

GHID

PENTRU SPECIALIȘTI ÎN
COMUNICARE

CHIȘINĂU, 2024

În comparație cu un conflict armat sau cu alte mijloace din setul de instrumente hibride, dezinformarea ar putea părea ceva moale și pufos, chiar lipsită de importanță. Dar redactorul-șef al Federației Ruse (FR), Margarita Simonyan, susține că FR este necesară "din aproximativ același motiv pentru care țara are nevoie de un Minister al Apărării". Potrivit acesteia, FR este capabilă să "conducă un război informațional împotriva întregii lumi occidentale", folosind "arma informațională". În 2023, Kremlinul a cheltuit 1,9 miliarde de dolari pentru acest război informațional.

Lăsarea acestei "arme informaționale" nesupravegheată permite adversarului să obțină sprijin pentru politici utile pentru ei. Acest lucru se realizează prin erodarea încrederii publice în instituții, creșterea polarizării care poate duce la violență, adâncirea diviziunilor sociale existente și suprimarea vocilor independente care ar putea critica aceste evoluții. Prin urmare, combaterea atacurilor informaționale sau a manipulărilor și interferențelor informațiilor străine (FIMI) este o modalitate de a proteja democrația. Lista de mai jos oferă câteva principii care vă ajută să abordați un atac informațional cu sugestii și exemple.



1. Faza pregătitoare:

- creați materiale care explică activitatea instituției dumneavoastră;
- subliniați valorile și povestea dumneavoastră;
- configurați monitorizarea.



2. Confruntarea cu un atac:

- evaluați situația prin colectarea informațiilor;
- împărtășiți descoperirile cu partenerii.



3. Informarea publicului și a partenerilor cheie:

- trimiteți un mesaj formal publicului țintă și, dacă este necesar,
- respingeți informațiile incorecte.



4. Comunicare proactivă:

- includeți-vă aliații;
- asigurați-vă că informările și alte materiale sunt accesibile online.



5. Ocupați-vă de atacator:

- fie ignorați, raportați, expuneți sau contracarați.



6. Evaluați-vă răspunsul:

- Evaluatează-ți răspunsul.

Înainte de atac

1. Pregătiți instituția:

Pregătirea este fundamentul și nucleul pe care îl folosiți în timp ce sunteți atacați. Pentru a fi pregătit, creați materiale care să explice ce face instituția dumneavoastră și să sublinieze valorile și povestea dumneavoastră. Stabiliți o monitorizare pentru a obține un avertisment timpuriu și construiți o rețea de parteneri și experți care vă împărtășească obiectivele și valorile.

În timpul atacului

2. Evaluați situația:

- adunați informații,
- împărtășiți constatările dvs..

3. Informarea publicului și a partenerilor-cheie:

- informați-vă partenerii;
- trimiteți un mesaj oficial către publicul țintă;
- dacă este necesar, dezmințiți informațiile incorecte.

4. Comunicați în mod proactiv:

- includeți-vă aliații;
- asigurați-vă că ședințele de informare etc. pot fi ușor de găsit online.

5. Ocupați-vă de atacator:

- fie ignorați, fie raportați, fie expuneți, fie contracarați.

După atac

6. Evaluați-vă răspunsul:

Experiența te face mai puternic. După atac, evaluați și analizați răspunsul dvs. trecând în revistă procesele și pregătirile. Solicitați feedback de la parteneri și puneți în aplicare sugestiile acestora. Începeți să vă pregătiți pentru următorul atac.

1. Pregătiți-vă

Dacă aveți noroc și o criză încă nu a început, folosiți-vă timpul pentru a pregăti materialele care vă vor ajuta la prezentarea poveștii instituției. Povestea ar trebui să includă obiectivele și valorile pe care le reprezentați (misiune, viziune etc.), ar trebui să fie accesibilă online și utilizată în activitățile de comunicare.

- a. Cunoaște-ți adversarul:** instituțiile UE, serviciile de securitate internă, ONG-urile, mediul academic etc. publică rapoarte și analize. Studiindu-le, rămâneți la curent cu tendințele emergente și cele mai bune practici în comunicarea strategică. Utilizați călătoriile în străinătate și găsiți alte oportunități de a împărtăși cu colegii și experții dvs. la nivel internațional pentru a învăța din experiența altora. Cu alte cuvinte - pentru a ști ce instrument să utilizați din cutia de instrumente, trebuie să știți ce poate și va fi folosit împotriva dvs. Apoi folosiți aceste cunoștințe pentru a crește gradul de conștientizare a amenințărilor și pentru a menține o conștientizare sănătoasă a nivelului de amenințare în instituția dvs.
- b. Imaginați-vă atacul:** gândiți-vă la sarcinile instituției dvs. și imaginați-vă cum ar putea fi realizată această activitate. Rețineți că mass-media controlată de statul rus folosește de obicei un sâmbure de adevăr, îl înfășoară în dezinformare și îl încadrează pentru a vă ridiculiza sau a vă deteriora reputația.
- c. Pregătiți conținutul:** gândiți-vă cum ar putea afecta astfel de știri sau conținut social media angajații și partenerii dvs. și modul în care vă desfășurați activitatea. Ce ar face partenerii tăi? Ce ar aștepta de la tine? Ar veni oamenii pe străzi sau ar lua cu asalt clădirea? Mai bine fiți pregătiți pentru aceste scenarii:
 - I.** creați o descriere clară, ușor de citit și factuală a mandatului instituției dumneavoastră;
 - II.** scrieți un Q&A (întrebări/răspunsuri) despre activitatea de zi cu zi;
 - III.** pregătiți mesaje-cheie, cu fapte și cifre (nu veți avea timp pentru acest lucru în timpul unei crize, dar partenerii și superiorii dvs. așteaptă acest conținut și numai dvs. îl puteți oferi);
 - IV.** veniți și cu niște narațiuni de dezinformare și demințiri pentru ei.
- d. Afișați-vă munca:** distribuiți acest conținut colegilor, experților și conducerii. Utilizați materialul pregătit pentru a instrui oamenii care ar trebui să facă comentarii presei.

-
- e. Monitorați:** stabiliți o situație de referință cu privire la modul în care instituția dumneavoastră este văzută în mass-media și spațiul public (rețele sociale). Dacă este posibil, faceți câteva cercetări de fond cu privire la punctele de pornire și persoanele care vorbesc despre instituția dvs. Rețineți că, practic, nu există mass-media liberă în Rusia și există multe mijloace de a transmite un mesaj care poate viza sau influența direct instituția dvs.:
- I.** comunicări oficiale ale guvernului - declarații ale secretarului de presă al Kremlinului (Dmitri Peskov) sau ale ministerelor (Maria Zakharova);
 - II.** declarații ale oficialilor de rang înalt; profile guvernamentale pe social media (ambasade din întreaga lume, Kremlin, ministere);
 - III.** mesagerie globală finanțată de stat - media destinată publicului extern (FR, Sputnik) sau publicului intern; instituții socio-culturale rusești;
 - IV.** cultivarea surselor proxy – de la puncte de răspândire aliniate Rusiei la persoane private (răspândirea mesajelor pro-Kremlin) la state străine;
 - V.** transformarea rețelelor sociale în arme – infiltrarea conversațiilor interne (grupuri Facebook, secțiuni de comentarii ale mass-mediei online); campanii împotriva sau pentru ceva; alimentarea discordiei civile sau a protestelor, cumpărarea de reclame cu conținut politic; și
 - VI.** manipularea cibernetică a informațiilor - pirateria informatică și eliberarea documentelor furate; falsificarea scrisorilor; clonarea site-urilor web; perturbarea accesului la mijloace de informare în masă fiabile.
- f. Fiți proactivi:** asigurați-vă că materialul pe care l-ați pregătit este accesibil online, precum și pentru partenerii importanți. Colaborați cu mass-media, organizați informări de fundal, stabiliți o prezență pe rețelele sociale și utilizați-o pentru a educa oamenii despre activitatea organizației dvs. Dacă este posibil, includeți sfaturi despre cum să verificați informațiile și sursa acestora. Acest lucru vă va permite să abordați potențialele concepții greșite, informații false sau dezinformare. Nu în ultimul rând, nu subestimați informațiile pe care le puteți aduna și împărtăși atunci când vă întâlniți față în față cu publicul în timpul unei “zile a porților deschise”, a unei mese rotunde, a unei întâlniri cu părțile interesate, a unui eveniment de campanie etc.

Nu vă fie frică să recunoașteți că ar putea exista modificări ale politicii, o decizie care nu a fost luată încă sau există întreruperi ale serviciului din cauza întreținerii etc. Adăugați context și raționament de ce se întâmplă anumiți factori, deoarece acest lucru oferă publicului o privire din culise.

Indiferent cât de bine vă pregătiți, un atac informațional ar putea avea loc. În cazul în care, urmați acești pași:

2. Evaluați situația

Acest pas este important pentru dumneavoastră și pentru instituția pe care o reprezentați, pentru a obține o imagine de ansamblu asupra la ceea ce se întâmplă. În același timp, trimiteți un semnal preliminar altora că sunteți conștienți de ceea ce s-a întâmplat și lucrați la detalii.

- a. Cartografiați situația:** aflați mai întâi dacă este într-adevăr un atac informațional sau doar câteva postări pe social media cu câteva comentarii. Dacă nu aveți o echipă de monitorizare a mass-mediei și a rețelelor sociale și, de asemenea, nu aveți instrumente de ascultare socială (de exemplu, Brandwatch, Meltwater,

Talkwalker), utilizați The Breakout Scale pentru a înțelege cât de rea (sau bună) este situația. Indicele impact-risc ar putea fi, de asemenea, util, la fel ca biblioteca de reclame Facebook.

Rețineți că sarcinile menționate mai sus necesită timp. Prin urmare, fie configurați monitorizarea internă (dacă nu este deja activă), fie cereți ajutor din afara instituției dvs. Conștientizarea situației este crucială pentru a răspunde atacului, iar obținerea unor rapoarte și analize bune de monitorizare necesită feedback. Mai bine testați această colaborare în timpul unui exercițiu de comunicare în situații de criză.

- b. Cereți ajutor:** dacă aveți o relație bună de lucru cu partenerii externi, cum ar fi ONG-uri, mass-media, mediul academic sau colegi din străinătate, abordați-i. Rețineți că apărarea unei țări este o sarcină pentru întreaga societate. Abordarea unui atac informațional poate fi, de asemenea, o chestiune de securitate a statului și, prin urmare, aveți dreptul să cereți ajutor, nu trebuie să rezolvați problemele singuri.
- c. Verificați faptele:** verificați dacă afirmațiile din mesajele care vizează instituția dvs. sunt adevărate.
- d. Informați părțile:** împărtășiți-vă constatările cu colegii și partenerii cheie. Cu cât aud mai repede de la instituția responsabilă, cu atât mai bine.
- e. Fiți transparent:** aduceți jurnaliști, experți și alți parteneri externi care pot evalua și/sau raporta într-un mod neutru și transparent.
-

- f. **Trimiteți un mesaj inițial:** trimiteți un mesaj publicului țintă spunând că sunteți conștienți de ceea ce s-a întâmplat și că vă confrunțați cu situația. Acest lucru vă va oferi ceva timp pentru a dezvolta un răspuns mai exhaustiv.

La sfârșitul acestei faze, ar trebui să puteți răspunde la întrebări precum:

- cine este publicul țintă al dezinformării și puteți ajunge la acesta;
- cât de urgentă este situația și este nevoie de un răspuns imediat;
- Care sunt mesajele, canalele, instrumentele, opțiunile și partenerii pe care îi puteți utiliza pentru a dezamorsa situația.

3. Informarea publicului și a partenerilor cheie

Acest pas este important pentru dumneavoastră și pentru instituția pe care o reprezentați, pentru a obține o imagine de ansamblu asupra la ceea ce se întâmplă. În același timp, trimiteți un semnal preliminar altora că sunteți conștienți de ceea ce s-a întâmplat și lucrați la detalii.

- a. **Trimiteți un mesaj formal:** fiți cât mai transparenți posibil, împărtășiți informații neutre și veridice cu publicul țintă.
- b. **Corectarea erorilor factuale:** dacă se răspândesc informații incorecte despre instituția Dvs, respingeți-le cu fapte relevante. Având o secțiune de întrebări frecvente pe web site este un exemplu clasic și bun despre cum să faceți acest lucru fără a fi nevoie să răspundeți la fiecare întrebare.
- c. **Referință:** în cazul în care experți din afara instituției s-au alăturat dezbaterii publice din proprie inițiativă și au făcut declarații bune și credibile în cadrul procesului, consultați-i acolo unde este posibil.
- d. **Nu uitați de valorile dvs.:** folosiți-vă mesajele pentru a le reaminti oamenilor valorile instituției pe care o reprezentați. Deși sună plictisitor sau prea corect din punct de vedere politic, scopul final este simplu: promovarea unei culturi a civilizației, atât online, cât și în lumea reală, consolidarea mesajelor democratice și promovarea narațiunilor sănătoase. NB! În timp ce Rusia ar putea pretinde că apără valorile religioase tradiționale, atunci modul în care o face este departe de ceea ce poate fi numit civil.

4. Comunicare proactivă

Luăți o poziție clară și comunicați-o proactiv. Partajați-vă datele și analizele cu partenerii și publicul larg și faceți-o din nou și din nou. Acest lucru asigură înțelegerea comună între aliații voștri - aceasta este piatra de temelie pentru a fi pregătiți pentru posibile atacuri informaționale.

- a. **Angajați-vă în dialog:** comunicați cu partenerii cheie și cu publicul și implicați-i în situație.
- b. **Faceți informațiile (mesajele) cheie ușor de găsit și de accesat:** alcătuiți un pachet de informare cu informații veridice pentru a vă susține poziția și încărcăți-l pe web-site. Acesta va deveni un punct de referință pentru viitor.
În plus, asigurați-vă că site-ul dvs. Este în conformitate cu optimizarea motorului de căutare (SEO), deoarece majoritatea oamenilor nu ajung direct pe site-ul dvs., ci prin Google.
- c. **Spuneți povești:** împachetați mesajele în povești care se adresează publicului țintă. Mesajele dvs. ar trebui să ofere cititorului o imagine de ansamblu ușor de înțeles a ceea ce se întâmplă, la ce se referă și să fie ușor de verificat. Faptele și narațiunile se vor completa reciproc.
- d. **Utilizați lideri de opinie:** luați legătura cu lideri de opinie (sau chiar influenceri) care vă pot transmite mesajul către publicul țintă (la nivel local, dar mai ales la nivel internațional).
- e. **Optimizați:** într-o criză, adesea nu există timp pentru a dezvolta noi canale. În schimb, utilizați evenimente, inițiative, web site-uri existente (de exemplu, Wikipedia, care ocupă un loc înalt în motoarele de căutare) pentru a vă răspândi mesajul.

5. Luați măsuri

În timp ce confruntarea cu un atacator sau cu proxy-urile sale ar putea părea imposibilă, există modalități de a contracara folosind aliații și partenerii tăi.

- a. **Ignorați:** uneori este mai bine să nu reacționați deloc. Acest lucru are sens într-o situație în care a avut loc un atac de dezinformare, dar propagarea acestuia este limitată și, prin urmare, impactul său este redus.

-
- b. Raportați:** dacă atacatorul încalcă legile sau regulile, raportați acest lucru poliției sau altor autorități competente.
 - c. Ștergeți/blocați:** unul dintre pilonii unei societăți libere este libertatea de exprimare. Cu toate acestea, în cazuri excepționale, ștergerea conținutului sau a contului cuiva poate fi justificată. Colaborați cu platformele pentru a elimina bifele albastre sau alte semne de verificare din conturile cunoscute pentru conținut greșit/dezinformare.
 - d. Expuneți:** în anumite situații, cea mai bună opțiune poate fi expunerea autorului atacului și atribuirea vinei. Acest lucru merită luat în considerare numai dacă atacatorul este cunoscut (cu suficientă certitudine) și potențialul prejudiciu care poate rezulta nu depășește potențialul impact pozitiv.
 - e. Contracarați:** voluntarii sau partenerii din ONG-uri ar putea:
 - I.** provoca crearea de conținut și răspândirea de informații eronate/dezinformare să demonstreze că nu fac parte dintr-un atac informațional;
 - II.** să expună lipsa de expertiză a acestor actori răi;
 - III.** să utilizeze contra-narațiuni pline de umor, ridiculizând conținutul (cereți partenerilor să o facă sau voluntarilor);
 - IV.** să calmeze discuția emoțională;
 - V.** să organizeze un miting de sprijin în viața reală;
 - VI.** să verifice sursele de informații și mass-media fiabile, să păstreze lista publică;
 - VII.** să expună, să numească și să rușineze modul în care Kremlinul colaborează cu grupurile locale ale societății civile, formatori de opinie, grupurile de reflecție, biserica etc.;
 - VIII.** să utilizeze mijloace juridice împotriva actorilor locali cunoscuți care se află în spatele dezinformării;
 - IX.** să organizeze un cod de conduită sau zece porunci pentru influențatori.
 - f. Fiți pregătiți:** chiar și o glumă sau o postare aparent nevinovată pe social media poate deveni declanșatorul unui atac de dezinformare.
-

6. Evaluați răspunsul

În timp ce exercițiile oferă o mare oportunitate de a găsi probleme în sistemele dvs., tratarea lucrului real ar trebui să fie, de asemenea, luată ca o oportunitate de învățare.

- a. Treceți prin acoperirea (socială) media:** discutați în cadrul echipei sau instituției dvs. ce a mers bine și ce ar putea fi îmbunătățit.
- b. Discutați cu partenerii dvs.:** cereți feedback pentru a identifica domeniile de îmbunătățire. Monitorizarea a fost suficientă? Ați primit toate informațiile necesare de la parteneri? Dacă nu, cum poate fi remediat acest lucru?
- c. Pregătiți-vă pentru următorul atac:** includeți acest feedback în planificarea și îndrumările făcute și împărtășiți aceste lecții cu alții.

CENTRUL PENTRU
COMUNICARE STRATEGICĂ
ȘI COMBATERE A DEZINFORMĂRII

