Government
Communication
Service

RESIST

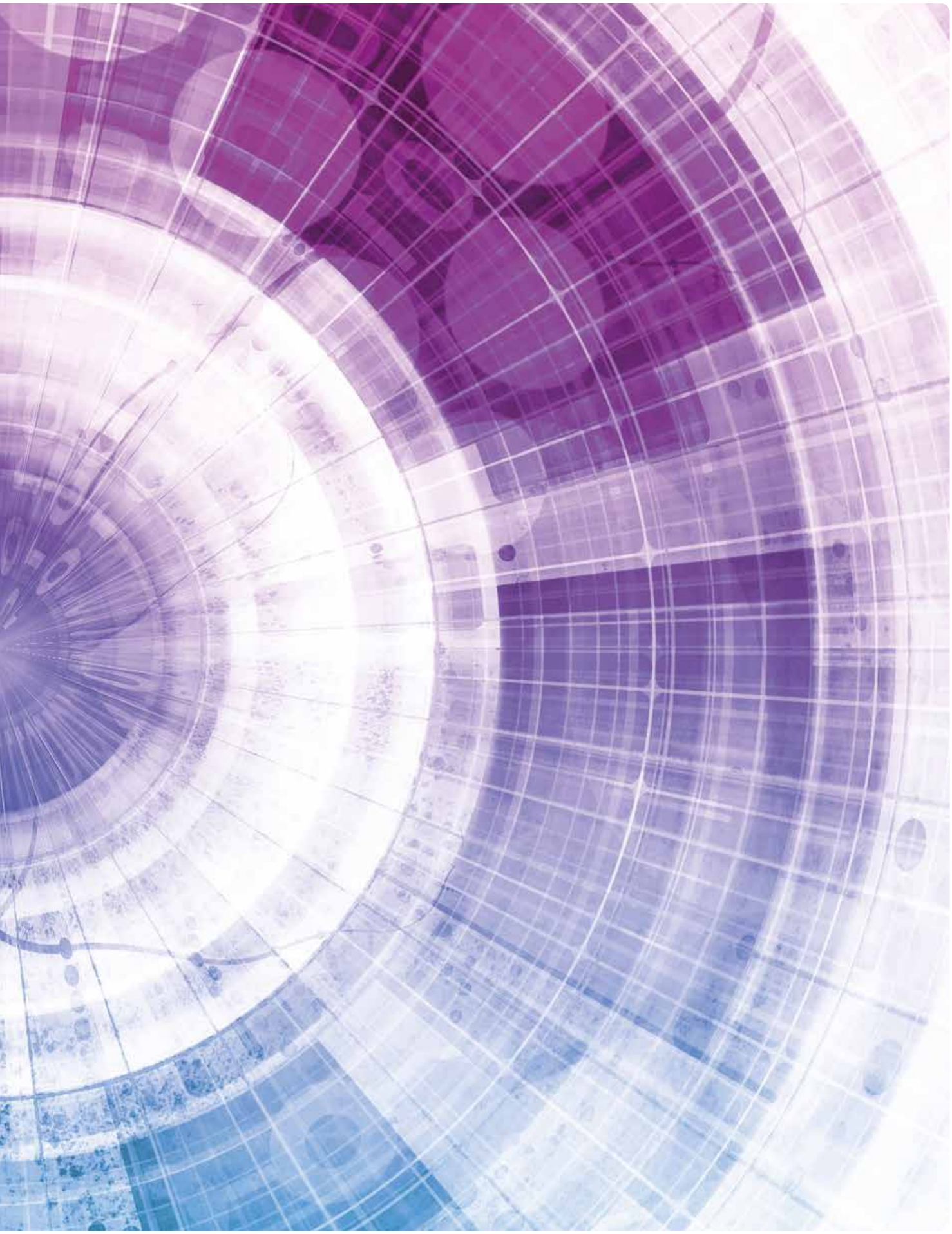
Příručka pro boj s dezinformacemi

Úvod

Šíření dezinformací spočívá v úmyslném vytváření a šíření nepravdivých a/nebo zmanipulovaných informací, které mají příjemce oklamat nebo uvést v omyl. Účelem je buď způsobit škodu, nebo získat nějaký politický, osobní či finanční prospěch. Neúmyslné sdílení nepravdivých informací se označuje jako „misinformace“.

Jednotlivé kapitoly příručky RESIST vysvětlují, jak rozpoznat dezinformace, jak využívat monitoring médií k včasnému varování, jak vypracovat rozbor situace, jak provést analýzu dopadů pro lepší pochopení cílů, dopadů a dosahu dezinformací, jak zajistit efektivní strategickou komunikaci bojující s dezinformacemi a také jak sledovat výsledky vaší práce.

Obsah



Rozpoznání dezinformací

Poznejte, jak funguje šíření dezinformací, a to s ohledem na jeho cíle a nejrozšířenější techniky. Zjistěte, jak se záměry a jednotlivé techniky kombinují, aby se maximalizoval jejich dopad.

Dezinformace slouží především k šíření vlivu. Lidé se neustále snaží ovlivňovat druhé – reklamní průmysl a další obory založené na vztazích s veřejností se snaží ovlivňovat naše chování každý den. Vliv také patří k základním stavebním kamenům diplomacie a zahraniční politiky, které legitimním způsobem využívají informace k dosažení kýžených výsledků. Naproti tomu původci dezinformační činnosti se snaží ovlivňovat ostatní pomocí nepravd, které slouží k dosažení určitého cíle. Vědomě při tom zneužívají zranitelnosti lidí, kterým znemožňují činit informovaná rozhodnutí.

Různí původci využívají dezinformací k dosažení různých cílů. Značná část dezinformací se vytváří a šíří za účelem ekonomického prospěchu nebo prosazování politických názorů. Tyto aktivity přispívají ke kontaminaci informačního prostoru, jejich dopad je však často jen omezený. Problematičtější situace nastává, když dezinformace šíří nepřátelské státní nebo polostátní subjekty v rámci nějaké rozsáhlejší kampaně. Často budete muset zareagovat, aniž byste měli jistotu, kdo přesně za dezinformacemi stojí a jaké jsou jejich skutečné cíle.

Pokud máte bojovat s dezinformacemi, musíte je nejprve pomocí určitých vodítek rozpoznat. Existuje několik jednoduchých technik, které se často využívají – shrnuli jsme je do **modelu dezinformačních principů nazvaného „FIRST“:**

- **Falešný obsah** – manipulování s obsahem, například padělané dokumenty nebo obrazové materiály upravené ve Photoshopu;
- **Identita** – skrývání zdroje nebo udávání nepravdivého zdroje, například falešné účty na sociálních sítích;
- **Rétorika** – využívání zaujatých nebo nepravdivých argumentů, například trollové provokující uživatele na diskuzním fóru;
- **Symbolika** – zneužívání komunikační hodnoty událostí, například u teroristických útoků; a
- **Technologie** – zneužívání technologické výhody, například internetoví boti automaticky pomáhající šíření zpráv.

Tyto techniky se často různými nepředvídatelnými a nejednoznačnými způsoby kombinují tak, aby byl jejich dopad co možná největší. Zároveň se v průběhu času vyvíjejí, zejména s tím, jak se objevují stále nové a nové technologie. Vzhledem k proměnlivé povaze dezinformací je důležitější pochopit tyto nejrozšířenější/výchozí techniky spíše než hledat nějaký ustálený typ dezinformací.

Příklady:

25 tisíc lidí proti EU

V listopadu 2017 informovala česká verze ruského státního portálu Sputnik o tom, že na demonstraci proti „korekci“ pomníku maršála Koněva na Praze 6 se sešlo „přes 100 tisíc obyvatel českého hlavního města a řada známých politiků“. Podle informací Policie České republiky i nezávislých novinářů však na místě bylo přítomno pouze 100 účastníků. V podobném duchu se nesla zpráva z dubna 2019, kterou zveřejnila televizní stanice ruského ministerstva obrany TV Zvezda. Podle té „v Praze vyšlo protestovat proti EU 25 tisíc lidí“, přičemž podle informací Policie České republiky bylo na místě přibližně 600 osob.
CTHH dementuje zprávu Sputnik, CTHH dementuje zprávu TV Zvezda

Heart of Texas

Během amerických prezidentských voleb v roce 2016 se objevila řada falešných účtů, falešných stránek na sociálních sítích a různých podvodníků, pomocí kterých se manipulovalo s politicky angažovanými uživateli sociálních sítí. Jedna z těchto stránek se jmenovala „Heart of Texas“ (srdce Texasu) a spravoval ji falešný účet, který patřil společnosti Internet Research Agency (Agentura pro výzkum internetu) z Petrohradu. Tato stránka se zaměřovala na diskuze o různých tématech souvisejících s migrací, přičemž k oslovení příjemců využívala symboliku, rétoriku a falešnou identitu. Podařilo se jí získat na 350000 příznivců. Kromě toho bylo identifikováno více než 40 uzavřených Facebookových skupin, které spadaly do stejné vlivové operace.
Robert S. Mueller, „Indictment Case 1:18-Cr-00032-DLF United States of America v. Internet Research Agency“

„Pryč z EU“

Koncem března 2019 byl Centrem nezávislosti České republiky zveřejněn dokument s názvem „Pryč z EU“. O filmu, který nabízí jednostranný a zkreslený pohled na EU, informovala především alternativní média. Informace o něm se šířily také prostřednictvím řetězových e-mailů, které tvrdily, že EU zakázala promítání i vysílání dokumentu.
Manipulátoři, HOAX: Brusel cenzuruje už i dokumentární film a analýza dokumentárního filmu Pryč z EU

Útok migrantů na Evropanku

V roce 2016 kamery před pražským policejním prezidiem zachytily napadení a oloupení mladé dívky několika mladíky. Útok následoval po hádce související s distribucí drog. Video se začalo virálně šířit po sociálních sítích, protiislámská facebooková stránka však záznam vytrhla z kontextu a popsala ho jako útok muslimských imigrantů na Evropanku a pokus o její znásilnění. Příspěvek byl ze stránky posléze stažen, ale než se tak stalo, video viděl téměř milion lidí a další tisíce ho sdílely. Přestože s muslimy případ neměl nic společného, objevoval se v tomto kontextu na sociálních sítích ještě o tři roky později.
HATEFREE, HOAX: České video napadení dívky muslimy

Cíle dezinformací

Dezinformace slouží především k šíření vlivu. Lidé se neustále snaží ovlivňovat druhé – například reklamní průmysl a další obory založené na vztazích s veřejností využívají každý den stovky malých triků, aby ovlivnily naše chování. Dezinformace nás mají ovlivňovat tím, že pomocí nepravdy pomáhají k dosažení určitého cíle.

Subjekty, které je šíří, se nám snaží zabránit v informovaném a soudném rozhodování. Pokoušejí se dosáhnout určitého cíle tím, že úmyslně obcházejí standardní rozhodovací procesy. Lžou, aby nás přiměli myslet nebo jednat určitým způsobem. Důvodů je mnoho, přičemž jejich závažnost může být různá. Níže uvádíme pět nejrozšířenějších.

1. **Ekonomické:** cílem dezinformační činnosti je finanční zisk. Například tzv. clickbaity pomáhají zajistit co nejvíce „kliknutí“. Dosahují toho pomocí titulku, multimediálního obsahu nebo jiných signálů, které uživatele falešně nalákají k návštěvě určité webové stránky. Drobné za zobrazení reklamy se pak mohou proměnit v tisícové částky, pokud se příběh začne virálně šířit. V podobných případech je cíl čistě ekonomický. Tyto webové stránky však mohou ukrývat malware nebo jiné formy sledovacího softwaru používaného ke kriminální činnosti a také mohou mít sekundární politické dopady v souvislosti s obsahem článků, které zneužívají aktuální rozpory ve veřejném mínění.

Příklad: skupina podnikatelů vytvoří v předvolebním období kontroverzní články s clickbaitovými titulky. Ty však neodkazují na skutečné články, ale spíše na stránky s reklamním obsahem, které se automaticky pokoušejí instalovat malware.

2. **Protože můžu:** cílem dezinformační činnosti je provést něco obtížného nebo troufalého. Podobné jednání vychází z „hackerské“ nebo „hráčské“ mentality, která předpokládá, že systémy je třeba „přehrát“ nebo nějak technologicky vytěžit. Důležitý je primárně rozsah výzvy, osobní prospěch a získání respektu ostatních za své schopnosti. Mezi sekundární následky pak může patřit nabourání se do kritických systémů, únik důvěrných materiálů, zneužití algoritmů či jiných digitálních systémů a také neetické používání uživatelských dat k lepšímu zacílení dezinformací, například u reklam viditelných pouze vybraným uživatelům.

Příklad: programátor se nechá vyprovokovat jiným členem online komunity, aby zmanipuloval výsledky Twitterové ankety, ve které uživatelé vybírají nejoblíbenější celebritu.

3. **Diskreditace:** cílem šíření dezinformací je negativně ovlivnit důvěryhodnost, spolehlivost a pověst. Strůjci dezinformací zacílí na určitou osobu nebo organizaci a pomocí lží se ji snaží poškodit. Zjevná oběť útoku však nemusí nutně představovat hlavní cíl dezinformací – tím může být například izolace zranitelné skupiny příjemců, která je závislá na službách určité organizace, pomocí diskreditace této organizace. Diskreditování patří k nejčastějším účelům dezinformační činnosti a dobře doplňuje ostatní cíle, jako je například polarizace a informační vlivové operace.

Příklad: někdo padělá dokumenty, které diskreditují vedení České televize. Do diskuze v digitálním prostoru se infiltruje narativ naznačující, že Česká televize je nedůvěryhodná, a publikum se přesouvá na nedůvěryhodné kvazimediální portály.

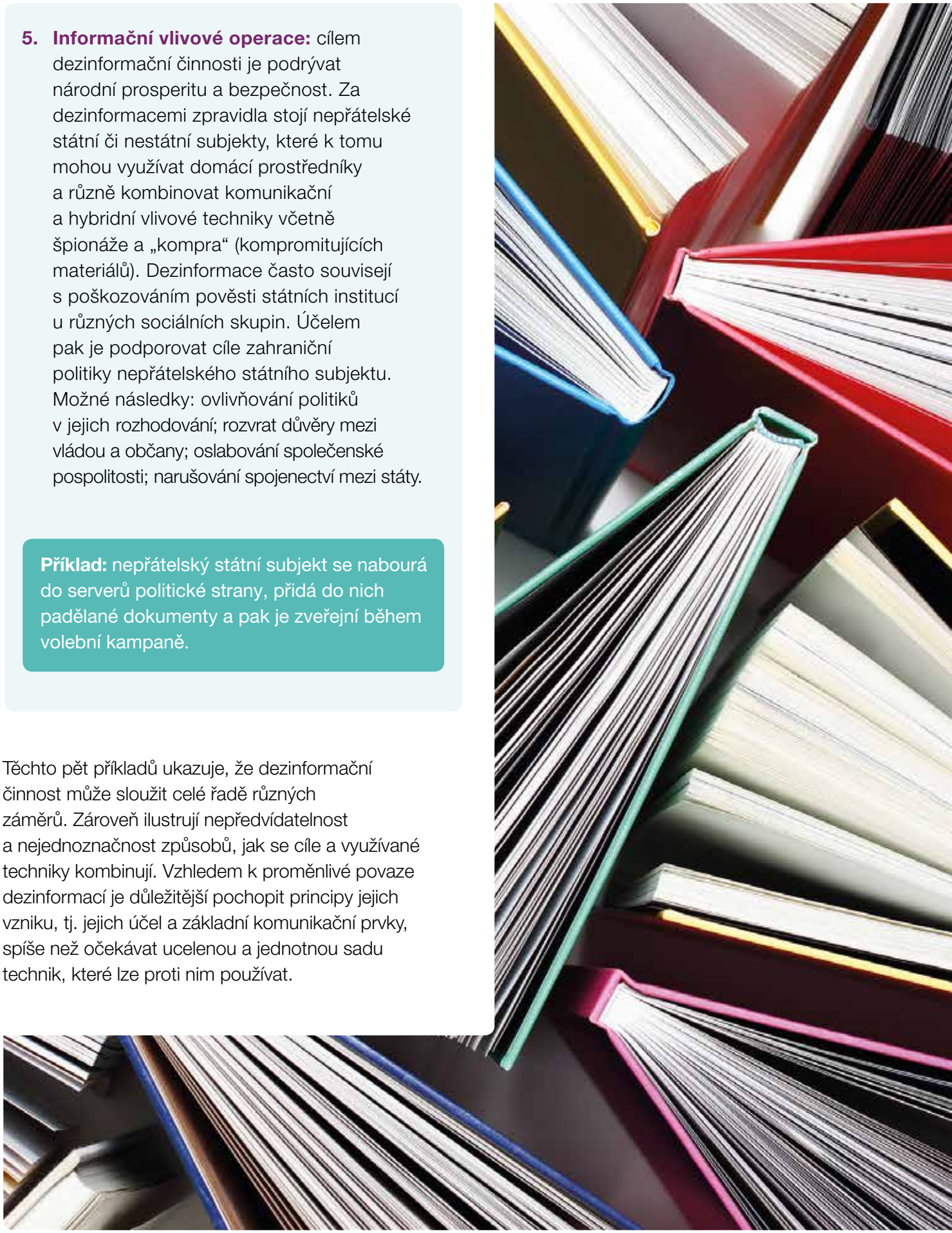
4. **Polarizace:** cílem dezinformační činnosti je zhoršovat stávající rozpory tím, že je ještě prohloubí. Šiřitelé dezinformací k tomu využívají stávající diskuzi, do které infiltrují určitý podvodný obsah s cílem vyprovokovat reakci obou táborů a tím omezovat prostor pro umírněný kompromis. Účely jsou obvykle politické nebo společenské. Možné následky: poškození pověsti či důvěryhodnosti; časté hádky namísto konstruktivního dialogu, například vyvolávané online trolly; intenzivnější polarizace politické debaty, například rozdmýcháváním citlivých otázek typu migrace; provokace s dopady na veřejné zdraví, například ze strany hnutí proti očkování; podněcování k násilí.

Příklad: komentáře k reportáži o úmrtích způsobených chřipkou zahltí skupina lidí, která lživě tvrdí, že úmrtí způsobila vakcína proti chřipce, a zároveň píše komentáře napadající rodiče neočkovaných dětí. Prostor pro umírněnou, konstruktivní diskuzi je tak minimální.

5. **Informační vlivové operace:** cílem dezinformační činnosti je podrývat národní prosperitu a bezpečnost. Za dezinformacemi zpravidla stojí nepřátelské státní či nestátní subjekty, které k tomu mohou využívat domácí prostředníky a různě kombinovat komunikační a hybridní vlivové techniky včetně špionáže a „kompra“ (kompromitujících materiálů). Dezinformace často souvisejí s poškozováním pověsti státních institucí u různých sociálních skupin. Účelem pak je podporovat cíle zahraniční politiky nepřátelského státního subjektu. Možné následky: ovlivňování politiků v jejich rozhodování; rozvrat důvěry mezi vládou a občany; oslabování společenské pospolitosti; narušování spojenectví mezi státy.

Příklad: nepřátelský státní subjekt se naboural do serverů politické strany, přidá do nich padělané dokumenty a pak je zveřejní během volební kampaně.

Těchto pět příkladů ukazuje, že dezinformační činnost může sloužit celé řadě různých záměrů. Zároveň ilustrují nepředvídatelnost a nejednoznačnost způsobů, jak se cíle a využívané techniky kombinují. Vzhledem k proměnlivé povaze dezinformací je důležitější pochopit principy jejich vzniku, tj. jejich účel a základní komunikační prvky, spíše než očekávat ucelenou a jednotnou sadu technik, které lze proti nim používat.



Zvyšování dopadu

Pochopení cílů dezinformační činnosti a jejích hlavních technik představuje důležitý krok, ale celý problém je mnohem komplexnější. Tyto cíle a komunikační techniky se zpravidla různě kombinují, aby jejich původci dosáhli co možná největšího komunikačního dopadu.

Dezinformační techniky lze používat tak, aby se navzájem doplňovaly a dohromady vytvořily komplexní „finty“ či „manévry“, které podporují konkrétní cíle. Původci mohou využívat celou škálu různých dezinformačních technik, s jejichž pomocí sestavují složité operace.

Rozčílený maňásek (sockpuppet)

1. Najděte společenské téma, které je citlivé nebo v sobě nese určitou symbolickou hodnotu (symboly).
2. Založte si dva nebo více účtů na sociálních sítích pod falešnou identitou (maňásek).
3. Vypracujte falešný provokativní obsah, který se týká zvoleného tématu (falešný obsah).
4. Zveřejněte tento obsah prostřednictvím jednoho z účtů a následně jej kritizujte prostřednictvím těch ostatních (rétorika).
5. Použijte internetové boty k rozšíření falešného obsahu mezi oba názorové tábory (internetoví boti).

Potenciální dopady: polarizace debaty, vyvolání zmatku, podrytí legitimních stanovisek, zasetí konfliktu.

Alternativní narativ

1. Formulujte narativ, který podporuje váš cíl.
2. Připravte dezinformace, které podporují váš narativ – například falešné zprávy, příspěvky na blogu, reklamy (falešný obsah).
3. Publikujte dezinformace prostřednictvím vlastních kanálů nebo alternativních webových stránek (sociální bublina).
4. Zapojte kontroverzní blogery/komentátory, čímž se narativ „potvrdí“ a rozšíří dál (zmanipulované autorství).
5. Využijte trolling k útoku na uživatele, kteří argumentují proti vašemu narativu (rétorika).

Potenciální dopady: odvedení pozornosti od skutečných problémů, podrytí legitimních stanovisek, vytlačení legitimních narativů.

Zmanipulovaný únik informací

1. Získejte přístup k interním dokumentům a e-mailům cílové organizace pomocí kybernetických útoků (například cílený phishing).
2. Připravte padělané dokumenty, které obsahují diskreditující informace a které se stylově i formálně podobají získaným dokumentům (falešný obsah).
3. Přidejte do uniklých materiálů padělané dokumenty.
4. Zajistěte šíření „zmanipulovaného úniku“ prostřednictvím zavedených kanálů (například Wikileaks), abyste získali pozornost uznávaných médií.
5. Zesilujte negativní mediální pokrytí pomocí internetových botů a trollů (internetoví boti a rétorika).

Potenciální dopady: diskreditace a/nebo falešné obvinění osoby nebo instituce, podrývání důvěry, vyvolání zmatku.

Zacílení na základě velkých dat (tzv. big data)

1. Proveďte analýzu cílových příjemců mezi velmi angažovanými skupinami na sociálních sítích a identifikujte psychografické spouštěče, které souvisejí s klíčovými tématy (symbolika).
2. Založte na sociálních sítích uzavřené skupiny koncipované tak, aby oslovily konkrétní cílové příjemce (sociální bublina).
3. Naverbujte do těchto uzavřených skupin cílové příjemce tím, že se budete vydávat za legitimní organizaci nebo hnutí (tzv. astroturfing).
4. Šiřte v těchto skupinách dezinformace ve formě falešných zpravodajských článků a memů (rétorika a symbolika).
5. Podněcujte cílové příjemce k akci – mohou například pomoci s šířením dezinformací nebo své názory projevovat na veřejnosti (agitace).

Potenciální dopady: polarizace debaty, změna chování, podrývání důvěry.

Zmanipulovaná citace

1. Najděte vhodnou citaci osobnosti, kterou si přejete poškodit.
2. Publikujte článek, ve kterém tuto citaci využijete vytrženou z kontextu v rámci určitého tématu tak, aby se hodila do vašeho preferovaného narativu (zmanipulované autorství).
3. Uveďte zdroje, které citaci zmiňují, a to napříč různými zpravodajskými platformami a jazyky.
4. Sdílejte svůj zmanipulovaný článek pomocí různých aktérů a platforem, pokaždé s drobnými obměnami v textu.
5. Odkazujte na tyto prostředníky jako na zdroje zmanipulovaného tvrzení, které jste tímto způsobem „vyprali“, aby působilo legitimně

Potenciální dopady: zastření pravdy, legitimizace falešných tvrzení, podrývání důvěry.

Roztleskávání (cheerleading)

1. 1Identifikujte odlišné názory na téma, které má nějaký dopad na oblast vašeho zájmu (rétorika, symbolika).
2. Zaplavte informační prostor pozitivním obsahem (cheerleading) prostřednictvím internetových botů a trollů.
3. Pomocí pozitivních komentářů a příspěvků zajistěte vytlačení odlišných názorů.
4. Vytvořte online skupiny, které podporují vaše stanovisko (filtrová bublina).
5. Udržujte si početnou armádu přispěvatelů (internetových botů a trollů), kteří jsou připraveni zapojit se do jakékoli diskuze (rétorika).

Potenciální dopady: umlčení odlišných názorů, zahlcení informačního prostoru, změna narativu.

Včasné varování

Co je třeba udělat

Osvojte si analytické dovednosti potřebné k monitoringu online prostředí. Zaměřte se na strategie k identifikaci témat, příjemců a zainteresovaných subjektů (tzv. influencerů), kteří jsou zásadní pro práci vaší organizace, a vypracujte postupy pro přípravu a obranu proti dezinformacím.

V současné době již pravděpodobně provádíte monitoring médií, ať už těch tradičních, nebo digitálních. To znamená, že máte nějaké základní znalosti o svých klíčových příjemcích i zainteresovaných subjektech a také povědomí o veřejných diskuzích, které se týkají vašich prioritních svěřených oblastí. Nyní potřebujete tuto práci zaměřit konkrétně na odhalování dezinformací.

První krok spočívá ve sladění vašich zájmů a priorit s vašimi monitorovacími potřebami. Zpracování tabulky níže vám pomůže nasměrovat váš digitální monitoring na témata, která jsou nejnáchylnější k dezinformacím. Můžete ji využít například k vyhodnocení těch nejzásadnějších témat za daný rok, případně pro plánování kampaně. Nejdůležitějším přínosem je, že začnete mapovat rizika a získáte vodítko pro mediální/online monitoring.

	Priority	Postoje	Původci dezinformací	Narativní rizika	Nejhorší scénář
Cíle v dané oblasti	Jaké jsou vaše prioritní svěřené oblasti a cíle?	Jaké jsou v těchto oblastech převládající postoje, které by mohly být zneužity k šíření dezinformací?	Které skupiny ohrožují vaše cíle dezinformacemi?	Které aspekty vašich narativů jsou zranitelné vůči dezinformacím?	Jaké jsou nejhorší možné scénáře či rizika v případě, že se dezinformace začnou šířit?
Příjemci	Kdo jsou klíčoví influenceři a příjemci, kteří nějak ovlivňují vám svěřené oblasti?	Jaké jsou převládající postoje vůči vaší organizaci nebo vašim cílům, které by mohly být zneužity k šíření dezinformací?	Kteří klíčoví aktéři/influenceři šíří nebo se zapojují do šíření dezinformací?		

Monitoring digitálních médií vám umožní získat **základní** povědomí o tom, jak jsou vaše prioritní svěřené oblasti v rámci těchto médií vnímány, ze strany zainteresovaných subjektů a také mezi různými skupinami příjemců. Rozsah úsilí vynaloženého k digitálnímu monitoringu samozřejmě závisí především na dostupných zdrojích. Naštěstí máte k dispozici rozsáhlé portfolio podpůrných nástrojů.

Měli byste si vybrat různorodé nástroje, ze kterých si sestavíte vlastní **sadu** či **panel nástrojů** na míru vašim konkrétním potřebám. Níže uvádíme několik zdrojů, které máte jako komunikátor k dispozici:

- **Hootsuite**
  Nástroj k monitorování sociálních sítí, který vyhledává konkrétní termíny v reálném čase – umožní vám sledovat zmínky o vaší značce, produktech nebo relevantních klíčových slovech, které vás zajímají. Dostupný na webových stránkách hootsuite.com.

- **Tweetdeck**
  Nástroj nabízející přehledový panel na Twitteru, ve kterém můžete sledovat více timelinů, účtů a vyhledávaných termínů v reálném čase. Dostupný na webových stránkách tweetdeck.twitter.com.

- **Buzzsumo**
  Nástroj pro rozbor sociálních sítí, který umožňuje efektivní rozbory obsahu na základě různých metrik, jako jsou například sdílení a zmínky, napříč všemi sociálními sítěmi. Dostupný na webových stránkách buzzsumo.com.

Seznam dalších nástrojů je k dispozici v kompletní příručce GCS RESIST.

Možné signály šíření dezinformací

- ✓ Přítomnost zjevně falešných účtů, případně velký počet anonymních účtů.
- ✓ Náhlý nárůst aktivity, známky koordinovaného neautentického chování.
- ✓ Odkazování na nedůvěryhodné zdroje informací.
- ✓ Opakování stejných nebo podobných zpráv napříč různými účty.
- ✓ Posílání příspěvků ve více jazycích, které působí jako výstup z automatického překladače.
- ✓ Posílání příspěvků v nestandardních časech.

První dva kroky vám pomohou sestavit soubor nástrojů a materiálů s informacemi o vašich svěřených oblastech, zainteresovaných subjektech a cílovém publiku. Tyto činnosti jsou samy o sobě užitečným cvičením, ovšem hlavní zaměření této práce spočívá v dezinformacích. V předchozí kapitole jste si přečetli, že cíle dezinformační činnosti mohou být různé, včetně ekonomického prospěchu, přehrání systému, diskreditace, polarizace a vlivových operací. Výstupy z předchozích kroků vám pomohou vybudovat pomyslnou síť, která zachytí stěžejní veřejné postoje vůči vašim prioritním svěřeným oblastem. Dalším krokem je analyzovat získaná data podrobněji a hledat v nich ukazatele signalizující:

- skupiny, které pravděpodobně mají zájem na sdílení dezinformací; a
- citlivá místa v rámci diskuzí/témat/narativů, která by mohla být potenciálně zneužita k dezinformační činnosti.

Hledejte příklady komunikace, která staví na dezinformačních principech shrnutých v modelu FIRST: falešný obsah, identita, rétorika, symbolika a technologie. Existují nějaké náznaky toho, že zde operují zájmové skupiny, které se pokoušejí tyto techniky využívat? Existuje ve vašem cílovém publiku potenciální odbytiště pro dezinformace? I když žádné varovné signály nevidíte, je v každém případě užitečné zvážit potenciální rizika, kterých by se dezinformátoři mohli snažit zneužít, a také nejhorší možné scénáře toho, čeho by šíření dezinformací mohlo dosáhnout. Výstupy lze využít jak pro dlouhodobé plánování, tak pro týdenní plánování nebo plánování konkrétní kampaně.

Rozbor situace

Osvojte si základní dovednosti potřebné k vytváření analýz, jejichž výstupy lze sdílet s ostatními a na jejichž základě lze následně vypracovat konkrétní opatření.

Monitoring se stává přínosným ve chvíli, kdy se promění v **rozbor**. Jedná se o typ analýzy, který proměňuje **zajímavá data v data, na jejichž základě lze vypracovat konkrétní opatření**. Odpovídá tedy na otázku: „Co s tím?“ Účelem výstupu z rozboru dezinformací je sdílet signály včasného varování, které jste shromáždili v rámci monitoringu digitálních médií – například s politickými týmy, které potřebují briefing k aktuální situaci. Rozbor se zpravidla realizuje ve formě zpráv, které se rozesílají denně, týdně, nebo ad hoc dle potřeby. Značnou část dat lze získat automaticky z monitorovacích nástrojů nebo přehledového panelu, které jsme popsali v předchozí kapitole.

Zahraniční mediální pokrytí případu otravy v Salisbury

Týden po otravě v Salisbury se v ruských domácích médiích, prostřednictvím oficiálních vládních vyjádření a také v digitálních médiích, objevilo tucet „alternativních“ narativů. K nasazení a následnému rozšíření těchto narativů byla využita kombinace dezinformačních technik včetně rétoriky a symboliky. O měsíc později již existovalo více než 30 narativů, které do informačního prostoru nasadily převážně ruské zdroje a které sdílela řada různých vlivných subjektů. Výchozí bod při zpracování rozboru této situace by spočíval v popsání různých narativů předkládaných zahraničními médii, vysvětlení toho, jak rezonují mezi různými příjemci, a vyhodnocení, zda jsou narativy součástí nějakého opakujícího se vzorce, nebo se jedná o jednorázovou záležitost. Na základě těchto informací lze formulovat určitá počáteční doporučení ohledně možné reakce.

DFRLab (2018) „Skripal Poisoning: If not Russia, Then…“

Kvalitní zpráva shrnující výsledky rozboru může mít pouze jednu či dvě stránky: **na začátek soustřeďte ty nejdůležitější informace a rychle se propracujte k části, která odpovídá na otázku: „Co s tím?“** Nezapomínejte, že váš výstup z provedeného rozboru může být pro některé kolegy z vaší organizace vůbec prvním setkáním s daty získanými z digitálního monitoringu, která slouží jako základ pro analýzu dezinformací. Měl by být použitelný jako briefing pro politické funkcionáře, poradce a vyslance, proto doporučujeme vyhnout se žargonu a používat dostatek obrazových materiálů, pomocí kterých objasníte vývojové tendence a rozložíte složitější jevy na jednotlivé, lépe pochopitelné součásti.

Výstup z rozboru dezinformací by měl obsahovat alespoň tyto informace:

- klíčové rozbory a poznatky: základní shrnutí včetně stručného komentáře, který vysvětluje „co s tím?“ a obsahuje vaše doporučení pro případná opatření;
- sekce o klíčových tématech a záležitostech, které obsahují:
  - relevantní výstupy z vašeho oddělení ohledně prioritních záležitostí, například vyjádření ministra;
  - příklady dezinformací souvisejících s těmito výstupy, včetně podrobností o tom, kde a jak se šíří;
  - klíčové interakce a práce s dezinformacemi;
  - vývojové tendence a změny v postojích v průběhu času; zde můžete využít také případná data z průzkumů, které máte k dispozici;
  - váš komentář a doporučení pro vhodnou reakci.

Šablona pro výstup z rozboru dezinformací	
Klíčové rozbory	Shrnutí tří hlavních bodů, které by zainteresované strany měly vědět, včetně případných doporučení k akci.
Shrnutí události	Stručné vysvětlení celé záležitosti.
Dezinformační narativy	Identifikace každého nepravdivého narativu, včetně uvedení zdroje a data.
Příklady dezinformací	Jakýkoli vizuální materiál, např. snímky klíčových příspěvků na Twitteru, případně jiné podklady, např. citace z tiskových prohlášení.
Další relevantní poznatky	Cokoli dalšího, co je pro danou záležitost relevantní.
Vývoj v čase	Zda/jak se dezinformace mění a stručná analýza toho, jak se mění.
Doporučení	Doporučení pro reakci a nastínění navrhované strategie.

Analýza dopadů

Vypracujte rozhodovací proces na základě jednotné metodologie pro posuzování rizika a priority odhalené dezinformační činnosti. Analýza by měla být adaptabilní a přizpůsobit se složitosti a závažnosti případu.

Jakmile odhalíte dezinformace, které se týkají vaší práce, je třeba posoudit jejich pravděpodobné cíle, dopady a dosah. Můžete tak učinit například zodpovězením série otázek, které vám poskytnou vodítko při rozhodování, zda zareagovat.

Vzhledem k nejistotě, která dezinformační činnost provází, bývá posuzování jejích dopadů poměrně obtížné. V rámci komunikační práce je proto vyhodnocování rizik a dopadů často výsledkem zkušeností a kvalifikované intuice. Pokud však máme bojovat s dezinformační činností uceleným a jednotným způsobem napříč všemi vládními orgány a institucemi, potřebujeme využívat společný přístup a provádět podobná vyhodnocení. Je například velmi užitečné vyjadřovat riziko z hlediska pravděpodobnosti, že něco nastane. Při zodpovídání otázek uvedených níže uvažujte v těchto stupních pravděpodobnosti:

Kvalitativní termín	Zkratka	Rozsah pravděpodobnosti
Velmi nepravděpodobné	VN	méně než 10 %
Nepravděpodobné	N	15 – 20 %
Realisticky pravděpodobné	RP	25 – 50 %
Pravděpodobné	P	55 – 70 %
Velmi pravděpodobné	VP	75 - 85 %
Téměř jisté	TJ	více než 90 %

Výstup z rozboru dezinformací by měl obsahovat alespoň tyto informace:

- Jaký je záměr šíření dezinformací?
- Jaké dezinformační techniky se využívají?
- Jaké jsou pozorovatelné dopady?
- Kdo z toho má prospěch?
- Pro koho je to nevýhodné?

Na základě předchozího monitorování a rozboru se zamyslete nad následujícími otázkami. K posouzení pravděpodobnosti svých hypotéz využijte stupnici nejistoty, pokud to bude nutné.

Tato analýza by vám měla pomoci posoudit pravděpodobné dopady šíření dezinformací. Vypracujte si svou vlastní tabulku a přizpůsobte ji svým hlavním otázkám.

Ovlivňují dezinformace schopnost vaší organizace dělat svou práci?	Ovlivňují dezinformace osoby, které jsou závislé na vašich službách?	Představují dezinformace závažné riziko pro širokou veřejnost?
Schopnost poskytovat služby	Klíčové zainteresované strany	Národní bezpečnost
Pověst/důvěryhodnost	Klíčoví příjemci	Bezpečnost veřejnosti
Svěřené oblasti/cíle	Specifické segmenty příjemců	Veřejné zdraví
Jednotliví pracovníci/bezpečnost pracovníků	Zranitelné skupiny příjemců	Atmosféra debaty

Dosah dezinformací

- **Malý zájem:** omezené šíření a rezonování mezi příjemci.
- **Sociální bublina:** určité rezonování mezi specifickými segmenty příjemců s podobným světonázorem a/nebo automatické šíření.
- **Trending:** určité šíření online, může zahrnovat otevřenou debatu a protiargumenty.
- **Méně významná zpráva:** určité pokrytí v mainstreamových médiích.
- **Titulní zpráva:** ovlivňuje každodenní provoz.

Měli byste také provést posouzení rizik z hlediska rozsahu, v jakém budou podle vás dezinformace u příjemců rezonovat. Je pravděpodobné, že během několika hodin zmizí, nebo má potenciál stát se zítřejší titulní zprávou?

Jakmile dokončíte všechny doporučené kroky, měli byste být schopni přidělit jednotlivým dezinformacím určitý stupeň priority. Je pravděpodobné, že se dané dezinformace stanou součástí zásadní celovládní krize? Nebo stačí pouze monitorovat vývoj situace? Základní princip spočívá v tom, že cíle, dopady a dosah dezinformací by měly ovlivnit urgenci a prioritu, které danému případu přidělíte.

	Popis	Opatření	Příjemci	Nástroje
vysoké	Dezinformace mají potenciál ovlivnit např. národní bezpečnost a je velmi pravděpodobné, že se z nich stane titulní zpráva. Vyžadují okamžitou pozornost a postoupení na vyšší úrovně.	Uvědomte o celé záležitosti a její prioritě vedení. Sdílejte rozbor a analýzu. Připravte se na koordinovanou vládní reakci.	- Vedení - Odborní referenti pro daný úsek	- Sdílení rozboru - Briefingy - Prioritu má krátkodobá komunikace
Střední	Dezinformace mají potenciál negativně ovlivnit svěřenou oblast, pověst celého úseku nebo určitou významnou zainteresovanou skupinu a získaly značnou popularitu online. Vyžadují reakci.	Uvědomte o celé záležitosti vedení. Sdílejte rozbor a analýzu mezi relevantními kolegy. Záležitost prošetřete a připravte vyjádření pro média založené na známých skutečnostech.	- Odborní referenti pro tvorbu politiky - Odborní referenti pro daný úsek	- Rozbor - Briefingy - Vyjádření pro tisk - Prioritu má krátkodobá a střednědobá komunikace
Nízké	Dezinformace mají potenciál ovlivnit atmosféru debaty a šíří se pouze v omezeném rozsahu. Debata by se měla standardním způsobem sledovat, ale není nezbytné / žádoucí zakročit.	Sdílejte rozbor a analýzu, pokud je to v dané situaci vhodné. Záležitost prošetřete a připravte vyjádření pro tisk / narativy založené na známých skutečnostech. Proveďte základní analýzu debaty a sledujte případné změny.	- Odborní referenti pro komunikaci, odborní referenti pro tvorbu politiky	- Rozbor - Vyjádření pro tisk - Základní analýza - Prioritu má střednědobá a dlouhodobá komunikace

Strategická komunikace

Na základě pravděpodobného rizika a dopadů dezinformační činnosti vyhodnoťte komunikační možnosti – k dispozici jich máte celou řadu od ignorování dezinformace až po vypracování kampaňové strategie.

Nyní můžete přistoupit ke zvážení možných komunikačních reakcí. Během přípravy každé reakce byste vždy měli dodržovat určité klíčové principy vládní komunikace, například styl reakce, schvalovací proces či strategii reakce. Doporučujeme také zvážit vypracování obsahu v různých časových horizontech, například krátkodobé/reaktivní možnosti, střednědobé/proaktivní možnosti a dlouhodobé/strategické možnosti.

Ne všechny dezinformace vyžadují reakci.
V mnoha případech se veřejné mínění samo napraví. Jakákoli veřejná reakce na dezinformace, pro kterou se nakonec rozhodnete, by v každém případě měla prezentovat **pravdu, a to dobře sdělenou.**

Proti-značka, nikoli proti-narativ

Boj proti jednotlivým narativům nemusí být příliš efektivní a v mnoha případech nepravdivé informace naopak rozšíří či utvrdí. Zpravidla platí, že první dojem vydrží nejdéle, a ve všudypřítomném zahlcování informacemi se lidé při určování důvěryhodnosti sdělení často uchylují ke zkratkám – známá témata či sdělení mohou být lákavá, přestože jsou nepravdivá.

To znamená, že potřebujete propracovanější a strategičtější přístup, než je pouhé vyvracení nepravdivých informací. Měli byste vypracovat a dodržovat přesvědčivý, sdílený narativ tak, aby veškerá komunikace probíhala uceleně, v kontrastu s potenciální rozmanitostí dezinformačních narativů. Bojujte proti **záměru,** nikoli pouze proti sdělení.

Přesnost a dodržování základních hodnot

Komunikace státní správy musí ztělesňovat hodnoty, které vyznává: např. pravdivost, otevřenost, spravedlivost a přesnost. Jedině taková komunikace vám umožní vybudovat a udržet si důvěru vašich příjemců.

Aktuálnost

V boji proti dezinformacím je klíčová rychlost a obratnost vaší reakce. To může znamenat například práci v kratších lhůtách, než je obvyklé, nebo vypracování závazných postupů pro reakci, které vyvažují potřebu rychlého jednání s nutností formálního schválení ze strany vedení a ministrů. Stejně tak to ale může znamenat vyčkávání, například při čekání na zveřejnění více informací.

Progresivnost

Dezinformační narativy často dosahují kýženého dopadu, protože dané téma podávají jako senzaci a dokážou okamžitě upoutat pozornost. Pokud s nimi mají vaše komunikační opatření soupeřit, musejí být dostatečně progresivní a zajímavá. Vždy je samozřejmě nutné dodržovat principy uvedené výše – zároveň byste však měli zvážit, kdy je výhodné odchýlit se od obvyklých vládních reakcí podle šablony a vypracovat vlastní přístup nebo narativ, který v zahlceném informačním prostoru zaujme.

Spolupráce se spřátelenými vlivnými subjekty

Kdo by byl nejdůvěryhodnější tváří vaší reakce? Externí aktéři mohou hrát nedocenitelnou roli při oslovování skeptických příjemců, zejména pokud jsou považováni za hodnověrný zdroj informací.

Příklady:

Counter-brand: reakce vlády Spojeného království na otravu v Salisbury
Kauza otravy v Salisbury zůstává předmětem celé řady dezinformací. Namísto řešení jednotlivých dezinformačních narativů premiérka zdůraznila, že existují pokusy „zakrýt pravdu šířením záplavy dezinformací". Toto stanovisko tvoří základ sdíleného britského narativu o dezinformacích týkajících se případu otravy a zároveň předchází neproduktivní diskuzi ohledně každého jednotlivého nepravdivého příběhu, který se v tisku objevil.

Přesnost a dodržování základních hodnot: stanovisko českého ministerstva zahraničních věcí ke zřízení spolku samozvané Doněcké lidové republiky v Ostravě
V červnu 2016 byl u Krajského soudu v Ostravě registrován spolek „Zastupitelské centrum DLR, z.s.", který dne 1. září otevřel v Ostravě „konzulát" a jmenoval předsedkyni spolku, Nelu Liskovou, „honorární konzulkou DLR v ČR". Ministerstvo zahraničních věcí reagovalo již 28. srpna 2016 vyjádřením, v němž jednoznačně odmítlo, že by DLR mohla mít v ČR diplomatickou misi či konzulární úřad vzhledem k tomu, že není státem, ČR ji za stát neuznává a nemá s ní tak navázány diplomatické styky. Podalo návrh soudu na zrušení tohoto spolku, který byl následně zrušen.

Stanovisko MZV ke zřízení spolku samozvané DLR v Ostravě

Aktuálnost: reakce londýnské metropolitní policie na útok na mostě Westminister Bridge v roce 2017
Bezprostředně po teroristickém útoku na mostě Westminister Bridge v roce 2017 zveřejnila metropolitní policie aktuální informace na svém Twitterovém účtu, přičemž první příspěvek publikovala pouhých sedm minut po útoku. Obsahoval přesné informace o právě probíhající situaci, avšak vycházel z šablony předschválené pro podobné scénáře, která vznikla v rámci vývoje strategické komunikace policie.

Progresivnost: Macronova reakce na únik e-mailových zpráv
Když prezidentská kampaň tehdy ještě kandidáta Emanuela Macrona čelila zveřejnění 9 gigabytů uniklých e-mailových zpráv, pracovníci kampaně úspěšně obnovili svou kontrolu nad narativem vydáním stanoviska, že oni sami do archivu zpráv umístili řadu falešných dokumentů. Tento progresivní přístup, se kterým hackeři nepočítali, umožnil pracovníkům kampaně opět převzít iniciativu.
The Daily Beast, „Did Macron outsmart campaign hackers?"

Spolupráce s partnery: Komunikační strategie mezinárodní koalice proti Islámskému státu
Teroristické komunity typu Islámského státu jsou ve své komunikační činnosti obratné, rychlé a proaktivní. Komunikační útvar koalice proti Islámskému státu a jeho partneři proto také museli přistoupit k obratné a rychlé komunikaci, aby získali v informačním prostředí výhodu.

Vzhledem k tomu, že komunikační útvar hned zpočátku vynaložil čas a zdroje na vybudování mezinárodní komunity všech zainteresovaných stran napříč jednotlivými vládami, získal si důvěru a hodnověrnost ke komunikaci jménem partnerů brzy po zformování koalice. Tento přístup jim umožnil odstranit překážky a zbytečné vrstvy procesu, které by mohly další komunikační úsilí ztěžovat.

Dále byste měli vypracovat schvalovací proces, upravený na míru vaší organizaci. Zvažte, kdo má obsah schvalovat, jak rychle lze schválení zajistit a zda je možné vytvořit předem schválené šablony, které odpovídají rizikům určeným během práce na včasném varování.

Jakmile dokončíte analýzu dopadů, budete mít určenou také prioritu dezinformací. To vám umožní zvolit vhodné komunikační nástroje, které následně můžete přizpůsobit relevantním cílovým skupinám. Obecně platí, že **čím vyšší priorita, tím více je třeba se zaměřit na krátkodobé reakce**, alespoň zpočátku. Nezapomeňte, že v závislosti na prioritě celé záležitosti může být nezbytná kombinace krátkodobých, střednědobých a dlouhodobých přístupů

Stručný návod na efektivní odhalování a vyvracení nepravdy

Při boji s dezinformacemi prostřednictvím komunikace z vaší strany potřebujete vědět, jak efektivně vypracovat sdělení, které uvede věci na pravou míru. Následující rady jsou převzaty z příručky The Debunking Handbook (Cook, Lewandowsky, 2012), která výborně doplňuje příručku RESIST.

1. Zaměřte se na fakta, nikoli na dezinformace.
2. Výslovně čtenáře upozorněte na nepravdy.
3. Nabídněte alternativní vysvětlení – nenechávejte pro čtenáře mezery v informacích.
4. Používejte obrazové materiály, grafiku a ilustrace, aby bylo sdělení pro čtenáře atraktivnější.

	Opatření	Cílové skupiny	Nástroje
Krátkodobá reaktivní komunikace	Dezinformační činnost vyžaduje okamžitou reakci. Využijte rychlou komunikaci, kterou dezinformace vyvrátíte, uvedete na pravou míru nebo potlačíte na základě doložených faktů.	- Tradiční média (novináři / redaktoři) - Zainteresované strany a influenceři - Platformy sociálních sítí - Klíčoví příjemci	- Prvotní prohlášení k nastalé situaci - Tiskové prohlášení - Vyjádření ministra - Briefing pro novináře - Otázky a odpovědi - Placená reklama - Optimalizace pro vyhledávače (SEO) - Odhalte původce s pomocí spřátelených influencerů
Střednědobá proaktivní komunikace	Dezinformační činnost vyžaduje promyšlenou reakci. Využijte kombinaci komunikačních nástrojů, abyste prosadili vlastní hodnoty / značku. Propojte proaktivní opatření s vaší běžnou, každodenní komunikaci a spolupracujte se zainteresovanými stranami / vlivnými subjekty na vybudování konsenzu ohledně vašeho stanoviska.	- Tradiční média (novináři / redaktoři) - Zainteresované strany a influenceři - Platformy sociálních sítí - Široká veřejnost	- Vypracování kampaně, narativu a značky - Práce s komunitou, podpora dialogu a zapojení lidí - Budujte vztahy se zainteresovanými stranami a vlivnými subjekty - Workshopy / školení
Dlouhodobá strategická komunikace	Dezinformační činnost vyžaduje ucelenou, průběžnou reakci orientovanou na postupnou změnu situace v dlouhodobějším horizontu. Vypracujte a prosazujte strategické narativy týkající se daného tématu, které vám umožní formovat informační prostor, podporovat své vlastní stanovisko a potlačovat ostatní (zvyšování prahu).	- Tradiční média (novináři / redaktoři) - Mladé, úspěšné osobnosti - Zainteresované strany a influenceři - Platformy sociálních sítí - Široká veřejnost	- Zapojení do kampaně, narativu a značky - Programové financování, např. pro participační obsah - Hledání talentů a podpora / vytváření influencerů - Budujte vztahy se zainteresovanými stranami a vlivnými subjekty - Workshopy / školení - Plánování pro krizové situace

Model OASIS

Veškeré plánované komunikační činnosti a kampaně vládních subjektů ve Spojeném království využívají model OASIS, který zajišťuje účinnou a efektivní komunikaci. Je výhodný v tom, že poskytuje ucelený rámec pro vládní komunikaci a zároveň umožňuje zasazení jednotlivých komunikačních činností do kontextu dlouhodobých kampaní a strategických narativů.

	OASIS	RESIST
Cíle	Na základě záměrů dané politiky určete, čeho má komunikační činnost dosáhnout. Vypracujte komunikační cíle, které jsou realizovatelné, měřitelné a orientované na výsledky spíše než na výstupy.	Zasaďte své cíle do kontextu získaných poznatků o daném případu šíření dezinformací (včasné varování, rozbor situace, analýza dopadů), abyste mohli formulovat jasné cíle související s požadovanými změnami v postojích a chování. Slaďte dezinformační cíle s obecnějšími cíli dané politiky.
Rozbor příjemců	Kdo je cílovým publikem kampaně a jak jej potřebujete ovlivnit, abyste dosáhli svých cílů? Jaké příležitosti/překážky v této souvislosti existují?	Díky analýzám prováděným v rámci včasného varování a rozboru situace získáte jasné informace o cílových příjemcích dezinformací. Na základě toho zacílíte své vlastní aktivity, i když nikoli nezbytně na stejné příjemce. Zvažte, jak dezinformace ovlivnily příjemce a jaké problémy to představuje pro vaši reakci.
Strategie/ nápady	Nastavte svůj přístup ve vztahu k pozici/sdělení; kanálům; partnerům/influencerům. Vypracujte komunikační plán včetně jeho přijetí z pohledu cílového publika a tento přístup otestujte, abyste mohli posoudit jeho efektivnost.	Úroveň reakce odvozená na základě analýzy dopadů by měla sloužit jako vodítko pro vaši strategii tím, že poskytne parametry potřebné reakce. Napoví vám, jak strukturovat komunikaci, aby se předešlo negativním dopadům.
Realizace	Určete, jak by se měla komunikace realizovat, a vypracujte jasný plán, ve kterém přidělíte zdroje a stanovíte harmonogram realizace.	Nástroje v rámci vaší zvolené úrovně reakce by měly posloužit jako základ pro úvahy o realizaci vašeho komunikačního plánu během rozhodování, jak přidělit zdroje a zajistit realizaci s pomocí navržených nástrojů.
Hodnocení / evaluace	V průběhu kampaně monitorujte výstupy, poznatky a výsledky a po jejím dokončení proveďte vyhodnocení, pomocí kterého zjistíte efektivnost vaší komunikační činnosti.	Bodování / hodnocení vaší plánované komunikace slouží rozdílnému účelu, než sledování výsledků modelu RESIST, jelikož se zaměřuje konkrétně na komunikační činnost spíše než na vaši reakci na dezinformace jako takovou.

Sledování výsledků

Vyhodnoťte kvalitu rozhodování i výsledky prováděných činností. Výstup z vyhodnocení zpracujte v běžném formátu, který lze sdílet a který umožňuje organizační rozvoj a vzdělávání.

V kontextu dezinformační činnosti spočívá sledování výsledků v těchto dvou aktivitách:

- dokumentování a sdílení dat o případech dezinformací a
- vyhodnocování dopadů vašich rozhodnutí a opatření.

Nezapomeňte, že byste se neměli snažit sledovat výsledky dezinformací, nýbrž efektivnost a relevantnost vašeho úsilí.

Jedině tak dokážete zajistit, aby protiopatření byla vždy přesně zacílená a odpovídala analýze i dlouhodobým cílům.

Pokud jste v průběhu identifikace a reakce na dezinformační činnost postupovali podle modelu RESIST, velká část dat je již zaznamenána v příslušné složce. Nyní je třeba tato data spárovat se závěry vyhodnocení, čímž získáte záznam o celém procesu.

Rozpoznání dezinformací

Vypracujte základní přehled dezinformačních technik využívaných při šíření dezinformací, včetně vizuálních příkladů.

- Co bylo cílem šíření dezinformací?
- Jaké dezinformační techniky byly využity?
- Jak se jednotlivé dezinformační techniky kombinovaly, aby se maximalizoval jejich dopad?

Včasné varování

Zvažte své přípravné práce a rozsah, v jakém vám pomohly řešit dezinformace.

- Je váš digitální monitoring dostatečně zaměřen na vaše priority?

Rozbor situace

Jakmile jste identifikovali dezinformace, zvažte, jak dobře vaše prvotní analýza a briefing k aktuální situaci pomohly vašemu týmu zajistit reakci.

- Byli jste schopni nabídnout kolegům přesný a včasný briefing?
- Byly některé z vašich předpokladů mylné? Z čeho vycházely?

Analýza dopadů

Zvažte své vyhodnocení pravděpodobných cílů, dopadů a dosahu dezinformací.

- Určili jste dezinformacím na základě jejich cílů, dopadů a dosahu správnou prioritu?

Strategická komunikace

Vypracujte přehled reakcí, které jste v rámci své komunikační činnosti uskutečnili, rozepsaný do jednotlivých opatření, cílových skupin a nástrojů.

Sledování výsledků

Shromážděte tyto informace do jedné složky, spolu s vaším vyhodnocením uskutečněných opatření.

- Jaké byly dopady vašeho úsilí řešit danou dezinformaci?
- Jaké poznatky a poučení tento případ přinesl?

Další zdroje

Úplné znění příručky RESIST k boji proti dezinformacím je k dispozici na webové stránce https://gcs.civilservice.gov.uk/guidance/resist-counter-disinformation-toolkit/.

O autorech

James Pamment je vedoucím Katedry strategické komunikace na Lundské univerzitě a hlavním analytikem Centra pro studium asymetrických hrozeb (CATS, Centre for Asymmetric Threats Studies) na švédské Univerzitě národní obrany. V týmu na Lundské univerzitě působí Henrik Twetman, Alicia Fjällhed, Howard Nothhaft a Emma Rönngren.

Překlad příručky a adaptaci na české prostředí zajistilo se souhlasem autorů Centrum proti terorismu a hybridním hrozbám Ministerstva vnitra.