Myndigheten för psykologiskt försvar

Att möta informations-påverkan

Handbok för journalister

ATT MÖTA INFORMATIONSPÅVERKAN – HANDBOK FÖR JOURNALISTER

Myndigheten för samhällsskydd och beredskap (MSB)
finansierade framtagandet av det ursprungliga underlaget.

Foto: Microgen/iStock

Tryck: Brand factory

Produktion: Familjen

Publikationsnummer: MPF/2023:521-1

ISBN: 978-91-527-8748-9

Innehåll

Inledning

Inledning

Det försämrade omvärldsläget aktualiserar behovet av att öka kunskapen om informationspåverkan och påverkanskampanjer. Myndigheten för samhällsskydd och beredskap och Myndigheten för psykologiskt försvar har i samarbete med Medieinstitutet Fojo tagit fram den här handboken för att öka kunskapen om informationspåverkan och påverkanskampanjer.

> *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."*
>
> **Ur *Att möta informationspåverkan – handbok för kommunikatörer***

MSB har i samarbete med Medieinstitutet Fojo vid Linnéuniversitetet arbetat för att stärka redaktioners förmåga att identifiera och hantera påverkan. Från den 1 januari 2022 har Myndigheten för psykologiskt försvar i uppdrag att skydda Sverige mot otillbörlig påverkan och kan vid behov ge stöd till redaktioner som är utsatta för påverkan.

Syftet med det psykologiska försvaret är att värna det öppna och demokratiska samhället, den fria åsiktsbildningen samt Sveriges frihet och oberoende. I uppdraget ingår att identifiera, analysera, möta och förebygga otillbörlig informationspåverkan och annan vilseledande information som är riktad mot Sverige eller svenska intressen.

Den här handboken bygger på *"Att möta informationspåverkan – handbok för kommunikatörer"* från 2018, som togs fram av Institutionen för strategisk kommunikation vid Lunds universitet på uppdrag av MSB. Handboken har anpassats av Fojo för att fungera som ett stöd för dig som är journalist. Den tredje och sista delen i handboken, *"Bemöt och hantera informationspåverkan"*, har till exempel innehåll som bygger på material från Fojos projekt Demokratijouren, och på organisationen First Drafts (2015–2022) material om journalistiskt arbete mot desinformation.

Del 1 | Bli medveten om informations-påverkan

Det här 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 på informationspåverkan 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 privatpersoner, 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 till att korrigera felaktigheter utifrån 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, som främmande makt utnyttjar genom informationspåverkan.

Stödjer främmande makts agenda

Informationspåverkan är potentiellt skadlig kommunikation som främmande makt eller deras ombud ligger bakom, medvetet eller omedvetet. Informationspåverkan används för att stödja främmande makts agenda och utformas så att den utnyttjar uppfattade sårbarheter i samhället.

> **Det handlar om en medveten inblandning från främmande makt i inomstatliga angelägenheter, där det görs försök att skapa misstro medborgare emellan samt mellan medborgare och stat. Genom att studera ett samhälle och dess motsättningar, kontroverser och utmaningar riktas insatserna mot dessa sårbarheter i syfte att öka splittringen i landet.**

Enskilda aktiviteter eller större kampanjer

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

Äkthet kan vara svår att bedöma

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 bara för att avsändaren uttrycker liknande åsikter. Det är också viktigt att understryka att vilseledande metoder används systematiskt inom informationspåverkan, i syfte att underminera demokratin. En grundläggande princip för att bemöta informationspåverkan är därför att värna den fria debatten, yttrandefrihetens principer och det demokratiska samtalet – även om det försvårar uppgiften. Detta kan inte understrykas nog.**

Tekniker som används för att vilseleda

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 och använder tekniker för att vilseleda såsom 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. Det 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 den offentliga debatten kan bilden av opinionsläget eller tankeströmningar förändras, vilket i sin tur kan påverka beslutsfattande.

Agerar i egenintresse

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

Utnyttjar sårbarheter

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

Flera olika sårbarheter utnyttjas

Föreställ dig att människors 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.

Processen bygger på några enkla principer. För det första är den beroende av att händelsen eller informationen är korrekt, och att den bygger på fakta. För det andra utgår den från att påståendet är verifierat av trovärdiga källor i form av verkliga människor, vars anseende kommer att undermineras om de talar osanning. Processen förutsätter också att de medier som plockar upp berättelsen är balanserade i sin bevakning, att de dubbelkollar fakta och källor samt 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 slutsatser föregås av en konstruktiv debatt.

> **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 för att kompromettera informationsflödet. De identifierar sårbarheter i opinionsbildningsprocessen, i hur kritisk information färdas genom medielandskapet och i hur människors 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 bottar som skapar en skenbild av en livlig offentlig debatt. När dessa aktiviteter genomförs avsiktligt, ibland i koordinerade kampanjer för att underminera demokratiska processer, går det inte alltid att förlita sig på ett självsanerande system. Därför måste du som journalist ha kunskap och förståelse om informationspåverkan för att till exempel kunna bedöma tips korrekt, nyhetsvärdera flöden i sociala medier och kontrollera källor.

Opinionsbildning

SÅRBARHETER I MEDIESYSTEMET

Det moderna mediesystemet har flera sårbarheter, särskilt i förhållande till det föränderliga tekniklandskapet, nya journalistiska affärsmodeller och den tilltagande mängden alternativa nyhetskällor online. Allt från förfalskade brev och manipulerade bilder till klickjakt, algoritmer och bottar i sociala medier gör mediesystemet sårbart för den som vill utnyttja det för egen vinning. Det gäller oavsett om fenomenen drivs av ekonomiska eller politiska motiv, eller helt enkelt av nyfikenhet för att se om det går.

SÅRBARHETER I OPINIONSBILDNINGEN

Opinionsbildning har alltid varit sårbar, exempelvis med tanke på social bevisföring – det vill säga vad någon påstår sig ha upplevt själv. I dagens informationsmiljö, där falska konton i sociala medier och troll snedvrider debatten online, är det lättare än någonsin att fabricera sociala bevis, provocera och väcka ilska och upprördhet. Det bidrar till att polarisera den politiska debatten, vilket innebär en sårbarhet i den allmänna opinionsbildningen.

KOGNITIVA SÅRBARHETER

Vissa sårbarheter uppstår till följd av hur den mänskliga hjärnan fungerar. Vi människor 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 som använder sociala medier. Datapunkterna kan användas för att förutsäga åsikter och beteenden. Inom informationspåverkan utnyttjas våra tankemönster och informationen om oss för att påverka våra uppfattningar, våra beteenden och vårt beslutsfattande.

Skillnader mellan informationspåverkan och annan kommunikation

För att kunna identifiera fall av informationspåverkan behöver du bedöma i vilken utsträckning kommunikationen är vilseledande, sker avsiktligt och har som 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 agera. Du kommer inte nödvändigtvis att kunna se alla indikationer samtidigt, men ju fler du identifierar desto högre är sannolikheten att det handlar om informationspåverkan.

> **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 som hot, dataintrång, utpressning eller mutor faller utanför denna diskussion och ska rapporteras till polisen.**

Vilseledande

Tillförlitlig kommunikation är öppen och transparent. Innehållet är trovärdigt och kan verifieras. Informationspåverkan är i stället 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 och stärker vår demokrati, även om den naturligtvis ibland kan skapa friktion. Informationspåverkan stör och försvagar i stället samhällets funktionalitet och vårt demokratiska samtal.

Frågor att fundera över som journalist

- Kan det finnas någon annan agenda bakom en konflikt än den mest uppenbara att ta hänsyn till vid övervägande om publicering?
- Vilken roll tycker du att medierna borde ha i det rådande informationsklimatet?
- Hur skulle journalistik kunna stärka det demokratiska samtalet?
- Vad händer med journalistikens trovärdighet om medier och journalister låter sig luras av falska konton och handlingar?
- Hur skulle medier kunna granska den opinionsbildning (och eventuella bakomliggande agendor) som sker på sociala medier, när exempelvis så kallade filterbubblor påverkar vilka röster som hörs?

Del 2 | Identifiera informations-påverkan

Strategier och tekniker för informationspåverkan

Två strategier som används för informationspåverkan

För att identifiera informationspåverkan behöver du först känna till två övergripande strategier som används:

- strategiska narrativ
- målgruppsanpassning.

Kunskap om dessa kan hjälpa dig att känna igen informationspåverkan och bidra till insikter om syftet med påverkansaktiviteterna.

Strategiska narrativ – berättelser som ska uppnå ett visst mål

Informationspåverkan innefattar vanligtvis någon form av berättande (på engelska *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 också hört berättelser om hur människan landade på månen, men 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 i stället att det är fejkat. Det här 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 har konstruerats och kommuniceras i syfte att uppnå ett visst mål kallas de för strategiska narrativ.

Det går till exempel att hitta på saker om vissa etniska eller religiösa grupper som passar in i folks förutfattade meningar om dessa grupper, det vill säga passar in i det existerande narrativet. Diskussionen kan påverkas på tre olika sätt:

- genom att lyfta fram delar av det existerande narrativet
- genom att trycka undan andra narrativ
- genom att göra nya kopplingar till orelaterade händelser för att distrahera.

Att identifiera strategiska narrativ och logiken bakom påverkansaktiviteter är ett viktigt steg i att förbereda och ta fram lämpliga strategier för att möta påverkan.

Positivt eller konstruktivt: ”Det här är sanningen!”

Försöker 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 samtalet. I detta avseende används ofta till exempel humor, mem (på engelska *memes*) eller konspirationsteorier.

Tekniker för målgruppsanpassning

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, alltså vem den tilltänkta målgruppen är:

- Riktas narrativen mot hela befolkningen, eller mer specifikt mot enskilda grupper eller individer?
- Används storskalig dataanalys (på engelska *big data*) för att utforma riktade insatser mot personer med liknande personlighetsdrag och åsikter?
- Används målgruppsanpassning för att utnyttja sårbarheter eller beteendemönster hos den specifika gruppen eller individen?

Om du vet vem en berättelse riktar sig till blir det lättare att förstå syftet bakom informationspåverkan, och hur den är tänkt att fungera i det specifika fallet. Den analysen hjälper dig i sin tur att fatta beslut om hur du ska värdera materialet.

Samhällsnivå: bred publik

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

Sociodemografisk inriktning: specifika grupper

Specifika målgrupper identifieras utifrån demografiska faktorer som ålder, inkomst, utbildning eller etnicitet. På så sätt går det att skapa budskap som är anpassade för att tilltala gruppens medlemmar.

Psykografisk inriktning: individer

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

Tekniker som används inom informationspåverkan

Inom informationspåverkan används en rad tekniker för att påverka människors beslut. Teknikerna är under ständig utveckling, men de vanligaste teknikerna kan delas in i sex övergripande grupper. Varje grupp karaktäriseras av att teknikerna där utgår från liknande principer. Genom att förstå hur dessa tekniker ser ut och fungerar kan du lättare känna igen och identifiera fall av informationspåverkan.

Samma tekniker kan användas antingen som en naturlig del av det demokratiska samtalet när de tillämpas på ett öppet och accepterat sätt, eller som en teknik inom informationspåverkan när 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.

I stället bör du utgå från din bedömning av i vilken grad aktiviteten är avsiktligt vilseledande i syfte att skada samhället, och dessutom använda din analys av strategiska narrativ och målgruppsanspassning 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 någon specifik teknik förekommer, används den på ett sätt som kan vara skadligt för allmänheten eller samhället?

Tekniker inom informationspåverkan

SOCIAL OCH KOGNITIV HACKNING

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

VILSELEDANDE IDENTITETER

- Lockfåglar (*shilling*)
- Imitatörer och bedragare
- Förfalskningar
- Potemkinkulisser
- Falska medier

SYMBOLHANDLINGAR

- Läckor
- Hackning
- Offentliga demonstrationer

ILLASINNAD RETORIK

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

DESINFORMATION

- Fabricering
- Manipulation
- Falsk tillskrivning
- Satir och parodi

TEKNISK MANIPULATION

- Bottar
- Sockpuppets
- Deep fakes
- Nätfiske

Social och kognitiv hackning

Social och kognitiv hackning utnyttjar människors sociala relationer och tankeprocesser. Det liknar hackning av exempelvis datorsystem på så sätt att en fientlig aktör försöker lura eller ”hacka” en process genom att utnyttja dess sårbarheter. Vi föredrar till exempel 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.

Tabell 1. Ordförklaringar tekniker inom social och kognitiv hackning.

Tekniker inom social och kognitiv hackning	
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 pekas 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?

Påverkansaktörer kan efterlikna trovärdiga informationskällor som personer, organisationer eller plattformar och använda sig av vilseledande identiteter för att utnyttja budbärarens förtroendekapital.

Tabell 2. Ordförklaringar tekniker inom vilseledande identiteter.

Tekniker inom vilseledande identiteter	
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 internettroll som får betalt för att skriva kommentarer.
Imitatörer och bedragare	Imitatörer 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. Falska sidhuvuden, stämplar eller namnteckningar kan användas för att få rena falsarier att se äkta ut.
Potemkinkulisser	Resursstarka aktörer kan gå ett steg längre och skapa falska och vilseledande institutioner och nätverk. Falska 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.

Känn igen vilseledande identiteter

RUBRIKEN

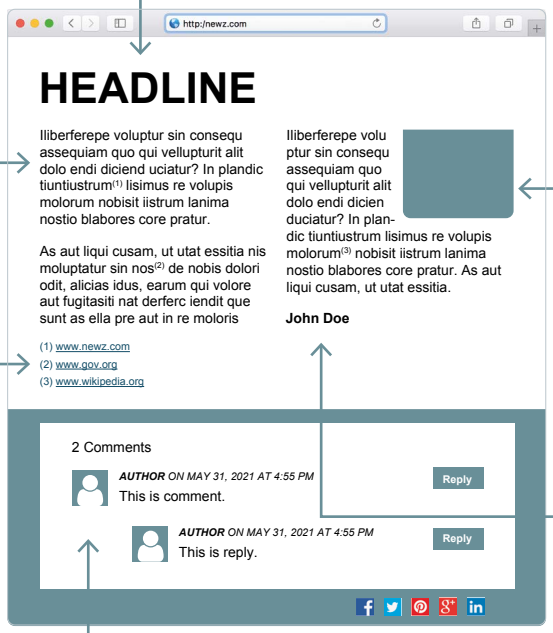
Rubriker försöker framkalla intresse och respons från läsaren. Läs alltid mer än bara rubriken och kontrollera att rubriken stämmer överens med resten av artikelns eller sidans innehåll.

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

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



BILDER

Bilder speglar inte alltid verkligheten. De 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 har använts tidigare i något annat sammanhang.

KÄLLOR

Om texten refererar till andra källor, se till att kontrollera dem och spåra informationens ursprung. Bedöm om källorna används korrekt i texten.

FÖRFATTARE

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

KOMMENTARER

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

UPPMÄRKSAMHET

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

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.

Tabell 3. Ordförklaringar tekniker inom symbolhandlingar.

Tekniker inom symbolhandlingar	
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).

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 i 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. Sådana troll kallas även hybridtroll.

Tabell 4. Ordförklaringar tekniker inom illasinnad retorik.

Tekniker inom illasinnad retorik	
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.

Desinformation

Med desinformation avses felaktig eller manipulerad information som sprids i syfte att avsiktligt vilseleda. Det 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 samt trovärdiga individer eller organisationer.

Tabell 5. Ordförklaringar tekniker inom desinformation.

Tekniker inom desinformation	
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.

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 genom en kombination av mänsklig och teknisk manipulation.

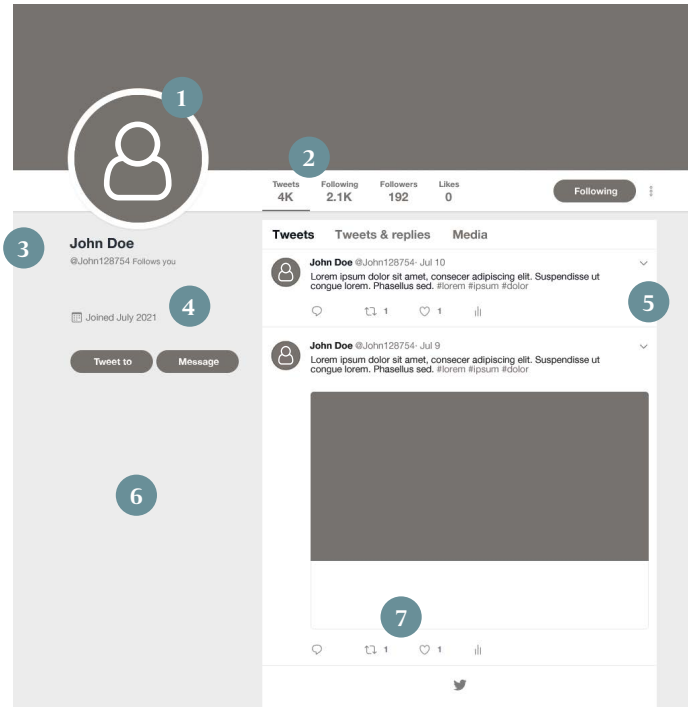
Lägg märke till att det inom teknisk manipulation ofta används nya verktyg för att utföra traditionella påverkanstekniker, till exempel för att skapa vilseledande identiteter online eller för att skapa och sprida desinformation. Det här är ett område som utvecklas långt mycket snabbare än vår förmåga att analysera potentiella konsekvenser och användningsområden. Problem med så kallade deep fakes, maskin- och djupinlärning samt artificiell intelligens, AI, har aktualiserats och vi kan förvänta oss att denna typ av teknologi kommer att användas mer i framtiden.

Tabell 6. Ordförklaringar tekniker inom teknisk manipulation.

Tekniker inom teknisk manipulation	
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.
Deepfakes	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

Bottar är effektiva verktyg för att bedriva påverkan i sociala medier. Samtidigt är de relativt enkla att avslöja.



1 PROFILBILD

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

2 AKTIVITET

Många bottar är mycket 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 bottar genererar sina användarnamn automatiskt. Upptäcker du konton med användarnamn som verkar vara slumpmässiga kan det vara ett tecken på en bot.

4 KONTOTS SKAPANDEDATUM

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

5 SPRÅK

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

6 INFORMATION

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

7 INTERAKTION

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

Påverkanstekniker kan 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.

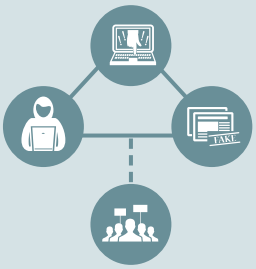
Ett förfalskat dokument kan exempelvis få större spridning med hjälp av bottar. Effekten förstärks ännu mer om insatsen samordnas med att vinklade artiklar sprids på falska nyhetsplattformar, som sedan kommenteras av en koordinerad grupp som använder trolltekniker.

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.

Frågor att fundera över när du som journalist ska värdera material

- 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 inblandning via deras ombud?
- Ser du tecken på kombinationer av metoder som antyder en samordnad aktion eller kampanj?
- Har du verktyg för att kunna kontrollera bilders äkthet?

Del 3 | Bemöt och hantera informations-påverkan

Råd och strategier för att möta informationspåverkan

För journalister handlar bemötandet av informationspåverkan om flera saker. Ett mediehus kan attackeras som organisation eller företag på samma sätt som till exempel en myndighet när det gäller spridande av desinformation, hackning av sociala medier och liknande. Den typen av informationspåverkan hanteras sällan i det journalistiska arbetet, utan tas om hand av andra i organisationen – allra helst utifrån en strategi. Samtidigt berör organisationens hantering ändå ditt arbete som journalist. Till exempel finns en del att lära därifrån och ta efter i det journalistiska hantverket. Därför innehåller den här delen av handboken både råd om organisationens hantering av informationspåverkan och råd till dig som journalist.

Råden till organisationen riktar sig i första hand till mediehusets kommunikatörer, marknadsavdelning eller liknande. Om ett mediehus upplever sig utsatt för informationspåverkan kan organisationen från och med 1 januari 2022 vända sig till Myndigheten för psykologiskt försvar, som har i uppdrag att på begäran ge råd och stöd till utsatta medier.

Det avsnitt som handlar om det journalistiska arbetet finns inte med i handboken för kommunikatörer. Det bygger därför på forskning och rapporter från den brittiska ideella organisationen First Draft (aktiv 2015–2022), som länge var ledande när det gällde att stödja journalister och mediehus i arbetet mot desinformation. Även rapporter, riktlinjer och råd från internationella organisationer som Africa Check och EU:s East StratCom har tagit i beaktande.

Sist i delen finns några sammanfattande råd om hat och hot mot journalister. Det är närbesläktat med desinformation och informationspåverkan, och förekommer inte sällan samtidigt. Om du vill veta mer om det här området finns fördjupande information och en helpdesk hos Demokratijouren vid Fojo. Du når den via Fojos webbplats.

Råd till organisationen

Förbered och bygg beredskap

Den viktigaste delen i att bygga beredskap för att hantera informationspåverkan är förberedelser. Alla som arbetar på företaget bör vara förberedda på att attacker av olika slag och grad kan komma. Genom att etablera fungerande strukturer blir det möjligt att snabbt och effektivt agera och mildra effekterna.
Förberedelserna består av tre huvudsakliga delar:

- skapa medvetenhet om informationspåverkan
- utveckla budskap, narrativ och en förståelse för på vilket sätt organisationens målgrupper och intressenter är sårbara för olika typer av informationspåverkan
- genomför en risk- och sårbarhetsanalys av organisationen för att identifiera och förebygga informationspåverkan.

Skapa medvetenhet och mötesplatser

En annan 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 ett mediehus i synnerhet står inför. På samhällsnivå är det bästa försvaret att skapa mötesplatser där journalister tillsammans med exempelvis ledare, företrädare för sociala medieplattformar, forskare, kommunikatörer och privatpersoner kan utbyta kunskap och lärdomar om att möta informationspåverkan.

För ett enskilt mediehus finns det flera saker att göra för att bygga upp en kapacitet inom organisationen. En sådan sak är att utse någon eller några som har det yttersta ansvaret för frågan, och som bygger upp sin kompetens inom området för att sedan kunna kommunicera med ledningen och vara rådgivande generellt. Ni kan också identifiera behovet av och möjligheterna till utbildning inom organisationen. Vidare kan mediehuset börja bygga nätverk, både inom och utanför det egna mediehuset, för ömsesidigt stöd och utbyte av erfarenheter. En fjärde sak att ta med i förberedelserna är att transparens och god kännedom om mediehusets verksamhet kan förebygga spridning av desinformation om mediehuset i fråga.

> **Börja bygga ett nätverk både inom och utanför det egna mediehuset för ömsesidigt stöd och utbyte av erfarenheter.**

Bygg förtroende genom strategisk kommunikation

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

> **Ett av målen med informationspåverkan är att undergräva människors förtroende för samhällets institutioner, dit många traditionella medier räknas. Effekten kan därför minimeras genom att fokusera på motåtgärder som bygger förtroende för organisationen.**

När det blir skarpt läge kan det vara svårt att få fram ett korrekt budskap. Därför är det viktigt att förbereda det budskap ni ska skicka ut. Budskapet bör formuleras utifrån organisationens värderingar, och på ett sådant sätt att det enkelt kan anpassas till specifika händelser. På samma sätt som ni använder budskap för att berätta om nya initiativ eller en ny reportageserie kan ni också använda budskap för att skapa medvetenhet om falska berättelser, eller för att motbevisa dem.

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

> **Organisationens bemötande begränsas av det faktum att det alltid handlar om att svara på någon annans agenda. Angriparen kan tyckas sätta villkoren, vilket gör att hela principen för att möta informationspåverkan är problematisk. Det känns ofta som om påverkansaktören agerar medan ni reagerar, och att ni hela tiden ligger steget efter i motståndarsidans senaste försök.**

Organisationens bemötande begränsas av det faktum att det alltid handlar om att svara på någon annans agenda. Angriparen kan tyckas sätta villkoren, vilket gör att hela principen för att möta informationspåverkan är problematisk. Det känns ofta som om påverkansaktören agerar medan ni reagerar, och att ni hela tiden ligger steget efter i motståndarsidans senaste försök.

Därför kan det vara klokare att fokusera på insatser som försvarar demokratiska värderingar såsom fri debatt och yttrandefrihet – det är generellt också själva kärnan och drivkraften för mediehus. Journalistiken bör värna och skydda den opinionsbildande processen, och det kan göras genom att försöka minimera effekten av sårbarheter i mediesystemet, opinionen och mänskliga tankeprocesser. Här är det viktigt att ha en 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 bidra till att samhällets funktioner undermineras. Öppen och demokratisk debatt måste alltid skyddas och uppmuntras.

Lär känna organisationens berättelse och målgrupp

Ett starkt narrativ om en organisation kommer ur en tydlig värdegrund och målbild inom organisationen. Anpassa budskapen som skickas ut till det övergripande narrativet som organisationen vill kommunicera.

Genom att analysera och försöka förstå vilka faktorer som bidrar till de narrativ som ert mediehus vill förmedla skapar ni en förståelse för mediehusets sårbarheter. Angrepp i form av informationspåverkan möts bäst genom att upprätthålla och stå fast vid de värderingar ert mediehus står för.

Lär känna er målgrupp för att förstå var den största sårbarheten för informationspåverkan finns. Det kan till exempel handla om en viss åldersgrupp, eller boende på en viss ort. De mest sårbara delarna bör prioriteras när det gäller att förbereda ett budskap. Kanske behövs också ett nätverk med nyckelpersoner som kan hjälpa till att nå ut till de mest sårbara målgrupperna.

Det finns experter att anlita när det gäller målgruppsanalys. Den analysen kan vara till stor hjälp för att minska skadan om mediehuset utsätts för informationspåverkan.

Känn till mediehusets risker och sårbarheter

Förutom åtgärder som medvetenhet, mötesplatser och kännedom om berättelse samt målgrupper bör ni också bedöma hur informationspåverkan kan hota mediehusets verksamhet. En sådan analys kan ni göra i följande steg:

1. **Utgångspunkt**. Vilken roll har ert mediehus i samhället?
   Vilka metoder kan ni använda för att identifiera och utvärdera hot och risker? Vilka gränsdragningar och perspektiv kommer ni att tillämpa i analysen?
2. **Riskbedömning**. Vilka är de tänkbara hoten och riskerna?
   Vad är sannolikheten för att riskerna ska realiseras, och vilka är de tänkbara konsekvenserna? Vilka situationer bör ni bedöma i relation till mediehusets krishanteringsförmåga? Vilka förebyggande åtgärder bör ni vidta?
3. **Sårbarhetsbedömning**. Hur påverkas ert mediehus av olika scenarion?
   Vilka konsekvenser skulle informationspåverkan kunna få, och hur kan er organisation hantera, stå emot och återhämta sig från dem?

Skräddarsy respons och motstrategier

Det finns ingen färdig lösning för att bemöta alla fall av informationspåverkan. Informationspåverkan förekommer i olika former, och alla mediehus har olika sårbarheter och förutsättningar. Därför är det viktigt att skräddarsy responsen. Genom grundliga förberedelser kan ni skapa övergripande ramar för lämpliga motstrategier som passar förutsättningarna, och som går att anpassa till den specifika situationen.

En lämplig respons bör stå i proportion till hur allvarlig situationen bedöms vara. MPF föreslår fyra olika nivåer av respons, där varje nivå också har förslag till mer specifika metoder:

1. Bedöm situationen.
2. Informera.
3. Förespråka.
4. Försvara.

Den första responsnivån handlar om att bedöma situationen. Det är en neutral åtgärd som samtidigt signalerar att mediehuset är medvetet om situationen och planerar att ta reda på fakta.

Den andra nivån består i att informera allmänheten och nyckelintressenter om situationen och om hur ni som mediehus ser på frågan. Det är en något mindre neutral åtgärd, där ni även redovisar fakta.

Den tredje nivån innebär kommunikativa åtgärder, där mediehuset förespråkar en viss position. Det innebär att ni aktivt argumenterar för era egna fakta eller budskap i relation till de vinklade eller falska budskapen.

Den fjärde nivån handlar om att försvara mediehuset genom att rikta specifika insatser mot påverkansaktören eller -aktörerna.

Faktabaserad respons respektive argumenterande respons

Om felaktig information får cirkulera utan att korrigeras kan det bidra till att andras uppfattningar om mediehuset, era målgrupper och era arbetsmetoder baseras på felaktigheter.

Därför bör den första åtgärden alltid vara responsnivåerna 1 och 2, att bedöma situationen och informera den identifierade målgruppen. Det är utgångspunkten för en så kallad faktabaserad respons, som kan tillämpas i de flesta fall av misstänkt informationspåverkan.

Fundera på hur den felaktiga informationen kan påverka mediehuset och dess verksamhet. Försök att ta reda på vem som sprider informationen, hur stor spridning den har och vilket eller vilka ämnen som berörs. Systematisera insamlandet. Om det sprids felaktig information kan första steget vara att svara med en rättelse. Många experter anser att desinformation bäst bemöts med korrekt information, men andra menar att ett rättat budskap bara får effekt bland dem som är intresserade av att ta reda på sanningen. Organisationens förberedande arbete med målgrupper och narrativ underlättar vid bedömningen av vilken åtgärd som är lämplig i det specifika fallet.

Responsnivåerna 3 och 4, att förespråka och försvara, är argumenterande. Sådan respons bör användas sparsamt, men kan vara nödvändig i särskilt allvarliga situationer. I sådana fall bör mediehusets ledning vara med i processen. Se också till att åtgärderna är förenliga med demokratiska principer, yttrandefrihet och andra regelverk, till exempel mediehusets regler för kommentarsfält på sociala medier.

Faktabaserad respons – bedöm och informera

De två första stegen i arbetet med att möta informationspåverkan är bedöma och informera. De är tillsammans det som kallas en faktabaserad respons, och kan användas i alla situationer.

STEG 1: BEDÖM

För att få grepp om vad som pågår måste ni göra en bedömning av situationen. Vad är det som händer? Vem är inblandad? Vad står på spel? Ju mer kunskap ni kan skaffa er om situationen, desto bättre blir er respons.

KARTLÄGG SITUATIONEN

Orientera er och skapa medvetenhet om vad som pågår.

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 ni har bedömt situationen kan ni börja kommunicera med era målgrupper. I det här steget är er kommunikation inriktad på att delge neutral information och fakta, samt att kommunicera hur händelsen hanteras. Kom ihåg att alltid målgruppsanpassa kommunikationen.

GÖR ETT UTTALANDE

Ge neutral information och dela relevanta fakta som ni har.

KORRIGERA

Gör ett uttalande som besvarar eller korrigerar ett falskt påstående med relevanta fakta. Till exempel kan ett formulär med vanliga frågor och svar, en FAQ, vara ett användbart verktyg.

HÄNVISA

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

BETONA VÄRDEGRUNDEN

Påminn målgruppen om vad er 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 organisationen arbetar med frågan genom att kommunicera med målgruppen. Detta ger er andrum att utarbeta en mer genomgripande respons.

Argumentbaserad respons – förespråka och försvara

Det tredje och fjärde steget i att bemöta informationspåverkan är att förespråka och försvara. Dessa steg innehåller åtgärder som bara är lämpliga i mer allvarliga situationer, där det tydligt går att identifiera informationspåverkan. Tillsammans är stegen det som kallas argumentbaserad respons.

STEG 3: FÖRESPRÅKA

Att förespråka sin position är en upptrappning från att neutralt informera, och innebär mer aktiv och utåtriktad kommunikation. I det här steget är det viktigt att alltid tänka på vilket mandat ni som tar fram kommunikationen har och på organisationens värdegrund när ni utformar organisationens 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 eller tillfällen där intressenter kan mötas och diskutera händelsen eller specifika problem, och 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 er egen position. Det är viktigt att informationspaketet bygger på fakta och verifierad information.

STORYTELLING

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

STEG 4: FÖRSVARA

Det sista steget, försvara, innefattar en direkt respons mot angriparen. Åtgärderna kan i vissa sammanhang framstå som kontroversiella, och ska därför bara användas i extrema situationer. Se till att diskutera alla åtgärder inom denna nivå med kollegor och chefer innan de implementeras, så att ni inte överskrider ert 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 att den inte har fått stor spridning eller uppmärksamhet. Då skulle respons i stället kunna bidra till att sprida den falska bilden.

RAPPORTERA

Om en angripare bryter mot lagen eller mot en medieplattforms användarregler bör ni anmäla till polisen eller plattformens ägare. Anmälan till plattformens ägare får inte missbrukas eller göras lättvindigt, utan bara 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, men varje blockering bör motiveras och knytas till de regler som gäller. Blockering får inte användas 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. Det ska dock inte göras lättvindigt, och måste föregås av en konsekvensanalys som tar hänsyn till vilka konsekvenser det får för organisationen och för den som exponeras.

Arbeta proaktivt i sociala medier

Sociala medier är inte bara en plattform som låter användare interagera med varandra, utan kan också användas som ett verktyg för informationspåverkan. Sociala medier har sin egen logik som ni måste känna till, förstå och ta hänsyn till vid eventuella motåtgärder.

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

Proaktivt arbete i sociala medier innebär att bygga nätverk och taggar som gör att mediehusets kommunikation når rätt människor. Här underlättar de förberedelser som du kan läsa om under rubriken ”Förbered och bygg beredskap” i den här handboken. Det finns också automatiserade verktyg som kan hjälpa er att ha koll på vad som händer i sociala medier i realtid, så att ni snabbt kan ingripa om desinformation börjar spridas.

Bemöt och hantera påverkan i sociala medier

Bedöm. Handlar det om påverkan eller är det engagerade medborgare som debatterar? Om ni misstänker informationspåverkan, kartlägg situationen så noga som möjligt. Vem eller vilka kommunicerar? Hur är tonen i kommunikationen? Hur reagerar de inblandade på information? Finns det länkar eller annat material? Vilka taggar används? Är några inblandade konton bottar?

Utforma ett budskap utifrån bedömningarna, och välj vilka målgrupper ni vill nå i ett första läge. Identifiera användare och taggar som ni kan använda. Informationen ni ger bör vara neutral, och ni bör lyfta mediehusets värderingar i de sammanhang där det är lämpligt.

Förespråka. Om ni ska ta steget att förespråka handlar det om att positionera er tydligare i debatten, till exempel genom egna budskap. Det kan också handla om att delta mer aktivt i debatten och på så sätt skapa ett bredare engagemang för frågan i era målgrupper.

Försvara. Om situationen eskalerar till ett läge där det inte går att ha en konstruktiv dialog, till exempel för att mediehusets budskap trängs undan av spam och destruktiva inlägg, kan det vara dags att gå i försvarsställning. Det kan handla om att blockera eller ignorera dem som sprider desinformationen. Om ni göra detta är det viktigt att ni öppet och transparent förklarar varför. Yttrandefrihet med en fri och öppen debatt är ett av kärnvärdena i vårt samhälle.

Ta vara på lärdomar

Att samla in och dokumentera exempel på informationspåverkan är centralt för att förstå problemet bättre, och för att bättre kunna möta påverkan i framtiden.

En logg över händelseförloppet, med information om åtgärder och tidpunkter, är ett sätt att dokumentera det som har hänt. Loggen kan ni sedan använda som utgångspunkt när ni utformar rutiner och arbetssätt för eventuella framtida påverkansförsök.

Ni kan också använda kunskapen för att ta fram utbildningsmaterial och för att effektivisera organisationens och samhällets beredskap. Om samhället i stort ska kunna bemöta informationspåverkan behöver alla dela med sig av sina erfarenheter och lära av varandra. Det gäller både internt inom en organisation och externt. Vilka kan ert mediehus lära sig av – andra mediehus, civilsamhället eller myndigheter?

Uppgifter att samla i er logg

- Beskriv händelsens bakgrund, förlopp och sammanhang.
- Vilka aktörer var inblandade?
- Vilka karaktärsdrag hos informationspåverkan fanns med?
- Utnyttjades några sårbarheter?
- Vilka tekniker användes?
- Vilka målgrupper och narrativ användes?
- Reflektera över vilken effekt angriparen vill uppnå, och motivera er bedömning. Hur agerade ni?
- Reflektera också över ert val av åtgärder. Vilken effekt fick de? Vad tror ni hade hänt om ni inte hade agerat?
- Spara även bevis i form av till exempel skärmdumpar.

Råd till dig som journalist

Internet i allmänhet och sociala medier i synnerhet har blivit en stor del av de flestas vardag. Därför är det rimligen också en del av det journalistiska uppdraget att bevaka och förstå hur sociala medier fungerar. Det hjälper dig att undvika att du själv sprider desinformation, men också att du eller mediehuset utnyttjas i påverkanskampanjer.

I det här avsnittet kan du läsa om den journalistiska metoden fact-checking, som används för att verifiera sådant som har publicerats – bland annat i sociala medier. Innehållet bygger på den globala, ideella organisationen First Drafts olika rapporter. First Drafts studier var länge ledande inom det här området. De principer och de metoder som det redogörs för är också de som brukas av organisationer som är godkända av och anslutna till International Fact Checking Network, IFCN. Publiceringar inom den journalistiska genren fact-checking är dessutom helt transparanta och läsaren kan följa varje steg i verifieringen och på sätt lära sig att själv verifiera.

Fact-checking som journalistisk metod

Arbetssättet fact-checking är uppdelat i två huvudgrenar:

1. **Granskning av sådant som har blivit viralt i sociala medier.** Det kan handla om allt från falska tävlingar och reklam till inlägg om inställda luciatåg och efterlysta personer. Eftersom påverkansaktörer letar efter sprickor och konflikter i samhället är det inte osannolikt att den här typen av inlägg kan vara påverkansförsök, även om inlägget till synes inte alls verkar ha något med informationspåverkan att göra.
2. **Granskning av makthavares påståenden, för att kontrollera fakta som makthavare kommunicerar.** Även sådana påståenden kan ha koppling till informationspåverkan och de tekniker som används. Det kan till exempel vara att påståenden knyts till vanliga narrativ inom informationspåverkan, eller genom att underlaget till påståendet kommer från sajter som har en tydlig agenda att splittra och polarisera. Kom ihåg att skilja på fakta och åsikter. Syftet med att möta informationspåverkan är inte att motarbeta yttrandefriheten, utan att medverka till ett sunt debattklimat.

Sammanfattningsvis handlar båda grenarna av fact-checking om att verifiera det som har publicerats och om traditionell källkritik.

System för verifiering

First Draft formaliserade ett system för verifiering som fungerar i stort oavsett vad det är som ska verifieras, till exempel en bild, ett inlägg eller ett konto:

- **Ursprung:** Är det som du ska verifiera faktiskt den ursprungliga bilden eller inlägget eller kontot?
- **Källa:** Vem skapade bilden, inlägget eller kontot?
- **Tid:** När skapades bilden, inlägget eller kontot?
- **Plats:** Var skapades bilden, inlägget eller kontot?
- **Agenda:** Varför skapades bilden, inlägget eller kontot?

Det finns gott om verktyg för att till exempel verifiera bilder och sökningar i sociala medier. Många verktyg är gratis och relativt enkla att använda. Dessutom vidareutvecklas befintliga verktyg hela tiden, och nya tillkommer ofta. Det bästa sättet att lära sig är att helt enkelt våga prova och vara nyfiken. Många verktyg har utmärkta instruktioner som är lätta att hitta vid sökning.

Det finns inget facit eller ”rätt sätt”.

> **Att arbeta med verifiering av exempelvis bilder, inlägg eller konton är ofta ett detektivarbete, där du använder flera olika verktyg för att få fram ledtrådar att lägga ihop.**

Om det dyker upp ett telefonnummer, en mejladress eller andra kontaktuppgifter under din granskning är den vanliga arbetsgången enligt IFCN:s principer att du ringer, mejlar eller skriver ett meddelande till den som har spridit informationen för att fråga var informationen kommer ifrån, varför den är publicer-

ad eller delad och så vidare.

För att verifiera rena fakta gäller allmänna journalistiska principer för källkritik – till exempel att du försöker hitta två av varandra oberoende källor och som bedöms äkta eller trovärdiga.

Det har också blivit påtagligt under de senaste åren att journalister och mediehus behöver vara extra noga med verifiering av material och källor vid plötsliga och/eller dramatiska nyhetshändelser. Sådana händelser gör ofta att mycket information börjar cirkulera snabbt, samtidigt som redaktioner gärna vill vara först med nyheter om det som hänt.

Fact-checking vid publiceringar om informationspåverkan

Fact-checking bygger inte på några annorlunda journalistiska eller etiska principer än mer traditionell journalistik. Om du ska göra en journalistisk publicering om informationspåverkan, till exempel en kartläggning av ett fall av informationspåverkan i mediehusets spridningsområde, är det dock viktigt att du bedömer om en publicering skulle kunna öka spridningen av det mediehuset egentligen vill stoppa. Problemet kan göras större än vad det egentligen är. Samtidigt är det bra att inte vänta för länge. När desinformationen väl har fått riktig fart i till exempel sociala medier är det svårt att påverka spridningen.

Exakt var gränsen går skiljer sig dock från fall till fall, och här får varje redaktion försöka lära sig var gränsen går för deras bevakningsområde. Det innehåll som ska granskas bör också ha en viss relevans för publiken och det ska ha betydelse om innehållet är korrekt eller inte.

> **En tänkbar fallgrop med fact-checking är att det kan finnas risk att fokus flyttas från det som verkligen är viktigt till detaljer som egentligen inte har så stor betydelse.**

Viktigt med transparens

Vid publicering är det viktigt att överväga hur du använder bilder. När fact-checkingorganisationer världen runt publicerar sina granskningar publicerar de ofta både den manipulerade/felaktiga bilden och den ursprungliga bilden. Det framgår tydligt vilken bild som är vilken.

I den standard som International Fact Checking Network, IFCN, använder ska publiceringen också vara transparent med hur granskningen gjordes. Publiceringen ska redogöra för alla steg och källor i granskningen. Om det behövs bör en expert intervjuas för att tolka det som har framkommit. Det är centralt inom fact-checking att redogöra för processen i publiceringen, och beskrivningen har också en pedagogisk effekt. Publiken lär sig hur de ska kontrollera material på nätet, och kan kanske börja göra det själva.

Fundera över dina val och avvägningar

Som journalist bör du ha förståelse för hur dina val av nyheter, vinklar, bilder och rubriker får betydelse, inte minst i sociala medier, och att det du publicerar kan finnas kvar på internet mycket länge. Samtidigt går det naturligtvis inte att förutse allt som kan hända med till exempel en artikel, och för journalister och mediehus är relevansen för allmänheten det vikti-

gaste i de flesta fall.

> **Dina artiklar kan användas i ett helt annat syfte än vad som var tänkt från början. Här har du som journalist och mediehuset ett extra ansvar för intervjuade och andra som medverkar i materialet.**

De allt vanligare betalväggarna gör också att publiken i många fall saknar tillgång till all information som behövs för att få en korrekt uppfattning om materialets innehåll. Reflektera gärna tillsammans över det på redaktionen, när du och kollegorna skriver rubriker, ingresser och pufftexter till sociala medier.

När du modererar i sociala medier

Det har blivit en vanlig journalistisk arbetsuppgift att moderera en redaktions kommentarsfält i sociala medier. Där kan bottar och automatiserade konton förekomma, vilket du kan läsa mer om i den här handboken. När det gäller moderering ger många redaktioner signaler om att det underlättar att ha tydliga regler för kommentarer. Det är ett stöd när moderatorn ska motivera varför inlägg döljs eller tas bort, eller när konton rentav blockeras. Reglerna kan till exempel handla om att de som kommenterar ska hålla sig till ämnet och att personangrepp inte är tillåtna.

Bemöt och hantera hat och hot som når dig som journalist

Informationspåverkan kan ses som en taktik att för att ta makten över den information som sprids. Ett annat sätt att göra detta är att utsätta journalister för hat och till med hot om fysiskt våld. Det har MSB redogjort för i bland annat rapporten ”Mediebranschen 2016 – hot, risker och sårbarheter”.

I rapporten står det att MSB bedömer att risken är hög för att personal på mediehus i Sverige ska bli skadade fysiskt eller psykiskt. MSB beskriver också att hat och hot numera tillhör vardagen för många journalister. Detta bekräftas även av bland annat undersökningen ”Journalisters utsatthet 2019” av JMG på Göteborgs universitet och av Tidningsutgivarnas ”Hot mot kvinnliga opinionsbildare” från 2017.

Utöver de rent personliga effekterna påverkar hat och hot mot journalister också det demokratiska systemet på flera sätt. Det kan dels bli svårare att rekrytera och behålla journalister, dels göra att journalister inte vågar eller vill skriva om vissa ämnen som de på förhand vet genererar hatiska och kränkande kommentarer.

2020 gav Medieinstitutet Fojo ut antologin "Det nya normala – ett hot mot demokratin", med vittnesmål från svenska journalister om hat och hot i deras vardag. Flera internationella organisationer som UNESCO och European Center for Press- and Media Freedom arbetar också med de här frågorna.

Stöd från Demokratijouren

Medieinstitutet Fojo har sedan 2017 ett uppdrag från kulturdepartementet

att arbeta med de här frågorna. Arbetet sker genom projektet Demokratijouren, som har mer information om ämnet. På Fojos webbsidor om Demokratijouren kan du få grundläggande råd om:

- hur frilansare eller [redaktioner kan öka sin beredskap
- information om det särskilda stöd till just journalister som olika samhällsinstanser och myndigheter har tagit fram
- tips om aktuell statistik, forskning och expertkunskap om hat och hot mot Sveriges journalister.

> **I en akut farlig situation ska du kontakta polis och ansvarig chef eller uppdragsgivare.**

Sveriges arbetsmiljölagstiftning kräver att alla företag med minst en anställd ska ha rutiner för att hantera ett hot mot en anställd. Det ingår i det systematiska arbetsmiljöarbetet. Oavsett om du är frilans, anställd eller chef har Demokratijouren information om hur du kan skapa rutiner för att vara beredd när hotet kommer. Det finns också råd om vad du kan göra i förebyggande syfte för att skydda dig mot hat och hot, och hur du kan agera när du blir utsatt.

Demokratijourens tio tips för att hantera hat och hot i arbetet

1. Tänk efter före. Gör en riskanalys innan, under och efter en publicering som du anar kan dra till sig hat och hot.
2. Utse en stödperson på eller utanför arbetet. Bestäm i förväg vem du ska vända dig till om och när du blir utsatt för hat och hot.
3. Skaffa en handlingsplan. Som chef, medarbetare eller frilans, bestäm på förhand vad du ska göra och vem du kontakta i krisen.
4. Ta ställning mot hatet. Tydliggör att det inte accepteras. Skriv en redaktionell policy mot hat och kränkande kommentarer.
5. Gör stödet till en rutin. Analysera dagligen vilka publiceringar som kan dra till sig hat och hot. Följ och uppmärksamma när en reporters mående behöver följas extra noga. Utse någon som gör det till sin uppgift.
6. Undvik att jobba ensam. Om arbetet är direkt farligt att utföra ensam, avbryt omedelbart. Efterlys arbetsgivarens instruktioner för ensamarbete. Hitta sätt att vara fler, även om du är frilans eller om ni är få på redaktionen.
7. Låt någon annan sköta mejlen. När det stormar digitalt, överlåt till en kollega eller chef att rensa bort hatet och hoten. Polisanmäl hoten och arkivera resten.
8. Googla inte dig själv – men be någon annan ha koll på vad som skrivs om dig på nätet.
9. Visa att du ser vad som händer andra. Sträck ut en hand till kollegor och utsatta i branschen. Erbjud backning och stöd.
10. Prata om att du blir utsatt, givet att du vill, vågar och kan. Det finns massor av stöd och kärlek att hämta. Du är inte ensam.

Till punkterna 1, 3 och 4 finns det mallar att hämta från Demokratijourens sidor på Fojos webbplats.

Frågor att fundera över när du som journalist ska bemöta informationspåverkan

- Finns det någon handlingsplan på din arbetsplats, om den skulle bli utsatt för ett påverkansförsök? Kan ni lära av andra, till exempel kommunikatörer i offentliga förvaltningar?
- Finns det någon handlingsplan på din arbetsplats när det gäller hat och hot mot medarbetare? Har ni koll på vilka resurser som finns i form av till exempel Fojos projekt Demokratijouren?
- Flera bedömare anser att informationspåverkan är ett hot mot demokratin. Hur kan medierna bli bättre på att bevaka detta, och beskriva för allmänheten vad som pågår?
- Den relativt nya journalistiska genren fact-checking, det vill säga att kontrollera om publiceringar eller uttalanden är falska, existerar knappt i Sverige till skillnad från större delen av västvärlden. Vilka konsekvenser får det för den svenska publiken?
- Har du något exempel på när du i efterhand känner att du borde ha hanterat en viss publicering annorlunda, till exempel när det gäller rubrik och bild? Det kan till exempel handla om hänsyn till intervjuade som kanske inte har räknat med att deras citat ska användas i helt andra sammanhang, som exempelvis i informationspåverkan.

Ordlista

Ordlista

Artificiell Intelligens, AI

AI är en maskins förmåga att visa människoliknande drag, såsom resonerande, inlärning, planering och kreativitet. AI möjliggör för tekniska system att uppfatta sin omgivning, hantera vad de uppfattar och lösa problem, med syfte att uppnå ett specifikt mål (exempelvis att tolka en bild, sammanfatta en text eller komponera en melodi).

Bandwagon-effekten

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

Bottar

Datorprogram som utför automatiserade uppgifter.

Deep fake

Ljud eller rörlig bild som manipulerats med hjälp av algoritmer.

Desinformation

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

Dold annonsering (*dark ads*)

Annonser som bara kan ses av specifika individer, med budskap som skräddarsys 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 har 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 som denne inte står för, och sedan argumentera mot dessa ståndpunkter i stället 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.

Mem, internetmem (*memes*)

Bilder, fraser, aktiviteter, koncept och filmer – ofta med humoristiskt innehåll – som sprids på internet, främst via sociala medier.

Nätfiske

När 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 genom 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 har fått lika mycket uppmärksamhet, men som inte är relevant i frågan.

I SAMARBETE MED

Fojo
Linnéuniversitetet

Myndigheten för psykologiskt försvar
Våxnäsgatan 10
653 40 Karlstad
E-post: registrator@mpf.se
Telefon: 010 - 183 70 00