagram.com/AMO.cz

O autorech

Ivana Karásková

je zakladatelkou a vedoucí projektů MapInfluenCE, který mapuje čínský a ruský vliv v regionu střední Evropy, a China Observers in Central and Eastern Europe (CHOICE), kolaborativní platformy sdružující více než 120 analytiků specializujících se na Čínu. Kromě toho působí Ivana také jako European China Policy Fellow v MERICS v Berlíně. Je českou zástupkyní v týmu expertů na Čínu při European Center of Excellence for Countering Hybrid Threats (Hybrid CoE) v Helsinkách. Odborně se věnuje čínské zahraniční a bezpečnostní politice, čínskému působení v Evropě, čínským dezinformacím a postavení Číny v globálním systému. Získala doktoráty v oboru mezinárodních vztahů na Fakultě sociálních věd Univerzity Karlovy. Absolvovala studijní a výzkumné stáže v Číně a na Tchaj-wanu a jako Fulbright scholar působila na Weatherhead East Asian Institute na Columbia University v New Yorku.

Ivana pravidelně hovoří na slyšení Evropského parlamentu k tématům čínské zahraniční politiky a čínského vlivu ve světě. Její výzkum se objevil ve zprávách pro americký Kongres. Citovaly ji The New York Times, Politico, BBC, Al Jazeera, Le Monde, Deutsche Welle, Financial Times, South China Morning Post a další.

Od dubna 2023 působí jako zvláštní poradkyně místopředsedkyně Evropské komise a komisařky pro hodnoty a transparentnost Věry Jourové, kde konzultuje přípravu tzv. Defense of Democracy package.

Nikoleta Nemečkayová

je analytičkou Asociace pro mezinárodní otázky (AMO) se zaměřením na dezinformace, svobodu médií a strategickou komunikaci. Magisterské i bakalářské studium absolvovala na Masarykově univerzitě v Brně v oborech mezinárodní vztahy a překladatelství anglického jazyka. V minulosti pracovala jako analytička pro Kremlin Watch program v Evropských hodnotách, kde se zabývala zejména proruskými dezinformacemi a propagandou šířenou v zemích střední a východní Evropy. Dříve se této oblasti věnovala i během stáže pro Infosecurity.

Kara Němečková

pracuje v Asociaci pro mezinárodní otázky (AMO) jako analytička se zaměřením na Čínu a také jako manažerka pro vnější vztahy projektů MapInfluenCE a China Observers in Central and Eastern Europe (CHOICE). Kara absolvovala bakalářské a magisterské studium v oboru mezinárodní vztahy na univerzitě Sciences Po v Paříži. V roce 2019 se zúčastnila studijního pobytu na Univerzitě Fudan v Šanghaji. V minulosti absolvovala stáže na Generálním konzulátě České republiky v Šanghaji a v Institut Montaigne v Paříži. V roce 2021 pracovala v kanceláři místního koordinačního úřadu OSN v Kambodži v rámci programu UN Volunteers.

Filip Šebok

je projektový manažer a analytik se zaměřením na Čínu v Asociaci pro mezinárodní otázky (AMO). Pracuje na projektech MapInfluenCE a China Observers in Central and Eastern Europe (CHOICE). Zaměřuje se na čínskou domácí a zahraniční politiku, vztahy Číny se zeměmi střední a východní Evropy a na čínskou zahraničněpolitickou rétoriku. Filip absolvoval bakalářské a magisterské studium v oboru mezinárodní vztahy na Fakultě sociálních studií Masarykovy univerzity v Brně a bakalářské studium v oboru kulturní studia Číny na Filozofické fakultě téže univerzity. Druhý magisterský titul získal na Renmin University of China v Pekingu v čínskojazyčném programu mezinárodních vztahů. V minulosti pracoval pro slovenské výzkumné organizace Stratpol a CEIAS. Zkušenosti získal také během stáží na Ministerstvu zahraničních věcí v Bratislavě a zastupitelském úřadě Slovenské republiky v Pekingu. Na podzim 2022 působil jako James S. Denton Fellow v organizaci Center for European Policy Analysis (CEPA) ve Washingtonu. Filip je členem Expert Pool v European Center of Excellence for Countering Hybrid Threats (Hybrid CoE) v Helsinkách.