



Myndigheten för
samhällsskydd
och beredskap

Att möta informationspåverkan

Handbok för kommunikatörer

Att möta informationspåverkan

Handbok för kommunikatörer

Att möta informationspåverkan – Handbok för kommunikatörer

Denna publikation finns även utgiven på engelska

Countering information influence activities: A handbook for communicators

Order No: MSB1263 - Revised December 2018 ISBN: 978-91-7383-911-2

Myndigheten för samhällsskydd och beredskap (MSB)

Produktion: Advant

Publikationsnummer: MSB1260 - reviderad december 2018

ISBN: 978-91-7383-910-5

Innehåll

Förord	5
Inledning	7
Vilken är kommunikatorens roll?	8
Vår metod	9
DEL I. Att bli medveten om informationspåverkan	11
Vad är informationspåverkan?	11
Hur utnyttjas samhällets sårbarheter i informationspåverkan?	13
Hur skiljer sig informationspåverkan från annan kommunikation?	15
DEL II. Att identifiera informationspåverkan	17
Vad är syftet med informationspåverkan?	17
Strategiska narrativ	17
Målgrupper	18
Vilka tekniker används inom informationspåverkan?	18
Social och kognitiv hackning	20
Vilseledande identiteter	21
Teknisk manipulation	23
Desinformation	25
Illasinnad retorik	26
Symbolhandlingar	27
Hur kan påverkanstekniker kombineras?	28
DEL III. Att möta informationspåverkan	31
Hur kan jag förbereda organisationen?	32
Skapa medvetenhet	32
Bygg förtroende genom strategisk kommunikation	32
Känn till organisationens risker och sårbarheter	34
Hur väljer jag rätt respons?	35
Bedöm, informera, förespråka eller försvara?	35
Utforma en faktabaserad respons	38
Särskilda hänsyn för sociala medier	40
Hur tar jag till vara på lärdomar?	42
Strategiska ställningstaganden	44
Ordlista	45
Mer information	46

Förord

Det försämrade omvärldsläget aktualiserar behovet av att öka kunskapen om hur myndigheter kan identifiera, förstå och möta informationspåverkan. Påverkanskampanjer har blivit allt mer sofistikerade och kan användas såväl i fredstid som i krig och berör våra myndigheters ansvar och roller.

Informationspåverkan kan utnyttja samhällets sårbarheter och utmana samhällets funktionalitet, våra grundläggande värden som demokrati, rättssäkerhet och mänskliga rättigheter, ytterst liv och hälsa. Samtidigt är grundläggande i arbetet med att möta informationspåverkan att värna den fria debatten, fri opinionsbildning, yttrandefrihetens principer och det demokratiska samtalet.

Vår regering har bestämt att myndigheter ska kunna identifiera och möta påverkanskampanjer och neutralisera propagandakampanjer. MSB arbetar därför sedan 2014 aktivt med att identifiera, förstå och möta informationspåverkan. En viktig del i detta arbete är att genom kunskapsspridning skapa medvetenhet i samhället om informationspåverkan.

I arbetet med att öka kunskapen om informationspåverkan har önskemål framförts, främst från bevakningsansvariga myndigheter, om en handbok med principer och metoder för att kunna identifiera, förstå och möta informationspåverkan. MSB har därför i samarbete med forskare på Lunds universitet tagit fram denna handbok, som främst riktar sig till kommunikatörer i offentlig förvaltning. Den ska ses som ett stöd för de situationer då en organisation riskerar att bli, eller misstänker sig bli utsatt för informationspåverkan.

Ett stort tack till Institutionen för strategisk kommunikation vid Lunds universitet, vars forskning ligger till grund för handboken, samt de remissinstanser som med sina kloka synpunkter har bidragit till att utveckla handboken. Ett stort tack riktas också till de myndigheter och organisationer som bidragit till att göra handboken bättre och användbar i deras egen organisation.



Dan Eliasson
Generaldirektör

Inledning

Inledning

Bakgrunden till att handboken tagits fram är det förändrade och försämrade omvärlds- och säkerhetsläget. Den illegala annekteringen av Krim och konflikten i Ukraina har visat att säkerhetshoten idag kan anta en annan karaktär. I denna typ av konflikt används i huvudsak andra medel än militära.

Påverkanskampanjer är det begrepp som används för att beskriva denna nya typ av säkerhetshot. I en påverkanskampanj utnyttjar främmande makt samhällets sårbarheter för att uppnå sina mål utan att behöva använda militära medel. Med andra ord är påverkanskampanjer något vi behöver försvara oss emot för att värna målen för Sveriges säkerhet; befolkningens liv och hälsa, samhällets funktionalitet och förmågan att upprätthålla grundläggande värden som demokrati, rättssäkerhet och mänskliga fri- och rättigheter.

MSB definierar påverkanskampanjer som en från främmande makt koordinerad verksamhet som innefattar vilseledande eller oriktig information eller annat för ändamålet särskilt anpassat agerande och som syftar till att påverka beslut av politiska eller andra svenska offentliga beslutsfattare, opinioner hos hela eller delar av den svenska befolkningen, beslut eller opinioner i ett annat land, där Sveriges suveränitet, målen för vår säkerhet eller andra svenska intressen kan komma att påverkas menligt.

En påverkanskampanj består av flera påverkansaktiviteter, en sådan aktivitetstyp är informationspåverkan. Den här handboken hjälper dig som kommunikatör att bli medveten om vad informationspåverkan är för att sedan kunna identifiera och möta denna typ av säkerhetshot.

Att använda information för att påverka människor är inte något nytt. Inom bland annat PR och reklam används information för att påverka allt från människors val att köpa en viss produkt till att stötta en viss politisk kandidat. Vi som medborgare förväntar oss att denna typ av kommunikation följer vissa regler, till exempel att den sker öppet, att den baseras på korrekt information och att den presenteras på ett sätt som gör det möjligt för människor att fatta välavvägda beslut.

Men långt ifrån all påverkan följer dessa regler. Information kan användas i det fördolda eller på ett vilseledande sätt av främmande makt i syfte att till exempel underminera demokratiska processer, kontrollera det offentliga samtalet och påverka beslutsfattande för att på så vis öka det egna inflytandet. Detta kallas för informationspåverkan. I ett globalt perspektiv finns ett antal aktuella exempel där just denna typ av påverkan identifierats, såsom presidentvalen i USA (2016) och Frankrike (2017). Informationspåverkan har ett fientligt syfte men definieras inte som krigshandlingar, även om det ibland betecknas som informationskrigföring i gråzonen mellan krig och fred. Informationspåverkan är att betrakta som fientlig eftersom den riskerar att underminera medborgarnas förtroende för viktiga samhällsinstitutioner, isolera sårbara samhällsgrupper och bidra till social och politisk polarisering.

Vårt samhälle bygger på tillit, både genom allmänhetens förtroende för samhällets institutioner och tilliten mellan människor och grupper i samhället. Förtroende och tillit är en förutsättning för att demokratin ska fungera väl. Informationspåverkan undergräver dessa värden genom att så frön av misstro och underblåsa motsättningar i samhället. När informationspåverkan används av främmande makt och riktas mot allmänheten kan rikets säkerhet således hotas. Förmågan att upprätthålla förtroendet och möta informationspåverkan med tillförlitlig kommunikation är helt avgörande för ett motståndskraftigt samhälle.

Vilken är kommunikatörens roll?

Som kommunikatör har du möjlighet att spela en viktig roll i arbetet med att förebygga, identifiera och möta informationspåverkan. Du medverkar till att din organisation håller vad den lovar och vårdar allmänhetens förtroende. Du kommunicerar med dina målgrupper, hjälper dem när de har frågor och förser dem med samhällsviktig information. Som kommunikatör vet du vad dina målgrupper tycker är viktigt och vad som står på dagordningen.

Även om det verkar osannolikt kan din organisation en dag utsättas för informationspåverkan. Du kanske upptäcker att det sprids felaktig information om din organisation, att det dyker upp falska versioner av er webbplats eller att era konton på sociala medier har kapats. Informationspåverkan kan även riktas direkt mot organisationens målgrupper, genom att de blir föremål för s.k. näthat, trolldning eller vilseledande information. Målet kan vara att underminera förtroendet för din organisation, att föra fram felaktig information i viktiga diskussioner inom ert verksamhetsområde eller att öka spänningar mellan era målgrupper. I samtliga fall har du som kommunikatör möjlighet att spela en viktig roll i arbetet med att stärka och stötta en konstruktiv demokratisk debatt.

VARFÖR KOMMUNIKATÖRER?

- Ni bygger broar mellan organisationer och allmänheten.
- Ni arbetar sedan tidigare med kriskommunikation vilket kan vara ett relevant verktyg för att möta informationspåverkan.
- Ni kan vara bland de första som upptäcker tecken på informationspåverkan.

Som kommunikatör har du redan verktyg som behövs för att möta informationspåverkan. Denna handbok ger dig ytterligare kunskap som kan stödja dig i arbetet. Du får lära dig om teknikerna som kan användas emot dig och hur du känner igen tidiga varningssignaler på att något är på gång. Du får råd om hur du förbereder din organisation för att snabbt och effektivt möta informationspåverkan och vägledning till att fatta rätt beslut om motåtgärder baserat på den specifika situationen och ditt mandat som kommunikatör.

Vår metod

Syftet med denna handbok är att hjälpa dig som kommunikator att utveckla dina kunskaper om och förmåga att identifiera och möta informationspåverkan. Målet är att öka medvetenheten kring, och kunskapen om informationspåverkan. Handboken är tänkt att göra det lättare att identifiera vanliga metoder som används inom informationspåverkan som organisationen kan bli utsatt för, samt tillgängliggöra en verktygslåda med kommunikativa åtgärder som kan användas för att utforma en lämplig respons. Handboken erbjuder inte ett facit till hur du ska gå till väga. Alla organisationer är olika, har olika målgrupper, står inför olika typer av utmaningar och behöver ta hänsyn till dessa faktorer i sin respons.



DEL I: ATT BLI MEDVETEN OM INFORMATIONSPÅVERKAN

Vad är informationspåverkan?

Hur utnyttjar informationspåverkan samhällets sårbarheter?

Hur skiljer sig informationspåverkan från annan kommunikation?



DEL II: ATT IDENTIFIERA INFORMATIONSPÅVERKAN

Vad är syftet med informationspåverkan?

Vilka tekniker används inom informationspåverkan?

Hur kan dessa tekniker kombineras?



DEL III: ATT MÖTA INFORMATIONSPÅVERKAN

Hur kan jag förbereda organisationen?

Hur väljer jag rätt respons?

Hur tar jag till vara på lärdomar?

DEL I.

Att bli medveten om informationspåverkan

Vad är informationspåverkan?

Hur utnyttjar informationspåverkan samhällets sårbarheter?

Hur skiljer sig informationspåverkan från annan kommunikation?

DEL I. Att bli medveten om informationspåverkan



Det här avsnittet beskriver hur informationspåverkan utnyttjar sårbarheter i samhället. I avsnittet presenteras även ett verktyg för att bedöma misstänkt aktivitet och identifiera fall av informationspåverkan.

Vad är informationspåverkan?

Fri debatt, åsiktsskillnader och försök till att övertyga människor är viktiga delar i ett välfungerande demokratiskt samhälle. Men vad händer när någon fabricerar bevis, använder falska experter eller argumenterar på ett avsiktligt missledande sätt? Sådan kommunikation är skadlig för samhället och ett problem för den demokratiska processen. En lämplig respons utgår från fakta, källkritik och yttrandefrihetens principer i syfte att skydda vårt demokratiska samhälle.

I de flesta demokratier finns en fri och levande politisk debatt där enskilda medborgare, journalister, akademiker och representanter från civilsamhället ser det som sin uppgift att utöver den viktiga granskningen av makten också påvisa fall av uppenbart felaktig och vilseledande information. Statliga aktörer kan stötta arbetet genom att exempelvis ge ekonomiskt stöd och bidra med att korrigera felaktigheter kopplat till den egna verksamheten. Detta system har länge tjänat demokratier väl, i alla fall i teorin. Men dagens debatt om falska nyheter antyder att systemet präglas av sårbarheter, vilka främmande makt utnyttjar genom informationspåverkan.

Informationspåverkan är potentiellt skadlig kommunikation som främmande makt eller deras ombud ligger bakom (medvetet eller omedvetet). Det handlar om en medveten inblandning från främmande makt i inomstatliga angelägenheter där försök görs att skapa misstro medborgare emellan samt mellan medborgare och stat. Informationspåverkan används för att stötta främmande makts agenda och utformas så att de utnyttjar uppfattade sårbarheter i samhället. Genom att studera ett samhälle, dess motsättningar, kontroverser och utmaningar riktas insatserna mot dessa sårbarheter i syfte att öka splittringen i landet.

Informationspåverkan kan genomföras som enskilda aktiviteter eller som en del av en större påverkanskampanj. I det senare fallet används ett brett spektrum av tekniker från och utanför kommunikationsfältet. Utöver kommunikativa verktyg används allt ifrån diplomatiska och ekonomiska sanktioner till militära styrkedemonstrationer för att påverka samhället.

PÅVERKANSKAMPANJERS ANATOMI

Användandet av påverkanstekniker

PR, marknadsföring, diplomati, opinionsjournalistik och lobbyverksamhet är exempel på accepterade sätt att påverka människors åsikter och beteenden. Informationspåverkan efterliknar dessa, men kan också inbegripa smutskastning i olika former men använder teknikerna för att vilseleda, som att medvetet ljuga eller fabricera information.

Stör den offentliga debatten

Främmande makt använder informationspåverkan för att influera områden och debatter när de gynnas av detta. Detta kan göras både direkt och indirekt, genom allt från öppen propaganda till dold finansiering av grupper i civilsamhället som går främmande makts ärenden. Genom att störa offentlig debatt kan vår bild av opinionsläge eller tankeströmningar förändras och därmed påverka beslutsfattande.

Agerar i egenintresse

Informationspåverkan syftar till att uppnå särskilda mål som gynnar en främmande makt. Målet kan utgöras av allt från att destabilisera ett samhälle politiskt, att hindra specifika beslut från att fattas eller att skapa polarisering mellan grupper i samhället.

Utnyttjandet av sårbarheter

Alla samhällen har sina utmaningar. Ibland består dessa av spänningar mellan olika grupper, ojämlikhet, korruption, säkerhet eller andra centrala frågor i samhället. Inom informationspåverkan identifieras och utnyttjas dessa sårbarheter systematiskt.

Informationspåverkan präglas av en viss tvetydighet. Det innebär att det ibland är svårt att avgöra vad som är ett äkta inslag i samhällsdebatten. Politiska debatter kan vara känsliga, obekväma och ibland till och med smutsiga.

Det är en naturlig del av den demokratiska processen som bygger på öppenhet och möjlighet till debatt mellan personer med olika åsikter. Men en sådan diskussion blir svår att föra på ett produktivt och konstruktivt sätt om främmande makt introducerar vilseledande information i syfte att störa och styra samtalet.

Det är viktigt att komma ihåg att en avsändare inte automatiskt sympatiserar med främmande makt enbart för att denne uttrycker liknande åsikter. Det är viktigt att understryka att inom informationspåverkan används vilseledande metoder systematiskt i syfte att underminera demokratin. En grundläggande princip vid mötandet av informationspåverkan är därför att värna den fria debatten, yttrandefrihetens principer och det demokratiska samtalet – detta kan inte nog understrykas – även om det försvårar uppgiften.

Hur utnyttjas samhällets sårbarheter i informationspåverkan?

Föreställ dig att våra åsikter uppstår till följd av en rationell process. Det börjar med att någonting händer eller att ny information blir känd. Vittnen, forskare, tjänstemän och andra individer med trovärdighet inom ett område tolkar eller förklarar situationen utifrån ett större sammanhang. Media plockar upp beskrivningarna och sprider dem vidare genom sina kanaler. Informationen når på så sätt olika samhällsgrupper, både online och offline, inklusive dig. Självklart fungerar inte opinionsbildning riktigt så här i praktiken, men i stora drag är det så processen för opinionsbildning i ett demokratiskt samhälle kan förstås.

Denna process bygger på några enkla principer. För det första är den beroende av att händelsen eller informationen är korrekt och att den bygger på fakta. Vidare utgår den från att påståendet är verifierat av trovärdiga källor i form av verkliga människor vars anseende kommer att undermineras om de talar osanning. Det förutsätter att de medier som plockar upp berättelsen är balanserade i sin bevakning, att de dubbelkollar fakta och källor och att de strävar efter att tjäna allmänhetens intresse. Vi förväntar oss även att samtalen i de olika samhällsgrupperna tar hänsyn till olika röster och åsikter samt att man för en konstruktiv debatt innan några slutsatser dras.

Informationspåverkan utnyttjar tillfällen när opinionsbildningen avviker från den process som beskrivits ovan. Genom opportunistiska, kreativa och tekniskt avancerade metoder kan främmande makt rikta sina påverkanstekniker mot processens sårbarheter i syfte att kompromettera informationsflödet. De identifierar sårbarheter i opinionsbildningsprocessen, i hur kritisk information färdas genom medielandskapet och med utgångspunkt i hur våra hjärnor bearbetar information.

Fakta kan förfalskas eller manipuleras. Falska experter kan kallas in och vittnen kan mutas eller hotas. Nyhetstjänster kan drivas som ensidiga propagandakanaler och det digitala offentliga samtalet kan föras mellan automatiserade botar som skapar en skenbild av en livlig offentlig debatt. När dessa aktiviteter genomförs avsiktligt, ibland i form av koordinerade kampanjer i syfte att underminera demokratiska processer, kan vi inte alltid förlita oss på ett självsanerande system. Här kan du som kommunikator spela en viktig roll.

Opinionsbildning

NY INFORMATION

Ny information når oss, genom t.ex. en händelse, en vetenskaplig upptäckt, ett avslöjande i media eller ett politiskt beslut.



EXPERTER, TJÄNSTEMÄN OCH KÄLLOR

Ny information observeras och dokumenteras av vittnen, experter och tjänstemän som förklarar eller tolkar informationen.



MEDIA OCH KULTUR

Informationen når allmänheten genom media och andra kulturyttringar. Exempelvis genom tidningar, TV, radio, bloggar eller sociala medier.



ALLMÄNHETEN

Informationen når allmänheten och bearbetas genom diskussion och dialog inom olika grupper i samhället, både ansikte mot ansikte och på sociala medier.



INDIVIDEN

På så sätt når informationen dig som individ, genom de sociala sammansättningar du ingår i och de kanaler du konsumerar.



SÅRBARHETER I MEDIESYSTEMET

Vårt moderna mediasystem har flera sårbarheter, särskilt i förhållande till samtidens föränderliga tekniklandskap, nya journalistiska affärsmodeller och den tilltagande mängden alternativa nyhetskällor online. Allt från förfalskade brev och manipulerade bilder till klickjakt, algoritmer och botar på sociala medier gör mediasystemet sårbart för den som vill utnyttja det för egen vinning. Detta oavsett om det drivs av ekonomiska eller politiska motiv, eller helt enkelt för att se om det går.

SÅRBARHETER I OPINIONSILDNINGEN

Opinionsbildning har alltid varit sårbar, exempelvis utifrån tanken om social bevisföring (dvs. vad någon påstår sig ha upplevt själv). I dagens informationsmiljö, där falska konton på sociala medier och troll snedvrider debatten online, är det lättare än någonsin att fabricera sociala bevis, provocera, väcka ilska och upprördhet. Detta bidrar till att polarisera den politiska debatten och är därför en sårbarhet i den allmänna opinionsbildningen.

KOGNITIVA SÅRBARHETER

Vissa sårbarheter uppstår till följd av hur våra hjärnor fungerar. Vi är helt enkelt inte gjorda för att hantera all den information vi utsätts för i dagens samhälle. Genom exempelvis så kallade psykografiska metoder kan personlig information om oss på nätet användas för att förstå hur vi fungerar, till och med bättre än vi förstår oss själva. Enligt vissa uppskattningar finns det upp till 800 datapunkter för varje individ på sociala medier som kan användas för att förutsäga åsikter och beteenden. Inom informationspåverkan utnyttjas våra tankemönster tillsammans med information om oss för att påverka våra uppfattningar, beteenden och beslutsfattande.

Hur skiljer sig informationspåverkan från annan kommunikation?

Det är inte kommunikatörens roll att undersöka huruvida främmande makt är ansvarig för specifika kommunikationsaktiviteter. Du förväntas agera i de fall du misstänker att informationspåverkan används i debatter kopplat till ditt verksamhetsområde, eller i syfte att underminera den offentliga debattens integritet och samhällets säkerhet. Det gäller med andra ord att förstå den egna organisationens roll i ett större sammanhang, i ett samhällsperspektiv.

För att identifiera fall av informationspåverkan behöver du bedöma i vilken utsträckning kommunikationen är vilseledande, sker avsiktligt och i syfte att störa. Genom att väga samman dessa faktorer vid bedömningen av ett misstänkt fall har du möjlighet att fatta ett informerat beslut om hur du ska utforma din respons. Samtliga indikationer kommer inte nödvändigtvis kunna ses framträda samtidigt, men ju fler du identifierar desto högre är sannolikheten att det handlar om informationspåverkan.

VILSELEDANDE

Tillförlitlig kommunikation är öppen och transparent. Innehållet är trovärdigt och kan verifieras. Informationspåverkan är medvetet vilseledande.

AVSIKTLIG

Tillförlitlig kommunikation syftar till att bidra till och stärka konstruktiv debatt, även om innehållet eller argumenten kan vara kontroversiella i sig. Informationspåverkan har däremot som avsikt att underminera det konstruktiva samtalet och den öppna debatten.

STÖRANDE

Tillförlitlig kommunikation är en naturlig del av vårt samhälle som, även om den naturligtvis ibland kan skapa friktion, stärker vår demokrati. Informationspåverkan stör och försvagar samhällets funktionalitet och vårt demokratiska samtal.

Det är ingen slump att tekniker som används inom informationspåverkan ofta överlappar dem som används inom journalistik, offentlig diplomati, lobbyverksamhet och PR. Att efterlikna dessa metoder är ett sätt att dölja informationspåverkan och få den att framstå som tillförlitlig information. Olaglig påverkan såsom hot, dataintrång, utpressning eller mutor faller utanför denna diskussion och ska rapporteras till polisen.

DEL II.

Att identifiera informationspåverkan

Vad är syftet med informationspåverkan?

Vilka tekniker används inom informationspåverkan?

Hur kan olika tekniker kombineras?

DEL II. Att identifiera informationspåverkan



En förutsättning för att möta informationspåverkan är förmågan att upptäcka potentiella fall. Det betyder att du måste veta vad du ska hålla utkik efter. I detta avsnitt presenteras en ingående beskrivning av de tekniker som används vid informationspåverkan. Avsnittet hjälper dig att utvärdera strategiska narrativ och tekniker för målgruppsanpassning, ger en introduktion till de vanligaste teknikerna och visar hur de kan kombineras till koordinerade insatser.

Vad är syftet med informationspåverkan?

För att identifiera informationspåverkan behöver du först känna till två övergripande strategier som används inom informationspåverkan, nämligen strategiska narrativ och tekniker för målgruppsanpassning. Kunskap om dessa kan hjälpa dig att identifiera informationspåverkan och bidra till insikter om syftet med påverkansaktiviteterna.

Strategiska narrativ

Informationspåverkan innefattar vanligtvis någon form av berättande (eng. storytelling). Skildringen av en händelse, fråga, organisation, plats eller grupp formuleras vanligtvis för att passa in i ett befintligt narrativ. De flesta har till exempel hört talas om rymdkapplöpningen mellan USA och Sovjetunionen under kalla kriget. De flesta har hört berättelser om hur människan landade på månen, andra har hört berättelser om att allt är en lögn. På video kan vi se hur astronauter planterar en flagga på månen, vissa tar detta som ett bevis för att månlandningen ägt rum och andra hävdar istället att detta är fejkat. Dessa är typiska narrativ som används omedvetet för att sortera ny information. När vi hör nya berättelser om rymdresor sorterar vi informationen och värderar den i relation till vilken av dessa versioner vi tror på. När sådana berättelser konstruerats och kommunicerats i syfte att uppnå ett visst mål kallas de för strategiska narrativ.

Man kan till exempel hitta på saker om vissa etniska eller religiösa grupper som passar in i folks förutfattade meningar om dessa grupper, dvs. det existerande narrativet. Diskussionen kan påverkas på tre olika sätt: antingen genom att man lyfter fram delar av det existerande narrativet, genom att trycka undan andra narrativ eller genom att göra nya kopplingar till orelaterade händelser för att distrahera.

Att identifiera strategiska narrativ och logiken bakom påverkansaktiviteter utgör ett viktigt steg i att förbereda och ta fram lämpliga responsstrategier för att möta påverkan. Fundera på om du kan se strategiska narrativ användas på något av följande tre sätt.

STRATEGISKA NARRATIV

Positivt eller konstruktivt: "Det här är sanningen!"

Försök att konstruera en sammanhängande berättelse om en viss fråga som passar in i, kompletterar eller utvecklar befintliga narrativ.

Negativt eller nedbrytande: "Det här är lögn!"

Syftar till att förhindra uppkomsten av sammanhängande narrativ, eller underminera befintliga narrativ i en fråga.

Undvikande: "Titta här borta!"

Avleder uppmärksamhet från en viss fråga eller ett visst argument genom att distrahera samtalen. I detta avseende används ofta t.ex. humor, memes eller konspirationsteorier.

Målgrupper

Att analysera strategiska narrativ är ett av flera tillvägagångssätt för att förstå logiken bakom misstänkta fall av informationspåverkan. Ett annat sätt är att analysera vem dessa strategiska narrativ talar till, dvs. vem den tilltänkta målgruppen är. Riktas narrativen mot hela befolkningen eller mer specifikt mot enskilda grupper eller individer? Använder man storskalig dataanalys (eng. big data) för att utforma riktade insatser mot personer med liknande personlighetsdrag och åsikter? Använder man målgruppsanpassning för att utnyttja sårbarheter eller beteendemönster kopplat till den specifika gruppen eller individen? Om man vet vem en berättelse riktar sig till blir det lättare att förstå syftet bakom och hur informationspåverkan är tänkt att fungera i det specifika fallet.

MÅLGRUPPER

Samhällsnivå: bred publik

Informationspåverkan inriktas mot breda grupper i samhället eller samhället som helhet genom att nyttja stora, gemensamma narrativ.

Sociodemografisk inriktning: specifika grupper

Specifika målgrupper identifieras baserat på demografiska faktorer som ålder, inkomst, utbildning eller etnicitet. På så sätt kan man skapa budskap anpassade för att tilltala gruppens medlemmar.

Psykografisk inriktning: individer

Data om individer används för att identifiera specifika personlighetsdrag såsom politiska preferenser eller beteendemönster, som kan ligga till grund för individuellt anpassad kommunikation.

Målgruppsanalysen kan avslöja intentionen bakom informationspåverkan. Om du analyserar de strategiska narrativ och kommunikationstekniker som används kan du skapa dig en uppfattning om vem som är den tilltänkta mottagaren och på så sätt skapa en förståelse för syftet och målsättningen med påverkansaktiviteten. Den analysen hjälper dig i sin tur att fatta beslut om lämpliga motåtgärder

Vilka tekniker används inom informationspåverkan?

Inom informationspåverkan används en rad tekniker för att påverka människors beslut. Teknikerna är under ständig utveckling där vanligt förekommande tekniker kan delas in i sex övergripande grupper. Inom varje grupp karaktäriseras teknikerna av liknande principer. Genom att förstå hur dessa tekniker ser ut och fungerar har du möjlighet att lättare känna igen och identifiera fall av informationspåverkan.

Teknikerna är i de flesta fall neutrala. Samma teknik kan användas som en naturlig del av det demokratiska samtalet (i de fall de tillämpas på ett öppet och accepterat sätt) eller som en teknik inom informationspåverkan (i de fall de används för att vilseleda allmänheten). Att en viss teknik förekommer inom ditt område är därför inte nödvändigtvis ett säkert tecken på att det rör sig om informationspåverkan.

Istället bör du utgå ifrån din bedömning av i vilken grad aktiviteten är avsiktligt vilseledande i syfte att skada samhället och använda din analys av strategiska narrativ och målgruppsanpassning för att besvara följande frågor:

- Hur starka är indikationerna på vilseledande och störande syften?
- Vad säger de strategiska narrativen och den tilltänkta målgruppen om syftet med kommunikationen?
- Om användandet av någon specifik teknik förekommer, används den på ett sätt som kan vara skadligt för allmänheten eller samhället?

Tekniker inom informationspåverkan



SOCIAL OCH KOGNITIV HACKNING (sid 20)

- Dold annonsering (dark ads)
- Bandwagon-effekten
- Tystnadsspiralen
- Ekokammare och filterbubblor



VILSELEDANDE IDENTITETER (sid 21)

- Lockfåglar (shilling)
- Imitatörer och bedragare
- Förfalskningar
- Potemkinkulisser
- Falsa medier



TEKNISK MANIPULATION (sid 23)

- Botar
- Sockpuppets
- Deepfakes
- Nätfiske



DESINFORMATION (sid 25)

- Fabricering
- Manipulation
- Falsk tillskrivning
- Satir och parodi



ILLASINNAD RETORIK (sid 26)

- Personangrepp (Ad hominem)
- Whataboutism
- Störtflod av argument (gish-gallop)
- Halmgubbar (strawman)
- Kapning av argument



SYMBOLHANDLINGAR (sid 27)

- Läckor
- Hackning
- Offentliga demonstrationer

Social och kognitiv hackning

Social och kognitiv hackning utnyttjar våra sociala relationer och tankeprocesser. Det liknar hackning av exempelvis datorsystem i avseendet att en fientlig aktör försöker lura eller "hacka" en process genom att utnyttja dess sårbarheter.

Vi föredrar t.ex. vanligtvis att anpassa oss till vad människor som liknar oss tänker och gör, och har ibland svårt att tänka rationellt när vi exponeras för känslomässigt laddat innehåll. Dessa förutsägbara beteendemönster kan utnyttjas av fientliga aktörer som avsiktligt trycker på ömma punkter, exempelvis i känsliga samhällsfrågor, för att uppnå sitt syfte.



DOLD ANNONSERING (DARK ADS)

Budskap som skräddarsys efter en individs psykografiska profil. Genom data från bland annat sociala medier går det att skapa databaser över individer med specifika uppfattningar, intressen eller personlighetsdrag. Annonser som endast kan ses av specifika individer kan innehålla budskap som tilltalar just deras preferenser eller åsikter.

BANDWAGON-EFFEKTEN

Personer som upplever sig vara del av en majoritet är mer benägna att dela med sig av sin åsikt. Botar och troll kan användas för att ge fler gilla-markeringar, kommentarer eller delningar på sociala medier för att ge intrycket att av vissa åsikter är mer populära än de egentligen är. Detta skapar social acceptans för ett budskap eller en åsikt vilket spelar på vårt kognitiva behov av social likriktning.

TYSTNADSSPIRALEN

Personer som upplever sig vara i minoritet är mindre benägna att dela med sig av sina åsikter. I motsats till bandwagon-effekten kan intrycket att man är i minoritet göra att man inte vill eller vågar uttala sig. Detta spelar på vår rädsla för att exkluderas eller pekats ut som avvikande.

EKOKAMMARE OCH FILTERBUBBLOR

Naturliga grupperingar inom vilka personer framförallt kommunicerar med andra som delar samma åsikter och uppfattningar. Ekokammare och filterbubblor kan uppstå både på och utanför internet. Personer med liknande åsikter kanske läser samma tidningar eller huvudsakligen umgås med likasinnade. De exponeras därför sällan för ideologiskt annorlunda åsikter. På nätet kan detta utnyttjas för att sprida riktad information till specifika grupper.

Vilseledande identiteter

När vi bedömer information tittar vi ofta på källan. Vem kommunicerar med mig och varför? Vad vet de om frågan? Vilka utger de sig för att vara? Aktörer kan efterlikna trovärdiga informationskällor som personer, organisationer eller plattformar och använda sig av vilseledande identiteter för att utnyttja budbärarens förtroendekapital.



LOCKFÅGLAR (SHILLING)

En lockfågel är en person som ger intryck av att vara fristående men som i själva verket samarbetar med eller tar emot betalning av någon annan. Lockfåglar används ibland för att skriva positiva produktrecensioner på webbutiker och för att ge trovärdighet till en person eller ett budskap. Det kan likställas med inköpt publik som garanterar applåder efter en föreställning. Inom informationspåverkan kan lockfåglar exempelvis vara en grupp internet troll som får betalt för att skriva kommentarer.

IMITATÖRER OCH BEDRAGARE

Imitatorer låtsas att de är någon annan än de egentligen är, dvs. ikläder sig någon annans identitet. Det kan röra sig om bedragare som påstår sig ha expertkunskap eller kvalifikationer de egentligen saknar, som att utge sig för att vara läkare eller advokat utan att ha genomgått den utbildning som krävs.

FÖRFALSKNINGAR

Att fabricera och förfalska information är ett effektivt sätt att få desinformation att framstå som autentisk information. Falsa sidhuvuden, stämplat eller namnteckningar kan användas för att få rena falskarier att se äkta ut.

POTEMKINKULISSER

Resursstarka aktörer kan gå ett steg längre och skapa falska och vilseledande institutioner och nätverk. Falsa företag, forskningsinstitut och tankesmedjor är exempel på det som kallas potemkinkulisser som kan skapas och användas för att skänka äkthet till desinformation.

FALSKA MEDIER

Desinformation kan också spridas genom förfalskade nyhetssajter som efterliknar äkta sådana. På internet kan man exempelvis skapa en falsk webbplats som är i stort sett identisk med en riktig webbplats, men med annat innehåll.

Källkritik på nätet

RUBRIKEN

Rubriker försöker framkalla intresse och respons från läsaren. Läs alltid mer än bara rubriken och kontrollera att rubriken stämmer överens med resten av artikelns eller sidans innehåll.

URL

Att imitera välkända plattformar är en vanlig teknik inom informationspåverkan. Se till att du är på rätt plattform genom att ta en närmare titt på URL-adressen.

INNEHÅLL

Gör en bedömning av textens innehåll. Är den informativ, argumenterande, baserad på fakta, känslor eller åsikter? Läs alltid hela texten innan du delar eller sprider den vidare.

KÄLLOR

Om texten refererar till andra källor, se till att kontrollera dessa och spåra informationens ursprung. Gör en bedömning om källorna används korrekt i texten.

KOMMENTARER

Kommentarer på hemsidor och sociala medier kommer oftast från vanliga människor som uttrycker sina åsikter. Det kan dock även förekomma trollkonton och botar i kommentarsfälten. Var uppmärksam på vilka som kommenterar.

BILDER

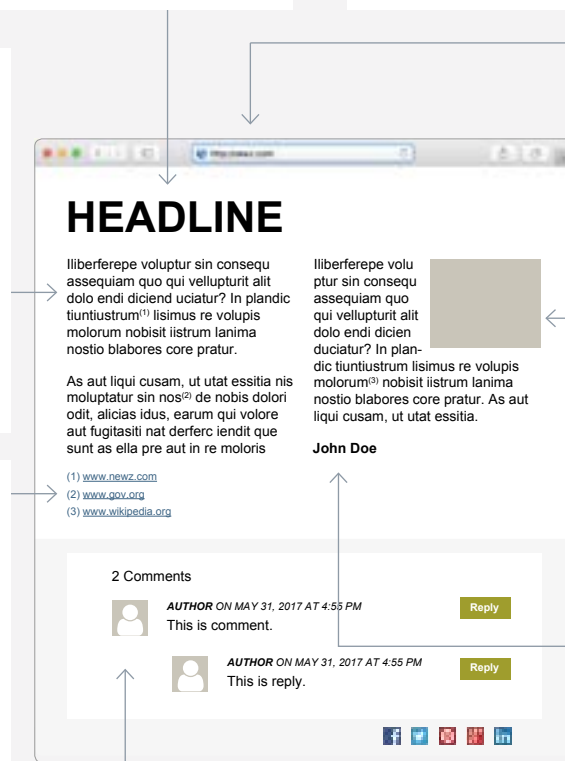
Bilder speglar inte alltid verkligheten. Bilder kan enkelt manipuleras genom att element tas bort, redigeras eller läggs till. Det är heller inte säkert att bilden har en verklig koppling till innehållet. Genom en bildsökning kan du ta reda på om bilden använts tidigare i något annat sammanhang.

FÖRFATTARE

Var uppmärksam på texter utan författare. Om det finns en författare, fundera över vem det är och varför den personen skrivit texten.

UPPMÄRKSAMHET

Att en text gillas eller delas mycket betyder inte att innehållet stämmer. Var försiktig med att dela något enbart baserat på uppmärksamhet den fått från andra.



Teknisk manipulation

Informationspåverkan drar ofta nytta av modern teknologi för att uppnå effekt. Med avancerade tekniska kunskaper kan individer manipulera informationsflödet på internet genom automatiserade konton och algoritmer eller en kombination av mänsklig och teknisk manipulation. Lägga märke till att det inom teknisk manipulation ofta används nya verktyg för att utföra traditionella påverkanstekniker, exempelvis för att skapa vilseledande identiteter online eller för att skapa och sprida desinformation. Detta är ett område som utvecklas långt mycket snabbare än vår förmåga att analysera potentiella konsekvenser och användningsområden. I närtid har problem med så kallade deep fakes, maskin- och djupinlärning samt artificiell intelligens (AI) aktualiserats och vi kan förvänta oss att denna typ av teknologi i framtiden kommer användas i ökad utsträckning.



BOTAR

Botar är datorprogram som utför automatiserade uppgifter, till exempel att dela vissa typer av information på sociala medier eller för att svara på vanliga frågor på en kundtjänstplattform. Inom informationspåverkan kan de användas till att förstärka utvalda budskap på nätet, spamma forum och kommentarsfält, gilla eller dela inlägg på sociala medier, eller för att genomföra cyberattacker.

SOCKPUPPETS

Falska konton som hör till en individ som inte avslöjar sin riktiga identitet eller sina avsikter. Dessa falska identiteter används för att gå med i grupper och delta i debatter online. Två eller flera sockpuppets kan användas samtidigt för att simulera båda sidor i en debatt.

DEEPPFAKES

Moderna inlärningsalgoritmer kan användas för att manipulera ljud och video på väldigt avancerade sätt. Man kan exempelvis producera falska men väldigt trovärdiga videoklipp där politiker läser upp påhittade tal. Man kan även byta ansikten på personer i befintliga videoklipp eller rekonstruera en persons röst digitalt.

NÄTFISKE

Nätfiske är en teknik som lurar användare att uppge lösenord eller annan känslig information på internet. Nätfiske omfattar även automatiserad spamning via e-postmeddelanden som framstår som om de skickats från en känd avsändare men som egentligen tillhör en bedragare som är ute efter personlig information. Spjutfiske (spear-phishing) är en sofistikerad typ av nätfiske för att komma åt information på säkra datorsystem.

Så upptäcker du en bot

Botar är effektiva verktyg för att bedriva påverkan på sociala medier. Men de är samtidigt relativt enkla att avslöja. Dessa sju steg hjälper dig att identifiera botar på sociala medier. Botar förekommer i olika former och kan se väldigt olika ut. Imitatörsbotar försöker efterlikna riktiga användare och kan vara svåra att upptäcka. Spambotar, å andra sidan, fokuserar på att sprida information snabbt och brett och är därför lättare att känna igen.



1 PROFILBILD

Antingen använder botar en stulen profilbild eller så saknar de profilbild helt och hållet. Gör en bildsökning för att verifiera profilbildens äkthet.

2 AKTIVITET

Många botar är väldigt aktiva, ibland med upp till 50 inlägg om dagen. Var vaksam mot konton med ett misstänksamt högt antal inlägg per dag.

3 NAMN

De flesta botar genererar sina användarnamn automatiskt. Upptäcker du konton med användarnamn som tycks vara slumpmässigt kan detta vara ett tecken på en bot.

4 KONTOTS SKAPANEDATUM

Många botkonton är skapade i direkt anslutning till att boten ska användas och är därför väldigt nya. Ibland används äldre konton men då tas ofta gamla inlägg bort, vilket resulterar i ett stort gap mellan skapandedatumet och första inlägget.

5 SPRÅK

Botar använder ibland automatisk översättning för att sprida budskap på flera språk. Detta leder till uppenbara grammatiska fel eller osammanhängande meningar. Konton som publicerar liknande innehåll på olika språk kan vara botar.

6 INFORMATION

Botkonton saknar ofta personlig information, alternativt använder påhittad eller förfalskad information. Kontrollera den information som anges.

7 INTERAKTION

Granska vilka inlägg och andra användare kontot interagerar med. Botar samordnas ofta och förstärker varandra, samtidigt som de har få följare som inte är botar.

Desinformation

Med desinformation avses felaktig eller manipulerad information som sprids avsiktligt i syfte att vilseleda. Detta är en hörnsten i klassisk propaganda och utgör grunden till nutida diskussioner om ”falska nyheter”. Att medvetet använda desinformation för att vilseleda är inget nytt men digitala plattformar har skapat nya möjligheter och förändrat desinformationens karaktär. Felaktig information kan uppstå i form av manipulerad text, bild, video eller ljud. Dessa element kan användas för att stötta felaktiga narrativ, skapa förvirring eller för att misskreditera trovärdig information, individer eller organisationer.



FABRIKATION

Felaktig information som publiceras på ett sätt som får mottagaren att tro att den är sann. Fabricerade e-postmeddelanden från en politiker kan till exempel produceras och läckas till pressen för att undergräva politikerns trovärdighet.

MANIPULATION

Information som manipuleras för att kommunicera ett vilseledande och felaktigt budskap, exempelvis genom att lägga till, ta bort eller ändra element i text, bild, video- eller ljudklipp.

FALSKT ELLER FELAKTIGT SAMMANHANG

Presentation av korrekt fakta i ett orelaterat sammanhang för att framställa en fråga, händelse eller person på ett vilseledande sätt. Till exempel kan bilder tagna i andra sammanhang användas för att förstärka narrativet i en nyhetsartikel.

SATIR OCH PARODI

Satir och parodi är i vanliga fall harmlösa underhållningsformer. Inom informationspåverkan kan humor dock användas som verktyg för att sprida vilseledande information och förlöjliga eller kritisera individer, narrativ eller åsikter. Humor kan även användas för att legitimera kontroversiella åsikter.

Illasinnad retorik

Retorik är ett accepterat och naturligt inslag i en demokratisk samhällsdebatt, där alla har rätt att uttrycka sin åsikt. Illasinnad retorik drivs i ett annat syfte. Det kan handla om att utnyttja ett offentligt samtal i syfte att vilseleda eller distrahera publiken. Det kan också handla om strategier för att bedra, vilseleda och avskräcka vissa aktörer från att delta i samhällsdebatten.

En aktör som ofta använder sig av illasinnad retorik är troll. Troll är användare på sociala medier som avsiktligt provocerar andra genom sina kommentarer och handlingar online. Deras aktivitet bidrar till ökad polarisering, tystar kritiska röster och överröstar den öppna debatten. Troll kan drivas av personliga motiv eller arbeta på uppdrag av någon annan (även kallat *hybridtroll*).



PERSONANGREPP (AD HOMINEM)

Att attackera, misskreditera och förlöjliga personen bakom ett argument istället för att kritisera argumentet i sig. Personangrepp används ofta i syfte att tysta ner, hindra och avskräcka andra från att delta i diskussionen.

WHATABOUTISM

Att ta fokus från ett argument genom att belysa ett liknande fenomen som inte fått lika mycket uppmärksamhet, men som inte är riktigt relevant i frågan.

STÖRTFLOD AV ARGUMENT (GISH-GALLOP)

Att översvämma motparten med en flod av argument, fakta och källor, varav många är falska eller orelaterade till frågan.

HALMGUBBAR (STRAWMAN)

Att tillskriva sin meningsmotståndare argument och ståndpunkter denne inte står för, och sedan argumentera mot dessa ståndpunkter istället för motståndarens faktiska ståndpunkter.

KAPNING AV ARGUMENT

Att ta över en debatt och ändra dess riktning. Detta är särskilt effektivt på sociala medier i förhållande till hashtags och memes.

Symbolhandlingar

Handlingar säger mer än ord. Ibland kan syftet med en handling främst vara att kommunicera ett budskap. Detta kallas för en symbolisk handling. Till skillnad från vanliga handlingar motiveras symboliska handlingar av en kommunikativ logik och en strategisk inramning. De kan utformas så att budskapet är uppenbart för alla, som i exempelvis terrorhandlingar där aktörer spelar på den allmängiltiga rädslan för besinningslöst våld. Andra gånger är de mer subtila, som när man använder sig av kulturella symboler som bara är relevanta för en viss målgrupp.



LÄCKOR

Läckor har en stark symbolisk betydelse eftersom de kan avslöja orättvisor och mörkläggningar som annars inte kommit till allmänhetens kännedom. Inom informationspåverkan tas dock läckt information ofta ur sitt sammanhang och används för att systematiskt undergräva en aktörs trovärdighet och förvränga informationsmiljön. Den läckta informationen kan ha erhållits exempelvis genom datorintrång eller stöld.

HACKNING

Hackning innebär att skaffa sig obehörig åtkomst till en dator eller ett nätverk, och är i sig ett brott. Inom informationspåverkan fungerar hackning ibland som en symbolisk handling där själva intrånget är sekundärt. Det egentliga målet är att väcka misstanke om att ett system är exponerat eller osäkert, vilket kan underminera förtroendet för systemet ifråga eller en organisation med ansvar för detsamma.

OFFENTLIGA DEMONSTRATIONER

Demonstrationer är symboliska handlingar som används för att uttrycka stöd för en viss politisk fråga eller ståndpunkt. De är viktiga delar i vår demokratiska dialog. Inom informationspåverkan kan demonstrationer orkestreras för att ge ett falskt intryck av stöd för en viss fråga på gräsrotsnivå (så kallad astroturfing).

Hur kan påverkanstekniker kombineras?

För att identifiera fall av informationspåverkan behöver du väga samman bedömningen av de strategiska narrativ, målgrupper och tekniker som används. I bedömningen bör du tänka på att flera tekniker ofta kombineras för att uppnå en större effekt.

Ett förfalskat dokument kan exempelvis få större spridning med hjälp av botar. Effekten förstärks än mer om insatsen samordnas med att vinklade artiklar sprids på falska nyhetsplattformar som sedan kommenteras av en koordinerad grupp som använder trolltekniker. Fundera därför över om det finns bevis på inte bara enstaka utan även ett flertal, samordnade aktiviteter som riktas mot din organisation. På nästa sida hittar du några exempel på hur kombinationer av tekniker kan se ut.

Vi har föreslagit några olika frågor du kan ha i åtanke för att bedöma kommunikation och identifiera informationspåverkan. Vilka är narrativen och vem riktar de sig till? Finns det belägg som stödjer påståendet att någon försöker vilseleda eller störa det offentliga samtalet? Misstänker du direkt inblandning från främmande makt eller indirekt via deras ombud? Ser du tecken på kombinationer av metoder som antyder en samordnad aktion eller kampanj? Om din bedömning ligger till grund för att misstänka fall av informationspåverkan hittar du förslag till motåtgärder i handbokens nästa del (Del III: Att möta informationspåverkan).

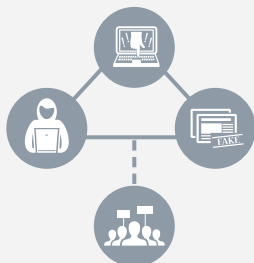
Kombinerade tekniker

Ovanstående tekniker påträffas sällan enskilt utan kombineras ofta för att uppnå effekt. Du bör vara på din vakt för de teknikkombinationer du kan komma att utsättas för. Antalet tänkbara kombinationer är i teorin oändligt stort, men några av de vanligaste kombinationerna kan vara värdefulla att känna till.



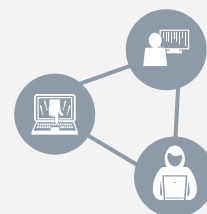
Polarisering

Polarisering kombinerar social hackning, vilseledande identiteter och desinformation för att underblåsa extrema positioner i samma fråga. Ofta används troll och botar för att förstärka extrema åsikter.



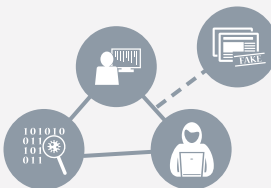
Informationstvätt

Informationstvätt kombinerar vilseledande identiteter, desinformation, teknisk manipulation, symboliska handlingar och social- och kognitiv hackning för att gradvis förvränga och avkontextualisera information så att det blir mycket svårt för mottagaren att avgöra vad som är sant eller falskt.



Provokation

Provokation utnyttjar känsliga frågor i samhället för att hetsa människor och skapa ilska och osämja. Kombinationen utnyttjar främst social- och kognitiv hackning, vilseledande identiteter och skadlig retorik.



Översvämning

Översvämning syftar till att överbelasta en målgrupp med information vilket bland annat kan uppnås genom spamming och trollning på sociala medier eller genom att sprida desinformation via mediekällor för att tränga ut tillförlitlig information.

DEL III.

Att möta

informationspåverkan

Hur kan jag förbereda organisationen?

Hur väljer jag rätt respons?

Hur tar jag till vara på lärdomar?

DEL III. Att möta informationspåverkan



I det här avsnittet diskuteras olika metoder för att möta informationspåverkan. Avsnittet beskriver hur du kan förbereda din organisation, diskutera olika motåtgärder och ger förslag på hur din organisations kunskap och erfarenheter kan spridas vidare för att bidra till en kunskapsöverföring över organisationsgränser.



FÖRBEREDA

Skapa medvetenhet
Bygg förtroende
Bedöm risker



AGERA

Välj respons
Gör faktakoll
Nyttja sociala medier



LÄRA

Beskriva
Reflektera
Dela

Hur kan jag förbereda organisationen?

Den viktigaste delen för att bygga beredskap är förberedelser. Genom att förbereda människor och etablera fungerande strukturer för att möta informationspåverkan möjliggörs ett snabbt och effektivt svar och ett mildrande av effekterna. Förberedelserna består av tre huvudsakliga delar: Att skapa medvetenhet om informationspåverkan. Att utveckla budskap, narrativ och en förståelse för på vilket sätt dina målgrupper och intressenter är sårbara för olika typer av informationspåverkan. Att genomföra en risk- och sårbarhetsanalys av din organisation i syfte att identifiera och förebygga informationspåverkan.

Skapa medvetenhet

En viktig del i att skapa en beredskap för att hantera informationspåverkan handlar om att öka medvetenheten om de hot och sårbarheter som samhället i allmänhet och din organisation i synnerhet står inför. På samhällsnivå är det bästa försvaret att skapa mötesplatser där exempelvis ledare, journalister, företrädare för sociala medieplattformar, forskare, kommunikatörer och medborgare kan utbyta kunskap och lärdomar om att möta informationspåverkan.

Som kommunikatör finns det även saker du kan göra för att bygga upp en kapacitet inom din organisation. För det första kan du vara en viktig kontaktpunkt genom din kunskap inom området. Det är framförallt viktigt att du för diskussioner med den högsta ledningen och kommunicerar internt med kollegor i frågor kopplade till ämnet. För det andra bör du ha en rådgivande roll gentemot dina chefer och kollegor avseende vilka åtgärder som bör vidtas i händelse av att organisationen utsätts för informationspåverkan. I detta ingår att identifiera behov av och möjligheter till utbildning. För det tredje bör du bygga nätverk bestående av yrkesverksamma även utanför din organisation som baseras på ömsesidigt stöd och utbyte av erfarenheter. För det fjärde kan en ökad transparens och kännedom om din organisations verksamhet förebygga spridningen av felaktiga uppgifter.

Bygg förtroende genom strategisk kommunikation

Ett av målen med informationspåverkan är att undergräva människors förtroende för samhällets institutioner. Effekten kan därför minimeras genom att fokusera på motåtgärder som bygger förtroende för organisationen. Detta är en mycket viktig del i alla strategier för att möta informationspåverkan.

Förbereda kommunikation

Då det kan ta tid att få budskap godkända i krissituationer är det viktigt att förbereda generiska budskap. Dessa budskap bör formuleras utifrån organisationens värderingar och på ett sådant sätt att de enkelt kan anpassas till specifika händelser. På samma sätt som organisationer använder budskap för att berätta om nya initiativ eller en ny produkt kan budskap också användas för att skapa medvetenhet om falska berättelser eller för att motbevisa dem.

FÖRBEREDA BUDSKAP

Att delge korrekt information i rätt tid möjliggörs av gediget förarbete, där färdiga budskap tagits fram och godkänts redan innan något händer. Ett gott exempel är Londonpolisen som skickade sin första tweet endast sju minuter efter terrorattacken i Westminster i mars 2017. Meddelandet innehöll korrekt information om den pågående situationen, och var baserat på en kommunikationsmall som tagits fram för liknande situationer och snabbt kunde anpassas efter det aktuella händelseförloppet.

När budskapet utformas är det viktigt att ta hänsyn till de berättelser som cirkulerar om din organisation och vilka övergripande narrativ som drivs. Narrativen hänger samman med målgruppens uppfattningar. Tänk på hur enskilda meddelanden bidrar till den värdegrund och det narrativ din organisation vill kommunicera, särskilt i relation till olika målgrupper. Budskap som bygger förtroende för din organisation spelar en viktig roll i att utveckla motståndskraft mot vilseledande och falsk information.

VILKEN ÄR VÅR BERÄTTELSE?

Budskap ska anpassas till det övergripande narrativ som du vill kommunicera.

Ett starkt narrativ kommer ur en tydlig värdegrund och målbild inom din organisation.

Analys och förståelse för vilka faktorer som bidrar till de narrativ som din organisation vill förmedla skapar samtidigt en förståelse för organisationens sårbarheter.

Angrepp möts bäst genom att upprätthålla de värderingar som din organisation står för.

Lär känna din målgrupp

Genom att först etablera din organisations kärnvärden, budskap och önskade narrativ kan du därefter kartlägga olika sårbarheter och vilka av din organisations målgrupper och intressenter som är mest sårbara för informationspåverkan. Dessa målgrupper och intressenter är prioriterade att nå i fall då informationspåverkan identifierats.

Som kommunikator har du sedan tidigare erfarenhet av målgruppsanalys. Här behöver du använda metoden för att analysera vilka målgrupper som är mest sårbara för informationspåverkan och varför. Som kommunikator handlar det om att identifiera vilka delar av din organisation, dess målgrupper och användare som kan bli föremål för informationspåverkan och överväga vilken typ av meddelanden som de kan vara mottagliga för. När du gjort detta kan du ta fram förslag för hur man kan nå ut till dessa målgrupper med motbudskap och förebyggande kommunikation.

MÅLGRUPPSANALYS

Målgrupper uppstår inte i ett vakuum

De skapas snarare dynamiskt genom interaktion mellan människor som delar åsikter, uppfattningar och intressen. Det är viktigt att förstå vad som förenar medlemmar i en målgrupp.

Kartlägg intressenterna

Informationspåverkan är inte nödvändigtvis riktad mot er, utan kan i första hand vara riktad mot andra målgrupper. Samhällets mest sårbara grupper kan vara de som påverkas mest. Det är viktigt att vara medveten om vilka målgrupper som kan vara utsatta och bedöma deras sårbarheter i relation till olika narrativ.

Kartlägg era narrativ

Identifiera egna narrativ som kan användas för att möta informationspåverkan. Hur kan dessa narrativ nå ut till sårbara målgrupper? Tänk på vilka nyckelkommunikatörer som har hög trovärdighet hos sårbara målgrupper och försök nå ut till dem.

Syftet med att genomföra en målgruppsanalys är att ta fram kommunikationsverktyg som kan användas om ni skulle utsättas för informationspåverkan. De är ett led i att skapa en beredskap med åtgärder som kan anpassas till situationer där informationspåverkan används för att undergräva din organisations förtroende.

Målet med motåtgärderna är att återställa det skadade förtroendet så snabbt och effektivt som möjligt. Bland dessa verktyg ingår arbetet med att förbereda budskap och narrativ som kan riktas mot delar av din publik. Här ingår förberedelser för att förstå hur olika målgrupper i allmänhet och nyckelintressenter i synnerhet kan påverkas av informationspåverkan och hur du kan utforma dina motbudskap.

Känn till organisationens risker och sårbarheter

Förutom ovanstående åtgärder bör organisationer även göra en bedömning av hur informationspåverkan kan hota verksamheten och organisationens förmåga att uppfylla sitt uppdrag. En risk- och sårbarhetsanalys ingår sedan tidigare i offentliga organisationers strategiska planering och förberedelser inför olika typer av kriser. Informationspåverkan skulle kunna läggas till i redan existerande risk- och sårbarhetsanalyser och i det arbetet fokusera på att identifiera utsatta användare och andra målgrupper, ta fram färdiga budskap och narrativ samt genomföra en analys av den övergripande risken att informationspåverkan stör organisationens kärnverksamhet.

RISK- OCH SÅRBARHETSANALYS

Steg 1: Utgångspunkt

Vilken roll och vilka ansvarsområden har din organisation?
Vilka metoder kan användas för att identifiera och utvärdera hot och risker?
Vilka gränsdragningar och perspektiv kommer tillämpas i analysen?

Steg 2: Riskbedömning

Vilka är de tänkbara hoten och riskerna?
Vad är sannolikheten för att dessa ska realiseras och vilka är de tänkbara konsekvenserna?
Vilka situationer bör bedömas i relation till organisationens krishanteringsförmåga?
Vilka förebyggande åtgärder bör vidtas?

Steg 3: Sårbarhetsbedömning

Hur påverkas din organisation av olika scenarion?
Vilka konsekvenser skulle informationspåverkan kunna få och hur kan din organisation hantera, stå emot och återhämta sig från dessa?

Steg 4: Riskhantering

Vad gör ni om informationspåverkan upptäcks? Se avsnittet nedan för exempel.

Hur väljer jag rätt respons?

Det finns ingen färdig lösning som kan användas för att bemöta alla fall av informationspåverkan. Som den här handboken visat förekommer informationspåverkan i olika former. Alla organisationer präglas inte heller av samma sårbarheter eller förutsättningar. Därför är det viktigt att skraddarsy responsen. Genom grundliga förberedelser kan du skapa övergripande ramar för lämpliga motstrategier som passar din organisation och som kan anpassas till den specifika situationen. Här är det viktigt att tänka på de olika förväntningar som finns på kommunikatörer. En lämplig respons avgörs helt av din roll som kommunikatör och det mandat som organisationens ledning har gett dig.

Bedöm, informera, förespråka eller försvara?

En lämplig respons bör stå i proportion till hur allvarlig du bedömer att situationen och hotet är. Vi föreslår fyra olika grader av respons där varje nivå innefattar förslag till mer specifika metoder.

Den första responsnivån handlar om att bedöma situationen. Detta är ett första steg och en neutral åtgärd som samtidigt signalerar att ni är medvetna om situationen och står i begrepp att ta reda på fakta. Den andra nivån består i att informera allmänheten och nyckelintressenter om situationen och hur ni som organisation ser på frågan. Detta är en något mindre neutral åtgärd där ni redovisar det ni anser vara fakta i målet. Dessa kategorier är utgångspunkten för en faktabaserad respons och kan tillämpas i de flesta fall av misstänkt informationspåverkan.

Den tredje nivån innefattar kommunikativa åtgärder där ni förespråkar en viss position. Detta innebär att ni aktivt argumenterar för era egna fakta eller budskap i relation till vinklade eller falska budskap. Den fjärde nivån handlar om att försvara organisationen genom att rikta specifika insatser mot angriparen. Dessa kategorier utgör grunden för en argumenterande respons och bör användas sparsamt, samtidigt som de kan vara nödvändiga i särskilt allvarliga situationer.

Faktabaserad respons

De två första stegen i arbetet med att möta informationspåverkan är bedöma och informera. Dessa utgör en faktabaserad respons och kan användas i alla situationer.

Nedan introduceras förslag på åtgärder som kan användas i de fyra stegen



STEG 1: BEDÖM

För att få ett begrepp om vad det är som pågår måste du göra en bedömning av situationen. Vad är det som händer? Vem är inblandad? Vad står på spel? Ju mer kunskap du kan skaffa dig om situationen desto bättre blir din respons.

KARTLÄGG SITUATIONEN

Orientera dig och skapa medvetenhet om vad som pågår. Använd diagnosverktyget för att avgöra om det rör sig om informationspåverkan.

FAKTAKOLL

Kontrollera den information som cirkulerar – vad är sant?

TRANSPARENT UTREDNING

Ta hjälp av externa aktörer, till exempel journalister, för att utreda frågan på ett transparent sätt.



STEG 2: INFORMERA

När du gjort en bedömning av situationen kan du börja kommunicera med dina målgrupper. I detta steg inriktas din kommunikation på att delge neutral information och fakta, samt att kommunicera kring hur händelsen hanteras. Kom ihåg att alltid målgruppsanpassa din kommunikation.

GÖR ETT UTTALANDE

Delge neutral information och dela relevant fakta som är tillgänglig för er.

KORRIGERA

Gör ett uttalande som besvarar eller korrigerar ett falskt påstående med relevant fakta. I detta avseende kan ett FAQ-formulär vara ett användbart verktyg.

HÄNVISA

I situationer där externa aktörer och experter är involverade i debatten kan det vara en fördel att hänvisa till dessa för att stärka din position.

BETONA VÄRDEGRUNDEN

Påminn målgruppen om vad din organisation står för.

MEDDELA INTRESSENTER

Sprid information om händelsen till kollegor och andra viktiga intressenter. Ju fortare de får veta vad som pågår desto bättre.

GÖR ETT PRELIMINÄRT UTTALANDE

Visa att ni arbetar med frågan genom att kommunicera med målgruppen. Detta ger dig andrum att utarbeta en mer genomgripande respons.

Argumentbaserad respons

Det tredje och fjärde steget kallar vi argumentera och försvara. Dessa steg innehåller åtgärder som endast är lämpliga i mer allvarliga situationer där informationspåverkan tydligt kan identifieras. Tillsammans utgör de en argumentbaserad respons.

Nedan finner du exempel på respons i de olika stegen.



STEG 3: FÖRESPRÅKA

Att förespråka sin position är en upptrappning från att neutralt informera, och innebär mer aktiv och utåtriktad kommunikation. I detta steg är det viktigt att alltid tänka på vilket mandat du har och organisationens värdegrund när du utformar din respons.

DIALOG

För dialog med viktiga intressenter och personer ur relevanta målgrupper för att skapa engagemang för frågan.

UNDERLÄTTA

Gör det enkelt för informationen att nå målgruppen. Organisera platser/tillfällen där intressenter kan mötas och diskutera händelsen eller specifika problem där ni har möjlighet att tydliggöra er position.

SAMARBETA

Ta kontakt med nyckelaktörer i samhället som kan hjälpa till att sprida ert budskap till relevanta målgrupper.

PÅHÄNG

Använd befintliga händelser, initiativ eller debatter för att nå ut med er position.

PAKETERA

Sätt ihop ett informationspaket om händelsen som presenterar händelseförloppet och lägger fram fakta som underbygger den egna positionen. Att detta baseras på fakta och verifierad information är viktigt.

STORYTELLING

Relatera händelsen till ett bredare narrativ om exempelvis din organisation och era värderingar, gör det lätt för målgruppen att förstå vad som pågår och att verifiera på så vis informationen.



STEG 4: FÖRSVARA

Sista steget, försvara, innefattar en direkt respons mot angriparen. Åtgärderna kan i vissa sammanhang framstå som kontroversiella och ska därför endast användas i extrema situationer. Se till att diskutera alla åtgärder inom denna nivå med kollegor och chefer innan de implementeras så att du inte överskrider ditt mandat eller riskerar att förvärra situationen.

IGNORERA

Ibland är det bäst att inte göra något alls. Att ignorera användare eller händelser är lämpligt om det är tydligt att informationspåverkan förekommer, men inte fått stor spridning eller uppmärksamhet. Detta då respons istället skulle kunna bidra till att sprida den falska bilden.

RAPPORTERA

Om en angripare bryter mot lagen eller en medieplattformens användarregler bör det anmälas till polisen eller plattformens ägare. Anmälan till plattformens ägare får inte missbrukas eller göras lättvindigt, utan endast vid uppenbara överträdelser, för att undvika att den offentliga debatten tystas.

BLOCKERA

Kommunikatörer måste alltid vara medvetna om vikten av att respektera och upprätthålla yttrandefriheten! Aktiviteter som stör verksamheten kan motivera blockering och avstängning från en plattform. Varje blockering bör dock motiveras och relateras till gällande regelverk och inte för att slippa svåra diskussioner.

AVSLÖJA

En strategisk respons på informationspåverkan kan vara att avslöja den aktör som ligger bakom till exempel ett falskt konto. Detta ska dock inte göras lättvindigt och måste föregås av en konsekvensanalys som beaktar vilka konsekvenser det får för organisationen och för den som exponeras.

Valet av responsnivå bör vägas mot din och din lednings bedömning av hur allvarlig situationen är. Svaga indikationer på att en aktivitet är ett fall av informationspåverkan bemöts bäst med åtgärder som ryms inom de två första stegen, det vill säga genom att bedöma situationen och informera allmänheten på ett neutralt sätt. Vid mer aggressiv informationspåverkan kan samma metoder kombineras med verktyg från de två senare responskategorierna, det vill säga med förespråkande och försvarande metoder. Du uppmanas dock till försiktighet vid användning av de två senare stegen. Om du anser att metoderna är motiverade för den specifika situationen behöver du se till att du har mandat från ledningen att utföra dem och att se till att de är förenliga med demokratiska principer, yttrandefrihet och med offentliga regelverk i övrigt.

Utforma en faktabaserad respons

En viktig aspekt av de två första responskategorierna (att bedöma och informera) är att din kommunikation är neutral och faktabaserad. Tillsammans utgör de ett faktabaserat bemötande. Om en förespråkande respons används bör detta ses som ytterligare ett lager. Det innebär att även den förespråkande responsen ska baseras på din bedömning och de fakta du har till ditt förfogande i frågan. Om felaktig information tillåts cirkulera utan att korrigeras kan det bidra till att uppfattningar om din organisation, dina målgrupper eller frågor inom ditt verksamhetsområde baseras på felaktigheter. Att bedöma situationen och informera den identifierade målgruppen bör därför alltid vara den första åtgärden.

För att göra en relevant faktakoll behöver du först fundera på hur felaktig information kan påverka din organisation, hur det riskerar att påverka er verksamhet och hur ni går tillväga för att identifiera den. Vem sprider informationen, hur stor spridning har den fått och vilket ämne berörs? Organisationer kan till exempel fokusera på att bedöma de artiklar som innehåller citat från organisationens representanter, inlägg som blir virala och får stor spridning online eller påståenden om den egna organisationen och dess verksamhetsområde. Genom att samla in fakta på ett systematiskt sätt kan du se till att ni utvärderar den information och de frågor som ni bedömer relevanta kopplat till ert ansvarsområde.

Utvärdering

- Inhämta neutrala expertomdömen och/eller korrekt information från relevanta och pålitliga källor
- Efterfråga mer information av den person eller organisation som gjort påståendet
- Leta upp det falska påståendets originalkälla

Om informationen bedöms vara felaktig bör du först svara med en rättelse. Många experter anser att desinformation bäst bemöts med korrekt information. Andra menar att budskapet enbart får en effekt bland de som är intresserade av att ta reda på sanningen. Ditt förberedande arbete med målgrupper och narrativ skapar möjligheter för en välgrundad bedömning av vilken åtgärd som är lämplig i det specifika fallet.

Kom ihåg att om du har möjlighet och mandat att göra en argumentbaserad respons bör denna följa de ramar som fastställts inom faktabaserad respons.

Utforma en faktabaserad respons

- Be personen som publicerat felaktigheten att rätta eller ta tillbaka publiceringen
- Ta fram ett faktablad eller liknande underlag som är lätt att dela på nätet
- Försök att inte repetera felaktig information i din kommunikation
- Kom ihåg att inte all felaktig information måste bemötas
- Ifrågasätt debattens inramning, inte enbart innehållet
- Överväg att bedriva dialog som ett komplement eller alternativ till din förberedda kommunikation

Särskilda hänsyn för sociala medier

Sociala medier är inte bara en plattform som låter användare interagera med varandra, de kan även användas som ett verktyg för informationspåverkan. Sociala medier har sin egen logik, denna logik måste användaren känna till, förstå och ta hänsyn till vid eventuella motåtgärder för att möta informationspåverkan.

Det kan vara svårt att veta vem som ligger bakom ett konto på sociala medier och varifrån informationen kommer. Diskussionen kan exempelvis göra anspråk på att företräda den allmänna opinionen på falska grunder. Sociala medier är utmanande eftersom informationsspridning kan ske snabbt, och kräver att man tar hänsyn till element såsom *taggar*, *namnetiketter*, *länkar* och *bifogade filer*. Ett typiskt inlägg på sociala medier innehåller ett eller flera av dessa element som dessutom kopplar samman budskapet med andra konton, idéer och debatter. På så sätt bör inlägget betraktas som en del av ett eller flera större nätverk av pågående samtal online.

TAGGAR

Skapar ett sökord för ett inlägg. Taggar påverkar ofta spridning och cirkulation av inlägg.

NAMNETIKETTER (NAME CALLS)

Används för att länka till en organisation eller individs konto så att de får en notifikation om inlägget.

LÄNKAR

Ger en hyperlänk till en annan webbplats. Länkar förkortas ofta så att webbplatsens riktiga URL inte syns.

BIFOGADE FILER

Multimediafiler, till exempel en bild eller ett videoklipp. Dessa kan förändra ett inläggs innebörd och bör inte förbises.

Proaktivt arbete på sociala medier innebär att bygga nätverk och taggar som gör att organisationens kommunikation når rätt människor. Som kommunikatör bör du förbereda budskap som kan godkännas på förhand och tas fram vid händelse av kris. På så sätt kan ni ge en snabb respons i de fall ni behöver möta informationspåverkan. Sociala medier gör det också möjligt för en organisation att i realtid upptäcka eventuella hot eller sårbarheter som rör organisationens anseende. På så sätt kan sociala medier användas både som ett verktyg för dialog och som ett öppet analysverktyg för att förstå viktiga trender och samtida riktningar i samhällsdebatten.

Möta påverkan på sociala medier

De fyra responsnivåerna utgör en verktygslåda för att möta påverkan. Nedan följer ett exempel på hur verktygen kan tillämpas för att möta påverkan på sociala medier.



BEDÖM

Bedöm situationen med hjälp av din kunskap om informationspåverkan. Handlar det om påverkan eller är det engagerade medborgare som debatterar? Om du misstänker att informationspåverkan försiggår, kartlägg situationen så noggrant som möjligt. Vilka användare kommunicerar med dig? Är de fientliga mot dig eller reagerar de på något som spridits med syftet att skapa fientliga reaktioner? Vilka taggar används? Finns det bifogade länkar eller annat material? Vilka källor hänvisas det till? Är några konton botar? En snabb bedömning skapar förutsättningar för att agera.



INFORMERA

Utforma ditt budskap baserat på din bedömning. Välj noggrant vilka målgrupper du vill nå i första hand, och identifiera användare och hashtags du kan nyttja. Fokusera på att nå ut med neutral information och betona organisationens värderingar i de kanaler du anser lämpliga.



FÖRESPRÅKA

Om du anser det lämpligt att gå vidare till förespråkanivån kan du använda tillgängliga verktyg för att positionera dig tydligare i debatten, till exempel genom förberedda budskap eller multimedia. Det kan också vara lämpligt att delta mer aktivt i debatten och skapa ett bredare engagemang för frågan hos dina målgrupper. Detta uppnås genom att kommunicera direkt med andra användare och involvera följare i debatten.



FÖRSVARA

Om situationen eskalerar till ett läge där konstruktiv dialog är omöjlig och budskap trängs undan av spam och destruktiva inlägg kan det vara lämpligt att gå i försvarsställning. Beroende på din organisations riktlinjer och plattformens regler kan du ha rätt att blockera eller ignorera störande användare. Rådgör alltid med chefer och kollegor innan du agerar! Yttrandefriheten är ett av vårt samhälles kärnvärden och vi ska alltid göra vad vi kan för att upprätthålla öppen och fri demokratisk debatt. Om du bestämmer dig för att blockera eller ignorera en användare, se till att vara helt transparent med anledningen till ditt val.

Hur tar jag till vara lärdomar?

Att samla in och dokumentera exempel på informationspåverkan är centralt för att förstå problemet bättre och därmed bättre kunna möta påverkan i framtiden. Exempel på den respons du har lämnat och bedömningar av huruvida responsen har fungerat är viktiga att dokumentera för att i ett senare skede använda dem för att skapa en logg över händelseförloppet med information om åtgärder och tidpunkter, samt för att utforma rutiner och arbetssätt för eventuella framtida påverkansförsök. Kunskapen kan även användas för att utveckla utbildningsmaterial och effektivisera organisationens och samhällets beredskap. Informationen bör delas med kommunikatörer i liknande roller, myndigheter med uppgiften att identifiera och möta informationspåverkan (t.ex. MSB) och i vissa fall med allmänheten.

På nästa sida finns några exempel på lärdomar som du bör spara och ha till hands när du bemöter informationspåverkan.

Lärdomar

BESKRIV

- Beskriv händelsens bakgrund, förlopp och kontext.
- Vilka aktörer var inblandade? (undvik spekulation om källor när du inte vet).
- Vilka av informationspåverkans utmärkande karaktärsdrag kunde observeras?
- Vilka sårbarheter utnyttjades?
- Vilka påverkanstekniker användes? Vilka målgrupper och narrativ nyttjades?
- Passar händelsen in i ett större sammanhang?

REFLEKTERA

- Vilken effekt tror du att angriparen vill uppnå? Vad baserar du din bedömning på?
- Hur agerade du? Reflektera över vilka åtgärder du vidtog och varför du valde dem.
- Vad tror du hade hänt om du inte agerat?
- Vilken effekt fick ditt agerande?
- Vad fungerade bra och vad kunde du gjort annorlunda?
- Vilka lärdomar kan du dra av händelsen?

DELA

- Har du sparat bevis eller data som rör ärendet?
- Diskutera informationspåverkan med dina chefer och kollegor och dela med dig av dina erfarenheter.
- Upprätthåll regelbunden kontakt med kollegor inom och utanför din egen organisation som arbetar med liknande frågor.
- Dela med dig av dina kunskaper och erfarenheter inom och utanför din egen organisation genom exempelvis utbildning och möten.

Strategiska ställningstaganden

Ditt bemötande begränsas av det faktum att det alltid svarar på någon annans agenda. Angriparen kan tyckas sätta villkoren, vilket gör att hela principen för att möta informationspåverkan är problematisk. Det känns ofta som att de agerar och du reagerar och att du hela tiden ligger steget efter i motståndarsidans senaste försök.

Det kan därför vara klokare att fokusera på insatser som försvarar demokratiska värderingar såsom den fria debatten och yttrandefrihet. Ditt uppdrag är att i relation till din organisations uppdrag skydda den opinionsbildande processen genom att minimera effekten av sårbarheter i mediasystemet, opinionen och mänskliga tankeprocesser. Här är det viktigt att du utgår ifrån strategisk, väl avvägd och samtidigt faktabaserad respons.

Det är värt att upprepa att arbetet med att möta informationspåverkan aldrig får leda till att den offentliga debatten tystas ner. Det skulle motverka själva syftet med att möta informationspåverkan, leda till ökad polarisering och till att samhällets funktioner undermineras. Öppen och demokratisk debatt måste alltid skyddas och uppmuntras.

- Höj tröskeln för informationspåverkan genom att bidra till medvetenhet och beredskap
- Utveckla proaktiva, välavvägda och förnuftiga kommunikationsmetoder som lägger fokus på målgruppen (snarare än motståndaren) och försvarar samhällets gemensamma värderingar
- Upprätthåll en faktabaserad respons, som kan utvecklas till en förespråkande respons under vissa omständigheter
- Dela med dig av metoder som fungerar och lär av varandra
- Var vaksam men inte paranoid!

Ordlista

Bandwagon-effekten – Att personer som upplever sig vara en del av en majoritet är mer benägna att dela med sig av sin åsikt.

Botar – Datorprogram som utför automatiserade uppgifter.

Desinformation – Felaktig eller manipulerad information som sprids avsiktligt i syfte att vilseleda.

Dold annonsering (dark ads) – Annonser som endast kan ses av specifika individer med budskap som skraddarsys efter individens psykografiska profil.

Ekokammare och filterbubblor – Naturliga grupperingar online eller offline där människor kommunicerar med andra som delar samma åsikter och uppfattningar.

Falska medier – Förfalskade nyhetssajter som konstruerats för att efterlikna äkta nyhetssajter.

Hackning – När aktörer skaffar sig obehörig åtkomst till en dator eller ett nätverk.

Halmgubbe (strawman) – Att tillskriva sin meningsmotståndare argument och ståndpunkter denne inte står för, och sedan argumentera mot dessa ståndpunkter istället för motståndarens faktiska ståndpunkter.

Lockfåglar (shilling) – Personer som ger intrycket av att vara fristående men som i själva verket samarbetar med eller tar emot betalning av någon annan.

Memes (även kallad internetmem) – Åsyftar bilder, fraser, aktiviteter, koncept och filmer, ofta med humoristiskt innehåll, som sprids på internet, främst via sociala medier.

Nätfiske – Användare luras att uppge sina lösenord eller annan känslig information på internet.

Potemkinkulisser – Falska företag, forskningsinstitut och tankesmedjor som används för att desinformation ska upplevas som information.

Sockpuppets – Falska konton som används för att delta i debatter online där två eller flera sockpuppets används för att elda på diskussionerna.

Strategiska narrativ – Berättelser som konstrueras för att stötta ett specifikt syfte.

Symbolhandlingar – Handlingar som utförs för att främst kommunicera ett budskap.

Tystnadsspiral – Att personer som upplever sig vara en del av en minoritet är mindre benägna att dela med sig av sin åsikt.

Whataboutism – Att ta fokus från ett argument genom att belysa ett liknande fenomen som inte fått lika mycket uppmärksamhet, men som inte är riktigt relevant i frågan.

Mer information

Handboken och fullständig bibliografi finns på MSB:s hemsida:

<https://www.msb.se>

Vill du lära dig mer om informationspåverkan rekommenderar vi att du läser handboken som nämns ovan. Du finner även mer information i följande rapporter och artiklar:

Countering Information Influence Activities: The State of the Art,
Pamment J., Nothhaft H., Twetman, H. & Fjällhed A., 2018

Att förbygga och hantera påverkansförsök – en handbok
Brottsförebyggande rådet (BRÅ), 2017

Källkritik på internet
Internetstiftelsen i Sverige (IIS), 2016

Personlig säkerhet
SÄPO, 2018

Debunking handbook
John Cook och Stephan Lewandowsky, 2012

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

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

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

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

Du kan även ta del av information och exempel från andra internationella organisationer:

EU vs Disinfo
www.euvdisinfo.eu

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

NATO Strategic Communications Centre of Excellence
www.stratcomcoe.org

