Swedish Civil Contingencies Agency

Jak čelit informačním vlivovým aktivitám

Příručka pro komunikátory

Jak čelit informačním vlivovým aktivitám

Příručka pro komunikátory

Jak čelit informačním vlivovým aktivitám – Příručka pro komunikátory

Švédská agentura pro civilní pohotovost – Swedish Civil Contingencies Agency (MSB)

Do českého jazyka z angličtiny přeložilo se svolením Švédské agentury pro civilní pohotovost Centrum proti terorismu a hybridním hrozbám Ministerstva vnitra ČR.

Publikace je dostupná ve švédštině a angličtině
Att möta informationspåverkan – Handbok för kommunikatörer
Order. No: MSB1260 – Revised December 2018 ISBN: 978-91-7383-864-1
Countering information influence activities – A handbook for communicators
Order. No: MSB1263 – March 2019 ISBN: 978-91-7383-867-2
Layout: Advant

Obsah

Předmluva

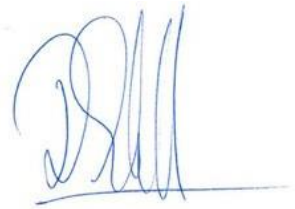
Zhoršující se úroveň bezpečnostního prostředí vyvolala potřebu švédských úřadů zaměřit se na shopnosti identifikace, pochopení a potírání informačních vlivových aktivit. Vlivové kampaně jsou stále sofistikovanější a mohou být využívány v rámci válečných konfliktů i v období míru. To má vliv na činnosti a role státních orgánů.

Informační vlivové aktivity mohou narušit fungování naší společnosti. Využívají zranitelných míst a zpochybňují základní hodnoty našeho způsobu života, jako jsou lidská práva, demokracie a právní řád, čímž v důsledku ohrožují životy a zdraví našich občanů. Zachování demokratického dialogu – právo na otevřenou diskusi, právo svobodně dospět k vlastním názorům a právo na svobodné vyjadřování – je zásadní pro položení pevných základů společenské odolnosti vůči informačním vlivovým operacím.

Švédská vláda je přesvědčena, že naši veřejní činitelé by měli být schopni identifikovat informační vlivové aktivity, odolávat jim a být schopni neutralizovat propagandistické kampaně. Švédská agentura pro civilní pohotovost (Swedish Civil Contingencies Agency) od roku 2014 aktivně pracuje na rozvoji schopností pro rozpoznávání, porozumění a potírání nepřátelských informačních vlivových kampaní. Ústředním prvkem v boji proti informačnímu vlivu je zvyšování povědomí veřejnosti.

Orgány odpovědné za národní bezpečnost vyjádřily potřebu vzniku příručky, která bude popisovat principy a metody identifikace, porozumění a boje proti informačním vlivovým aktivitám. Ve spolupráci s výzkumnými pracovníky na Lundské univerzitě proto Švédská agentura pro civilní pohotovost vytvořila tuto příručku, určenou především komunikátorům pracujícím ve veřejné správě. Měla by sloužit jako podpůrný materiál v situacích, kdy se organizace domnívá, že byla vystavena informační vlivové kampani nebo je takovým útokem potenciálně ohrožena.

Rád bych poděkoval pracovníkům Odboru strategické komunikace Lundské univerzity, jejichž výzkum se stal základem této příručky. Zvláštní poděkování také patří agenturám a organizacím, které přispěly k vylepšení příručky svou expertízou a cennými komentáři.



Dan Eliasson, generální ředitel

Úvod

Úvod

Vznik této příručky je reakcí na zhoršující se bezpečnostní situaci v současném světě. Nelegální anexe Krymu a konflikt na Ukrajině ukázaly, jak mohou dnešní bezpečnostní hrozby nabýt zcela odlišného charakteru, než jaký obvykle spojujeme s mezinárodním konfliktem. V tomto typu konfliktu jsou aktéry k dosažení cílů používány jiné než vojenské prostředky.

Tento nový typ bezpečnostní hrozby je nazýván vlivovou kampaní. Zahraniční mocnosti používají vlivové kampaně, aby využily slabin ve společnosti k dosažení svých cílů bez vojenské síly. Je zapotřebí se tomuto fenoménu bránit, abychom ochránili národní bezpečnost Švédska – včetně života a zdraví občanů, fungování společnosti a naší schopnosti zachovat základní hodnoty, jako jsou demokracie, právní řád, lidská práva a další základní svobody.

Švédská agentura pro civilní pohotovost definuje „vlivovou kampaň" jako soubor činností koordinovaných zahraniční mocností, který zahrnuje šíření zavádějících nebo nepřesných informací. Může se jednat také o další specificky přizpůsobené akce, zaměřené na ovlivňování rozhodování švédských politiků nebo jiných veřejných činitelů, působení na veřejné mínění části nebo celého švédského obyvatelstva, a dále i tlak na stanoviska či rozhodnutí jiných zemí, která by mohla nepříznivě ovlivnit suverenitu, bezpečnost nebo jiné zájmy Švédska.

Vlivová kampaň se skládá z řady vlivových činností, jednou z nichž je informační ovlivňování. Jako komunikátorovi vám tato příručka pomůže lépe si uvědomit, co to jsou informační vlivové operace, jak lze tento typ bezpečnostní hrozby identifikovat a jak mu následně čelit.

Působení prostřednictvím informačních vlivových aktivit není novým fenoménem. Každý den, na celém světě, využívají obory jako public relations či reklama cílené informace, za účelem ovlivnit osobní rozhodování lidí – tak aby kupovali konkrétní značku nebo podporovali určitého politického kandidáta. Jako občané očekáváme, že tato komunikace bude dodržovat určitá pravidla. Například, že komunikace bude probíhat otevřeně, bude založena na pravdivých a přesných informacích a celkově bude probíhat za podmínek, které nám umožní činit informovaná rozhodnutí.

Ne všichni aktéři však hrají dle těchto pravidel. Do oběhu mohou být cizími mocnostmi pokoutně vypouštěny klamné informace tak, aby podkopávaly základní demokratické procesy, kontrolovaly veřejný dialog a ovlivňovaly rozhodování. Takové procesy označujeme jako informační vlivové aktivity. Existuje řada případů z celého světa, v nichž byly takové vlivové aktivity identifikovány, například nedávné prezidentské volby v USA (2016) a ve Francii (2017). Přestože se jedná o akty agrese, nejsou považovány za akty válečné, i když někdy jsou situovány do šedé zóny mezi válkou a mírem. Informační vlivové aktivity by měly být považovány za nepřátelské projevy, jelikož podkopávají důvěru veřejnosti v důležité instituce, izolují zranitelné komunity a přispívají ke společenské a politické polarizaci.

Naše společnost je založena na důvěře. Na důvěře veřejnosti ve společenské instituce a na důvěře mezi jednotlivci a komunitami, které naši společnost tvoří. Důvěra je základním stavebním kamenem dobře fungující demokracie. Informační vlivové aktivity narušují důvěru vyvoláváním pochybností a využíváním existujících rozporů. Působení zahraničních aktérů vlivovými technikami na obyvatelstvo může z hlediska národní bezpečnosti představovat hrozbu. Pro odolnou a zdravou demokratickou společnost je nezbytná schopnost udržet důvěru a odpovídajícím způsobem – prostřednictvím věrohodných a na faktech založených sdělení – reagovat na informační vlivové operace.

Jaká je role komunikátora?

Jakožto komunikátor máte možnost hrát důležitou roli v prevenci, identifikaci a boji proti informačním vlivovým aktivitám. Pomáháte vaší organizaci dodržovat její závazky a budovat obraz důvěryhodnosti. Komunikujete s cílovými skupinami, odpovídáte na otázky a poskytujete důležité informace. Máte přehled o tom, jak vaše publikum smýšlí a co je pro něj podstatné.

Může se to zdát nepravděpodobné, ale jednoho dne se může i vaše organizace stát cílem informační vlivové kampaně. Například zjistitíte, že jsou o vaší organizaci šířeny nepravdivé informace, objeví se falešná verze vašich webových stránek nebo dojde k napadení účtů organizace na sociálních médiích. Cílové publikum vaší organizace se může stát terčem kyberšikany, trollingu nebo dezinformací. Účelem těchto útoků může být podkopání důvěryhodnosti vaší organizace, protlačení nepravdivých nebo zavádějících informací do důležitých diskusí nebo zvýšení napětí mezi cílovými skupinami. Ve všech těchto případech máte příležitost plnit zásadní úlohu při posilování a podpoře produktivní demokratické diskuse.

PROČ NA KOMUNIKÁTORECH ZÁLEŽÍ?

- Vytváříte myšlenkové mosty mezi vaší organizací a veřejností.
- Máte zkušenosti s různými formami krizové komunikace, které mohou být relevantní pro reakci na informační vlivové aktivity.
- Při výskytu informačních vlivových aktivit můžete být mezi prvními, kteří se s nimi setkají.

Jako komunikátor již máte mnoho dovedností potřebných k tomu, abyste mohli čelit informačním vlivovým aktivitám. Tato příručka obsahuje další informace, které vám s danou problematikou mohou pomoci. Dozvíte se, jaké techniky mohou být použity proti vám a jak včas rozpoznat varovné příznaky. Zjistíte, jak svou organizaci připravit na rychlou a účinnou reakci. Získáte též doporučení ohledně volby nejvhodnější reakce v rámci specifických podmínek vaší organizace a vašeho mandátu jako komunikátora.

Koncepce příručky

Účelem této příručky je zvýšit povědomí o informačních vlivových kampaních, prohloubit míru jejich pochopení a rozvíjet schopnost protireakce. Informace obsažené v příručce vám pomohou lépe rozpoznat obvyklé techniky ovlivňování a poskytnou vám soubor proaktivních kroků, které můžete použít k návrhu nejvhodnější odezvy. Tato příručka nepřináší univerzální řešení ani prostý seznam jednotlivých bodů k odškrtnutí. Každá organizace je specifická, komunikuje s jiným publikem a čelí různým výzvám, které je nutno zohlednit při volbě nejvhodnější reakce.

ČÁST I: CO JE INFORMAČNÍ OVLIŇOVÁNÍ

Co jsou informační vlivové aktivity?
Jak využívají slabin ve společnosti?
Čím se informační vlivové operace liší od jiných forem komunikace?

ČÁST II: JAK ROZPOZNAT INFORMAČNÍ OVLIVŇOVÁNÍ

Co je účelem informačních vlivových aktivit?
Jaké jsou hlavní techniky informačního ovlivňování?
Jak jsou tyto techniky obvykle kombinovány?

ČÁST III: JAK ČELIT INFORMAČNÍM VLIVOVÝM OPERACÍM

Jak mohu svou organizaci předem připravit?
Jakým způsobem zvolím přiměřenou reakci?
Jak zajistím know-how pro potenciální budoucí situace?

ČÁST I.
Co je informační ovlivňování

Co jsou informační vlivové aktivity?
Jak využívají slabin ve společnosti?
Čím se informační vlivové operace liší od jiných forem komunikace?

ČÁST I. Co je informační ovlivňování

Tato část popisuje, jak informační vlivové operace využívají slabin ve společnosti a poskytuje nástroje pro posuzování podezřelých aktivit a identifikaci případů informačního ovlivňování.

Co jsou informační vlivové aktivity?

Společenský dialog, pluralita názorů a fakty podložená otevřená diskuse jsou základními rysy zdravé demokratické společnosti. Co však nastane, pokud někdo uměle vytvoří důkazy, nastrčí falešné „experty“ nebo záměrně pracuje se zavádějícími argumenty? Tyto aktivity jsou společensky škodlivé a představují problém pro demokratické procesy, které se opírají o veřejný informovaný souhlas. V těchto případech jsou žádoucí odezvou fakta, kritické zhodnocení zdroje a potvrzení závazku jednání ve veřejném zájmu.

Ve většině demokratických zemí je samozřejmostí zdravá a živá politická debata. Jednotliví občané, novináři, akademici a zástupci občanské společnosti plní důležitou funkci kontrolního dohledu nad rozhodováním veřejných činitelů. Kromě toho považují za svůj úkol též poukázat na případy zjevně nepravdivých nebo zavádějících informací. Jejich úsilí mohou podpořit státní představitelé poskytováním finančních prostředků na rozvoj zdravé občanské angažovanosti a rovněž nápravou nepřesností souvisejících s vlastní prací. Přinejmenším teoreticky slouží tento systém liberálním demokraciím po celá staletí. Dnes tolik rozšířené debaty o fake news však naznačují, že slabiny demokratických systémů jsou nyní využívány novým způsobem.

Informační vlivové aktivity představují potenciálně škodlivé formy komunikace řízené zahraničními státními činiteli nebo jejich zástupci. Jedná se o záměrný zásah do vnitřních záležitostí země, za účelem vytvoření ovzduší nedůvěry mezi státem a jeho občany. Informační vlivové aktivity slouží k podpoře zájmů cizí moci, prostřednictvím využívání existujících slabin ve společnosti. Aktéři cizích států zkoumají aktuálně rezonující sporné otázky a kontroverzní témata, a využívají těchto zranitelností k narušení a polarizaci společnosti.

Informační vlivové operace mohou být nasazeny jednotlivě, ale též jako součást rozsáhlejší vlivové kampaně, čerpající z širokého spektra technik. Kromě komunikačních nástrojů lze k ovlivnění společnosti využít vše od diplomatických a ekonomických sankcí až po demonstrace vojenské síly.

STRUKTURA INFORMAČNÍ VLIVOVÉ KAMPANĚ

Využití vlivových technik
Public relations, marketing, diplomacie, názorová žurnalistika a lobbování jsou příklady přijatelných způsobů ovlivňování názorů a chování lidí. Informační vlivové aktivity tyto způsoby napodobují, ale používají tyto techniky klamavě a za nekalým účelem.

Narušení veřejné diskuse
Cizí mocnosti využívají informační aktivity k ovlivňování oblastí, ze kterých mohou mít prospěch. Toho lze dosáhnout jak přímo, tak nepřímo – od otevřené propagandy až po skryté financování občanských uskupení. Nelegitimní aktéři zasahující do legitimní veřejné debaty mohou změnit vnímání názorových proudů a ovlivnit rozhodování společnosti.

Jednání ve vlastním zájmu
Účelem vlivových aktivit je dosažení specifických cílů, z nichž má prospěch cizí moc. Příkladem takového cíle může být politická destabilizace společnosti, znemožnění přijetí konkrétních rozhodnutí nebo polarizace politické diskuse.

Využití zranitelností
Každá společnost má své vnitřní problémy – sociální nebo třídní napětí, nerovnost, korupce, bezpečnostní otázky nebo jiné problémy, které mají dopad na život ve společnosti. Cizí nepřátelské síly se snaží tyto slabiny identifikovat a systematicky je využívat k dosažení svých cílů.

Odlišení informačních vlivových aktivit od normální veřejné diskuse může být poměrně nejednoznačné a mnohdy velmi obtížné. Politické debaty mohou být nezřídka vyhrocené, nepříjemné až hrubé. Jsou však součástí demokratického procesu, který se opírá o pluralitu názorů a svobodnou diskusi. Konstruktivní debaty však nemohou probíhat v prostředí, v rámci kterého cizí mocnosti úmyslně šíří zavádějící informace za účelem jejich narušení a ovlivnění.

Je důležité podotknout, že osoba, která zastává názory podobné názorům cizí moci, se tímto automaticky nestává agentem této mocnosti. Když hovoříme o informačních vlivových aktivitách, máme tím na mysli systematické používání klamavých technik za účelem podrývání demokracie. Těmto pokusům o narušení demokracie je nutno čelit, a to při zachování základních demokratických principů, jako je svobodná a otevřená diskuse, svoboda projevu a demokratický dialog. Ty by měly být vždy základním kamenem reakce na informační vlivové kampaně, a to i přesto, že mohou naši úlohu ztížit.

Jak jsou zneužívány společenské slabiny?

Předpokládejme, že naše názory jsou výsledkem racionálního procesu: něco se stane nebo se objeví nová informace. Svědkové, výzkumní pracovníci, vládní úředníci a další aktéři s příslušnou odborností interpretují nebo vysvětlují situaci vrámci širšího kontextu. Od nich následně přeberou informace média a dále je šíří různými kanály, online i offline. Tímto způsobem přichází informace k občanům. V praxi se samozřejmě může tento proces případ od případu poněkud lišit, ale v hrubém nástinu je toto princip utváření názorů v demokratické společnosti.

Tento proces je založen na několika základních předpokladech. Informace o původní události musí být pravdivé a založené na faktech. Tvrzení musí být ověřena důvěryhodnými zdroji, za kterými stojí skutečně existující lidé, jejichž dobrá pověst by byla případným zkreslením informací poškozena. Média musí prezentovat informace o události vyváženě, musí ověřovat fakta a zdroje a celkově jednat ve veřejném zájmu. Rozdílné názory musí být vzájemně diskutovány tak, aby následně zformulované závěry byly dostatečně opodstatněné.

Informační operace jsou nastavené takovým způsobem, aby využívaly zranitelná místa výše popsaného procesu formování názorů, která vznikají při střetu jeho ideální podoby s realitou. Nepřátelští aktéři používají kreativní, oportunistické a technologicky vyspělé techniky ovlivňování tak, aby vstoupili do procesu toku informací a narušili jej. Neváhají využít zranitelnosti způsobů, kterými utváříme své názory. Jsou schopni spatřit slabiny ve způsobech, jimiž klíčové informace putují mediálním prostředím, i v tom, jak naše mozky informace zpracovávají.

„Fakta" mohou být zfalšována nebo zmanipulována, „odborníci" nemusí být vůbec odborníky a „svědci" mohou být zaujatí či podplacení. Zpravodajství mohou být provozována jako jednostranné propagandistické kanály. Internetové diskuse mohou být vedeny mezi automatizovanými boty, aby byla vytvořena iluze živé veřejné debaty. Pokud jsou tyto aktivity prováděny záměrně, prostřednictvím koordinovaných kampaní, jejichž cílem je podkopat demokratické procesy, nemůžeme vždy spoléhat na systémovou „autokorekci". Právě v těchto situacích můžete jakožto komunikátoři hrát důležitou roli.

Formování názoru

NOVÁ INFORMACE
Objeví se nová informace: událost, vědecký objev, mediální prohlášení nebo politické rozhodnutí.

ZDROJE A OFICIÁLNÍ PŘEDSTAVITELÉ
Informace je předána, vysvětlena a interpretována svědky, experty a oficiálními představiteli.

MÉDIA
Zpráva je veřejnosti komunikována prostřednictvím tisku, televize, rádia, blogů a sociálních sítí.

VEŘEJNOST
Informace se dostane k veřejnosti a je diskutována různými sociálními skupinami, a to jak osobně, tak na sociálních sítích.

VY
Prostřednictvím vámi sledovaných informačních kanálů a komunit, jejichž jste součástí, se informace dostane až k vám.

SLABINY MEDIÁLNÍHO SYSTÉMU
Moderní mediální systém má řadu slabých míst, zejména rychlý vývoj technologií, změny v novinářském obchodním modelu a rozšíření alternativních zdrojů. Podvržené zprávy, upravené fotografie, algoritmy, boti a konkurenční boj o prokliky na sociálních sítích – to vše činí mediální systém zranitelným vůči těm, kteří ho chtějí využít pro svůj vlastní prospěch, pro politický či ekonomický zisk nebo jen proto, aby viděli, zda je to možné.

SLABINY VEŘEJNÉHO MÍNĚNÍ
Veřejné mínění bylo vždy ovlivnitelné určitými jevy, jako je např. sociální schválení - tzn. kopírování takového chování druhých, které je interpretováno jako správné nebo žádoucí. V dnešním informačním prostředí, kde mohou být účty na sociálních médiích falešné a armády trollů znepřehledňují internetové diskuse, je však snazší než kdy jindy vytvořit „fakta", „důkazy", vzbudit hněv a pobouření. To vše činí veřejné mínění zranitelným vůči úmyslné manipulaci.

KOGNITIVNÍ LIMITY
Některé zranitelnosti vychází přímo z fungování lidského mozku. Kognitivní schopnosti člověka nestačí na to, abychom se dokázali vypořádat se všemi informacemi, které nás v moderním světě obklopují. Naproti tomu naše osobní údaje mohou být podrobeny psychografické analýze, schopné zjistit o nás více než víme sami. Na každého jednotlivce, jenž používá sociální média, existuje dle odhadů více než 800 datových údajů, které mohou být použity k předvídání širokého spektra chování. Informační vlivové operace využívají naše myšlenkové vzorce k ovlivňování našeho vnímání, chování a rozhodování.

Čím se informační vlivové aktivity liší od ostatních forem komunikace?

Úkolem komunikátora není zkoumat, zda za určitými komunikačními aktivitami stojí cizí moc. Pokud však získáte podezření, že se objevily informační vlivové operace vztahující se k práci, kterou vykonáváte, nebo ohrožující integritu veřejné diskuse a národní bezpečnosti vaší země, očekává se, že budete jednat. Pokuste se situaci co nejlépe posoudit. Jinak řečeno, je důležité, abyste chápali roli, kterou vaše organizace hraje ze společenského hlediska v širším kontextu.

Aby bylo možné identifikovat případy informačního ovlivňování, musíte vyhodnotit, do jaké míry je komunikace zavádějící a zda má destruktivní charakter, což jsou faktory, které je nutné vzát v úvahu pro přijetí informovaného rozhodnutí o případné reakci. Cíle a motivace vlivové činnosti nemusí být na první pohled zřejmé. Nicméně, čím více negativních faktorů identifikujete, tím vyšší je i pravděpodobnost, že se potýkáte s případem informačního ovlivňování.

KLAMÁNÍ

Seriózní komunikace je otevřená a transparentní. Obsah je důvěryhodný a lze jej ověřit. **Informační vlivové aktivity jsou záměrně zavádějící.**

ÚMYSL

Seriózní komunikace přispívá ke konstruktivní diskusi, i když argumenty nebo obsah mohou být kontroverzní. **Informační vlivové aktivity podkopávají konstruktivní dialog a brání otevřené diskusi.**

DESTRUKCE

Seriózní komunikace je přirozenou součástí naší společnosti a posiluje demokracii, přestože někdy vytváří tření. **Informační vlivové aktivity narušují demokratický dialog a oslabují fungování společnosti.**

Není náhodou, že techniky používané pro informační vlivové aktivity se často překrývají s žurnalistikou, veřejnými záležitostmi, veřejnou diplomacií, lobbováním a public relations. Kopírování legitimních metod je jedním ze způsobů, jak informační vlivové operace zamaskovat a vyvolat dojem důvěryhodnosti. Upozorňujeme, že nelegální vlivové aktivity, jako jsou výhružky, hacking, vydírání a úplatkářství, jsou mimo rámec této příručky a měly by být nahlášeny policii.

ČÁST II.
Jak rozpoznat informační ovlivňování

Co je účelem informačních vlivových aktivit?
Jaké jsou hlavní techniky informačního ovlivňování?
Jak jsou tyto techniky obvykle kombinovány?

ČÁSTII.Jak rozpoznat informační ovlivňování

Prvním krokem v boji proti informačním vlivovým aktivitám je jejich identifikace. To znamená vědět, co hledáme. Tato část příručky se věnuje pochopení strategických narativů, přístupů k cílení na publikum a podrobnějšímu rozboru technik používaných v rámci vlivových aktivit. Zabývá se též tím, jak mohou být tyto techniky kombinovány za účelem vytváření negativních společenských dopadů.

Co je účelem informačních vlivových aktivit?

Pro úspěšnou identifikaci informačních vlivových aktivit je nutné rozumět tomu, co jsou strategické narativy a cílové skupiny. Základní povědomí o těchto konceptech a jejich významu vám pomůže lépe chápat a rozpoznávat případy potenciálních informačních vlivových aktivit. Zároveň vám tato znalost umožní porozumět, jaké úmysly za těmito aktivitami patrně stojí.

Strategické narativy

Informační vlivové aktivity obvykle využívají sílu příběhu. Prezentace události, problému, organizace, místa nebo skupiny je obvykle formulována tak, aby zapadala do již existujícího narativu. Jako příklad lze uvést obecné povědomí o vesmírných závodech mezi Spojenými státy a Sovětským svazem během studené války. Většina lidí slyšela o přistání člověka na Měsíci, stejně jako o konspiračních teoriích o tom, že přistání na Měsíci bylo zinscenované. Existuje video, v němž astronaut na povrch Měsíce umisťuje vlajku. Pro někoho představují tyto záběry důkaz, jiní tvrdí, že je video falešné. Narativy opakovaně podvědomě uplatňujeme při třídění nových informací. Ve chvíli, kdy se setkáme s novou informací z oblasti cestování vesmírem, zpracováváme ji podle toho, kterému z těchto narativů věříme. Záměrně připravené a v komunikačních aktivitách využívané příběhy jsou označovány jako strategické narativy.

Někdo například může vytvořit informaci o určité náboženské nebo etnické skupině, která zapadá do již existujícího narativu – tedy do toho, co si lidé obvykle o těchto skupinách myslí. Dezinformace nás mohou ovlivnit třemi různými způsoby – zdůrazněním, či naopak potlačením, některého aspektu existujícího narativu nebo propojením narativu s nesouvisejícími událostmi za účelem odvedení pozornosti.

Identifikace použitých strategických narativů a odhalení logiky, která za nimi stojí, je důležitým krokem při plánování vhodné reakce. Zamyslete se nad třemi níže uvedenými přístupy. Vzpomenete si na nějaký strategický narativ, který používá jeden z těchto přístupů?

STRATEGICKÉ NARATIVY

Pozitivní/konstruktivní: „Toto je pravda!"
Snaží se vytvořit koherentní narativ o určité záležitosti, který bude zapadat do již zavedených strategických narativů. Může je také dále doplňovat či rozšiřovat.

Negativní/destruktivní: „Toto je lež!"
Pokouší se zabránit vzniku koherentního narativu nebo vyvrátit či podkopat existující narativ.

Nepřímý: „Podívej se támhle!"
Různými způsoby odvádí pozornost od původního problému: humor, memy, konspirační teorie, atd.

Cílové publikum

Analýza strategických narativů je jednou z metod směřujících k odhalení logiky informační vlivové kampaně. Související metodou je zamýšlet se nad cílovým publikem – v jakých skupinách tyto strategické narativy rezonují? Jedná se o narativy určené široké veřejnosti nebo jsou zaměřeny na konkrétní skupinu? Jsou využívána „big data" k zacílení na jednotlivce s určitými osobnostními rysy či názory? Pokud probíhá určitá forma cílení, je zaměřena na specificky zranitelné skupiny nebo jednotlivce, příp. na osoby se specifickými vzorci chování? Uvědomit si, na koho je pomocí strategického narativu cíleno, je důležitým krokem při posuzování závažnosti každého konkrétního případu.

CÍLOVÉ SKUPINY

Široká veřejnost: největší možné publikum
Informační vlivové aktivity zaměřené na společnost jako celek, a to prostřednictvím obecně přijímaných narativů.

Sociodemografické zacílení: specifické skupiny
Rozdělení publika na základě demografických faktorů (jako je věk, příjem, vzdělání a etnický původ) umožní přizpůsobit sdělení tak, aby působila na konkrétní skupinu.

Psychografické zacílení: jednotlivci
Analýzou a kategorizací velkých objemů dat lze informační vlivové aktivity zaměřit na jedince s určitými osobnostními rysy, politickými preferencemi, vzorci chování nebo jinými charakteristikami.

Společně s rozpoznáním strategických narativů a používaných komunikačních technik může analýza zacílení odhalit záměr informačních vlivových aktivit. Pokud pochopíte, *na koho je cíleno a proč*, bude snazší posoudit, *jaký je účel* těchto informačních vlivových operací. To vám následně pomůže rozhodnout, *která protiopatření jsou nejvhodnější*.

Jaké jsou hlavní techniky informačního ovlivňování?

Způsoby informačního ovlivňování se neustále vyvíjejí. Po prostudování široké škály příkladů jsme vytvořili šest skupin nejobvyklejších technik, na které je dobré být připraven. V jednotlivých skupinách jsou sdruženy techniky založené na principech podobného charakteru. Povědomí o existenci těchto technik a o tom, jak pracují, vám pomůže je rozpoznat.

Samotné techniky jsou ve většině případů neutrální – nejsou ani dobré, ani špatné. Mohou být použity otevřeným a přijatelným způsobem, jako přirozená součást demokratického dialogu, nebo naopak s nepřátelským, úmyslně klamným, záměrem jako součást informační vlivové kampaně. Použití jakékoli techniky samo o sobě však nutně neznačí informační ovlivňování.

Analyzujte způsob použití těchto technik, společně s posouzením strategických narativů a cílových skupin:

- Jak silné jsou indikátory, ukazující na zavádějící či rušivý záměr?
- Co o účelu komunikace napovídají strategické narativy a cílové skupiny?
- Pokud je nasazena určitá technika, může mít škodlivý dopad na veřejnost nebo na naši společnost?

Techniky informačního ovlivňování

SOCIÁLNÍ A KOGNITIVNÍ HACKING

- Temná reklama
- Stádový efekt
- Spirála mlčení
- Komnaty ozvěn a sociální bubliny

PODVODNÉ IDENTITY

- Shilling
- Podvodné jednání
- Podvrh
- Potěmkinovy vesnice
- Falešná média

TECHNOLOGICKÉ MANIPULACE

- Boti
- Falešné „loutkové“ účty
- Deepfake videa
- Phishing

DEZINFORMACE

- Fabulace
- Manipulace
- Falešné zdroje
- Satira a parodie

ZÁKEŘNÁ KOMUNIKACE

- Útok ad hominem
- Whataboutismus
- Zahlcení
- Slaměný panák
- Zmocnění se tématu

SYMBOLICKÉ AKTY

- Únik informací
- Hacking
- Veřejné demonstrace

Sociální a kognitivní hacking

Sociální a kognitivní hacking se týká činností, které využívají našich společenských vztahů a myšlenkových procesů. Podobně, jako při hackování počítače, se nepřátelští aktéři snaží nekalým způsobem využít zranitelnosti subjektu. Obvykle máme například tendence zapadat do rámce toho, co si myslí a dělají nám podobní lidé. Když jsme vystaveni materiálům útočícím na naše emoce, může být ohroženo naše racionální uvažování. Tyto a další předvídatelné vzorce chování mohou být zneužity nepřátelskými aktéry, kteří pro dosažení svých cílů záměrně využívají našich zranitelností, například ve společenských debatách o citlivých otázkách.

TEMNÁ REKLAMA

Za temnou reklamu (*dark ads*) jsou považovány zprávy přizpůsobené na míru psychografickému profilu konkrétních jednotlivců. Data vytěžená ze sociálních sítí a dalších zdrojů mohou být využita pro kategorizaci jednotlivců do skupin dle ideologických názorů či osobnostních sklonů. Reklamy, které se zobrazí pouze určitým jednotlivcům, mohou podporovat specifické chování a obsahovat sdělení atraktivní pro jedince konkrétních psychologických rysů.

STÁDOVÝ EFEKT

Lidé, kteří mají pocit, že patří k většině, vyjadřují své názory s větší ochotou. Počet liků, komentářů a sdílení příspěvků na sociálních médiích může být uměle navýšen boty tak, aby byl vyvolán dojem obecného společenského přijetí. To apeluje na kognitivní potřebu příslušnosti ke skupině a podporuje následné další zapojení skutečných uživatelů.

SPIRÁLA MLČENÍ

Lidé, kteří mají pocit, že patří k menšině, vyjadřují své názory méně ochotně.
V protikladu ke stádovému efektu může dojem společenské shody ohledně určité problematiky způsobit, že lidé s menšinovými názory zůstanou zticha. Jedná se o manifestaci strachu z ostrakizace nebo vyloučení z důvodu nepopulárního názoru.

KOMNATY OZVĚN A SOCIÁLNÍ BUBLINY

Skupiny, ve kterých lidé komunikují primárně s jedinci podobných názorů a přesvědčení, se nazývají komnaty ozvěn; existují jak online, tak v reálném životě. Například lidé s podobnými názory pravděpodobně čtou stejné noviny a také, což je ještě významnější, se navzájem společensky stýkají. Jsou tak jen zřídka vystaveni ideologicky odlišným názorům. Toho lze využít k online šíření cílených informací konkrétním skupinám.

Podvodné identity

Důvěryhodnost informací často hodnotíme dle jejich zdroje. Kdo se mnou komunikuje a proč? Co ví o dané problematice? A je skutečně tím, za koho/co se vydává? Nepřátelští aktéři, kteří se podílí na informačním ovlivňování, využívají „kapitál důvěry“ tím, že prostřednictvím podvodných identit napodobují legitimní zdroje informací (ať už se jedná o osoby, organizace nebo platformy).

SHILLING

Tzv. shill je osoba působící navenek dojemem nezávislosti, přičemž ve skutečnosti pracuje (z přesvědčení či za honorář) v partnerství s někým jiným. Příkladem mohou být placení recenzenti produktů na webových nákupních portálech, lidé v publiku najatí k organizovanému potlesku pro řečníka během veřejného setkání nebo skupina online trollů honorovaných za psaní negativních komentářů.

PODVODNÉ JEDNÁNÍ

Podvodná osoba se vydává za někoho, kým není, a s úmyslem klamat imituje osobní či profesní identitu jiného člověka. Taková osoba se může neprávem stavět do pozice odborníka či předstírat kvalifikaci, kterou ve skutečnosti nedisponuje (například lékařské či právnické vzdělání).

PODVRH

Falzifikace oficiálních dokumentů je efektivním způsobem, jak učinit dezinformace zdánlivě autentickými. Například padělané hlavičkové papíry, razítka či podpisy mohou být použity k vytvoření falešné dokumentace.

POTĚMKINOVY VESNICE

Aktéři disponující dostatečnými zdroji mohou zřídit falešné instituce a sítě, které následně svým jménem zaštiťují klamné informace. Potěmkinovy vesnice jsou falešné společnosti, výzkumné instituce nebo think-tanky, vytvořené za účelem vyvolání dojmu důvěryhodnosti či „legitimizace” cílené dezinformace.

FALEŠNÁ MÉDIA

Dezinformace mohou být také šířeny vytvořením falešných mediálních platforem, které mají podobnou webovou adresu a/nebo vypadají podobně skutečnému zpravodajskému serveru. Vytvoření falešných webových stránek, které vypadají téměř identicky jako ty autentické, přičemž však publikují velmi odlišný obsah, je relativně snadné a levné.

TITULEK

Účelem titulku je zaujmout a upoutat pozornost čtenáře. Abyste se přesvědčili, že titulek odpovídá obsahu článku, je nutné pokračovat ve čtení i dále.

URL

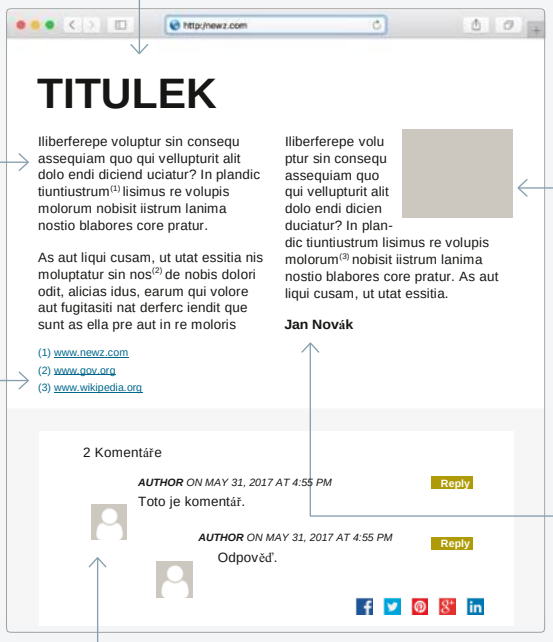
Imitace známých platforem pro vyvolání dojmu legitimity je běžnou technikou informační manipulace. Pro ujištění, že jste na správné platformě, zkontrolujte URL v adresním řádku.

OBSAH

Posuďte obsah textu. Je informativní, konfrontační, založený na faktech, emocích nebo názorech? Před sdílením si vždy přečtěte celý text.

FOTOGRAFIE

Ne vždy odpovídají fotografie realitě. Mohou být snadno zmanipulovány vymazáním, úpravou nebo přidáním prvků. Nemusí ani souviset s daným článkem. Vyhledáváním obrázků lze odhalit, zda byl obrázek již použit v jiném kontextu.



ZDROJE

Pokud text odkazuje na jiné zdroje, podívejte se na ně, abyste si ověřili původ informací. Posuďte, zda byla informace převzata správně.

AUTOR

U článků bez uvedeného autora buďte obezřetní. Je-li autor uveden, zvažte, o koho se jedná, a jaký to může mít vliv na podobu článku.

KOMENTÁŘE

Komentáře na webových stránkách a sociálních médiích nejčastěji pochází od obyčejných lidí, kteří vyjadřují své názory. Za některými komentáři však mohou stát trollové a boti. Přemýšlejte, kdo komentáře postuje.

SDÍLENÍ

Skutečnost, že text nasbíral hodně liků či je široce sdílený, automaticky neznamená, že obsah je správný. Nesdílejte obsah pouze na základě angažovanosti druhých.

Technologická manipulace

Informační vlivové aktivity často využívají nejnovější technologie. Nepřátelští aktéři používají pokročilé technické dovednosti pro manipulaci online toků informací – automatizované účty, algoritmy nebo kombinace lidských a technologických prvků. Uvědomme si, že k realizaci tradičních informačních vlivových aktivit, jako je vytváření podvodných identit nebo šíření dezinformací, se nyní často používají nové technologie. Tato oblast se vyvíjí mnohem rychleji než naše schopnost analyzovat a pochopit její potenciální využití a důsledky. V poslední době často diskutovaný vývoj deepfake videí, strojového učení a umělé inteligence potvrzuje, že tyto a jim podobné nástroje budou pro účely informačního ovlivňování využívány stále častěji.

BOTI

Boti jsou počítačové programy provádějící automatizované úkony, jako např. sdílení určitých typů informací na sociálních sítích nebo zodpovídání často kladených otázek na zákaznických platformách. Mohou však také být použiti pro zvýraznění konkrétních zpráv, pro spamování diskusních fór, pro navyšování počtu liků a sdílení příspěvků na sociálních médiích, a také pro provádění kybernetických útoků.

FALEŠNÉ “LOUTKOVÉ“ ÚČTY

Falešné účty spravované někým, kdo neodhaluje svou skutečnou identitu nebo záměry, se označují jako tzv. sockpuppet účty. Takové falešné identity jsou používány ke vstupu do online komunit a účastní se dění se záměrem vnést do debat nepravdivé či kontroverzní informace. Dva nebo více sockpuppet účtů může skrytě spolupracovat a uměle simulovat obě strany debaty.

DEEPFAKE VIDEA

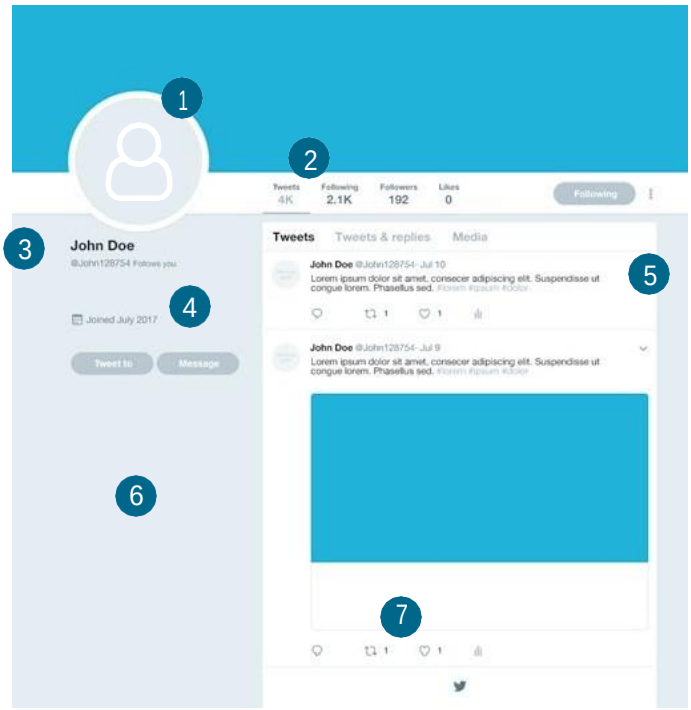
Pokročilé algoritmy strojového učení dnes umožňují takovou manipulaci s audio a video záznamem, jejíž výsledek vypadá velice přesvědčivě. Tak může vzniknout například video, ve kterém skutečný politik pronáší fiktivní řeč. Je dokonce možné namapovat tvář jiné osoby do již existujícího videozáznamu a digitálně rekonstruovat hlas.

PHISHING

Phishing je technika, jejímž cílem je přesvědčit uživatele, aby odhalil svá hesla nebo jiné citlivé informace online. Phishingovým útokem může být automatizované rozesílání e-mailů, které vypadají na první pohled legitimně, ale ve skutečnosti vedou k falešným webovým stránkám, jež následně vytěží zadané osobní údaje. Spear phishing je cílený, sofistikovanější typ phishingu, který se používá k získání přístupu k informacím v zabezpečených počítačových systémech.

Jak rozpoznat bota

Třebaže jsou boti účinným nástrojem ovlivňování na sociálních sítích, mohou být v některých případech rozpoznáni běžným uživatelem. Posouzení následujících sedmi znaků vám může pomoci online bota odhalit. Ale mějte se na pozoru – různé typy botů mohou vypadat velmi odlišně. Imitátorští boti jsou navrženi tak, aby vypadali jako skuteční uživatelé. Spam boti se naopak soustředí na šíření velkých objemů informací a často tak postrádají přirozené vlastnosti běžných uživatelů.



1. PROFILOVÝ OBRÁZEK

Boti obvykle zcela postrádají, nebo používají ukradený, profilový obrázek. Použijte vyhledávání obrázků k ověření pravosti podezřelých avatarů.

2. AKTIVITA

Spam boti jsou obvykle velmi aktivní, někdy generují více než 50 příspěvků denně.
U podezřelého účtu se zajímejte o počty příspěvků za den.

3. JMÉNO

Většina botů automaticky generuje svá uživatelská jména. Uživatelská jména tvořená sekvencí náhodných písmen a čísel mohou být boti.

4. DATUM ZALOŽENÍ

Účty botů bývají účelově vytvořeny a nemají tak žádnou uživatelskou historii. Někdy jsou za tímto účelem hacknuty starší účty a jejich předchozí příspěvky jsou odstraněny (proto mají tyto účty přestávky mezi intenzivními obdobími aktivity).

5. JAZYK

Někdy používají boti k šíření zpráv v různých jazycích automatický překlad, což má za následek zjevné gramatické chyby nebo nekoherentní věty. Účty, které publikují podobný obsah ve více jazycích, mohou být boti.

6. INFORMACE

Účty botů jsou vytvořeny tak, aby fungovaly anonymně. Neobsahují tedy osobní informace, případně používají informace fiktivní či falešné. Ověřte všechny poskytnuté informace.

7. SDÍLENÍ

Posuďte, se kterými příspěvky podezřelý účet interreaguje. Boti jsou často vzájemně koordinováni a podporují zprávy šířené dalšími boty. Pravděpodobně nebudou mít reálné sledující.

Dezinformace

Dezinformace jsou mylné, zmanipulované či zavádějící informace, které jsou záměrně šířeny za účelem uvést v omyl. Představují základní kámen klasické propagandy i současného fenoménu fake news. Záměrné využití nepravdivých informací za účelem manipulace není nic nového, digitální platformy však zásadně změnily povahu dezinformací. Falešný obsah může mít podobu pozměněného textu, obrazu, videa nebo audio nahrávky. Tyto prvky mohou být použity k posílení falešných narativů, vyvolání zmatku a diskreditaci legitimních informací, jednotlivců či organizací.

FABULACE

Informace bez faktického základu publikované způsobem, který má vzbuzovat zdání legitimity. Může se jednat například o falešný vymyšlený e-mail od politika, který „unikne“ do tisku, čímž naruší jeho důvěryhodnost.

MANIPULACE

Přidání prvku, odstranění části nebo změna obsahu textu, fotografie, videa nebo zvukového záznamu za účelem změny sdělení zprávy.

NERELEVANTNÍ OBSAH

Zavádějící využití věcně správného obsahu v rámci prezentace nesouvisející problematiky, události či osoby. Například článek obsahující fake news může použít fotografie vztahující se k jiné události pro navození dojmu autenticity.

SATIRA A PARODIE

Satira a parodie jsou obvykle neškodné formy zábavy. I humor však lze využít agresivně k šíření zavádějících informací a zesměšňování či kritizování jednotlivců, názorů nebo narativů. Humor může být také velmi účinným způsobem legitimizace kontroverzních názorů.

Zákeřná komunikace

Argumentace je přirozenou a akceptovanou součástí demokratické debaty, v níž má každý právo vyjádřit své názory a zapojit se do veřejného projednávání. Uchylovat se k zákeřným formám komunikace plným argumentačních faulů je však v rámci veřejné debaty nepřijatelné. Často již tak roztříštěnou povahu veřejných rozhovorů používání řečnických triků, jejichž cílem je uvádět v omyl, mystifikovat a odrazovat některé účastníky od účasti ve veřejné diskusi, dále znepřehledňuje.

Hojně se vyskytujícím prostředkem negativní komunikace online je tzv. troll. Trollové jsou uživatelé sociálních sítí, kteří prostřednictvím svých komentářů a chování online záměrně provokují ostatní. Jejich činnost přispívá k prohloubení polarizace, umlčuje nesouhlasné názory a dusí legitimní diskusi. Jednání trollů může vycházet z osobních pohnutek nebo, jako v případě *hybridních trollů*, pracují pod vedením někoho jiného.

ÚTOK AD HOMINEM

Argumenty, které namísto soustředění se na předmět diskuse, útočí, diskreditují nebo zesměšňují osobu oponenta, označujeme termínem ad hominem. Tento řečnický faul je používán k umlčení, odrazení nebo zastrašení oponenta.

WHATABOUTISMUS

Odvrácení kritiky vytvořením falešné paralely s podobným, ale pro diskusi irelevantním jevem.

ZAHLCENÍ

Zahlcení oponenta záplavou argumentů, faktů a zdrojů, z nichž mnohé jsou pochybné nebo nesouvisí s předmětem diskuse.

SLAMĚNÝ PANÁK

Snaha zdiskreditovat oponenta tím, že mu jsou přisuzovány postoje či názory, které nezastává a následná argumentace proti těmto postojům.

ZMOCNĚNÍ SE TÉMATU

Převzetí stávající debaty a změna jejího účelu či tématu. Tato metoda, jejíž pojmenování v anglickém jazyce zní doslova „hijacking“, tj. únos, je obzvláště účinná při využití hashtagů a memů, a může být také použita k narušení akcí nebo kontra-kulturních společenských hnutí.

Symbolické akty

Činy jsou mocnější než slova. Někdy skutečným účelem nějaké akce nemusí být ani tak dosažení určitého cíle, ale spíše demonstrace nějakého sdělení. V takových případech lze akci označit za symbolickou. Na rozdíl od běžných akcí jsou symbolické akty motivovány komunikativní logikou a rámcem strategického narativu. Příkladem velmi surových symbolických aktů může být terorismus a to, jak teroristé využívají všeobecně sdílený strach z nahodilého násilí. Sofistikovanější způsoby pak mohou používat specifické kulturní symboly, relevantní pro konkrétní cílové publikum.

ÚNIK INFORMACÍ

Únik informací zde chápeme jako zveřejnění informací, které byly získány nelegitimními prostředky. Má obvykle silný symbolický význam, jelikož může odhalit nepravosti a před veřejností zamlčované skutečnosti. Pokud jsou však úniky informací využívány jako prostředek informačních vlivových aktivit, informace bývají vyňaty z kontextu a jsou použity k diskreditaci aktérů a rozostření informačního prostředí. Podklady bývají získány např. pomocí hackingu nebo krádeží.

HACKING

Termínem hacking označujeme získání neoprávněného přístupu k počítači nebo síti, jedná se o trestný čin. Pokud je hacking součástí informačního ovlivňování, může sloužit jako symbolický akt, kdy je samotný zásah podružný. V těchto případech bývá skutečným cílem vyvolat nejistotu, zda je systém bezpečný nebo kompromitovaný, tak aby byla podkopána důvěra v dotyčný systém nebo v subjekt za tento systém odpovědný.

VEŘEJNÉ DEMONSTRACE

Legitimní demonstrace jsou symbolické akty vyjádření podpory určité politické otázce nebo pozice. Představují důležitý prvek demokratického dialogu. Nepřátelští aktéři však mohou demonstrace organizovat uměle, aby vzbudili dojem silné podpory nebo naopak odporu k určité otázce (známé též jako astroturfing).

Jak jsou tyto techniky obvykle kombinovány?

Aby bylo možno identifikovat případ informačního ovlivňování, musíte zhodnotit strategické narativy, cílové skupiny a použité komunikační techniky. Nezapomeňte, že je často používáno několik škodlivých komunikačních technik najednou, tak aby se vzájemně podporovaly a posilovaly.

Například podvržený dokument zasáhne širší publikum, pokud je šířen boty. Účinek bude dále posílen, jestliže budou zároveň publikovány články na zaujatých nebo falešných zpravodajských platformách, podporovaných armádou komentátorů-trollů. Posouzení případu potenciálního informačního ovlivňování by tedy mělo brát v úvahu, zda existují důkazy o vícečetných koordinovaných operacích namířených proti vaší organizaci. Na následující stránce naleznete několik příkladů, jak mohou koordinované vlivové aktivity vypadat.

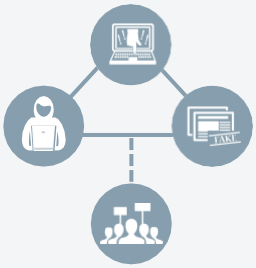
Níže naleznete také několik otázek, které můžete použít k posouzení komunikace a identifikaci informačních vlivových aktivit. Jaké narativy můžete identifikovat a na koho jsou zaměřeny? Existuje nějaký důkaz úmyslu klamat či destabilizovat? Máte podezření, že se jedná o zásah zahraničního aktéra nebo jeho zástupce? Zaznamenali jste kombinaci technik, která by svědčila o koordinovaném úsilí nebo kampani proti vaší organizaci? Pokud existují důvody k obavám, další část příručky předkládá doporučení pro vhodné reakce.

Koordinované techniky

Informační vlivové aktivity jsou často komplexní a jen zřídka narazíte na jednu techniku v izolované formě. Všímejte si možné kombinace technik namířených proti vám. I když teoreticky existuje nekonečné množství různých kombinací technik, stojí za to zmínit některé z obvyklých.

Polarizace

Polarizace umocňuje protikladné názorové extrémy v konkrétní otázce. Tato strategie může využívat sociální hacking, podvodné identity a dezinformace. K posílení extrémních názorů se často používají trollové a boti.

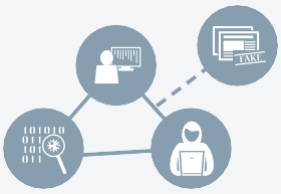


Laundering

„Praní špinavých informací" označuje metodu postupného zkreslování a dekontextualizace informací tak, až je nemožné zjistit, zda je jejich zdroj pravdivý. K vytvoření sítě falešných informací může tato strategie využívat podvodné identity, dezinformace, manipulaci pomocí technologií a symbolické akty v kombinaci se sociálním a kognitivním hackingem.

Provokace

Provokace zneužívá citlivé otázky k antagonizaci lidí, vyvolání hněvu a neshod. Tato strategie může využívat sociální a kognitivní hacking, podvodné identity a zákeřné formy komunikace tak, aby zneužívala emotivní vnímání běžných občanů.



Zahlcení

Zahlcení množstvím informací, ať jsou pozitivní, negativní nebo irelevantní, způsobí zmatení publika. Toho lze dosáhnout spamováním a trollingem na sociálních sítích nebo šířením dezinformací do legitimních mediálních zdrojů. Toto přehlcení vytlačuje korektní informace a odrazuje od konstruktivní debaty.

ČÁST III.
Jak čelit informačním vlivovým operacím

Jak mohu svou organizaci předem připravit?
Jakým způsobem zvolím přiměřenou reakci?
Jak zajistím know-how pro potenciální budoucí situace?

ČÁST III. Jak čelit informačním vlivovým operacím

V této části se budeme zabývat tím, jak čelit informačním vlivovým aktivitám. Pomůžeme vám připravit vaši organizaci na tuto hrozbu, budeme se věnovat možným opatřením v případě probíhajícího útoku, a navrhneme způsoby sdílení osvědčených postupů za účelem prohlubování znalostí napříč organizacemi.

PŘIPRAVTE SE

Zvyšujte povědomí
Budujte důvěru
Zhodnoťte rizika

JEDNEJTE

Zvolte reakci
Ověřte fakta
Použijte sociální sítě

POUČTE SE

Dokumentujte
Reflektujte
Sdílejte

Jak mohu svou organizaci předem připravit?

Příprava je nejdůležitější součástí každého plánu krizového řízení. Školení vašich spolupracovníků a budování kapacit pro zvládání hrozeb umožňuje v případě nutnosti rychlou a efektivní reakci, což může zmírnit negativní dopady informačních vlivových aktivit. Příprava se skládá ze tří hlavních fází: 1) sdílení informací a zvyšování povědomí, 2) pochopení potenciální zranitelnosti vašeho publika a klíčových stakeholderů vůči informačním vlivovým aktivitám, zároveň budování narativů a příprava oficiálních sdělení vztahujících se k oblastem potenciálních problémů, a 3) provedení analýzy rizik a zranitelností vaší organizace.

Zvyšování povědomí

Prvním krokem v řešení problému je připustit si, že problém existuje. Základním parametrem připravenosti je proto zvyšování povědomí o hrozbách, kterým čelí společnost jako celek, a o slabých místech, která lze považovat za zranitelná v rámci vaší organizace. Nejlepší obranou proti informačním vlivovým aktivitám na celospolečenské úrovni je budování schopnosti zvládat hrozby, a to vytvořením mezisektorových platforem, které leaderům, novinářům, zástupcům sociálních sítích, výzkumníkům, odborníkům v oblasti komunikace a také veřejnosti umožní sdílení znalostí, zkušeností a osvědčených postupů.

Jako odborník v oblasti komunikace ve veřejném sektoru můžete pro zvýšení odolnosti a obranné kapacity vaší organizace udělat několik věcí. Za prvé se můžete v rámci své organizace stát klíčovou kontaktní osobou pro tyto otázky. Je nezbytné diskutovat o této problematice s vedením i komunikovat interně se svými kolegy. Za druhé, po identifikaci potřeb, můžete manažerům a kolegům poskytovat školení a poradenství – tak, aby věděli, jak v případě informačního ovlivňování postupovat. Za třetí, pro sdílení zkušeností a vzájemnou podporu, můžete vytvářet kooperativní sítě s dalšími odborníky vně vaší organizace. Za čtvrté, abyste snížili riziko šíření dezinformací, můžete zvýšit transparentnost a povědomí o činnosti vaší organizace.

Budování důvěry prostřednictvím strategické komunikace

Jedním z cílů informačního ovlivňování je narušení důvěry mezi občany a společenskými institucemi. Proto může být efekt těchto aktivit minimalizován zaměřením se na protiopatření, která budují důvěru ve vaši organizaci. Podpora dobré pověsti a legitimity veřejných institucí je důležitým aspektem každé strategické komunikace.

Předem zformulovaná sdělení

Zformulovat a nechat si schválit vyjádření uprostřed probíhající krize vyžaduje čas. Proto je důležité připravit si předem obecná sdělení, která stvrzují hodnoty vaší organizace a zároveň mohou být snadno přizpůsobena konkrétní události. Stejně jako cílená sdělení k propagaci nové iniciativy nebo produktu mohou být připravená sdělení použita také ke zvýšení povědomí o nepravdivých zprávách a k jejich vyvrácení.

GENERICKÉ ZPRÁVY

Rychlou a precizní reakci na sociálních médiích umožňuje pečlivá příprava. Proto mějte předem připravené, a managementem odsouhlasené, krizové zprávy. Například po teroristickém útoku ve Westminsteru v březnu 2017 poslala metropolitní policie v Londýně svůj první tweet jen sedm minut po události. Tweet poskytl přesné, konkrétní informace o vývoji situace, přestože byl založen na obecné zprávě, předem připravené pro podobné scénáře, která byla rychle přizpůsobena aktuální události.

Při přípravě zpráv je důležité brát v úvahu, jaký je stávající obraz vaší organizace v očích veřejnosti a jakými narativy je tento pohled podporován. Narativy souvisí se způsobem, jakým je vaše organizace vnímána rozdílnými publiky. Napomáhají jednotlivé zprávy k budování žádoucí identity, hodnot a narativů vaší organizace zejména ve vztahu k různým klíčovým publikům? Zprávy, které podporují pozitivní vnímání vaší organizace, mohou hrát klíčovou roli při posilování odolnosti vůči zavádějícím a nepravdivým informacím.

JAKÝ JE VÁŠ PŘÍBĚH?

Zprávy by měly odpovídat zastřešujícímu narativu, který chcete vykreslit.

Silný narativ pramení z jasně stanovených hodnot a cílů vaší organizace.

Analýza a pochopení faktorů, které podporují žádoucí narativy vaší organizace, přináší zároveň odhalení potenciálních bodů zranitelnosti dobré pověsti vaší organizace.

Jakýkoli útok je nejlépe kompenzován prosazováním hodnot, které vaše organizace zastává.

Klíčová publika

Jasné stanovení základních hodnot, poslání a žádoucích narativů vaší organizace je podstatou pochopení vašich zranitelností a toho, kteří stakeholdeři jsou nejvíce ohroženi informačním ovlivňováním. Tyto skupiny by měly být v případě výskytu informační vlivové kampaně osloveny jako první.

Jako profesionální komunikátor již máte zkušenosti s prováděním analýzy cílového publika. Zde je rozdíl jen v tom, že se ptáte, které publikum je nejvíce ohroženo informačním ovlivňováním a proč. Určete, které oblasti činností vaší organizace budou s největší pravděpodobností vystaveny informačním vlivovým operacím a zvažte, jaký typ škodlivých zpráv na ně může mít nejzávažnější dopad. Po zmapování situace můžete zpracovat doporučení ohledně toho, jak přistoupit k preventivnímu informování a prosazování vašeho narativu u klíčového publika.

ANALÝZA CÍLOVÉHO PUBLIKA

Vaše cílové publikum neexistuje ve vakuu

Je dynamicky utvářeno vzájemnou interakcí lidí, kteří sdílejí stejná přesvědčení, názory a zájmy. Je důležité pochopit, co jednotlivce tvořící cílová publika navzájem spojuje.

Identifikujte své stakeholdery

Informační vlivové aktivity nemusí být nutně zaměřeny přímo na vaši organizaci, ale mohou mít v hledáčku jiné cílové skupiny, které jsou s vámi spojeny. Nejvíce postižené mohou být nejzranitelnější skupiny společnosti. Je důležité si uvědomit, které cílové skupiny jsou ohroženy, a posoudit jejich zranitelnost v rámci různých narativů.

Budujte klíčové narativy

Zvažte, které narativy mohou být použity k potlačení vlivových aktivit. Jak se mohou tyto narativy dostat ke zranitelným cílovým skupinám? Najděte komunikátory s vysokou důvěryhodností, kteří mohou sloužit jako prostředníci k případnému oslovení těchto skupin.

Účelem analýzy cílového publika je vyvinout komunikační nástroje, které mohou být použity, pokud budete vystaveni působení informačních vlivových aktivit. Tímto způsobem vlastně vytváříte krizový záložní plán, který může být později přizpůsoben konkrétním vlivovým kampaním snažícím se o poškození vaší pověsti.

Zde diskutovaná protiopatření mají pomoci obnovit důvěru co nejrychleji a nejúčinněji. Zahrnují připravené zprávy a narativy, které mohou být směrovány k různým cílovým skupinám vně i uvnitř vaší organizace. Abyste mohli komunikaci připravit, musíte nejprve pochopit, jakým způsobem mohou být různá publika ovlivněna dezinformacemi, a jak nejlépe navrhovat zprávy pro jednotlivé cílové skupiny.

Rizika a zranitelnosti vaší organizace

Kromě výše uvedeného by měla vaše organizace provést formální posouzení toho, jak mohou informační vlivové aktivity narušit její schopnost plnit své poslání. Veřejné instituce obvykle zahrnují analýzy rizik a zranitelnosti do strategického a krizového plánování. Hrozby plynoucí z infomačních vlivových operací by měly být do stávajících analýz doplněny. Je třeba zaměřit se především na zranitelné zainteresované/cílové skupiny, klíčové hodnoty, poslání a narativy, a na celková rizika ohrožení hlavních činností vaší organizace.

ANALÝZA RIZIK A ZRANITELNOSTI

1: Výchozí stav
Jakou roli má vaše organizace a jaké jsou její povinnosti?
Jaké metody lze použít k identifikaci a vyhodnocení rizik a hrozeb?
Jaké rámce či hlediska použijete ve své analýze?

2: Zhodnocení rizik
Jaké potenciální hrozby a rizika existují?
Jaká je pravděpodobnost těchto událostí a jaké jsou jejich možné důsledky?
Jaké situace by měly být posouzeny s ohledem na možnosti krizového řízení vaší organizace?
Jaká preventivní opatření by měla být přijata?

3: Zhodnocení zranitelnosti
Jaký vliv mohou mít různé scénáře na vaši organizaci?
Jaké jsou potenciální dopady informačních vlivových aktivit na vaši organizaci, a jak můžete tyto konsekvence zvládat, čelit jim a vzpamatovat se z nich?

4: Krizový management
Co byste měli udělat, pokud jsou identifikovány informační vlivové operace?
Příklady viz níže.

Jakým způsobem zvolím odpovídající reakci?

Na informační vlivové aktivity neexistuje jedna univerzální reakce. Jak již tato příručka ukázala, informační vlivové aktivity bývají velmi rozdílné. Vaše organizace navíc funguje za konkrétních podmínek a má svá specifická slabá místa. Díky důkladné přípravě můžete vytvořit obecný, pro vaši organizaci vhodný, rámec protiopatření, která mohou být dodatečně přizpůsobena různým situacím. Abyste v roli komunikátora zvolili nejlepší reakci na různé situace, postupujte s vědomím očekávání, jež jsou na vás kladena, a mandátu, který jste dostali od vedení vaší organizace.

Zhodnotit, informovat, obhajovat nebo bránit?

Vhodná odezva musí být přiměřená hrozbě. Navrhujeme čtyři stupně reakcí, z nichž každá se skládá z řady komunikačních technik.

Reakce fakty: V první fázi reakce je nutné **zhodnotit** situaci. Jedná se o neutrální odezvu, která signalizuje, že jste si dané záležitosti vědomi a zjišťujete fakta. Druhou fází je **informovat** veřejnost a klíčové stakeholdery o situaci a o způsobu, jakým ji vaše organizace vidí. Tato odezva již není zcela neutrální, nýbrž nastiňuje, jaká jsou z vašeho pohledu relevantní fakta. Tyto dva stupně jsou stavebními kameny jakékoli další racionální a na faktech založené reakce, a mohou být aplikovány na většinu podezřelých informačních aktivit.

Reakce obhajobou: Třetí fáze zahrnuje komunikativní akce, jejichž cílem je **obhajovat** určitou pozici. To znamená, že budete aktivně hájit svůj postoj, včetně použití metod přesvědčování a public relations, tak, abyste kladli odpor škodlivému vlivu, například dezinformacím. Čtvrtou fází je aktivně **bránit** svou organizaci tím, že podniknete konkrétní kroky proti agresorovi. Tyto způsoby odezvy jsou základem reakce obhajobou. Mohou být v mnoha případech namístě, používejte je však vždy s opatrností a v závislosti na závažnosti situace.

Reakce fakty

První dvě fáze v boji proti vlivovým aktivitám se týkají zhodnocení a informování. Jsou použitelné pro většinu situací a představují odezvu založenou na faktech.

Příklady uvedené níže jsou návrhy, jak v jednotlivých fázích reagovat.

FÁZE 1: ZHODNOCENÍ

Abyste pochopili, čemu vlastně čelíte, musíte situaci vyhodnotit. Co se doopravdy děje? Kdo je zapojen? Co je v sázce? Čím více informací o situaci zjistíte, tím lepší bude vaše reakce.

ZMAPUJTE SITUACI

Analyzujte situaci a snažte se pochopit maximum o tom, co se děje. Použijte nástroje popsané v částech I. a II., abyste zjistili, čemu čelíte.

OVĚŘTE FAKTA

Ověřte si fakta týkající se situace. Jsou pravdivá/korektní?

ZAJISTĚTE TRANSPARENTNOST

Pro zajištění transparentnosti zapojte do analýzy situace spolehlivé a nezávislé subjekty, jako jsou např. novináři.

FÁZE 2: INFORMOVÁNÍ

Po dokončení fáze zhodnocení můžete začít komunikovat s cílovými publiky. Soustřeďte se na poskytování neutrálních informací a faktů, a dejte lidem vědět, jak situaci řešíte. Nezapomeňte své zprávy přizpůsobit různým skupinám příjemců/stakeholderů.

UČIŇTE PROHLÁŠENÍ

V neutrálním tónu předložte fakta případu tak, jak je vidíte z vašeho pohledu.

KORIGUJTE

V prohlášení přímo reagujte na falešná obvinění a uveďte je na pravou míru. Může být přínosné použít výčet faktů v FAQ stylu.

ODKAŽTE SE

V některých případech může být užitečné odkázat se na nezávislé zdroje nebo aktéry, kteří mohou potvrdit vámi uváděná fakta a tak posílit vaši pozici.

POTVRĎTE HODNOTY

Připomeňte svému cílovému publiku hodnoty, které vaše organizace zastává.

UPOZORNĚTE STAKEHOLDERY

Čím dříve dáte kolegům a klíčovým stakeholderům vědět, co se děje, tím lépe.

VYDEJTE PROZATÍMNÍ VYJÁDŘENÍ

Vydáním prozatímního prohlášení sdělte, že situaci analyzujete. To vám poskytne čas na přípravu konkrétnější reakce.

Reakce obhajobou

Třetí a čtvrtá fáze patří obhajobě a obraně. Tyto kroky představují opatření, která jsou vhodná pouze v závažných situacích, kdy byla jasně identifikována informační vlivová kampaň. Společně představují odezvu založenou na defenzivě.

Příklady uvedené níže jsou návrhy, jak v jednotlivých fázích reagovat.

FÁZE 3: OBHAJOBA

Obhajoba zachází o krok dále než prosté neutrální informování. Představuje aktivnější zdůvodňování vašeho postoje. Při formulování odezvy vždy zvažte svůj mandát, berte v úvahu hodnoty vaší organizace a mějte na paměti postupy dobré komunikační praxe.

DIALOG

Aktivně komunikujte s klíčovými stakeholdery a veřejností, aby byli součástí řešení problému.

FACILITACE

Podpořte toky informací ke klíčovému publiku. Uspořádejte akce nebo setkání, které nabídnou zúčastněným stranám prostor k diskusi o konkrétním problému a vám poskytnou příležitost objasnit vaši pozici.

SPOLUPRÁCE

Spolupracujte s klíčovými komunikátory, kteří vám mohou pomoci šířit zprávu směrem k příslušným publikům.

PŘÍLEŽITOSTI

Využijte stávající události, iniciativy nebo debaty k podpoře vaší pozice.

DOKUMENTACE

Shromážděte dokumentaci, která popisuje průběh událostí a uvádí skutečnosti potvrzující vaši pozici. Je velmi důležité, aby byla tato dokumentace založena na faktech a ověřených informacích.

KONTEXT

Prezentujte událost v širším kontextu, například v rámci narativu vaší organizace a jejích hodnot. To stvrdí vaši pozici a pomůže cílovému publiku pochopit situaci.

FÁZE 4: OBRANA

Obrana zahrnuje návrh přímé reakce na agresora. Tento stupeň odezvy může být kontroverzní, proto by měl být vyhrazen pro extrémní případy. Než v této fázi podniknete jakékoli kroky, prodiskutujte je nejprve s kolegy a vedením, abyste se vyhnuli překročení svých pravomocí a nedošlo ke zhoršení situace.

IGNORACE

Někdy je nejlepší reakcí nedělat nic. Pokud bylo jednoznačně identifikováno informační ovlivňování, avšak nevzbudilo velkou pozornost, je mlčení vhodným postupem. V opačném případě by aktivní reakce mohla dezinformace zbytečně dále šířit.

NAHLÁŠENÍ

Pokud útočník porušil zákon nebo kodex chování sociální platformy, oznamte tuto skutečnost policii nebo dané platformě. Takové řešení by nemělo být bráno na lehkou váhu nebo dokonce zneužíváno. Aby nedocházelo k tlumení veřejné debaty, použijte ho pouze v případě jasného porušení pravidel.

BLOKACE

Komunikátoři by měli respektovat právo na vlastní názor a svobodu projevu! Pokud uživatel porušuje pravidla, je oprávněné blokovat mu přístup na danou platformu. Každý takový případ by však měl být jasně odůvodněn na základě kodexu chování dané platformy.

ODHALENÍ

Ačkoliv to není obecně doporučováno, strategickou reakcí na informační vlivové operace může být odhalení útočníka, skrytého např. za podvodým účtem. Opět, tento postup neberte na lehkou váhu. Nejdříve proveďte řádnou analýzu důsledků, které by zveřejnění aktéra mohlo mít pro vaši organizaci, stakeholdery a také pro samotnou osobu, jejíž identita bude odhalena.

Volba nejvhodnějšího stupně odezvy se odvíjí od posouzení závažnosti situace. Pokud máte zatím pouze podezření na výskyt informačních vlivových aktivit, budou se nejvhodnější reakce rekrutovat z prvních dvou fází – tj. **zhodnocení** situace a neutrálního **informování** veřejnosti. Toto je *faktická odezva*. V případě agresivnějších vlivových operací kombinujte faktickou odezvu s více asertivní třetí a čtvrtou fází – tj. **obhajobou** vaší pozice a **obranou** organizace proti útoku. Toto je *defenzivní reakce*. V těchto fázích však postupujte opatrně. Ujistěte se, že máte od svého vedení jasný mandát, a že vaše reakce není v rozporu s principy demokracie, svobodou projevu ani s dalšími relevantními předpisy a kodexy chování.

Reakce fakty a její další rozvoj

Nejdůležitějším aspektem prvních dvou úrovní odezvy je, že vaše komunikace musí být v neutrálním tónu a založená na faktech. To jsou dva parametry, které definují faktickou reakci. Reakce obhajobou by měla být považována za nadstavbu, která vždy vychází z neopomenutelné primární, faktické odezvy. Pokud nezasáhnete proti šíření nekorektních informací, může to vytvářet dojem, že vaše organizace, její poslání nebo cílové publikum jsou postaveny na omylech a nepravdách. Proto musí být vždy první reakcí vyhodnocení situace a informování klíčových cílových publik.

Abyste mohli odpovídajícím způsobem verifikovat fakta, musíte nejprve dezinformace identifikovat a pochopit, jak vaši organici ovlivňují, a jak mohou narušit její aktivity. Kdo dezinformace šíří? Jak dalece již byly rozšířeny? Kterých témat se týkají? Jedním z přístupů je zaměřit se na články obsahující citace představitelů vaší organizace, relevantní materiály, které se staly virálními online nebo veřejná tvrzení o vaší organizaci a její oblasti působnosti. Fakta shromažďujte systematicky, abyste mohli vyhodnotit otázky spadající do vaší kompetence.

Zhodnocení situace

- [x] Shromážděte názory nezaujatých odborníků a/nebo data z relevantních a důvěryhodných zdrojů.
- [x] Vyžádejte si další informace od osoby/organizace, která je původcem tvrzení.
- [x] Najděte původní zdroj falešných údajů.

Pokud jsou informace považovány za nepravdivé, je vhodné zajistit, aby byly uvedeny na pravou míru. Mnozí odborníci se domnívají, že dezinformacím lze nejlépe čelit informacemi přesnými. Někteří však tvrdí, že tímto způsobem je možné oslovit pouze ty, kteří mají zájem o nalezení pravdy. Vaše předchozí práce na cílových skupinách a narativech by vám měla pomoci určit, jak reagovat v různých případech.

Pokud máte oprávnění a mandát k vytvoření přesvědčivé reakce obhajobou, měla by být založena na výstupech z reakce faktické.

Příprava reakce fakty

- [x] Od autora/vydavatele lživé informace požadujte dementování nebo opravu zprávy.
- [x] Sestavte stručný document se základními fakty, který lze snadno sdílet online.
- [x] V rámci vaší komunikace se vyhýbejte opakování nepravdivé informace.
- [x] Mějte na paměti, že není nutné opravovat každou nepravdivou informaci.
- [x] Zpochybňujte premisu debaty, ne jen její obsah.
- [x] Zvažte zapojení se do dialogu jako doplněk/alternativu vámi připravené komunikace.

Specifika sociálních sítí

Sociální sítě nejsou jen platformy pro snadnou vzájemnou komunikaci mnoha uživatelů, ale mohou být také využívány jako nástroj informačního ovlivňování. Pokud chtějí tomuto vlivu uživatelé úspěšně čelit, musí pochopit a respektovat specifickou logiku, na níž jsou sociální média založena.

Zjistit, kdo stojí za účtem na sociální síti a odkud získává informace, může být obtížné. Jednotlivci, fóra a skupiny mohou lživě tvrdit, že reprezentují veřejné mínění. Sociální sítě představují komplikované informační kanály, protože informace se v nich mohou šířit velmi rychle, čemuž napomáhají i prvky jako jsou tagy, notifikace, odkazy a přílohy. Typický příspěvek na sociální síti bude obsahovat minimálně jeden z těchto prvků, které společně přispívají k začlenění příspěvku do sítě jiných účtů, myšlenek a diskusí. Každý příspěvek tedy může být považován za součást jedné nebo hned několika probíhajících online konverzací.

TAGY

představují vyhledávací termín (štítek), kterým je příspěvek označen. Tagy mají vliv na šíření a dosah příspěvku.

NOTIFIKACE

slouží k propojení na účet organizace či jednotlivce, za účelem distribuce oznámení o nových, profilově specifických, příspěvcích.

ODKAZY

poskytují propojení na další obsah. Podoba linku je často zkrácena, takže plné URL není viditelné.

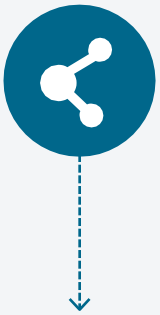
PŘÍLOHY

příspěvků obsahují multimediální soubory, jako např. fotografie nebo videa. Je nutné si uvědomit, že mohou změnit význam nebo vyznění příspěvku, neměly by tedy být přehlíženy.

Proaktivní působení na sociálních médiích zahrnuje budování sítí a vytváření hashtagů, jejichž existence organizaci umožní oslovit svými příspěvky správné cílové skupiny. Generické krizové posty mohou být připraveny a schváleny předem, což zajistí rychlou reakci v případě nepředvídané události. Sociální média také umožňují organizaci, aby v reálném čase odhalila potenciální ohrožení své pověsti. Proto se jedná o významný nástroj prosazování dialogu a spolupráce, a zároveň o otevřený analytický nástroj k pochopení důležitých trendů.

Potlačování vlivových aktivit na sociálních sítích

Výše uvedené čtyři stupně odezvy představují obecný přístup k boji proti vlivovým aktivitám. Níže uvedený příklad ilustruje, jak můžete tuto metodu využít k potlačení informačního ovlivňování na sociálních sítích.



ZHODNOCENÍ

Zhodnoťte situaci s využitím svých vědomostí o informačních vlivových kampaních. Jedná se o případ vlivových aktivit nebo pouze o angažované uživatele, kteří diskutují? Máte-li podezření na nelegitimní vliv, zmapujte situaci co nejpřesněji. Kteří uživatelé s vámi komunikují? Jsou to nepřátelští aktéři nebo reagují na provokaci? Jaké jsou používány hashtagy? Jsou připojeny nějaké odkazy nebo obrazové materiály? Rychlé posouzení situace vám umožní určit nejlepší postup.

INFORMOVÁNÍ

Na základě závěrů zhodnocení zformulujte sdělení. Pečlivě zvažte, které uživatele, hashtagy a cílové skupiny zahrnete. Zaměřte se na vyjasnění své pozice a stvrzení hodnot organizace. Komunikujte prostřednictvím vhodných a zavedených kanálů.

OBHAJOBA

Pokud je v dané situaci vhodné přejít na úroveň obhajoby, použijte důraznější komunikaci. Obhajujte svou pozici pomocí dostupných nástrojů, například s využitím připravených zpráv nebo multimédií. Abyste působili na větší angažovanost cílového publika v dané problematice, může být v této fázi vhodné zapojit se do debaty aktivněji. To znamená komunikovat přímo s uživateli a zapojit je do řešení problému.

OBRANA

Dosáhla situace bodu, kdy je produktivní dialog nemožný a legitimní zprávy jsou vytěsňovány spamem a nepřátelským obsahem? V závislosti na organizačních pokynech a kodexu chování daného sociálního média můžete mít právo určité uživatele blokovat nebo ignorovat. Před tím, než přikročíte k činům, zkonzultujte věc se svým vedením! Svoboda projevu je jednou ze základních hodnot naší společnosti a vždy bychom měli dělat vše, co je v našich silách, abychom udrželi svobodný, otevřený demokratický dialog. Pokud se rozhodnete zablokovat nebo ignorovat uživatele, buďte zcela transparentní ohledně důvodu vašeho rozhodnutí.

Jak zajistím poučení se z proběhlé situace?

Je velmi důležité shromažďovat a evidovat proběhlé případy informačních vlivových aktivit, aby se stále prohlubovalo vaše porozumění tomuto problému. Kromě toho je pro stanovení postupů nejlepší praxe ve vaší organizaci nezbytné dokumentovat použité reakce a posoudit jejich úspěšnost při dosahování požadovaného efektu. Vytvořte záznam událostí tak, jak se vyvíjely, a navrhněte proaktivní postupy pro případné budoucí útoky. Můžete také vytvořit školicí materiály, které zefektivní přístup vaší organizace a v obecné rovině budou přispívat ke společenské připravenosti. Sdílejte znalosti a zkušenosti s komunikátory v podobných funkcích, s veřejnými orgány pověřenými identifikací informačních vlivových aktivit (např. MSB ve Švédsku, *pozn. překladatele: v ČR v oblasti vnitřní bezpečnosti např. Centrum proti terorismu a hybridním hrozbám Ministerstva vnitra*) a v některých případech i s veřejností.

Na následující stránce uvádíme příklady okruhů informací, které byste měli dokumentovat v případech podezření na informační ovlivňování:

Poučení

DOKUMENTACE

- [x] Popište pozadí, vývoj a kontext události.
- [x] Kteří aktéři a sítě byli zapojeni? (Pokud nevíte, vyhněte se spekulacím.)
- [x] Jaké příznaky informačních vlivových aktivit jste zaznamenali?
- [x] Která zranitelná místa byla využita?
- [x] Jaké vlivové techniky byly použity? Které cílové skupiny a narativy byly využity?
- [x] Zapadá případ do širšího schématu operací?

REFLEXE

- [x] Jaké podle vás byly zamýšlené účinky? Na čem zakládáte své hodnocení?
- [x] Jak jste jednali? Reflektujte učiněné kroky a volby možností.
- [x] Co by se stalo, pokud byste nejednali tak, jak jste jednali?
- [x] Jaký efekt měly vaše reakce?
- [x] Co jste udělali dobře a co byste bývali udělali jinak?
- [x] Jak jste se z této zkušenosti poučili?

SDÍLENÍ

- [x] Zdokumentovali jste důkazy a data týkající se případu?
- [x] Diskutujte o informačních vlivových aktivitách s kolegy a vedením vaší organizace a sdílejte své zkušenosti.
- [x] Udržujte pravidelný kontakt s kolegy, kteří se zabývají podobnými otázkami ve vaší organizaci i v dalších organizacích.
- [x] Prostřednictvím porad a vzdělávacích akcí se podělte o své odborné znalosti a zkušenosti s ostatními, a to jak ve vaší organizaci, tak s ostatními kolegy.

Strategická úvaha

Jakýkoli pokus o potlačení vlivových aktivit je omezen skutečností, že reagujete na jednání někoho jiného. Prvotní podmínky nastavuje agresor, což činí boj proti informačním vlivovým operacím problematický. Není neobvyklé nabýt dojmu, že útočník jedná a vy až následně reagujete, takže jste vždy o krok pozadu za nejnovějšími pokusy využít našich společenských zranitelností.

Proto dává větší smysl zaměřit se na podporování demokratických hodnot, jako je otevřená diskuse a svoboda projevu. Vaším úkolem je, v kontextu činnosti vaší organizace, chránit proces nezávislého utváření názorů tím, že minimalizujete rizika plynoucí ze zranitelností mediálního systému, procesů tvorby veřejného mínění a způsobů lidského uvažování. Je tedy důležité, abyste vycházeli ze strategické, vyvážené a fakty podložené pozice.

Stojí za to zopakovat, že snahy čelit informačním vlivovým aktivitám by nikdy neměly tlumit veřejnou diskusi. To by bylo kontraproduktivní a vedlo by pouze k další polarizaci a narušování principů, na nichž je naše společnost založena. Otevřená a demokratická debata musí být vždy chráněna a podporována.

- [x] Zvyšte odolnost vůči informačním vlivovým aktivitám přípravou a zlepšováním povědomí.
- [x] Rozvíjejte proaktivní, přiměřené a rozumné metody komunikace, které se zaměřují na cílové publikum (spíše než na protivníka) a hájí hodnoty, které sdílíme.
- [x] Udržujte faktickou rovinu odezvy, kterou lze za určitých okolností rozvinout do defenzivní reakce.
- [x] Sdílejte postupy dobré praxe a učte se od sebe navzájem.
- [x] Buďte ostražití, ale ne paranoidní!

Slovníček pojmů

Bot – počítačový program, který provádí automatizované, opakované úlohy.

Dezinformace – záměrně nepravdivé nebo zavádějící informace, šířené za účelem manipulace osob k přijetí názorů či chování, které vyhovuje tvůrci těchto informací.

Falešná média – podvodné zpravodajské entity (servery) imitující jejich skutečné předlohy.

Hacking – využití slabin systému k překonání bezpečnostní bariéry a získání neoprávněného přístupu k počítači nebo síti.

Komnata ozvěn/sociální bublina – přirozeně utvářená skupina lidí, kteří sdílejí stejné názory a postoje, a kteří komunikují především v rámci této skupiny (v online i offline prostředí).

Mem – jednotka kulturní informace (idejí, symbolů nebo konceptů), která se šíří z člověka na člověka. Kulturní obdoba genu, schopná se replikovat, mutovat a reagovat na selekční tlaky. Termín poprvé použil Richard Dawkins v roce 1976. Memy mohou být vizuální materiály, fráze, koncepty nebo určité počínání, často humorného charakteru. Jsou primárně šířeny přes internet prostřednictvím sociálních sítí.

Phishing – oklamání uživatelů internetu za účelem získání jejich přístupových hesel nebo jiných citlivých informací.

Potěmkinovy vesnice – falešné společnosti, výzkumné instituce nebo think-tanky, vytvořené za účelem dodání důvěryhodnosti dezinformacím.

Shill – nezávislým dojmem působící mluvčí, který však ve skutečnosti jedná na základě spolupráce (i placené) s někým jiným.

Slaměný panák – taktika zkreslování názorů oponenta a jejich následné vyvracení – argumentační faul.

Sockpuppet účet – podvodný účet na sociální síti, sloužící k anonymnímu rozdmýchávání kontroverze v on-line debatách. Často šíří extrémní názory. Běžnou praxí je i používání více sockpuppet účtů k imitaci obou stran debaty.

Spirála mlčení – psychologický jev, kdy lidé, jejichž názor je nepopulární, raději mlčí, protože se bojí izolace nebo zesměšňování. Čím méně představitelé názorové menšiny sdílí své postoje, tím méně je budou sdílet i ostatní, kteří tyto názory také zastávají.

Stádový efekt – psychologický jev, kdy se lidé chovají určitým způsobem primárně proto, že se tak chovají ostatní. Lidé, kteří se domnívají, že patří k většině, sdílí své názory a projevují své chování s větší ochotou. Čím více jsou myšlenky a trendy obecně akceptovány, tím snadněji se dále šíří.

Strategický narativ – působivý příběh reprezentující náš způsob myšlení a jednání, který je koncipován jako komunikační podpora konkrétního záměru.

Symbolický akt – akt vykonaný primárně s cílem sdělit určitou zprávu, přičemž jakékoli jiné praktické důsledky tohoto jednání jsou podružné.

Temná reklama – reklamy nebo příspěvky s přizpůsobeným obsahem, vytvořeným prostřednictvím psychografického profilování, zobrazované pouze vybraným členům cílové demografické skupiny za účelem ovlivnění jejich názorů nebo chování.

Whataboutismus – taktika odražení kritiky vyvozením falešného srovnání s nesouvisejícím problémem – argumentační faul.

Další literatura

Tato příručka vychází ze zprávy *Countering Information Influence Activities: The State of the Art* – Pamment, Nothhaft, Twetman a Fjällhed, 2018, kterou můžete nalézt na stránkách MSB https:/www.msb.se

Vaší pozornosti doporučujeme také následující zprávy a články:

Debunking handbook
John Cook a Stephan Lewandowsky, 2012

Alternativa fakta – om kunskapen och dess fiender
Åsa Wikforss, 2017

Participatory propaganda: the engagement of audiences in spread of persuasive communications
Alicia Wanless a Michael Berk, 2018

Theoretical Fondations of Influence Operations: a review of relevant psychological research
Björn Palmertz pro MSB, n.d.

The Russian 'Firehose of falsehood' Propaganda Model – why it might work and options to counter it
Christopher Paul a Miriam Matthews pro RAND, 2016

Informace a další příklady můžete čerpat také z následujících mezinárodních zdrojů:

EU vs Disinfo
www.euvsdisinfo.eu

The European Center of Excellence for Countering Hybrid Threats
www.hybridcoe.fi

NATO Strategic Communications Centre of Excellence
www.stratcomcoe.org

Pozn. překladatele:
Centrum proti terorismu a hybridním hrozbám Ministerstva vnitra ČR
www.mvcr.cz/cthh/

Swedish Civil Contingencies Agency (MSB)
SE-651 81 Karlstad Phone +46 (0)771-240 240 www.msb.se/en
Příručka v anglickém jazyce: Order No. MSB1263 - March 2019 ISBN 978-91-7383-867-2