Swedish Civil Contingencies Agency

Combaterea activităților de influențare a informațiilor

Un manual pentru comunicatori

Combaterea activităților de influențare a informațiilor

Un manual pentru comunicatori

Activități de combatere a influenței informaționale – Un manual pentru comunicatori Agenția suedeză pentru contingențe civile (MSB)

Aspect: Advant

Număr comandă: MSB1263 – martie 2019 ISBN: 978-91-7383-867-2

Această publicație este disponibilă și în limba suedeză
Abordarea influenței informaționale – Manual pentru comunicatori
Ordine. Nr: MSB1260 – Revizuit în decembrie 2018 ISBN: 978-91-7383-864-1

Conținut

Prefață

Deteriorarea mediului de securitate a sporit necesitatea ca autoritățile suedeze să devină mai informate cu privire la modul de identificare, înțelegere și contracarare a activităților de influențare a informațiilor. Campaniile de influență au devenit din ce în ce mai sofisticate și pot fi folosite pe timp de pace și război. Acest lucru afectează rolul și responsabilitățile autorităților noastre guvernamentale.

Activitățile de influențare a informațiilor pot perturba modul în care funcționează societatea noastră prin exploatarea vulnerabilităților și contestarea valorilor fundamentale pentru modul nostru de viață, cum ar fi democrația, statul de drept și drepturile omului – punând în cele din urmă în pericol viața și sănătatea oamenilor noștri. Protejarea dialogului democratic – dreptul la dezbatere deschisă, dreptul de a ajunge la propriile opinii în mod liber și dreptul la libera exprimare – este esențială pe măsură ce lucrăm pentru a pune o bază solidă a rezilienței sociale pentru a contracara activitățile de influență informațională.

Guvernul suedez a decis că funcționarii noștri publici ar trebui să fie capabili să identifice și să contracareze activitățile de influențare a informațiilor și să neutralizeze campaniile de propagandă. Agenția suedeză pentru contingențe civile (MSB) lucrează activ din 2014 pentru a dezvolta capacitatea noastră de a identifica, înțelege și contracara campaniile ostile de influențare a informațiilor. Creșterea gradului de conștientizare a publicului este esențială pentru combaterea influenței informației.

Agențiile responsabile de securitatea noastră națională au exprimat necesitatea unui manual care să descrie principiile și metodele de identificare, înțelegere și contracarare a activităților de influențare a informațiilor. Prin urmare, în colaborare cu cercetătorii de la Universitatea Lund, MSB a produs acest manual, care se adresează în primul rând comunicatorilor care lucrează în administrația publică. Acesta ar trebui considerat material de sprijin pentru situațiile în care o organizație
suspectează că a fost expusă unei campanii de influențare a informațiilor sau că este expusă riscului unui astfel de atac.

Aș dori să mulțumesc Departamentului de Comunicare Strategică de la Universitatea Lund, a cărui cercetare stă la baza manualului. Mulțumiri speciale se îndreaptă și către agențiile și organizațiile care au contribuit la îmbunătățirea acestui manual prin comentariile și experiența lor înțeleaptă, făcându-l o resursă mai utilă.

Dan Eliasson, Director General

Introducere

Introducere

Acest manual a fost creat ca răspuns la deteriorarea situației de securitate din lumea de astăzi. Anexarea ilegală a Crimeei și conflictul din Ucraina au arătat cum amenințările la adresa securității de astăzi pot avea un caracter radical diferit de ceea ce asociem de obicei cu conflictul internațional. În acest tip de conflict, actorii folosesc în general alte mijloace decât cele militare pentru a-și atinge obiectivele.

Acest nou tip de amenințare la adresa securității se numește campanie de influență. Puterile străine folosesc campanii de influență pentru a exploata vulnerabilitățile societății pentru a-și atinge obiectivele fără forță militară. Trebuie să ne apărăm împotriva acestui fenomen pentru a proteja securitatea națională a Suediei – inclusiv viața și sănătatea poporului nostru, funcționarea societății și capacitatea noastră de a păstra valori fundamentale precum democrația, statul de drept, drepturile omului și alte libertăți fundamentale.

MSB definește "campania de influență" ca fiind un ansamblu de activități coordonate de o putere străină care implică promovarea unor informații înșelătoare sau inexacte sau a altor acțiuni special adaptate menite să influențeze deciziile politicienilor sau ale altor factori de decizie publici suedezi, opiniile întregii populații suedeze sau ale unei părți a acesteia, precum și opiniile sau deciziile luate în alte țări care ar putea aduce atingere suveranității Suediei; securitate sau alte interese.

O campanie de influență constă într-o serie de activități de influență, dintre care una este influența informațională. Acest manual vă va ajuta ca comunicator să deveniți mai conștienți de ce sunt activitățile de influențare a informațiilor, astfel încât să puteți identifica și contracara mai ușor acest tip de amenințare la adresa securității.

Folosirea informațiilor pentru a-i influența pe ceilalți nu este nimic nou. Domenii precum relațiile publice și publicitatea utilizează informații direcționate pentru a influența deciziile personale ale oamenilor din întreaga lume în fiecare zi – pentru a cumpăra un anumit brand sau pentru a sprijini un anumit candidat politic. În calitate de cetățeni, ne așteptăm ca o astfel de comunicare să respecte anumite reguli. De exemplu, comunicarea ar trebui să aibă loc în mod deschis, să se bazeze pe informații veridice și exacte și să fie prezentată astfel încât să ne permită să facem alegeri în cunoștință de cauză.

Dar nu toți agenții de influență joacă după aceste reguli. Informațiile pot fi utilizate în secret și în mod înșelător de către puterile străine pentru a submina procesele democratice critice, pentru a controla dialogul public și pentru a influența luarea deciziilor. Acestea sunt ceea ce numim activități de influențare a informațiilor. Există o serie de cazuri din întreaga lume în care au fost identificate astfel de activități de influență, pentru examinare recentele alegeri prezidențiale din SUA (2016) și Franța (2017). Deși acestea sunt acte agresive, ele nu sunt considerate acte de război, chiar dacă uneori sunt descrise ca operând în zona gri dintre război și pace. Activitățile de influență financiară ar trebui considerate ostile, deoarece subminează încrederea publicului în instituțiile sociale importante, izolează comunitățile vulnerabile și contribuie la polarizarea socială și politică.

Societatea noastră este construită pe încredere – pe încrederea publicului în instituțiile noastre sociale și pe încrederea dintre oamenii și comunitățile care alcătuiesc societatea noastră. Încrederea este esențială pentru buna funcționare a democrației. Activitățile de influențare a informațiilor erodează încrederea prin semănarea îndoielii și exploatarea diviziunilor. Atunci când actorii străini folosesc tehnici de influență împotriva unei populații, aceasta poate reprezenta o amenințare la adresa securității naționale. Capacitatea de a menține încrederea și de a răspunde în mod adecvat la activitățile de influențare a informațiilor cu mesaje bazate pe fapte și de încredere este esențială pentru o societate democratică rezilientă și sănătoasă.

Care este rolul comunicatorului?

În calitate de comunicator, aveți ocazia să jucați un rol important în prevenirea, identificarea și contracararea activităților de influențare a informațiilor. Vă ajutați organizația să își respecte promisiunile și să construiască o relație de încredere cu publicul. Comunicați cu publicul țintă, răspundeți la întrebările lor și le oferiți informații vitale. În calitate de comunicator, știi ce gândesc audiențele tale și ce este important pentru ei.

Poate părea puțin probabil, dar într-o zi chiar și organizația dvs. poate deveni o sursă de activități de influențare a informațiilor. De exemplu, puteți descoperi că se răspândesc informații false despre organizația dvs., că a apărut o versiune falsă a site-ului dvs. web sau că conturile dvs. de social media au fost sparte. Publicul țintă al organizației dvs. poate deveni ținta hărțuirii cibernetice, a trollingului sau a dezinformării. Scopul unor astfel de atacuri poate fi subminarea încrederii în organizația dvs., introducerea de informații false sau înșelătoare în dezbateri importante sau creșterea tensiunilor între publicul țintă. În toate aceste cazuri, aveți ocazia să jucați un rol esențial în consolidarea și sprijinirea dezbaterii democratice productive.

DE CE CONTEAZĂ COMUNICATORII?

- Construiești punți între organizația ta și public.
- Aveți deja experiență cu alte forme de comunicare în situații de criză care vor fi relevante atunci când răspundeți la activități de influențare a informațiilor.
- Este posibil să fiți printre primii care întâlnesc activități de influențare a informațiilor pe măsură ce apar.

În calitate de comunicator, aveți deja multe dintre abilitățile necesare pentru a contracara activitățile de influențare a informației. Acest manual oferă informații suplimentare pentru a vă sprijini în această activitate. Veți învăța ce tehnici pot fi folosite împotriva dvs. și cum să identificați semnele de avertizare. Veți primi sfaturi despre cum să vă pregătiți organizația pentru un răspuns rapid și eficient și îndrumări despre cum să alegeți cel mai bun răspuns pentru organizația dvs. pe baza circumstanțelor dvs. unice și a mandatului dvs. de comunicator.

Abordarea noastră

Scopul acestui manual este de a vă crește gradul de conștientizare și înțelegere a campaniilor de influențare a informațiilor și de a vă dezvolta capacitatea de a răspunde. Informațiile prezentate aici vă vor ajuta să recunoașteți mai ușor tehnicile comune de influență și vă vor oferi un set de soluții proactive pe care le puteți utiliza pentru a proiecta cel mai potrivit răspuns. Acest manual nu oferă o soluție universală sau o listă de verificare a pașilor de bifat. Fiecare organizație este diferită, colaborează cu audiențe diferite și se confruntă cu provocări diferite care trebuie luate în considerare atunci când se decide cum să se răspundă cel mai bine.

PART I: BECOMING AWARE OF INFORMATION INFLUENCE

What are information influence activities?

How do they exploit social vulnerabilities?

How are information influence activities different from other forms of communication?

PART II: IDENTIFYING INFORMATION INFLUENCE

What is the purpose of information influence activities?

What are the main information influence techniques?

How can these techniques be combined?

PART III: COUNTERING INFORMATION INFLUENCE

How do I prepare my organisation?

How do I choose an appropriate response?

How do I ensure that lessons are learned?

PARTEA I.

Conștientizarea influenței informaționale

Ce sunt activitățile de influențare a informațiilor? Cum exploatează

PARTEA I. Conștientizarea influenței informaționale

Această secțiune descrie modul în care activitățile de influențare a informațiilor exploatează vulnerabilitățile societății și oferă instrumente pentru evaluarea activității suspecte și identificarea cazurilor de influență a informațiilor.

Ce sunt activitățile de influențare a informațiilor?

Dezbaterea deschisă, diferențele de opinie și încercarea de a convinge sunt caracteristici esențiale ale unei societăți democratice sănătoase. Dar ce se întâmplă atunci când cineva fabrică evi-
Dence, oferă "experți" falși sau aduce argumente înșelătoare în mod deliberat? Astfel de activități sunt dăunătoare pentru societate și problematice pentru procesele democratice care se bazează pe consimțământul informat. Acestea ar trebui să fie întâmpinate cu fapte, critici din surse și un angajament față de interesul public.

Majoritatea țărilor democratice se bucură de o dezbatere politică sănătoasă și vibrantă, în care cetățenii, jurnaliștii, cadrele universitare și reprezentanții societății civile care, dincolo de sarcina importantă de a trage la răspundere factorii de decizie, consideră că este rolul lor să sublinieze cazurile de informații false sau înșelătoare. Actorii statali pot sprijini aceste eforturi prin furnizarea de finanțare în sprijinul unui angajament civil sănătos și prin corectarea inexactităților legate de propria lor activitate. Acest sistem a servit bine democrațiilor liberale timp de secole, cel puțin în teorie. Cu toate acestea, dezbaterile despre știrile false atât de răspândite astăzi sugerează că vulnerabilitățile din sistem sunt acum exploatate într-un mod nou.

Activitățile de influență informațională implică forme potențial dăunătoare de comunicare orchestrate de actori statali străini sau de reprezentanții acestora. Acestea constituie o ingerință deliberată în afacerile interne ale unei țări pentru a crea un climat de neîncredere între un stat și cetățenii săi. Activitățile de influențare a informațiilor sunt folosite pentru a promova interesele unei puteri străine prin exploatarea vulnerabilităților percepute în societate. Actorii statali străini studiază controversele și provocările unei societăți și exploatează aceste vulnerabilități pentru a perturba și polariza.

Activitățile de influențare a informațiilor pot fi desfășurate separat sau pot fi efectuate ca parte a unei campanii de influență mai ample, bazându-se pe un spectru larg de tehnici. În plus față de instrumentele de comunicare, totul, de la sancțiuni diplomatice și economice la demonstrații de forță militară, poate fi folosit pentru a influența societatea.

ANATOMIA UNEI CAMPANII DE INFLUENȚĂ INFORMAȚIONALĂ

Utilizarea tehnicilor de influență
Relațiile publice, marketingul, diplomația, jurnalismul de opinie și lobby-ul sunt exemple de modalități acceptate de influențare a opiniilor și comportamentelor oamenilor. Activitățile de influențare a informațiilor imită aceste forme de implicare, dar folosesc tehnicile în mod înșelător.

Perturbarea dezbaterii publice
Puterile străine folosesc activități de informare pentru a influența acele domenii și dezbateri de care pot beneficia. Acest lucru poate fi realizat atât direct, cât și indirect, prin orice, de la propagandă deschisă la finanțarea ascunsă a grupurilor societății civile. Atunci când actori nelegitimi intervin în dezbaterea publică legitimă, aceasta poate schimba percepția societății asupra opiniilor conducătoare și poate influența procesul decizional.

Acționarea în interes propriu
Activitățile de influență sunt destinate atingerii unor obiective specifice de care beneficiază o putere străină. Obiectivul ar putea fi orice, de la destabilizarea politică a unei societăți, împiedicarea luării unor decizii specifice sau polarizarea unei dezbateri politice.

Exploatarea vulnerabilităților
Toate societățile au provocările lor. Acestea pot fi tensiuni sociale sau de clasă, inegalitate, corupție, probleme de securitate sau alte probleme centrale ale vieții sociale. Puterile străine ostile identifică și exploatează sistematic aceste vulnerabilități pentru a-și atinge obiectivele.

Există o anumită ambiguitate a acestor activități, ceea ce poate face dificilă diferențierea între activitățile de influențare a informațiilor și dezbaterea publică autentică. Dezbaterile politice pot fi sensibile, inconfortabile și uneori chiar urâte. Dar ele fac parte din procesul democratic care se bazează pe o pluralitate de opinii și pe libertatea de a le dezbate. Cu toate acestea, o dezbatere constructivă nu poate avea loc dacă puterile străine ostile introduc informații înșelătoare în mod deliberat pentru a perturba și controla.

Este important să ne amintim că deținerea unor opinii similare cu cele ale unei puteri străine nu face în mod automat acea persoană un agent al acelei puteri străine. **Când vorbim despre activități de influențare a informației, vorbim despre utilizarea sistematică a tehnicilor înșelătoare pentru a submina democrația**. Astfel de încercări de a distruge democrația trebuie contracarate prin protejarea principiilor noastre democratice fundamentale – dezbaterea liberă și deschisă, libertatea de exprimare și dialogul democratic. Acestea ar trebui să fie întotdeauna piatra de temelie a răspunsului nostru la activitățile de influențare a informațiilor, chiar dacă îngreunează sarcina.

Cum sunt exploatate vulnerabilitățile sociale?

Să ne imaginăm că opiniile noastre apar ca rezultat al unui proces rațional: se întâmplă ceva sau o nouă informație iese la lumină. Martori, cercetători, oficiali guvernamentali și alte persoane cu expertiză credibilă interpretează sau explică situația într-un context mai larg. Mass-media preia aceste informații și le răspândește în diverse comunități, online și offline, așa vine la tine. Desigur, în practică poate diferi într-o oarecare măsură, dar în linii mari aceasta este teoria modului în care se formează opiniile într-o societate democratică.

Procesul se bazează pe câteva principii simple: Informațiile despre evenimentul original trebuie să fie autentice și bazate pe fapte. Afirmațiile trebuie verificate de surse credibile, care sunt într-adevăr oameni reali, cu o reputație de pierdut dacă distorsionează adevărul. Mass-media care raportează povestea trebuie să fie echilibrată în prezentarea lor, să verifice de două ori faptele și sursele și să se străduiască să servească interesul public. Comunitățile deliberative cântăresc diferențele de opinie și se angajează în dezbateri productive înainte de a ajunge la concluzii argumentate.

Activitățile de influențare a informației sunt orientate spre exploatarea diferitelor moduri în care idealul deliberării raționale este în contradicție cu realitatea. Actorii ostili folosesc tehnici de influență creative, oportuniste și avansate tehnologic pentru a se insera în acești pași pentru a corupe fluxul de informații. Ei identifică vulnerabilitățile în modul în care ne formăm opiniile, modul în care informațiile critice călătoresc prin peisajul media și modul în care creierul nostru procesează informațiile.

Probele pot fi falsificate sau manipulate, experții pot să nu fie deloc experți, iar martorii pot fi mituiți sau constrânși. Serviciile de știri pot fi conduse ca canale de propagandă unilaterale, iar dezbaterea publică online poate fi purtată între roboți automatizați pentru a crea iluzia unei dezbateri publice pline de viață. Atunci când aceste activități sunt desfășurate în mod deliberat, prin campanii coordonate menite să submineze procesul democratic, nu ne putem baza întotdeauna pe sistem pentru a ne autocorecta. Aici puteți juca un rol important.

Formarea opiniei

INFORMAȚII NOI

Informații noi ajung la noi: un eveniment, o descoperire științifică, o dezvăluire media sau o decizie politică.

EXPERȚI, FUNCȚIONARI ȘI SURSE

Aceste noi informații sunt documentate de martori, experți și oficiali care le explică sau le interpretează pentru alții.

MASS-MEDIA ȘI CULTURĂ

Ziarele, televiziunea, radioul, blogurile și rețelele sociale sunt folosite pentru a comunica mesajul publicului.

PUBLICUL

Informațiile ajung la public și sunt prelucrate atât prin discuții, cât și prin dialoguri între diferite grupuri sociale, atât față în față, cât și pe social media.

TU

Informațiile ajung la tine prin comunitățile din care faci parte și canalele de informare pe care le consumi.

VULNERABILITĂȚI ALE SISTEMULUI MEDIA

Sistemul nostru media modern are o serie de vulnerabilități, în special tehnologiile care evoluează rapid, schimbările modelului de afaceri jurnalistic și proliferarea surselor alternative de știri. Cu totul, de la scrisori falsificate și imagini photoshopate, la algoritmi, roboți și concurența pentru clicuri pe social media, sistemul media este vulnerabil la cei care doresc să-l exploateze în propriul beneficiu – pentru câștiguri politice sau economice sau doar pentru a vedea dacă se poate face.

VULNERABILITĂȚILE OPINIEI PUBLICE

Formarea opiniei publice a fost întotdeauna vulnerabilă la anumite fenomene, cum ar fi dovezile sociale – adică copierea comportamentului altora interpretat ca fiind "corect" sau dezirabil. Dar în mediul informațional de astăzi, unde conturile de social media pot fi falsificate și armate de troli poluează câmpurile de comentarii, este mai ușor ca niciodată să fabrici evadare, să stârnești furie și să provoci indignare. Toate acestea fac ca formarea opiniei publice să fie vulnerabilă la manipularea deliberată.

VULNERABILITĂȚI COGNITIVE

Unele vulnerabilități sunt rezultatul modului în care creierul nostru este conectat: în timp ce noi nu suntem proiectați
Pentru a face față tuturor informațiilor la care suntem expuși în lumea modernă, datele noastre personale pot fi valorificate prin analiză psihografică pentru a ne cunoaște mai bine decât ne cunoaștem pe noi înșine. Estimările sugerează că există până la 800 de puncte de date despre fiecare persoană care utilizează social media, care pot fi folosite pentru a prezice aproape totul despre tine. Activitățile de influențare a informațiilor exploatează tiparele noastre de gândire pentru a exercita influență asupra percepțiilor, comportamentelor și luării deciziilor.

Prin ce diferă activitățile de influențare a informației de alte forme de comunicare?

Nu este rolul comunicatorului să investigheze dacă puterea străină este responsabilă pentru activități specifice de comunicare. Trebuie să acționați numai atunci când suspectați că activitățile de influențare a informațiilor sunt utilizate în legătură cu activitatea pe care o desfășurați sau pentru a submina integritatea dezbaterii publice și securitatea națională a Suediei. Folosește-ți cea mai bună judecată pentru a face o evaluare. Cu alte cuvinte, este important să înțelegeți rolul pe care organizația dvs. îl joacă dintr-o perspectivă socială, într-un context mai larg.

Pentru a identifica cazurile de influență a informațiilor, trebuie să evaluați măsura în care comunicările sunt înșelătoare și sunt destinate să dăuneze și să provoace perturbări. Cântăriți acești factori atunci când luați în considerare o activitate de influență suspectată pentru a lua o decizie în cunoștință de cauză cu privire la modul de construire a răspunsului. Obiectivele și motivațiile din spatele activităților de influență pot să nu fie ușor evidente. Cu toate acestea, cu cât este mai mare numărul de astfel de factori pe care îi identificați, cu atât este mai mare probabilitatea de a avea de-a face cu un caz de influență a informațiilor.

ÎNȘELĂTOARE

Comunicarea fiabilă este deschisă și transparentă. Conținutul este credibil și poate fi verificat. Activitățile de influențare a informațiilor induc în eroare în mod deliberat.

INTENȚIONAT

Comunicarea fiabilă contribuie la o dezbatere constructivă, chiar dacă argumentele sau conținutul pot fi controversate. Activitățile de influențare a informațiilor sunt menite să submineze conversația constructivă și să împiedice dezbaterea deschisă.

PERTURBATOR

Comunicarea fiabilă este un aspect natural al societății noastre care consolidează democrația, deși uneori creează fricțiuni. Activitățile de influențare a informațiilor perturbă dialogul democratic și slăbesc funcționarea societății.

Nu este o coincidență faptul că tehnicile utilizate în activitățile de influență informațională se suprapun adesea cu jurnalismul, afacerile publice, diplomația publică, lobby-ul și relațiile publice – copierea metodelor legitime este una dintre modalitățile de a ascunde activitățile de influențare a informațiilor și de a le face să pară că furnizează informații fiabile. Vă rugăm să rețineți că activitățile ilegale de influență, cum ar fi amenințările, hacking-ul, șantajul și mita, sunt în afara domeniului de aplicare al acestei discuții și ar trebui raportate poliției.

PARTEA II.

Identificarea influenței informaționale

Care este scopul activităților de influențare a informației? Care sunt principalele tehnici de

PARTEA II. Identificarea influenței informaționale

Identificarea activităților de influențare a informațiilor este primul pas spre contracararea acestora. Aceasta înseamnă să știi ce să cauți. În această secțiune, oferim îndrumări pentru evaluarea narațiunilor strategice și a abordărilor de direcționare a publicului, precum și descrieri mai detaliate ale tehnicilor utilizate în activitățile de influență. Apoi discutăm despre modul în care aceste tehnici pot fi combinate pentru a produce efecte sociale negative.

Care este scopul activităților de influențare a informației?

Pentru a identifica cu succes activitățile de influențare a informațiilor, trebuie să fiți conștienți și de narațiunile strategice și grupurile țintă. Conștientizarea de bază a acestor concepte și a semnificației lor vă va ajuta să înțelegeți mai bine și să identificați cazurile suspecte de activități de influențare a informațiilor și vă va oferi o perspectivă asupra posibilei intenții din spatele unei activități.

Narațiuni strategice

Activitățile de influențare a informațiilor implică, de obicei, povestiri de un anumit fel. Portretizarea unui eveniment, a unei probleme, a unei organizații, a unui loc sau a unui grup este, în general, formulată pentru a se încadra într-o narațiune preexistentă. De exemplu, majoritatea oamenilor au auzit de cursa spațială dintre Statele Unite și Uniunea Sovietică în timpul Războiului Rece. Și majoritatea oamenilor știu câte ceva despre cum am trimis oameni pe Lună, precum și zvonurile că aselenizările au fost falsificate. Există un videoclip care arată un
Astronaut plantând un steag pe Lună. În timp ce unii vor lua acest lucru ca dovadă că s-a întâmplat, alții susțin că videoclipul este un fals. Aceste narațiuni sunt tipice pentru "cunoașterea" pe care o folosim inconștient pentru a sorta informații noi. Când auzim povești noi despre călătoriile spațiale, le sortăm în funcție de care dintre aceste narațiuni credem. Atunci când astfel de povești sunt planificate și utilizate în mod deliberat în activități de comunicare, ele sunt cunoscute sub numele de narațiuni strategice.

De exemplu, s-ar putea inventa ceva despre un anumit grup religios sau etnic care să se potrivească cu ceea ce oamenii cred deja despre aceste grupuri, adică narațiunea existentă. Dezinformarea ne poate afecta în trei moduri diferite – prin evidențierea unui aspect al unei narațiuni existente, prin suprimarea unui aspect al acesteia sau prin legarea narațiunii de evenimente fără legătură pentru a distrage atenția.

Identificarea narațiunilor strategice în joc și a logicii din spatele acestora este un pas important în conceperea unui răspuns adecvat. Luați în considerare cele trei abordări de mai jos. Puteți identifica o narațiune strategică care utilizează una dintre aceste abordări?

NARAȚIUNI STRATEGICE

Pozitiv sau constructiv: "Acesta este adevărul!"
Încearcă să stabilească o narațiune coerentă despre o anumită problemă care se potrivește, completează sau extinde narațiunile strategice existente, bine stabilite.

Negativ sau perturbator: "Aceasta este o minciună!"
Încercări de a preveni apariția unei narațiuni coerente sau de a respinge sau submina o narațiune existentă.

Distragerea atenției: "Uită-te aici!"

Distrage atenția de la problemele cheie prin intermediul umorului, meme-urilor sau teoriilor conspirației.

Publicuri țintă

Analiza narațiunilor strategice este o abordare pentru identificarea logicii din spatele unei campanii de influențare a informațiilor. O a doua abordare, conectată, este de a lua în considerare pentru cine rezonează aceste narațiuni strategice – care este publicul țintă? Sunt narațiunile destinate publicului larg sau vizează un anumit grup?
Sunt folosite "volumele mari de date" pentru a viza persoane cu anumite trăsături de personalitate sau sentimente? Dacă are loc o formă de direcționare, se pune accentul pe grupuri sau persoane cu vulnerabilități sau modele de comportament specifice? Înțelegerea persoanelor vizate prin utilizarea narațiunilor este un pas important în evaluarea gravității cazului specific în cauză.

GRUPURI ȚINTĂ

Publicul larg: cel mai larg public posibil
Activitățile de influențare a informațiilor vizează societatea în ansamblu prin alinierea mesajelor la narațiuni larg răspândite.

Direcționarea sociodemografică: grupuri specifice
Prin identificarea audiențelor pe baza factorilor demografici, cum ar fi vârsta, venitul, educația și etnia, mesajele pot fi adaptate pentru a atrage un anumit grup.

Direcționarea psihografică: persoane fizice
Prin analizarea și clasificarea volumelor mari de date, activitățile de influență pot viza persoane cu trăsături specifice de personalitate, preferințe politice, modele de comportament sau alte caracteristici de identificare.

Împreună cu o analiză a narațiunilor strategice și a tehnicilor de comunicare utilizate, analiza publicului țintă poate dezvălui intenția activităților de influențare a informațiilor. Dacă înțelegeți *cine* este vizat și de *ce*, va fi mai ușor să faceți o evaluare rezonabilă a *scopului* activităților de influențare a informațiilor. Acest lucru, la rândul său, vă va ajuta să decideți *ce contramăsuri sunt cele mai potrivite*.

Care sunt principalele tehnici de influențare a informației?

Activitățile de influențare a informațiilor sunt în continuă evoluție. Cu toate acestea, studiind o mare varietate de exemple, am abstractizat șase tehnici comune pe care ar trebui să le căutați. Subtehnicile sunt caracterizate de principii similare în cadrul fiecărui grup. Conștientizarea modului în care arată și funcționează aceste tehnici vă va ajuta să le recunoașteți.

În cele mai multe cazuri, tehnicile sunt neutre – nici bune, nici rele în sine. Acestea pot fi utilizate în moduri deschise și acceptate ca parte naturală a dialogului democratic sau cu o intenție înșelătoare și ostilă, ca parte a unei campanii de influențare a informației. Utilizarea oricărei tehnici nu este neapărat un semn al influenței informației.

Analizați utilizarea acestor tehnici împreună cu o evaluare a narațiunilor strategice și a grupurilor țintă:

- Cât de puternici sunt indicatorii intenției înșelătoare sau perturbatoare?
- Ce sugerează narațiunile strategice și publicul țintă despre scopul comunicărilor?
- Dacă se folosește o tehnică specifică, ar putea fi aceasta dăunătoare publicului sau societății noastre?

Tehnici de influențare a informațiilor

HACKING SOCIAL ȘI COGNITIV
- Anunțuri întunecate
- Efecte Bandwagon
- Spirala tăcerii
- Camere de ecou și bule de filtrare

IDENTITĂȚI ÎNȘELĂTOARE
- Shills
- Impostori și înșelători
- Falsurilor
- Satele Potemkin
- Conținut media fals

EXPLOATARE TEHNICĂ
- Roboţii
- Sockpuppets
- Deepfakes
- Înșelăciune

DEZINFORMARE
- Fabrica
- Manipulare
- Deturnarea
- Satiră și parodie

RETORICĂ RĂU INTENȚIONATĂ
- Ad hominem
- Whataboutism
- Gish-galop
- Om de paie
- Deturnarea

ACȚIUNI SIMBOLICE
- Scurgeri
- Hacking
- Demonstrații publice

Hacking social și cognitiv

Hacking-ul social și cognitiv se referă la activități care exploatează relațiile noastre sociale și procesele de gândire. Este similar cu hacking-ul unui computer în sensul că actori ostili încearcă să păcălească sau să "pirateze" aceste procese prin exploatarea vulnerabilităților. De exemplu, preferăm de obicei să ne potrivim cu ceea ce gândesc și fac oamenii care seamănă cu noi și poate fi dificil să gândim rațional atunci când suntem expuși la materiale încărcate emoțional. Aceste modele previzibile de comportament pot fi exploatate de actori ostili care declanșează în mod deliberat vulnerabilitățile noastre, de exemplu în dezbaterile sociale pe teme sensibile, pentru a-și atinge obiectivele.

ANUNȚURI ÎNTUNECATE

Mesajele adaptate profilului psihografic al unei persoane sunt considerate anunțuri întunecate. Datele culese din social media și din alte surse pot fi organizate într-o bază de date cu persoane cu opinii ideologice și trăsături de personalitate similare. Reclamele care sunt afișate numai anumitor persoane pot include mesaje care fac apel la înclinațiile lor psihologice și încurajează anumite comportamente.

EFECTUL BANDWAGON

Oamenii care simt că aparțin majorității sunt mai predispuși să-și exprime opiniile. Roboții pot crește numărul de aprecieri, comentarii și distribuiri ale unei postări pe rețelele sociale pentru a da impresia de acceptare socială. Acest lucru face apel la nevoia cognitivă de apartenență și facilitează implicarea ulterioară a utilizatorilor umani reali.

SPIRALA TĂCERII

Oamenii care simt că aparțin minorității sunt mai puțin susceptibili să-și exprime opiniile. Contrar efectului de bandwagon, aparența conformității sociale în jurul unei probleme poate determina persoanele cu opinii minoritare să rămână tăcute. Acest lucru se bazează pe teama de a fi exclus sau izolat din cauza unei opinii nepopulare

CAMERE DE ECOU ȘI BULE DE FILTRARE

Subgrupurile organice în care oamenii comunică în primul rând cu alții care dețin opinii și credințe similare se numesc camere de ecou; Ele există atât online, cât și în viața reală. De exemplu, persoanele cu opinii similare sunt susceptibile de a citi aceleași ziare și, mai important, de a socializa între ele. Astfel, ei sunt rareori expuși unor opinii ideologice diferite. Acest lucru poate fi exploatat online pentru a răspândi informații specifice către grupuri specifice.

Identități înșelătoare

Adesea evaluăm credibilitatea informațiilor uitându-ne la sursa lor. Cine comunică cu mine și de ce? Ce știu ei despre această problemă? Sunt ei cine pretind că sunt? Prin imitarea surselor legitime de informații (fie ele persoane, organizații sau platforme), actorii ostili implicați în activități de influențare a informațiilor exploatează "capitalul fiduciar" acumulat de sursele legitime prin utilizarea identităților frauduloase.

SHILLING

A shill is someone who gives the impression of being independent but, in reality, works in partnership with somebody else or receives payment to represent them. Examples include paid reviewers of products on shopping websites, audience members employed to applaud a speaker during a public meeting, or a group of online trolls paid to write negative comments.

IMPOSTERS AND CON-ARTISTS

Imposters pretend to be someone they are not, i.e. they adopt the personal or professional identity of another person. Con-artists claim to have expertise or credentials they lack, e.g. someone who falsely claims to be a medical doctor or a lawyer without having undergone the required training.

COUNTERFEITS

Fabricating official documents is an effective way of making disinformation appear authentic. For example, fake letterheads, stamps, and signatures can be used to produce forged documentation.

POTEMKIN VILLAGES

Malicious actors with sufficient resources can set up fake institutions and networks that serve to deceive and mislead. Potemkin villages are false companies, research institutions, or think tanks created to authenticate or 'legitimise' targeted disinformation.

FAKE MEDIA

Disinformation can also be circulated by creating fake media platforms that look like, or that have a web address similar to, a real news site. It is relatively easy and inexpensive to create a fake website online that looks almost identical to a real website but publishes very different content.

TITLU

Titlurile aspiră să genereze interes și un răspuns din partea cititorului. Continuați să citiți dincolo de titlu pentru a vă asigura că se potrivește cu conținutul articolului.

URL

Imitating well-known platforms to gain legitimacy is a common information influence technique. Make sure you are on the right platform by taking a closer look at the URL.

CONTENT

Assess the content of the text. Is it informative, argumentative, based on facts, emotions, or opinions? Always read the entire text before sharing.

IMAGES

Images do not always reflect reality. Images can be manipulated easily by deleting, editing, or adding elements. They may not even be connected to the story. Use image search to find out if an image has been used before in another context.

SOURCES

If the text refers to other sources, check the links to trace the origin of the information. Assess whether or not it has been used appropriately.

AUTHOR

Be wary of articles with no by-line. If the author is given, consider who that person is and the reason behind the article.

COMENTARII

Comentariile de pe paginile web și din social media provin cel mai adesea de la oameni obișnuiți care își exprimă opiniile. Dar unele comentarii pot fi postate și de troli și roboți. Luați în considerare cine face comentarii.

LOGODNĂ

Doar pentru că un text a fost apreciat sau distribuit foarte mult nu înseamnă că conținutul este corect. Aveți grijă să partajați conținut pur și simplu pe baza aparenței de implicare a altora.

Manipulare tehnică

Activitățile de influențare a informațiilor profită adesea de cele mai noi tehnologii. Actorii răuvoitori utilizează abilități tehnice avansate pentru a manipula fluxurile de informații online prin conturi și algoritmi automatizați sau printr-o combinație de abordări umane și tehnologice. Rețineți că noile tehnici sunt adesea utilizate pentru a efectua activități tradiționale de influențare a informațiilor, cum ar fi crearea de identități înșelătoare sau răspândirea dezinformării. Acesta este un domeniu care se dezvoltă mult mai repede decât capacitatea noastră de a analiza și înțelege potențialele sale utilizări și consecințe. Evoluțiile recente privind "deepfake-urile", învățarea automată și inteligența artificială au fost evidențiate în dezbaterea publică și ne putem aștepta ca astfel de instrumente să fie utilizate din ce în ce mai mult în scopuri de influențare a informațiilor în viitor.

BOTS

Bots are computer programs that perform automated tasks, such as sharing certain types of information on social media or answering FAQs on customer service platforms. However, they can also be used to emphasise particular messages online, to spam discussion forums and comments, to like and share posts on social media, and to implement cyber-attacks.

SOCKPUPPETS

Imposter accounts managed by someone who does not reveal their real identity or intentions are called sockpuppet accounts. Such false identities are used to join online communities and participate in debates to introducing false or controversial information. Two or more sockpuppets can be used in conjunction to artificially simulate both sides of a debate.

DEEPFAKES

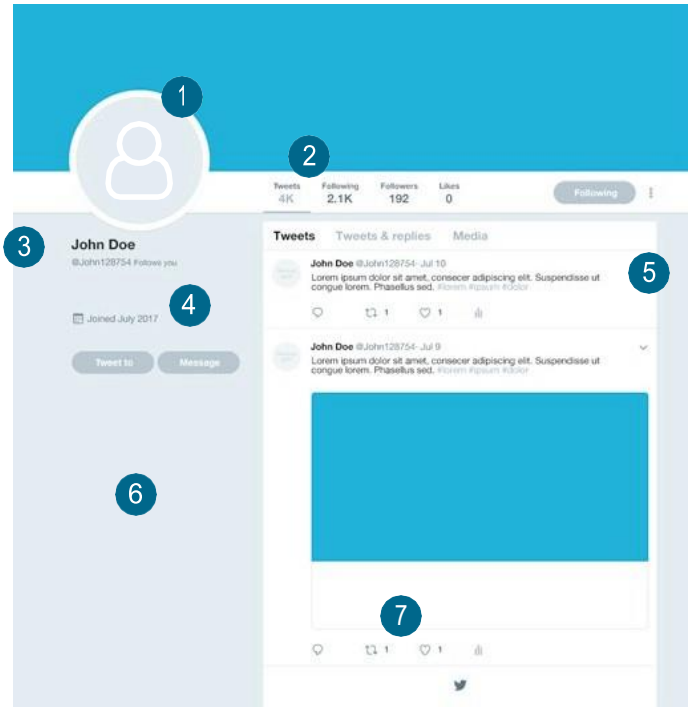
Advanced machine learning algorithms can now be used to manipulate audio and video very convincingly, for example of a real politician delivering a fictitious speech. It is even possible to superimpose the face of another person onto pre-existing video footage and digitally reconstruct a person's voice.

PHISHING

Phishing is a technique that tricks users into revealing their passwords or other sensitive information online. Phishing involves automated spamming of emails that look legitimate but actually lead to fake websites that harvest any personal information entered. Spear Phishing is a more sophisticated type of phishing used to access information on secure computer systems.

Localizați botul

În timp ce roboții sunt instrumente eficiente de influență pe social media, ei sunt, de asemenea, vulnerabili la expunere. Verificarea următoarelor șapte caracteristici vă poate ajuta să identificați un bot online. Dar fiți atenți - diferite tipuri de roboți pot arăta foarte diferit. Roboții imitatori sunt concepuți pentru a arăta ca utilizatori reali. Spam-bots, pe de altă parte, se concentrează pe diseminarea unor volume mari de informații și adesea nu au caracteristici naturale ale utilizatorului.



1 POZĂ DE PROFIL

De obicei, roboții fie nu au o imagine de profil, fie folosesc una furată. Utilizați căutarea de imagini pentru a verifica autenticitatea imaginilor de profil suspecte.

ACTIVITATE

Spamboții tind să fie extrem de activi, generând uneori mai mult de 50 în fiecare zi. Căutați conturi cu un număr suspect de mare de postări pe zi.

NUME

Majoritatea roboților își generează automat numele de utilizator. Numele de utilizator formate din litere și numere aparent aleatorii pot fi roboți.

DATA CREĂRII

Majoritatea conturilor bot sunt create cu un scop și, prin urmare, nu au istoric de utilizator. Uneori, conturile mai vechi sunt sparte și refolosite, eliminând postările vechi.
În consecință, astfel de conturi au decalaje mari între perioadele intense de activitate.

5 LANGUAGE

Bots sometimes use automatic translation to spread messages in multiple languages. This results in obvious grammatical errors or incoherent sentences. Accounts that publish similar content in multiple languages may be bots.

6 INFORMATION

Bot accounts are created to operate anonymously, so they lack personal information, or use fictional or forged information. Verify any information provided.

7 ENGAGEMENT

Review which posts a suspicious account engages with. Bots are often coordinated and reinforce messages spread by other bots. They are not likely to have real followers.

Dezinformare

Dezinformarea se referă la informații eronate sau manipulate care sunt diseminate în mod deliberat pentru a induce în eroare. Aceasta este piatra de temelie a propagandei clasice, dar este și baza fenomenului mai recent al știrilor false. Utilizarea deliberată a informațiilor false pentru a induce în eroare nu este nimic nou. Cu toate acestea, platformele digitale au schimbat fundamental natura dezinformării. Conținutul fals poate apărea sub formă de text, imagine, video sau audio manipulat. Aceste elemente pot fi folosite pentru a susține discursuri false, pentru a semăna confuzie și pentru a discredita informații, persoane și organizații legitime.

FABRICATION

Information with no factual basis published in a style that misleads the audience to believe it to be legitimate. For example, a fake e-mail from a politician might be produced and leaked to the press to undermine that politician's credibility.

MANIPULATION

Adding, removing, or changing the content of text, photo, video, or audio recording to communicate a different message.

MISAPPROPRIATION

The use of factually correct content presented on an unrelated matter to frame an issue, event or person in a deceptive way. For example, a false news article might use pictures from an unrelated event as proof of its existence.

SATIRE AND PARODY

Satire and parody are normally harmless forms of entertainment. However, humour can be used aggressively to disseminate misleading information and ridicule or criticise individuals, narratives or opinions. Humour can also be a very effective way of legitimising controversial opinions.

Retorică rău intenționată

Retorica este o parte acceptată și naturală a dezbaterii democratice, în care toată lumea are dreptul de a-și exprima opiniile și de a se angaja în deliberarea publică. O anumită cantitate de retorică este acceptată în dezbaterea publică, în timp ce retorica rău intenționată nu este. Retorica răuvoitoare exploatează natura adesea fragmentată a conversațiilor publice pentru a tulbura apele, a înșela și a induce în eroare și a descuraja anumiți actori să participe la dezbaterea publică.

Un vehicul comun pentru retorica rău intenționată online este trollul. Trolii sunt utilizatori de social media care provoacă în mod deliberat pe alții prin comentariile și comportamentul lor online. Activitatea lor contribuie la creșterea polarizării, reduce la tăcere opiniile divergente și înecă discuțiile legitime. Trolii pot fi conduși de motivații personale sau, ca în cazul *trolilor hibrizi*, pot lucra sub îndrumarea altcuiva.

AD HOMINEM

Atacarea, discreditarea sau ridiculizarea persoanei din spatele unui argument în locul argumentului pe sine se numește atac ad hominem. Acest lucru se face pentru a reduce la tăcere, descuraja sau descuraja adversarul.

CE SE ÎNTÂMPLĂ

Devierea criticii prin trasarea unor paralele false cu fenomene similare, dar irelevante.

GISH-GALOP

Copleșirea unui adversar cu un potop de argumente, fapte și surse, dintre care multe sunt false sau nu au legătură cu problema.

OM DE PAIE

Discreditarea unui adversar atribuindu-i poziții sau argumente pe care nu le deține și apoi argumentând împotriva acelor poziții.

DETURNAREA

Preluarea unei dezbateri existente și schimbarea scopului sau subiectului acesteia. Acest lucru este deosebit de eficient atunci când este aplicat hashtag-urilor și meme-urilor și poate fi, de asemenea, utilizat pentru a perturba evenimente sau mișcări sociale contra-cul- turale.

Acțiuni simbolice

Acțiunile vorbesc mai tare decât cuvintele. Unele acțiuni sunt calculate pentru a transmite un mesaj, mai degrabă decât pentru a atinge obiectivul acțiunii în sine. În astfel de cazuri, acțiunea este simbolică. Spre deosebire de orice acțiuni obișnuite, acțiunile simbolice sunt motivate
printr-o logică comunicativă și o încadrare narativă strategică. Acest lucru poate fi făcut foarte grosolan, de exemplu în modul în care fac teroriștii, mizând pe temerile universal împărtășite de violența aleatorie. De asemenea, se poate face într-o manieră sofisticată prin utilizarea unor simboluri culturale precise relevante numai pentru un anumit public țintă.

LEAKING

Leaking consists of releasing information that has been obtained by illegitimate means. This carries symbolic weight as leakers traditionally reveal injustices and cover-ups unknown to the public. However, when used as an information influence activity, leaked information is taken out of context and is used to discredit actors and distort the information environment. Leaked information is sometimes obtained through hacking or theft.

HACKING

Hacking involves acquiring unauthorized access to a computer or a network and is a crime. Hacking as an information influence activity, can serve as a symbolic act where the intrusion itself is secondary. The actual objective is to arouse suspicion that a system is insecure or compromised, in order to undermine confidence in the system in question or a body responsible for the same.

PUBLIC DEMONSTRATIONS

Legitimate demonstrations are symbolic actions used to promote a certain political issue or position. They are an important element of the democratic dialogue. Hostile actors, however, may orchestrate demonstrations to falsely give the impression of strong support or dislike of a particular issue (also known as astroturfing).

Cum sunt aceste tehnici combinate în mod obișnuit?

Pentru a identifica un caz de influență a informațiilor, trebuie să evaluați narațiunile strategice, publicul țintă și tehnicile de comunicare utilizate. Amintiți-vă că tehnicile de comunicare rău intenționate sunt adesea implementate în combinație pentru a se sprijini și consolida reciproc.

De exemplu, un document falsificat va ajunge la un public mai larg dacă este răspândit de roboți. Efectul va fi amplificat pe scară mai largă dacă este coordonat cu articole publicate pe platforme de știri părtinitoare sau false susținute de o armată de troli de comentatori.
Prin urmare, evaluarea dvs. ar trebui să ia în considerare dacă există dovezi ale unor acțiuni multiple, coordonate, îndreptate împotriva organizației dvs. Pe pagina următoare, oferim câteva exemple despre cum ar putea arăta activitățile de influență coordonate.

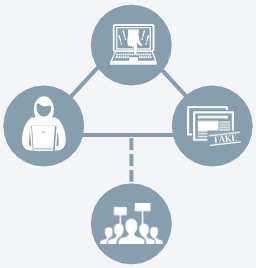
Vă sugerăm o serie de întrebări pe care le puteți utiliza pentru a vă ajuta să evaluați comunicările și să identificați activitățile de influențare a informațiilor. Ce narațiuni puteți identifica și cui se adresează? Există vreo dovadă a intenției de a înșela sau de a perturba? Suspectați interferența unui actor străin sau a unui reprezentant? Vedeți o combinație de tehnici care sugerează un efort coordonat sau o campanie împotriva organizației dvs.? Dacă descoperiți că există motive de îngrijorare, următoarea secțiune conține sugestii despre cum să răspundeți.

Tehnici coordonate

Operațiunile de influențare a informațiilor sunt adesea complexe și rareori veți întâlni o singură tehnică izolată . Fii în căutarea unei combinații de tehnici îndreptate împotriva ta. În timp ce teoretic combinațiile posibile sunt infinite, merită remarcate câteva combinații comune.

Polarizare

Polarizarea exacerbează extremele opuse într-o anumită problemă. Această strategie poate folosi hacking-ul social, identitățile înșelătoare și dezinformarea. Trolii și roboții sunt adesea folosiți pentru a întări opiniile extreme.

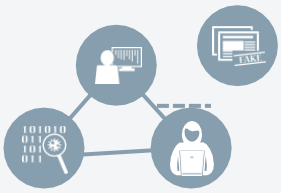


Spălare

Spălarea se referă la distorsionarea și decontextualizarea treptată a informațiilor, astfel încât devine imposibil de spus dacă sursa lor este adevărată sau falsă. Această strategie poate folosi identități înșelătoare, dezinformare, manipulare tehnică și acte simbolice în combinație cu hacking-ul social și cognitiv pentru a crea o rețea de informații false.

Provocare

Provocarea exploatează problemele sensibile pentru a antagoniza oamenii și pentru a genera furie și discordie. Această strategie poate folosi hacking-ul social și cognitiv, identitățile înșelătoare și retorica răuvoitoare pentru implicarea cetățenilor obișnuiți prin exploatarea vulnerabilităților lor emoționale.



Inundații

Inundațiile creează confuzie prin supraîncărcarea publicului cu informații, fie pozitive, negative sau irelevante.
Acest lucru poate fi realizat prin spam și trolling pe platformele de comunicare socială sau prin dezinformarea către surse media legitime. Inundarea elimină informațiile legitime și descurajează dezbaterea constructivă.

PARTEA III.

Contracara rea influenței informaționale

Cum îmi pot pregăti cel mai bine organizația? Cum aleg cel mai potrivit răspuns?

PARTEA III. Contracararea influenței informaționale

În această secțiune, vom discuta despre modul de contracarare a activităților de influențare a informațiilor. Vă vom ajuta să vă pregătiți organizația pentru a face față acestei amenințări, vom discuta despre acțiunile care pot fi întreprinse atunci când un atac este în curs de desfășurare și vă vom sugera cum ar trebui împărtășite cele mai bune practici pentru a promova învățarea organizațională.

PREGĂTI

Creșteți gradul de conștientizare
Construiți încrederea
Evaluați riscurile

ACT

Alegeți răspunsul Verifică-ți faptele
Utilizați rețelele sociale

ÎNVĂȚA

Descrieți,
reflectați,
distribuiți

Cum îmi pregătesc organizația?

Pregătirea este cea mai importantă parte a oricărui plan de gestionare a crizelor. Educarea colegilor și stabilirea structurilor de răspuns face posibilă atenuarea efectelor negative ale operațiunilor de influențare a informațiilor și răspunsul rapid și eficient. Pregătirea constă în trei faze principale: 1) schimbul de informații și creșterea gradului de conștientizare, 2) înțelegerea modului în care publicul cheie și părțile interesate pot fi vulnerabile la activitățile de influențare a informațiilor și dezvoltarea de narațiuni și mesaje în jurul potențialelor probleme și 3) efectuarea unei analize a riscurilor și vulnerabilității pentru organizația dvs.

Sensibilizarea

Primul pas spre rezolvarea unei probleme este recunoașterea faptului că problema există, prin urmare, un aspect esențial al pregătirii este creșterea gradului de conștientizare a amenințărilor cu care ne confruntăm ca societate și a problemelor care pot fi considerate vulnerabilități în special pentru organizația dvs. La nivelul societății în general, cea mai bună apărare împotriva activităților de influențare a informațiilor este dezvoltarea capacității de a contracara amenințările prin crearea unor platforme transsectoriale în care liderii, jurnaliștii, reprezentanții platformelor de comunicare socială, cercetătorii, profesioniștii din domeniul comunicării și cetățenii să poată face schimb de cunoștințe și de lecții de bune practici între ei și cu publicul larg.

În calitate de profesionist în comunicare într-o organizație din sectorul public, există mai multe lucruri pe care le puteți face pentru a ajuta la construirea rezilienței și a capacității defensive în cadrul organizației dvs. În primul rând, vă puteți prezenta ca punct cheie de contact pentru aceste probleme în cadrul organizației dvs. Este esențial să discutați aceste probleme cu conducerea superioară și să comunicați intern cu colegii. În al doilea rând, puteți acționa ca un consilier pentru managerii și colegii dvs., astfel încât aceștia să știe ce să facă dacă se confruntă cu activități de influențare a informațiilor. Aceasta include identificarea nevoilor și a oportunităților de formare. În al treilea rând, puteți construi rețele cu alți profesioniști din afara organizației dvs., pe baza sprijinului reciproc și a schimbului de experiență.
În al patrulea rând, puteți crește gradul de conștientizare și transparența cu privire la activitățile organizației dumneavoastră pentru a preveni răspândirea dezinformării.

Construirea încrederii prin comunicare strategică

Unul dintre obiectivele influenței informaționale este de a submina încrederea dintre oameni și instituțiile sociale. Prin urmare, efectul acestor activități poate fi minimizat prin concentrarea asupra contramăsurilor care construiesc încrederea în organizația dvs. Sprijinirea reputației și legitimității instituțiilor publice este un aspect important al oricărei strategii de contramăsură.

Pregătirea mesajelor

Deoarece poate dura ceva timp pentru ca mesajele să fie pregătite și aprobate în timpul unei crize, este important să pregătiți mesaje generice care să afirme valorile organizației dvs. și să poată fi ușor adaptate la un anumit eveniment. La fel cum organizațiile folosesc mesaje direcționate pentru a descrie o nouă inițiativă sau un nou produs, acestea pot fi, de asemenea, utilizate pentru a crește gradul de conștientizare a știrilor false și pentru a le respinge.

MESAJE PREGĂTITE

Răspunsurile rapide și precise pe platformele de comunicare socială sunt posibile prin lucrări pregătitoare solide – pregătirea în avans a mesajelor de răspuns la situații de criză, cu aprobarea conducerii superioare. De exemplu, Poliția Metropolitană din Londra a trimis primul său tweet la doar șapte minute după atacul terorist de la Westminster din martie 2017. Tweet-ul a furnizat informații exacte despre situația în desfășurare, dar s-a bazat pe un mesaj generic pregătit pentru scenarii similare care ar putea fi adaptate rapid la evenimentele actuale.

Atunci când proiectați mesaje, este important să luați în considerare ce povești circulă despre organizația dvs. și care sunt narațiunile generale care conduc aceste povești. Narațiunile vor fi legate de modul în care organizația dvs. este percepută de diferite segmente de public. Cum funcționează mesajele individuale
contribuie la identitatea, valorile și narațiunile pe care organizația dvs. dorește să le promoveze, în special în raport cu diferite publicuri cheie? Mesajele care susțin narațiuni pozitive despre organizația dvs. pot juca un rol crucial în dezvoltarea rezistenței la informații înșelătoare și false.

CARE ESTE POVESTEA TA?

Mesajele trebuie să fie aliniate cu narațiunea generală pe care doriți să o proiectați.

O narațiune puternică vine dintr-o valoare și obiective clare în cadrul organizației dvs.

Analiza și înțelegerea factorilor care contribuie la narațiunile preferate ale organizației dvs. construiesc simultan o înțelegere a vulnerabilităților reputaționale ale organizației dvs.

Orice atac este cel mai bine contracarat prin susținerea acelor valori pe care le reprezintă organizația dvs.

Cunoaște-ți publicul

Stabilirea clară a valorilor de bază, a mesajelor și a narațiunilor preferate pentru organizația dvs. este fundamentală pentru înțelegerea vulnerabilităților dvs. și a părților interesate care prezintă cel mai mare risc de influență a informațiilor. Dacă a fost detectată o campanie de influență, acestea sunt grupurile cărora trebuie să li se adreseze mai întâi.

În calitate de comunicator profesionist, aveți deja experiență în efectuarea analizei publicului țintă. Diferența aici este că întrebați care public este cel mai vulnerabil la influența informațiilor și de ce. Identificați zonele organizației dvs. care sunt cel mai probabil să fie supuse activităților de influențare a informațiilor și luați în considerare tipul de mesaje rău intenționate la care ar putea fi susceptibile. După ce ați făcut acest lucru, puteți pregăti sugestii pentru a ajunge la aceste audiențe cheie cu informații preventive și contra-mesaje.

ANALIZA PUBLICULUI ȚINTĂ

Audiențele cheie nu există într-un vid

Mai degrabă, ele sunt create dinamic prin interacțiunea dintre oameni care împărtășesc credințe, opinii și interese. Este important să înțelegem ce unește membrii unui public țintă.

Identificați-vă părțile interesate

Activitățile de influențare a informațiilor nu pot fi neapărat direcționate către organizația dvs., ci pot fi direcționate în primul rând către alte grupuri țintă asociate cu dvs. Cele mai vulnerabile grupuri din societate pot fi cele mai afectate. Este important să se cunoască grupurile-țintă expuse riscului și să se evalueze vulnerabilitățile acestora în raport cu diferitele discursuri.

Proiectează-ți narațiunea de bază

Identificați narațiunile care pot fi folosite pentru a contracara influența informațiilor. Cum pot aceste narative să ajungă la grupurile țintă vulnerabile? Includeți comunicatori cheie cu credibilitate ridicată ca posibili intermediari pentru a ajunge la aceste grupuri

Scopul realizării unei analize a publicului țintă este de a dezvolta instrumente de comunicare care pot fi utilizate în cazul în care sunteți supus unor activități de influențare a informațiilor. Aceasta este o formă de planificare de urgență care poate fi adaptată situațiilor în care metodele de influențare a informațiilor sunt utilizate pentru a vă submina reputația.

Contra-măsurile discutate aici sunt menite să vă ajute să restabiliți încrederea cât mai repede și mai eficient posibil. Acestea includ mesaje și narațiuni pregătite care pot fi direcționate către diferite categorii de public cheie și părți interesate din organizația dumneavoastră. Pentru a pregăti aceste mesaje, trebuie mai întâi să înțelegeți modul în care diferitele segmente de public ar putea fi afectate de dezinformare și cum să concepeți cel mai bine mesaje pentru fiecare public.

Cunoașteți-vă riscurile și vulnerabilitățile organizaționale

În plus față de cele de mai sus, organizația dumneavoastră ar trebui să pregătească o evaluare formală a modului în care activitățile de influențare a informațiilor îi pot amenința capacitatea de a-și îndeplini misiunea. Organizațiile din sectorul public includ analize ale riscurilor și vulnerabilității în planificarea strategică și în pregătirile pentru situații de criză. Vă sugerăm să adăugați activități de influențare a informațiilor la analizele de risc și vulnerabilitate existente, cu un accent special pe părțile interesate / publicul vulnerabil, valorile, mesajele și narațiunile cheie și riscul general pentru activitățile principale ale organizației dvs.

ANALIZA RISCURILOR ȘI VULNERABILITĂȚILOR

Pasul 1: Punctul de plecare
Ce rol joacă organizația dumneavoastră și care sunt responsabilitățile acesteia? Ce metode pot fi utilizate pentru a identifica și evalua riscurile și amenințările? Ce cadre sau perspective veți folosi în analiza dvs.?

Etapa 2: Evaluarea riscurilor
Care sunt posibilele amenințări și riscuri?
Care este probabilitatea ca aceste evenimente să aibă loc și care sunt posibilele consecințe?
Ce situații ar trebui evaluate în ceea ce privește capacitățile organizației dumneavoastră de gestionare a crizelor? Ce măsuri preventive ar trebui luate?

Pasul 3: Evaluarea vulnerabilității
Cum ar putea fi afectată organizația dvs. de diferite scenarii?
Care sunt consecințele potențiale ale activităților de influențare a informațiilor pentru organizația dvs. și cum puteți gestiona, rezista și recupera din aceste consecințe?

Pasul 4: Gestionarea riscurilor
Ce trebuie făcut dacă sunt identificate activități de influențare a informației? Vedeți exemplele de mai jos.

Cum aleg cel mai bun răspuns?

Nu există un răspuns universal la activitățile de influențare a informațiilor. După cum a arătat acest manual, activitățile de influențare a informațiilor pot varia foarte mult. Mai important, organizația dvs. funcționează în condiții unice și are propriile vulnerabilități specifice. Cu o pregătire temeinică, puteți crea un cadru general pentru contramăsuri care se potrivesc organizației dvs. și pot fi adaptate la o varietate de situații. Luați în considerare rolul dvs. de comunicator, așteptările care vi s-au pus și mandatul pe care vi l-a dat conducerea organizației dvs. pentru a determina cel mai bun răspuns pentru fiecare situație.

Evaluați, informați, susțineți sau apărați?

Un răspuns adecvat va fi proporțional cu amenințarea. Vă sugerăm patru categorii de răspuns, fiecare constând dintr-un număr de tehnici de comunicare.

Bazat pe fapte: Primul nivel de răspuns este **evaluarea** situației. Acesta este un răspuns neutru care semnalează că sunteți conștient de problemă și că stabiliți faptele. Al doilea nivel este **de a informa** publicul și părțile interesate cheie despre situație și despre modul în care organizația dvs. o vede. Acesta este un răspuns puțin mai puțin neutru, care prezintă ceea ce considerați a fi faptele cazului. Aceste acțiuni sunt pietrele de temelie pentru orice alt răspuns rațional, bazat pe fapte și pot fi aplicate majorității cazurilor de activități de influență suspectate.

Bazat pe advocacy: Al treilea nivel de răspuns implică acțiuni comunicative care **susțin** o anumită poziție. Aceasta înseamnă că vă veți susține în mod activ cazul, folosind tehnici retorice de persuasiune și relații publice pentru a argumenta, de exemplu, împotriva dezinformării. Al patrulea nivel este să vă apărați în mod activ organizația prin luarea de măsuri specifice împotriva agresorului. Aceste niveluri stau la baza unui răspuns bazat pe advocacy. Deși pot fi adecvate, acestea trebuie utilizate întotdeauna cu prudență, în funcție de gravitatea situației.

Un răspuns bazat pe fapte

Primele două niveluri pentru contracararea activităților de influență sunt evaluarea și informarea. Acestea sunt aplicabile în majoritatea situațiilor și constituie un răspuns bazat pe fapte.

Exemplele de mai jos sunt sugestii despre cum să răspundeți la fiecare nivel.

NIVELUL 1: EVALUEAZĂ

Pentru a înțelege cu ce aveți de-a face, trebuie să evaluați situația. Ce se întâmplă cu adevărat? Cine este implicat? Care este miza? Cu cât ai mai multe cunoștințe despre situație, cu atât răspunsul tău va fi mai bun.

HARTA SITUAȚIEI

Analizați situația și dezvoltați-vă conștientizarea cu privire la ceea ce se întâmplă. Utilizați instrumentele discutate în părțile I și II pentru a determina cu ce aveți de-a face.

VERIFICAREA INFORMAȚIILOR

Stabiliți faptele situației – ce este adevărat / corect?

INVESTIGAȚI TRANSPARENT

Implicarea actorilor independenți de încredere, cum ar fi jurnaliștii, în investigarea problemei și asigurarea transparenței.

NIVELUL 2: INFORMEAZĂ

După ce ați făcut evaluarea, puteți începe să comunicați cu publicul țintă. Concentrați-vă pe furnizarea de informații și fapte neutre și spuneți-le oamenilor cum abordați situația. Nu uitați să vă adaptați mesajele pentru fiecare public/grup de părți interesate.

FACEȚI O DECLARAȚIE

Prezentați faptele cazului așa cum le vedeți într-o manieră neutră.

CORECT

Faceți o declarație care răspunde direct acuzațiilor false cu fapte relevante. Utilizarea și fișa informativă în stil FAQ poate fi utilă.

SE REFERĂ

În cazurile în care actori sau surse independente pot corobora fapte, poate fi util să vă referiți la acestea ca sursă pentru a vă consolida cazul.

AFIRMĂ VALORI

Amintiți-le publicului ce reprezintă organizația dvs.

NOTIFICAREA PĂRȚILOR INTERESATE

Fie că sunt colegi sau părți interesate cheie, cu cât mai repede puteți informa oamenii ce se întâmplă, cu atât mai bine.

EMITEȚI O DECLARAȚIE DE DEȚINERE

Comunicați că analizați situația prin emiterea unei declarații de exploatație. Acest lucru vă va oferi timp pentru a dezvolta un răspuns mai aprofundat.

Un răspuns bazat pe advocacy

Al treilea și al patrulea nivel sunt de a pleda și de a apăra. Aceste etape conțin măsuri care sunt adecvate numai în situații grave în care a fost identificată în mod clar o campanie de influențare a informării. Împreună, acestea alcătuiesc un răspuns bazat pe advocacy.

Exemplele de mai jos sunt sugestii despre cum să răspundeți la fiecare nivel.

NIVELUL 3: AVOCAT

Advocacy este un pas înainte de furnizarea de informații neutre și implică argumentarea cazului dvs. mai activ. Luați întotdeauna în considerare mandatul dvs. și reamintiți-vă bunele practici de comunicare și valorile organizației dvs. atunci când vă proiectați răspunsul.

DIALOG

Implicați-vă activ într-un dialog cu principalele părți interesate și cu membrii publicului pentru a-i implica în răspunsul la această problemă.

FACILITAREA

Ajutați-vă să ajungeți cu ușurință la segmentele de public cheie. Organizați evenimente sau întâlniri care reunesc diferite părți interesate pentru a discuta o problemă specifică și pentru a vă oferi posibilitatea de a vă clarifica poziția.

MULTIPLICATORI

Interacționați cu comunicatori cheie care vă pot ajuta să vă răspândiți mesajul către publicul relevant.

CĂLĂRIND

Utilizați evenimente, inițiative sau dezbateri existente pentru a prezenta faptele cazului.

DECLARAȚIE OFICIALĂ

Pregătiți un dosar care descrie desfășurarea evenimentelor și prezintă fapte care vă susțin cazul. Este foarte important ca acest document să se bazeze pe fapte și informații verificate.

POVESTITOR

Raportați situația la o narațiune mai largă despre, de exemplu, organizația dvs. și valorile sale, care vă va ajuta publicul cheie să înțeleagă situația și să vă verifice poziția

NIVELUL 4: APĂRARE

Apărarea implică proiectarea unui răspuns direct la agresor. Acest pas poate părea controversat și, prin urmare, ar trebui rezervat pentru cazuri extreme. Asigurați-vă că discutați mai întâi toate acțiunile la acest nivel cu colegii și conducerea, pentru a evita depășirea mandatului sau agravarea ședinței.

IGNORA

De fiecare dată, cel mai bun răspuns este să nu faci nimic. Acest lucru ar putea fi potrivit dacă influența informațiilor a fost clar determinată, dar nu a atras prea multă atenție. În astfel de cazuri, un răspuns activ ar putea disemina și mai mult dezinformarea.

RAPORT

Dacă un atacator încalcă legea sau încalcă codul de conduită al unei platforme de socializare, raportați-l poliției sau platformei. Această acțiune nu trebuie luată cu ușurință sau abuzată – utilizați numai în cazul unei încălcări clare pentru a evita reducerea la tăcere a dezbaterii publice.

BLOCA

Comunicatorii ar trebui să fie conștienți de importanța respectului și a dreptului la libertatea de exprimare! Activitățile perturbatoare pot necesita blocarea unui utilizator de pe o anumită platformă. Cu toate acestea, fiecare caz ar trebui să fie motivat în mod clar pe baza codului de conduită al formularului.

EXPUNE

Deși, în general, nu este recomandat, un răspuns strategic la activitățile de influențare a informațiilor ar putea fi expunerea actorului din spatele, de exemplu, al unei relatări înșelătoare. Din nou, acest lucru nu ar trebui făcut ușor. În primul rând, efectuați o analiză adecvată a

consecințelor care la în considerare consecințele pe care expunerea vinovatului le-ar putea avea pentru propria organizație, pentru părțile interesate și pentru persoana care va fi expusă.

Alegerea celui mai adecvat nivel de răspuns depinde de evaluarea gravității situației. Un caz suspectat de influență a informațiilor doar cu indicatori slabi este cel mai bine abordat la nivelurile unu și doi, și anume **evaluarea** situației și **informarea** publicului într-un mod neutru. Acesta este un *răspuns bazat pe fapte.* Pentru un caz mai agresiv de influență informațională, utilizați metodele bazate pe fapte ale nivelurilor
unu și doi, împreună cu nivelurile trei și patru, adică susțineți-vă poziția și apărați-vă organizația împotriva atacului. Acesta este un *răspuns bazat pe advocacy*. Cu toate acestea, utilizați prudență la aceste niveluri. Asigurați-vă că aveți un mandat clar din partea conducerii dvs. și că răspunsul dvs. este în concordanță cu
principiile democratice și libertatea de exprimare, precum și alte reglementări și coduri de conduită care se pot aplica.

Dezvoltarea unui răspuns bazat pe fapte

Cel mai important aspect al primelor două niveluri de răspuns este că comunicarea trebuie să fie neutră și bazată pe fapte. Aceste două calități definesc un răspuns bazat pe fapte. **Un răspuns bazat pe advocacy ar trebui considerat un al doilea nivel care se bazează întotdeauna pe primul strat obligatoriu, bazat pe fapte.** Dacă informațiile inexacte sunt permise să circule fără corectare, acest lucru poate contribui la percepția că organizația dvs., publicul său cheie sau problemele sale de bază sunt construite pe presupuneri greșite și falsuri. Prin urmare, evaluarea situației și informarea publicului cheie identificat trebuie să fie întotdeauna primul răspuns.

Pentru a vă asigura că orice verificare a faptelor pe care o faceți este relevantă, trebuie mai întâi să înțelegeți modul în care informațiile false vă afectează organizația, modul în care acestea vă pot submina activitățile și să le identificați. Cine răspândește dezinformarea? Cât de mult s-a răspândit? Despre ce subiecte este vorba? O abordare este să vă concentrați asupra articolelor care conțin citate de la reprezentanții organizației dvs., recomandări relevante care au devenit virale online sau afirmații publice despre organizația dvs. și zona sa de activitate. Colectarea sistematică a faptelor, astfel încât să puteți evalua întrebările relevante pentru domeniul dvs. de responsabilitate.

Assessment

- ☑ Collect neutral expert opinions and/or accurate data from relevant and credible sources.
- ☑ Request more information from the person or organisation making the claim.
- ☑ Find the original source of the false data.

Dacă informațiile sunt considerate false, este adecvată furnizarea unei corecții. Mulți experți consideră că dezinformarea este cel mai bine contracarată prin informații exacte. Cu toate acestea, unii susțin că veți ajunge doar la cei interesați să descopere adevărul. Activitatea pregătitoare privind audiențele și narațiunile cheie ar trebui să vă ajute să stabiliți cum să răspundeți în fiecare caz.

Dacă aveți opțiunea și mandatul de a dezvolta un răspuns persuasiv bazat pe advocacy, acesta ar trebui să se bazeze pe liniile stabilite în răspunsul bazat pe fapte.

Developing a fact-based response

- ☑ Request a retraction or correction from the author/ publisher of the falsehood.
- ☑ Prepare a fact sheet or similar document that can be shared easily online.
- ☑ Be cautious of repeating false information in your communications.
- ☑ Remember that not every piece of false information needs to be corrected.
- ☑ Question the premise of the debate, not just the content.
- ☑ Consider engaging in dialogue as a supplement or alternative to your prepared communications.

Considerații speciale pentru social media

Social media nu sunt doar platforme în care utilizatorii pot interacționa cu ușurință între ei, ci pot fi, de asemenea, folosite ca un instrument de influențare a informațiilor. Platformele de socializare au propria lor logică. Utilizatorii trebuie să înțeleagă și să respecte această logică pentru a contracara cu succes activitățile de influențare a informațiilor.

Poate fi dificil să știi cine se află în spatele unui cont de social media și de unde își iau informațiile. Indivizii, forumurile și rețelele pot pretinde în mod fals că reprezintă opinia publică autentică. Social media reprezintă un mediu provocator, deoarece informațiile se pot răspândi rapid *și trebuie luate în considerare elemente precum* etichetarea, *notificările, linkurile* și *atașamentele*. O postare tipică pe rețelele sociale va conține unul sau mai multe dintre aceste elemente, care împreună contribuie la poziționarea postării într-o rețea de alte conturi, idei și dezbateri. Fiecare postare poate fi considerată o parte a uneia sau mai multor conversații online în curs de desfășurare.

ETICHETARE

Creează un termen de căutare pentru o postare. Etichetele influențează circulația și acoperirea unei postări.

NOTIFICĂRI

activați un link către un cont individual sau de organizație pentru a le notifica despre postările de interes

LEGĂTURI

furnizați un hyperlink către alte site-uri web. Linkurile sunt adesea abreviate, astfel încât adresa URL completă nu este vizibilă.

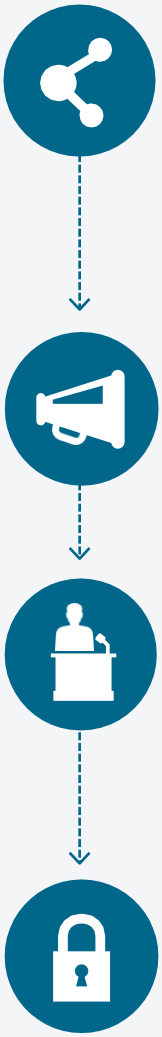
ATAȘĂRI

Includeți fișiere multimedia, cum ar fi o imagine sau un clip video, într-o postare. Rețineți că acestea pot schimba sensul sau intenția unei postări și nu trebuie trecute cu vederea.

Activitatea proactivă în social media include construirea de rețele și stabilirea de hashtag-uri care permit unei organizații să ajungă la persoanele potrivite cu mesajele lor. Posturile generice pentru gestionarea crizelor pot fi pregătite și eliberate în prealabil, asigurând un răspuns prompt atunci când apare un eveniment neprevăzut. Social media permite, de asemenea, unei organizații să descopere potențiale amenințări sau vulnerabilități la adresa reputației sale în timp real. Prin urmare, este un instrument de advocacy pentru dialog și mesaje și un instrument de informații open source pentru înțelegerea tendințelor importante.

Contracararea influenței asupra rețelelor sociale

Cele patru niveluri de răspuns furnizate mai sus sugerează o abordare generală a activităților de contracarare a influenței. Mai jos este un exemplu despre modul în care ați putea utiliza această metodă pentru a contracara influența informațiilor pe social media.



EVALUA

Evaluați situația folosind cunoștințele dvs. despre campaniile de influențare a informațiilor. Este un caz de influență informațională sau doar cetățeni preocupați care se angajează în dezbateri? Dacă suspectați o influență nelegitimă, cartografiați situația cât mai clar posibil. Ce utilizatori interacționează cu dvs.? Sunt actori ostili sau reacționează la provocare? Ce hashtag-uri sunt folosite? Există link-uri sau materiale vizuale atașate? O evaluare rapidă a situației vă va permite să determinați cea mai bună linie de acțiune.

INFORMA

Proiectați-vă mesajul pe baza concluziilor la care ați ajuns în evaluarea dvs. Selectați cu atenție utilizatorii, hashtagurile și publicul cu care să interacționați. Concentrați-vă pe clarificarea poziției dvs. și afirmați valorile organizației dvs. folosind canale stabilite și adecvate.

AVOCAT

Dacă este adecvat situației, afirmați-vă mai clar în dezbatere, prezentându-vă poziția folosind instrumentele pe care le aveți la dispoziție, cum ar fi mesajele pregătite sau multimedia. În această etapă, ar putea fi, de asemenea, potrivit să vă implicați mai mult în dezbatere pentru a crea un angajament mai mare față de această problemă în rândul audiențelor dvs. cheie . Acest lucru se face prin comunicarea directă cu alți utilizatori pentru a-i implica în problemă.

APĂRA

A ajuns situația într-un punct în care dialogul productiv este imposibil și mesajele legitime sunt eliminate de spam și conținut ostil?
În funcție de orientările organizației și de codul de conduită al platformei de socializare, este posibil să aveți dreptul să blocați sau să ignorați anumiți utilizatori. Luați sfaturile conducerii dvs. înainte de a acționa! Libertatea de exprimare este una dintre valorile fundamentale ale societății noastre și ar trebui să facem întotdeauna tot posibilul pentru a menține un dialog democratic liber și deschis. Dacă decideți să blocați sau să ignorați un utilizator, asigurați-vă că sunteți transparent cu privire la motivul deciziei dvs.

Cum mă asigur că lecțiile sunt învățate?

Este esențial să colectăm și să documentăm exemple de activități de influență a informațiilor pentru a înțelege mai bine problema. În plus, pentru a stabili cele mai bune practici pentru organizația dvs., este esențial să vă documentați răspunsurile și să evaluați succesul acestora în obținerea efectului dorit. Utilizați exemplele dvs. pentru a dezvolta un jurnal al evenimentelor pe măsură ce se desfășoară și proiectați rutine proactive pentru posibile atacuri viitoare. De asemenea, puteți elabora materiale de formare pentru a vă raționaliza abordarea organizațională și pentru a contribui la pregătirea societății în general. Împărtășiți-vă cunoștințele și experiența cu comunicatori în roluri similare și cu autoritățile publice însărcinate cu identificarea activităților de influențare a informațiilor (de exemplu, MSB în Suedia) și, în unele cazuri, cu publicul.

Pe pagina următoare am oferit câteva exemple de tip de informații pe care ar trebui să le salvați în caz de suspiciune de influență a informațiilor:

Learning

DESCRIBE

- [x] Describe the background, progression, and context of the event.
- [x] Which actors and networks were involved? (Avoid speculation if you don't know.)
- [x] Which characteristics of information influence activities did you observe?
- [x] Which vulnerabilities were exploited?
- [x] Which influence techniques were used? Which audiences and narratives were used?
- [x] Does the case fit into a broader pattern of activities?

REFLECT

- [x] What do you think where the intended effects? On what do you base your assessment?
- [x] How did you act? Reflect on the steps you took and the choices you made.
- [x] What do you think would have happened if you did not act as you did?
- [x] What were the effects of your response?
- [x] What did you do well and what would you do differently?
- [x] What have you learned from this experience?

SHARE

- [x] Have you saved evidence or data related to the case?
- [x] Discuss information influence activities with your organisation's leadership and colleagues and share your experience.
- [x] Maintain regular contact with colleagues working on similar issues within your organisation and in other organisations.
- [x] Share your expertise and experience with others both within your organisation and with other colleagues by participating in meetings and educational events.

Considerații strategice

Orice încercare de a contracara o activitate de influență este limitată de faptul că răspunzi agendei altcuiva. Agresorul pare să stabilească condițiile, ceea ce înseamnă că contracararea activităților de influențare informațională este problematică. Se poate simți ca și cum ei acționează și noi răspundem, că suntem întotdeauna cu un pas în urma ultimelor încercări de a ne exploata vulnerabilitățile sociale.

Prin urmare, este mai logic să ne concentrăm pe susținerea valorilor democratice, cum ar fi dezbaterea deschisă și libertatea de exprimare. Misiunea dvs. este de a proteja procesul de formare a opiniei independente în ceea ce privește organizația dvs. prin minimizarea efectelor vulnerabilităților în sistemul mass-media, opinia publică și procesele cognitive umane. Este important să pornim de la o poziție strategică, echilibrată, bazată pe fapte.

Merită repetat faptul că eforturile de contracarare a activităților de influențare a informațiilor nu ar trebui să reducă niciodată la tăcere dezbaterea publică. Acest lucru ar fi contraproductiv și nu ar face decât să conducă la o polarizare și mai mare și să submineze principiile pe care se bazează societatea noastră. Dezbaterea deschisă și democratică trebuie întotdeauna protejată și încurajată.

- ☑ Raise the threshold for information influence activities through awareness and preparation.
- ☑ Develop proactive, proportionate, and sensible methods of communication that focus on key audiences (rather than an adversary) and defend the values we share.
- ☑ Maintain a fact-based response that can be developed into an advocacy-based response under certain circumstances.
- ☑ Sharing best practices and learn from each other.
- ☑ Be vigilant but not paranoid!

Glosar

Efectul Bandwagon – Un fenomen psihologic în care oamenii fac ceva în primul rând pentru că alții o fac. Oamenii care simt că aparțin majorității sunt mai predispuși să-și împărtășească opiniile și să-și arate comportamentele, astfel încât ideile și tendințele cresc cu cât sunt adoptate mai mult.

Bot – Un program de calculator care efectuează sarcini automate, repetitive.

Dezinformare – Informații false sau manipulate în mod deliberat, diseminate cu scopul de a induce în eroare oamenii cu privire la opinii sau comportamente care servesc într-un fel creatorului informațiilor respective.

Anunțuri întunecate - Un anunț sau o postare cu conținut personalizat creat prin profilarea psihografică afișată numai pentru a selecta membrii unui grup demografic țintă pentru a le influența opiniile sau comportamentele.

Eco-cameră sau bulă de filtrare – O grupare naturală, online sau offline, în care oamenii comunică în primul rând cu alții care împărtășesc aceleași puncte de vedere și opinii.

Fake media – Site-uri de știri contrafăcute concepute pentru a imita site-urile de știri autentice.

Hacking – Exploatarea punctelor slabe pentru a încălca apărarea securității și pentru a obține acces neautorizat la un computer sau la o rețea.

Meme - O unitate de transmitere a ideilor, simbolurilor sau practicilor culturale care se răspândește de la o persoană la alta; un analog cultural al genei, deoarece memele se auto-replică, suferă mutații și răspund la presiuni selective. Inventat de Richard Dawkins în 1976. Memele pot fi imagini, fraze, concepte sau comportamente, adesea cu conținut plin de umor, care sunt răspândite în principal pe internet prin intermediul rețelelor sociale.

Phishing – Păcălirea utilizatorilor de internet pentru a-și furniza parolele sau alte informații sensibile.

Satele Potemkin – Companii false, institute de cercetare sau grupuri de reflecție create pentru a da credibilitate dezinformării.

Shill - Un promotor sau purtător de cuvânt care dă impresia că este independent, dar de fapt cooperează sau primește plăți de la altcineva.

Sockpuppet – Un cont fals de social media folosit pentru a semăna discordie în dezbaterile online anonim, argumentând adesea o poziție extremă. O tehnică comună este de a folosi sockpuppets pentru a argumenta ambele părți ale unei dezbateri.

Spirala tăcerii – Fenomenul psihologic când oamenii rămân tăcuți dacă simt că opiniile lor sunt nepopulare pentru că se tem de izolare sau ridicol; când oamenii care simt că aparțin minorității nu le împărtășesc opiniile, cu atât este mai puțin probabil ca alții care împărtășesc aceste opinii să le exprime.

Narațiune strategică - O poveste convingătoare care explică ceva despre modul în care gândim și acționăm, care este concepută ca o acțiune comunicativă pentru a sprijini un scop specific.

Omul de paie - Tactica retorică de a denatura argumentele unui adversar pentru a face mai ușoară respingerea lor - o eroare logică.

Act simbolic - Un act efectuat în primul rând pentru a comunica un mesaj, mai degrabă decât pentru a beneficia de orice alte consecințe practice ale acelei acțiuni.

Whataboutism – O tactică retorică ieftină de a muta critica de la sine prin

efectuarea unei comparații false cu o problemă fără legătură.

Lecturi suplimentare

Acest manual se bazează pe raportul din 2018 *Countering Information Influence Activities: The State of the Art* de Pamment, Nothhaft, Twetman și Fjällhed.

Puteți găsi raportul împreună cu o listă completă de referințe pe site-ul MSB: https://www.msb.se

De asemenea, recomandăm următoarele rapoarte și articole ca resurse utile:

Prevenirea şi gestionarea tentativelor de influenţare – manual
Consiliul Național Suedez pentru Prevenirea Criminalității (BRÅ), 2017

Sursa: critici pe internet
Fundația Internet din Suedia (IIS), 2016

Siguranța personală
SÄPO, 2018

Manual de demitizare
John Cook și Stephan Lewandowsky, în 2012

Fapte alternative – despre cunoaştere şi duşmanii ei
Åsa Wikforss, 2017

Propaganda participativă: implicarea publicului în răspândirea comunicărilor persuasive
Alicia Wanless și Michael Berk, în 2018

Fondări teoretice ale operațiunilor de influență: o revizuire a cercetărilor psihologice relevante
Björn Palmertz pentru MSB, n.d.

Modelul rusesc de propagandă "Furtunul minciunii" – de ce ar putea funcţiona şi opțiuni pentru a-l contracara
Christopher Paul și Miriam Matthews pentru RAND, 2016

De asemenea, puteți obține informații și exemple de la alte organizații internaționale:

UE vs Disinfo
www.euvsdisinfo.eu

Centrul European de Excelență pentru Contracararea Amenințărilor Hibride
www.hybridcoe.fi

Centrul de Excelență pentru Comunicații Strategice al NATO
www.stratcomcoe.org

Agenția suedeză pentru situații de urgență civilă (MSB)
SE-651 81 Karlstad Telefon +46 (0)771-240 240 www.msb.se/en
Ordinul nr. MSB1263 - martie 2019 ISBN 978-91-7383-867-2