STATSRÅDETS KANSLI

Att möta informationspåverkan

Handbok för kommunikatörer

Statsrådets kanslis publikations | 2019:13

Statsrådets kanslis publikations 2019:13

Att möta informationspåverkan

Handbok för kommunikatörer

Statsrådets kansli, Helsingfors 2019

Att möta informationspåverkan – Handbok för kommunikatörer

Denna publikation är en finlandssvensk version av den av Lunds universitet för Myndigheten för samhällsskydd och beredskap (MSB) i Sverige framtagna handboken Countering Information Influence Activities: A handbook for communicators (Order No: MSB1263 - Revised December 2018 ISBN: 978-91-7383-911-2), som ursprungligen gavs ut på engelska.

I översättningen av den finska versionen och i editeringen och anpassningen av den finska och finlandssvenska versionen till det finländska samhället har utöver den ursprungliga engelska versionen dessutom utnyttjas den svenska uppdaterade versionen Att möta informationspåverkan - Handbok för kommunikatörer (MSB1260 - reviderad i december 2018 ISBN:978-91-7383-910-5), som gavs ut i december 2018.

Myndigheten för samhällsskydd och beredskap (MSB) i Sverige har gett tillstånd till framtagningen och utgivningen av den finska och finlandssvenska publikationen.

Statsrådets kansli

ISBN: 978-952-287-731-4

Layout: Statsrådets förvaltningsenhet, publikationsverksamheten

Helsingfors 2019

Presentationsblad

Utgivare	Statsrådets kansli		7.5.2019
Publikationens titel	Att möta informationspåverkan. Handbok för kommunikatörer		
Publikationsseriens namn och nummer	Statsrådets kanslis publikationer 2019:13		
ISBN PDF	978-952-287-731-4	**ISSN PDF**	2490-1164
URN-adress	http://urn.fi/URN:ISBN:978-952-287-731-4		
Sidantal	58	**Språk**	svenska
Nyckelord	kommunikation, informationspåverkan, hybridpåverkan, beredskap, säkerhet, förvaltning, information		

Referat

I denna handbok avses med informationspåverkan verksamhet som systematiskt syftar till att påverka den allmänna opinionen, människors agerande och beslutsfattarna och därigenom hela samhällets funktionsförmåga. Medel för påverkan är till exempel att sprida felaktig eller missvisande information, utöva påtryckning eller utnyttja korrekt information tendentiöst. Det är fråga om strategisk verksamhet som syftar till att få objektet att fatta skadliga beslut och handla mot sitt eget intresse.[1]

Enligt denna definition är informationspåverkan skadlig kommunikation och bakom den kan finnas en statlig eller icke-statlig aktör som medvetet eller omedvetet kan agera för en stats räkning, individer, olika organisationer eller sammanslutningar, men även andra aktörer.

I handboken presenteras metoder för att förbereda sig på nya typer av hot i informationsmiljön och för att identifiera och analysera olika former av informationspåverkan. Dessutom ges i handboken instruktioner om hur man kan möta informationspåverkan.

Denna handbok är en finsk version av den av Lunds universitet för Myndigheten för samhällsskydd och beredskap (MSB) i Sverige framtagna publikationen Countering Information Influence Activities: A handbook for communicators (Order No: MSB1263 - Revised December 2018 - ISBN: 978-91-7383-911-2).

I översättningen av den finska versionen och i editeringen och anpassningen av den till det finländska samhället har utöver den ursprungliga engelska versionen dessutom utnyttjas den svenska uppdaterade versionen Att möta informationspåverkan – Handbok för kommunikatörer (Publikationsnummer: MSB1260 - Reviderad december 2018 - ISBN: 978-91-7383-910-5).

Myndigheten för samhällsskydd och beredskap (MSB) i Sverige har gett tillstånd till framtagningen och utgivningen av den finska publikationen.

1 Rekommendation om statsförvaltningens kommunikation (2016)

Förläggare	Statsrådets kansli
Distribution/ beställningar	Elektronisk version: julkaisut.valtioneuvosto.fi Beställningar: julkaisutilaukset.valtioneuvosto.fi

Kuvailulehti

Julkaisija	Valtioneuvoston kanslia		7.5.2019
Julkaisun nimi	Informaatiovaikuttamiseen vastaaminen. Opas viestijöille		
Julkaisusarjan nimi ja numero	Valtioneuvoston kanslian julkaisuja 2019:13		
ISBN PDF	978-952-287-731-4	**ISSN PDF**	2490-1164
URN-osoite	http://urn.fi/URN:ISBN:978-952-287-731-4		
Sivumäärä	58	**Kieli**	ruotsi
Asiasanat	viestintä, informaatiovaikuttaminen, hybridivaikuttaminen, varautuminen, turvallisuus, hallinto, informaatio		

Tiivistelmä

Tässä oppaassa informaatiovaikuttamisella tarkoitetaan toimintaa, jolla pyritään järjestelmällisesti vaikuttamaan yleiseen mielipiteeseen, ihmisten käyttäytymiseen ja päätöksentekijöihin sekä sitä kautta yhteiskunnan toimintakykyyn. Vaikuttamisen keinoja ovat esimerkiksi väärien tai harhaanjohtavien tietojen levittäminen ja painostaminen sekä sinänsä oikean tiedon tarkoitushakuinen käyttö. Kyse on strategisesta toiminnasta, jonka tavoitteena on saada kohde tekemään itselleen haitallisia päätöksiä ja toimimaan omaa etuaan vastaan.[1]

Tämän määritelmän mukaan informaatiovaikuttaminen on haitallista viestintää, jonka takana voivat olla valtiollinen toimija, ei-valtiollinen toimija, joka voi toimia myös tietoisesti tai tiedostamattaan jonkin valtion lukuun, yksilöt, erilaiset organisaatiot, järjestöt tai yhteenliittymät, mutta myös muut toimijat.

Opas tarjoaa keinoja, joilla informaatioympäristön uudenlaisiin uhkiin voidaan varautua ja jolla informaatiovaikuttamisen eri muotoja voidaan tunnistaa ja analysoida. Lisäksi opas antaa ohjeita informaatiovaikuttamiseen vastaamiseksi.

Tämä opas on suomenkielinen versio alun perin englanninkielisenä ilmestyneestä Lundin yliopiston Ruotsin Myndigheten för samhällsskydd och beredskap (MSB) -viranomaiselle laatimasta oppaasta Countering Information Influence Activities: A handbook for communicators (Order No: MSB1263 - Revised December 2018 ISBN: 978-91-7383-911-2).

Suomenkielisen julkaisun kääntämisessä, editoimisessa ja suomalaiseen yhteiskuntaan mukauttamisessa on hyödynnetty englanninkielisen alkuperäisen version lisäksi ruotsinkielistä joulukuussa 2018 julkaistua päivitettyä Att möta informationspåverkan – Handbok för kommunikatörer (Publikationsnummer: MSB1260 - Reviderad december 2018 - ISBN: 978-91-7383-910-5).

Suomenkielisen julkaisun tuottamiseen ja julkistamiseen on saatu lupa Ruotsin Myndigheten för samhällsskydd och beredskap (MSB) -viranomaiselta.

1 Valtionhallinnon viestintäsuositus 2016

Kustantaja	Valtioneuvoston kanslia
Julkaisun jakaja/ myynti	Sähköinen versio: julkaisut.valtioneuvosto.fi Julkaisumyynti: julkaisutilaukset.valtioneuvosto.fi

Description sheet

Published by	Prime Minister's Office		7 May 2019
Title of publication	Countering Information Influence Activities: A handbook for communicators (Finnish adaptation)		
Series and publication number	Publications of the Prime Minister's Office 2019:13		
ISBN PDF	978-952-287-731-4	**ISSN (PDF)**	2490-1164
Website address (URN)	http://urn.fi/URN:ISBN:978-952-287-731-4		
Pages	58	**Language**	Swedish
Keywords	Key words: communications, influence through information, hybrid influencing, preparedness, security, administration, information		

Abstract

In this handbook, influencing through information means systematic actions designed to influence public opinion, people's behaviour and decision-makers and through that the functions of society. The methods include dissemination of false and misleading information, exertion of pressure and manipulative use of information that is, in itself, correct. It is a question of a strategic activity designed to mislead the target to make self-damaging decisions or act against its own best interests.[1]

According to the definition, information influencing is harmful communications by a state actor, a non-state actor that can knowingly or unknowingly act on behalf of a state, individual, organisation, association or undertaking, but also by other actors.

The handbook also provides means to prepare for new kinds of threats posed by the information environment and to identify and analyse the different forms of information influencing as well as instructions on how to respond to them.

This handbook is a Finnish version of the book originally drawn up in English by the Lund University for the Swedish authority Myndigheten för samhällsskydd och beredskap (MSB): Countering Information Influence Activities: A handbook for communicators (Order No: MSB1263 - Revised December 2018 ISBN: 978-91-7383-911-2).

In translating and editing the book and adapting it to Finnish society, use was made of the original English version as well as the Swedish version updated in December 2018: Countering Information Influence Activities: Att möta informationspåverkan – Handbok för kommunikatörer (Publikationsnummer: MSB1260 - Reviderad december 2018 - ISBN: 978-91-7383-910-5).

A permission to produce and publish the Finnish version has been granted by the Swedish authority Myndigheten för samhällsskydd och beredskap (MSB).

1 Government Communications Guidelines 2016

Publisher	Prime Minister's Office
Distributed by/ Publication sales	Online version: julkaisut.valtioneuvosto.fi Publication sales: julkaisutilaukset.valtioneuvosto.fi

Innehåll

DEL III
Att möta informations-påverkan 36

FÖRORD

Vår omvärld har förändrats kraftigt under de senaste åren. De nya typer av hot och risker som framkommer i informationsomgivningen har fått oss att bedöma och utveckla vår beredskap och vårt agerande.

I och för sig är informationspåverkan inte något nytt. Tillvägagångssätt och metoder inom informationspåverkan har utnyttjats genom tiderna i olika delar av världen. Finland är inte något undantag i detta avseende. Förändringen i kommunikations- och informationsteknik har dock möjliggjort helt nya slags sätt att påverka människor och samhällen med kommunikativa metoder, både i gott och ont.

Fientliga påverkanskampanjer har blivit allt mer effektiva och lömska. Genom att utnyttja identifierade svagheter och sårbarheter hos objektet kan man effektivt påverka objektets agerande, tankar och åsikter. Syftet är att få objektet att fatta skadliga beslut och handla mot sitt eget intresse.[1]

Man ska hela tiden förbereda sig på informationspåverkan. Hatretorik och desinformation syftar till att provocera, undertrycka diskussionen och tysta ner röster samt till att underblåsa polarisering. Målet är att underminera den nationella värdegrunden, demokratin och förtroendet samt att undertrycka åsiktsfriheten och allmänhetens och pressens yttrandefrihet.

I beredskapen inför och motarbetandet av osaklig påverkan är det viktigt med ökad medvetenhet och samarbete. När objektet är samhället i sin helhet, dess olika funktioner, värderingar och normer, måste vi alla delta i detta arbete. Att möta informationspåverkan är inte enbart en uppgift för myndigheter, det är lika mycket en uppgift för företag, sammanslutningar, organisationer och individer.

1 Rekommendation om statsförvaltningens kommunikation (2016)

Vi vill rikta ett mycket varmt tack till Myndigheten för Samhällsskydd och beredskap (MSB) i Sverige för ett gott och långvarigt samarbete och för deras tillstånd att publicera deras utmärkta handbok om informationspåverkan, som baserar sig på forskning vid Lunds universitet, som editerad version i Finland på finska och på svenska. Samtidigt vill vi också tacka Dr. James Pamment från Lunds universitet. Handboken ger viktig information och praktiska instruktioner när vi förbättrar vår beredskap att möta informationspåverkan.

Inledning

Denna handbok har ursprungligen utarbetats med tanke på Sverige. Det svenska och det finländska samhället har mycket liknande grundläggande lösningar, så handbokens tankesätt kan mycket väl tillämpas i Finland också.

Myndigheten för Samhällsskydd och Beredskap (MSB) i Sverige definierar påverkanskampanjer som en från främmande makt koordinerad verksamhet som innefattar vilseledande eller oriktig information eller annat för ändamålet särskilt anpassat agerande. Syftet är att påverka beslut av politiska eller andra offentliga beslutsfattare, opinioner hos hela eller delar av befolkningen eller beslut eller opinioner i ett annat land, där mållandets suveränitet, målen för mållandets säkerhet eller andra intressen kan komma att påverkas menligt.

I denna handbok som publicerats i Finland definieras informationspåverkan inte enbart som statsstyrt eller statligt agerande. Erfarenheterna har visat att det också kan finnas andra aktörer. Ofta är det också svårt att tydligt visa vem aktören är. Därför är den tillämpade synvinkeln 360 grader. Fientliga påverkansförsök ska tas lika allvarligt, oberoende av vilket väderstreck eller hur nära eller fjärran de kommer från. Det är bra att komma ihåg detta. Målen är desamma i olika påverkansförsök.

Det finns många utvecklingstrender bakom framtagningen av handboken. En trend är det förändrade krigföringssättet. Den illegala annekteringen av Krim till Ryssland och konflikten i östra Ukraina har visat att hybridverksamhet som kombinerar olika metoder har många ansikten. Angriparen kan uppnå sitt mål till och med genom att använda i huvudsak andra medel än militära.

Betydelsen av informationspåverkan framhävs i den moderna hybridverksamheten. Ett begrepp som används för att beskriva detta säkerhetshot är påverkanskampanj. I en planerad påverkanskampanj på statlig nivå utnyttjar främmande makt sårbarheter i det samhälle som ska påverkas för att uppnå sina mål utan att använda militära medel.

En påverkanskampanj består av flera aktiviteter, en sådan aktivitetstyp är informationspåverkan. I eldlinjen för informationspåverkan står i första hand de band som håller ihop samhället, underminerat förtroende för beslutsfattare samt samhällets funktionalitet och dess grundläggande värden, såsom demokrati, rättssäkerhet och mänskliga rättigheter. Praktiska metoder är att påverka beslutsfattandet genom informationsbrus, att stämpla beslutsfattarna som inkompetenta eller att driva samhällssituationer till sin spets. Informationspåverkan kan också gälla beslut som innebär vittgående ekonomiska konsekvenser.

Handbokens grundläggande syfte är att gå igenom handlingsmodeller inom informationspåverkan, så att det blir lättare att identifiera sådan påverkan. Journalister och kommunikatörer är inte föremål för informationspåverkarnas försök att tysta ner röster av en slump. Yrkeskompetenta journalister, kommunikatörer och medborgaraktivister med stark etik gör fientlig informationspåverkan svårare genom att visa vad som håller på att hända och genom att till exempel lyfta fram falska påståenden som sprids i sociala medier eller nyhetsmedier.

Att använda information för att påverka är inte något nytt. Kommersiellt, politiskt och ideellt påverkansarbete har förekommit i mänsklighetens sociala vävnad från början. Vi som medborgare har hittills litat på att denna typ av kommunikation följer vissa regler. Grundläggande förväntningar har varit att sådan kommunikation sker öppet, att den baseras på korrekt information och att den presenteras på ett sätt som gör det möjligt att fatta välavvägda beslut.

Denna handbok handlar om kommunikation som inte följer dessa regler. Sätten att dela, använda och förädla information har förändrats så att det i länder som Finland och Sverige är möjligt att nå nästan hela befolkningen när som helst. En väsentlig förändring till exempel jämfört med det kalla kriget är att det idag är svårare att se motiven hos informationskällan. Den öppet identifierbara kommunikationen har minskat. Volymen av information som kommer direkt till det egna kommunikationsverktyget – telefonen, pekplattan osv. – har ökat.

Ett viktigt drag i fientlig informationspåverkan är att det är svårt att vidta motåtgärder. Det kan vara omöjligt att på ett pålitligt sätt hitta eller verifiera den ursprungliga informationskällan. Eftersom ett centralt tillvägagångssätt i informationspåverkan är att utnyttja spänningar och konflikter som förekommer i samhället, kan det vara svårt att särskilja informationspåverkan från en hetsig samhällsdebatt.

När det talas om fientlig informationspåverkan på statlig nivå avses det ofta att information används i det fördolda eller på ett vilseledande sätt så att syftet till exempel är att underminera demokratiska processer, kontrollera det offentliga samtalet och påverka

beslutsfattare. I ett globalt perspektiv har uppmärksamhet fästs till exempel vid agerandet i samband med presidentvalen i USA (2016) och i Frankrike (2017).

Den nordiska samhällsmodellen bygger på förtroende. 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. Förmågan att upprätthålla förtroendet och möta informationspåverkan med tillförlitlig kommunikation är viktig med tanke på samhällets hållbarhet.

Det primära syftet med denna handbok är att stärka demokratin och dess processer och att främja den öppna debatten som är viktig med tanke på samhällsutvecklingen.

Vilken är kommunikatörens roll?

Som kommunikatör har du en viktig roll i arbetet med att förebygga, identifiera och möta informationspåverkan. Det behövs inga sluga trick. För det första kan du medverka 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.

Din organisation eller du själv kan bli utsatt för informationspåverkan. Hur agerar du, om du 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 kunder och andra målgrupper, genom att de blir föremål för näthat, trollning eller vilseledande information. I alla dessa fall har du som kommunikatör en viktig roll, när din organisation söker ett konstruktivt responssätt.

Varför kommunikatörer?

- Kommunikatörer bygger broar mellan organisationer och allmänheten.
- I arbetet ingår kriskommunikation som kan vara ett relevant verktyg för att möta informationspåverkan.
- Kommunikatörer är ofta bland de första som upptäcker tecken på information-spåverkan.

Denna handbok ger kunskap som kan stödja dig i arbetet. Handboken innehåller metoder att identifiera och möta informationspåverkan. Dessutom får du råd om hur du förbereder din organisation för att effektivt möta informationspåverkan samt vägledning till att fatta beslut om motåtgärder.

Vår metod

Handboken är tänkt att göra det lättare att identifiera metoder som används inom informationspåverkan, samt tillgängliggöra en verktygslåda med kommunikativa metoder som kan användas för att svara på informationspåverkan. Alla organisationer är olika och står inför olika typer av utmaningar, så just din kommunikativa yrkeskompetens behövs för att tillämpa handboken.

DEL I
ATT BLI MEDVETEN OM INFORMATIONSPÅVERKAN

Vad är informationspåverkan?

Hur utnyttjas samhällets sårbarheter i informations-påverkan?

Hur skiljer sig informationspåverkan från annan kommuni-kation?

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 lärdomar?

DEL I
Att bli medveten om informationspåverkan

Vad är informationspåverkan?

Hur utnyttjas samhällets sårbarheter i informationspåverkan?

Hur skiljer sig informationspåverkan från annan kommunikation?

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

1.1 Vad är informationspåverkan?

Öppen debatt, åsiktsskillnader och försök att påverka människor hör till demokratin. Men vad händer om någon introducerar lögner i debatten? Om någon förvränger fakta, använder falska experter eller argumenterar på ett avsiktligt missledande sätt? Sådan kommunikation är skadlig för samhället och för demokratin. Syftet med faktabaserad argumentation, källkritik och yttrandefrihetens principer är att skydda vårt demokratiska samhälle.

I de flesta demokratier finns en fri och levande politisk debatt. Enskilda medborgare, journalister, forskare och representanter från civilsamhället granskar makten också påvisar samtidigt fall av uppenbart felaktig och vilseledande information.

Myndigheterna kan stötta detta arbete genom att exempelvis ge ekonomiskt stöd och bidra med att korrigera falsk information och felaktiga uppfattningar 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 olika aktörer utnyttjar genom informationspåverkan.

I denna i Finland utgivna handbok avses med informationspåverkan verksamhet som systematiskt syftar till att påverka den allmänna opinionen, människors agerande och beslutsfattarna och därigenom hela samhällets funktionsförmåga. Medel för påverkan är till exempel att sprida felaktig eller missvisande information, utöva påtryckning eller utnyttja korrekt information tendentiöst. Det är fråga om strategisk verksamhet som syftar till att få objektet att fatta skadliga beslut och handla mot sitt eget intresse. Enligt denna definition är informationspåverkan skadlig kommunikation och bakom den kan finnas en statlig aktör, en icke-statlig aktör, som medvetet eller omedvetet också kan agera för en stats räkning, individer, olika organisationer eller sammanslutningar men även andra aktörer.

Informationspåverkan kan syfta till att underblåsa misstro både bland befolkningen och mellan befolkningen och myndigheterna. Genom informationspåverkan stöder aktören sin egen agenda genom att utnyttja sårbarheter, svagheter och motstridigheter i samhället eller i objektet för påverkan. Målet kan vara att öka splittringen eller strävan att få objektet att fatta beslut som är dåliga för objektet, utan att objektet nödvändigtvis blir medvetet om det.

Informationspåverkan kan ske som enskilda åtgärder eller som ett led i en mer omfattande påverkanskampanj. I det sistnämnda fallet utnyttjas i omfattande grad olika kommunikativa eller andra typer av tekniker.

Ett samhälle kan påverkas fientligt på många olika sätt, allt från diplomatiska och ekonomiska medel till militärt våld.

Påverkanskampanjers anatomi

Användandet av påverkanstekniker

PR, marknadsföring, diplomati, opinionsjournalistik och lobbyverksamhet är exempel på accepterade sätt genom vilka olika organisationer försöker påverka människors åsikter och beteenden. Informationspåverkan efterliknar dessa tekniker.

Störandet av den offentliga debatten

Olika aktörer använder informationspåverkan både direkt och indirekt. Olika metoder kan vara t.ex. förfalskade dokument, ”hackat” material, narrativ samt att bekräfta, upprepa och sprida budskap. Genom att störa offentlig debatt kan man förändra vår bild av dess omfattning, innehåll eller inriktning. Detta kan påverka beslutsfattandet.

Strävan efter egen vinning

Informationspåverkan är målinriktad. Man kan störa beslutsfattandet till exempel genom att driva den politiska debatten till sin spets, underblåsa polariseringen mellan grupper i samhället eller genom att man försöker destabilisera ett samhälle politiskt.

Utnyttjandet av sårbarheter

Alla samhällen har sina utmaningar. Dessa kan bestå 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 vilken del av påverkan hör till samhällsdebatten och vilken inte hör till den. Känslor, tillspetsningar och rentav skarpa åsikter hör till politiska debatter.

Demokratin bygger på öppen och fri debatt. Det blir svårt att föra debatten på ett konstruktivt sätt om en aktör introducerar vilseledande information i syfte att störa och styra samtalet. Människor har rätt till sina åsikter och rätt att framföra dem eller föra kampanjer för dem.

Inom informationspåverkan används vilseledande metoder systematiskt i syfte att underminera demokratin. En grundläggande princip vid bemötande av informationspåverkan är därför att värna och skydda den fria och demokratiska debatten och yttrandefrihetens principer, även om det försvårar uppgiften.

1.2 Hur utnyttjas samhällets sårbarheter i informationspåverkan?

Föreställ dig att våra åsikter uppstår till följd av en rationell process. I en idealisk värld börjar informationsförmedling när någonting händer eller när ny information blir känd. Experter tolkar eller förklarar situationen. Media förmedlar nyheten och informationen når allmänheten.

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.

Huruvida denna modell lyckas är beroende av om händelsen är verklig eller informationen korrekt och om den bygger på fakta.

Har informationen eller händelsen verifierats av trovärdiga och verkliga källor? Medier kollar fakta och källor och strävar efter att tjäna allmänhetens intresse. I den offentliga debatten tar man hänsyn till olika synvinklar och åsikter. Det förs en konstruktiv debatt innan några slutsatser dras.

Inom informationspåverkan försöker aktören identifiera sårbarheter i den process som beskrivits ovan och rikta sin påverkan till processens sårbarheter och till förmedling av kritisk information i medier.

Fakta kan förfalskas eller manipuleras. Falska experter kan användas och vittnen kan mutas eller hotas. Nyhetstjänster kan drivas som ensidiga propagandakanaler och det digitala samtalet kan föras mellan automatiserade konton, dvs. botar, vilket skapar en skenbild av en livlig offentlig debatt.

När dessa aktiviteter genomförs avsiktligt i syfte att underminera demokratiska processer, kan vi inte alltid förlita oss på ett självsanerande system. Här innehar vi alla en viktig roll.

1.3 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

Ny information förklaras eller tolkas av till exempel experter och tjänstemän.

MEDIA OCH KULTUR

Informationen når allmänheten genom media, exempelvis tidningar, TV, radio, bloggar eller sociala medier.

ALLMÄNHETEN

Informationen når allmänheten. Den diskuteras i olika interaktiva situationer, exempelvis när människor möts och på sociala medier.

INDIVIDEN

Till slut når informationen dig genom de sociala sammansättningar du ingår i.

SÅRBARHETER I MEDIESYSTEMET

Till dessa sårbarheter hör den snabba förändringen i kommunikationstekniken och omvärlden, de nya journalistiska affärsmodellerna och den tilltagande mängden alternativa nyhetskällor online. Förfalskade budskap, manipulerade bilder, klickjakt, algoritmer och botar på sociala medier utgör verktyg för den som vill utnyttja sårbarheterna för egen vinning.

SÅRBARHETER I OPINIONSBILDNINGEN

Opinionsbildning har alltid varit sårbar. Vi hör till olika ekokammare och filterbubblor. I dessa kommunicerar människor med andra som delar samma åsikter eller uppfattningar. Där kan fördomarna stärkas ytterligare.

I dagens informationsmiljö är det lätt att provocera och att väcka ilska och upprördhet. Detta bidrar till att polarisera debatten, vilket falska konton och troll på sociala medier ytterligare stärker.

KOGNITIVA SÅRBARHETER

Vi lever i ett informationsflöde och kan inte hantera all den information vi utsätts för.

Enligt vissa uppskattningar finns det upp till 800 datapunkter för varje individ på sociala medier. Denna information kan användas för att förstå och förutsäga våra beteenden och vårt agerande. Systemen förstår oss bättre än vad vi själva gör.

1.4 Hur skiljer sig informationspåverkan från annan kommunikation?

För att identifiera informationspåverkan behöver kommunikatören bedöma i vilken utsträckning kommunikationen är vilseledande, sker avsiktligt och i syfte att störa. Bedömningen av dessa faktorer bidrar till beslutet om hur påverkan ska mötas. Alla ovan nämnda faktorer förekommer inte nödvändigtvis samtidigt. Ju fler kännetecken som identifieras, desto högre är sannolikheten att det handlar om informationspåverkan.

Kommunikatören bör agera, när informationspåverkan används i debatter kopplat till kommunikatörens verksamhetsområde, eller i syfte att underminera den offentliga debattens integritet eller samhällets säkerhet.

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 som avsikt att underminera det konstruktiva samtalet och den öppna debatten.

Störande

Tillförlitlig kommunikation stärker demokratin och är en naturlig del av samhället. Informationspåverkan stör och försvagar samhällets funktionalitet och det demokratiska samtalet.

Det är ingen slump att informationspåverkan utnyttjar samma tekniker 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 handbok och ska alltid rapporteras till polisen.

DEL II
Att identifiera informationspåverkan

Vad är syftet med informationspåverkan?

Vilka är de centrala teknikerna inom informationspåverkan?

Hur kan olika tekniker kombineras?

En förutsättning för att möta informationspåverkan är förmågan att upptäcka eventuella informationsoperationer. Man måste alltså veta vad man ska hålla utkik efter. I detta kapitel beskrivs de tekniker som används vid informationspåverkan. Avsnittet hjälper dig att utvärdera strategiska narrativ och hur narrativen riktas till vissa målgrupper. Avsnittet ger också en introduktion till de vanligaste teknikerna inom informationspåverkan, och visar hur strategierna och teknikerna kan kombineras till koordinerade insatser.

2.1 Vad är syftet med informationspåverkan?

För att identifiera informationspåverkan måste man känna till strategiska narrativ och målgrupper. När man känner till dessa hjälper det också att avslöja de bakomliggande strategierna och målen.

Strategiska narrativ

Informationspåverkan innefattar vanligtvis berättelser (eng. storytelling). Berättelsen om eller skildringen av en händelse, fråga, organisation, plats eller grupp formuleras för att passa in i ett befintligt narrativ. Ett bra exempel är rymdkapplöpningen mellan USA och Sovjetunionen under kalla kriget, som alla säkert har hört talas om. De flesta har också hört berättelser om att det är lögn att människan landade på månen och planterade en flagga där. När vi hör nya berättelser om rymdresor sorterar vi informationen i relation till vad vi tror på. Sådana avsiktligt konstruerade berättelser som används vid informationsoperationer kallas för strategiska narrativ. Framtagningen och användningen av narrativ kan ske i positivt eller fientligt syfte. I detta kapitel fokuseras på att identifiera det sistnämnda alternativet.

Man kan till exempel framföra påståenden om vissa etniska eller religiösa grupper, så att de passar in i ett mer omfattandet historiskt eller politiskt narrativ och i folks förutfattade meningar om dessa grupper.

Diskussionen kan påverkas åtminstone på tre olika sätt:

1. genom att man kompletterar eller lyfter fram delar av det existerande narrativet om gruppen i fråga,
2. 2) genom att man förvränger det existerande narrativet på ett sätt som är skadligt för den berörda gruppen,
3. om annan påverkan inte biter – genom att man fäster uppmärksamheten vid något annat genom att fördunkla narrativet.

När man planerar hur informationspåverkan ska mötas, är det viktigt att identifiera logiken bakom strategiska narrativ och påverkan. Fundera på hur en eller flera av följande metoder inom strategiska narrativ har använts i offentligheten.

STRATEGISKA NARRATIV

Positivt eller konstruktivt: "Det här är sanningen!"
Syftar till att konstruera en sammanhängande berättelse om en viss fråga som passar in i etablerade och befintliga narrativ eller kompletterar eller utvecklar dem.

Negativt eller nedbrytande: "Det där är lögn!"
Syftar till att förhindra uppkomsten av sammanhängande narrativ, eller underminera eller rentav eliminera befintliga narrativ i en fråga.

Distraherande "Titta här borta!"
Syftet är att avleda uppmärksamheten från en viss fråga genom att fördunkla frågan. I detta avseende kan användas t.ex. humor, memes eller konspirationsteorier eller så kan det ges många förklaringar som avviker från varandra i viss grad.

Målgrupper

Att analysera strategiska narrativ är en metod för att förstå logiken bakom informationspåverkan. Ett annat sätt är att analysera vem dessa narrativ talar till, dvs. vem den tilltänka målgruppen är. Riktas narrativen mot hela befolkningen eller mot vissa enskilda grupper eller individer? Använder man storskalig dataanalys (big data) för att utforma riktade insatser mot personer med liknande personlighetsdrag och åsikter? Utnyttjar man sårbarheter eller beteendemönster kopplat till den specifika gruppen eller individen? Det blir lättare att bedöma situationen när man förstår objektet för påverkan och de narrativ som används för att påverka objektet.

MÅLGRUPPER

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

Specifika grupper
Specifika målgrupper identifieras baserat på demografiska faktorer, t.ex. ålder, inkomst, utbildning eller etnicitet. På så sätt kan man skapa budskap som tilltalar den tilltänkta gruppens medlemmar.

Individer
I kommunikation som riktas till individer används storskalig dataanalys (big data) för att identifiera individernas personlighetsdrag, politiska preferenser eller beteendemönster.

Målgruppsanalysen kan avslöja intentionen bakom informationspåverkan. En analys av de strategiska narrativ och kommunikationstekniker som används gör det möjligt att förstå den tilltänkta mottagaren och syftet och målsättningen med påverkansaktiviteten.

2.2 Vilka tekniker används inom informationspåverkan?

Inom informationspåverkan används en rad tekniker som är under ständig utveckling. Vanligt förekommande tekniker kan delas in i sex övergripande grupper.

Teknikerna är i regel inte goda eller onda i sig, utan neutrala.

Kommunikativa tekniker kan användas på ett öppet och accepterat sätt, men även inom fientlig informationspåverkan. Att en viss teknik används innebär inte i sig att det rör sig om informationspåverkan.

De använda teknikerna bör analyseras med tanke på om det är fråga om avsiktligt vilseledande eller störande och relatera detta till analysen om strategiska narrativ och målgrupper. I analysen bör följande frågor alltid beaktas:

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

2.3 Tekniker inom informationspåverkan

HACKNING AV NÄTVERK OCH TANKEPROCESSER (s. 26)

- Dold annonsering (*dark ads*)
- Bandwagon-effekten (*bandwagon-effect*)
- Tystnadsspiralen (*spiral of silence*)
- Ekokammare och filterbubblor (*echo chambers and filter bubbles*)

VILSELEDANDE IDENTITETER (s. 27)

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

TEKNISK MANIPULATION (s. 29)

- Botar
- Sockpuppets
- Deepfakes
- Nätfiske

DESINFORMATION (s. 31)

- Falsk information
- Manipulation
- Tillskrivning
- Satir och parodi

ILLASINNAD RETORIK (s. 32)

- Personangrepp (*Ad hominem*)
- Whataboutism
- Störtflod av argument (*Gish-gallop*)
- Halmgubbar (straw man)
- Kapning av argument

SYMBOLHANDLINGAR (s. 33)

- Läckor
- Hackning
- Offentliga demonstrationer

Hackning av nätverk och tankeprocesser

Hackning av nätverk och tankeprocesser 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.

För oss är det exempelvis vanligtvis lättare att identifiera oss med vad människor som liknar oss tänker och gör. Eller så kan det vara svårt att handla rationellt, när vi exponeras för känslomässigt laddat innehåll. Dessa förutsägbara beteendemönster kan utnyttjas av fientliga aktörer som avsiktligt trycker på ömma punkter, exempelvis på sociala medier.

DOLD ANNONSERING (*DARK ADS*)

Budskap skräddarsys efter en individs psykografiska profil. Genom bl.a. storskalig dataanalys (big data) eller data från 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 (*BANDWAGON-EFFECT*)

Personer som upplever sig vara del av en majoritet är mer benägna att dela med sig av sin åsikt. Exempelvis botar kan användas för att ge fler gilla-markeringar, kommentarer eller delningar på sociala medier. Målet är att få verkliga användare att dela innehåll, så att de får mer synbarhet, uppmärksamhet och deltagande. Detta skapar social acceptans för ett budskap eller en åsikt.

TYSTNADSSPIRALEN (*SPIRAL OF SILENCE*)

Personer som upplever sig vara i minoritet är i sin tur sannolikt återhållsamma eller försiktiga med att dela med sig av sina åsikter. Intrycket att man är i minoritet kan 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 (*ECHO CHAMBERS AND FILTER BUBBLES*)

Grupperingar inom vilka personer framförallt kommunicerar med andra som delar samma åsikter och uppfattningar. Ekokammare och filterbubblor kan uppstå både på och utanför sociala medier. Personer med liknande åsikter använder medier på samma sätt eller umgås huvudsakligen med likasinnade. De exponeras därför sällan för ideologiskt annorlunda åsikter. Detta kan 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? Är de dem som de utger sig för att vara? Aktörer kan efterlikna trovärdiga informationskällor, som personer, organisationer eller plattformar, och på så sätt utnyttja den efterliknade källans 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. Inom informationspåverkan kan lockfåglar exempelvis vara en grupp troll 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 vara experter, såsom läkare eller advokater.

FÖRFALSKNINGAR

Att fabricera eller förfalska information är ett effektivt sätt att få en lögn att framstå som autentisk information. Falska brevpapper, stämplar eller namnteckningar kan användas för att få förfalskningar att se äkta ut.

POTEMKINKULISSER (*POTEMKIN VILLAGES*)

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

Falsk information kan spridas genom förfalskade nyhetssajter som efterliknar äkta sådana. På internet kan man exempelvis skapa en falsk sajt som ser ut som en riktig sajt eller vars adress är nästan identisk med riktiga webbadresser.

2.4 Källkritik på nätet

RUBRIK

Rubriker försöker oftast 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.

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.

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.

FÖRFATTARE

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

DELNINGAR OCH GILLA-MARKERINGAR

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 avancerad teknologi, även om påverkansteknikerna är traditionella. Informationsflödet på internet kan manipuleras genom automatiserade konton (botar) och algoritmer eller en kombination av mänsklig och teknisk manipulation.

Detta område utvecklas långt mycket snabbare än vår förmåga att analysera potentiella konsekvenser och användningsområden. Aktuella frågor är så kallade deep fakes, dvs. problem i samband med maskin- och djupinlärning samt artificiell intelligens. Det är klart att denna nya 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

Sockpuppets är 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. I verkligheten tillhör meddelandena 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.

2.5 Så upptäcker du en bot

Botar är effektiva verktyg för att bedriva påverkan på sociala medier. Men de är samtidigt relativt enkla att avslöja. Botar förekommer i olika former och de ser olika ut. Imitatörsbotar försöker efterlikna riktiga användare och kan vara svåra att upptäcka. Spambotar i sin tur 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 omvänd 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 SKAPANDEDATUM

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 så att de förstärker varandra. Botar har ofta endast andra botar som följare.

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.

FALSK INFORMATION

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

En öppen och fri offentlig debatt hör till ett demokratiskt samhälle. Alla har rätt att uttrycka sin åsikt. Det kan finnas försök att styra denna offentliga debatt med illasinnade retoriska metoder. Det kan handla om strategier för att bedra, vilseleda och tysta ner samhällsdebatten t.ex. genom att avskräcka deltagare.

Troll utnyttjar ofta illasinnad retorik. Troll är användare på sociala medier som avsiktligt provocerar andra genom sina kommentarer och sitt agerande. Trollen bidrar till ökad polarisering, tystar kritiska röster och överröstar andra i den öppna debatten. Troll kan drivas av personliga motiv eller arbeta på uppdrag av någon annan (dessa kallas även *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 rikta uppmärksamheten till ett liknande fenomen som inte fått lika mycket uppmärksamhet, men som inte är 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 (*HIJACKING*)

Att delta i en debatt genom att ta över den och ändra dess riktning. Detta är särskilt effektivt på sociala medier.

Symbolhandlingar

Handlingar säger mer än ord. Ibland kan syftet med en handling främst vara att kommunicera ett budskap. Detta kallas för en symbolisk handling. Symboliska handlingar motiveras av en kommunikativ logik och en strategisk inramning. Terrorattacker är exempel på mycket råa symbolhandlingar, där aktörer spelar på rädslan för slumpmässigt 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 den demokratiska debatten. Inom informationspåverkan kan demonstrationer orkestreras för att ge ett falskt intryck av stöd för en viss fråga på gräsrotsnivå (så kallad *astroturfing*).

2.6 Hur kan påverkanstekniker kombineras?

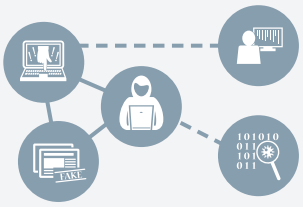
Inom informationspåverkan kombineras strategiska narrativ, målgrupper och tekniker. Genom att flera tekniker kombineras uppnås en större effekt.

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. Därför måste man fundera över om det finns bevis på inte bara enstaka utan även ett flertal, samordnade aktiviteter som riktas mot organisationen. På nästa sida hittar du några exempel på hur kombinationer av tekniker kan se ut.

Kommunikationen och identifieringen av informationspåverkan kan bedömas till exempel med följande frågor: Vilka är narrativen och vem riktar de sig till? Finns det belägg på att någon försöker vilseleda eller störa det offentliga samtalet? Misstänker man direkt inblandning från en utomstående aktör eller indirekt via deras ombud? Ser man tecken på kombinationer av metoder som antyder en samordnad aktion eller kampanj? Om det enligt bedömningen finns grund för att misstänka fall av informationspåverkan finns förslag till motåtgärder i handbokens nästa del.

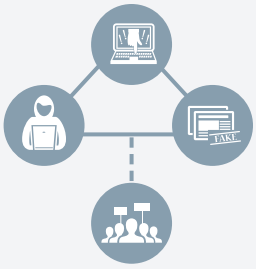
2.7 Så här kombineras olika tekniker inom informationspåverkan

Ovan beskrivna tekniker kombineras ofta. De påträffas sällan enskilt. Målet är att uppnå eller stärka en viss effekt. Antalet tänkbara kombinationer är i teorin oändligt stort, men de vanligaste teknikerna och kombinationerna kan vara värdefulla att känna till. Man bör vara på sin vakt för de tekniker och teknikkombinationer som kan förekomma samtidigt.



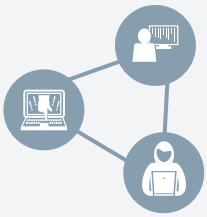
Polarisering

Polarisering kombinerar social hackning, vilseledande identiteter och desinformation. Målet är till exempel att underblåsa extrema positioner och åsikter i samma fråga. Troll och botar ingår i metoderna.



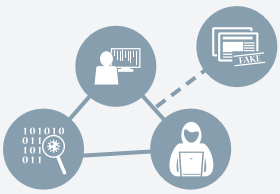
Informationstvätt

Informationstvätt kombinerar vilseledande identiteter, desinformation, teknisk manipulation, symboliska handlingar och hackning av nätverk och tankeprocesser. Därigenom förvrängs och avkontextualiseras informationen gradvis. Det blir mycket svårt för mottagaren att avgöra vad som är sant eller falskt.



Provokation

Provokation försöker hetsa människor och skapa ilska och osämja. Kombinationen utnyttjar främst hackning av nätverk och tankeprocesser, vilseledande identiteter och illasinnad retorik.



Översvämning

Översvämning syftar till att överbelasta en målgrupp med information. Detta kan uppnås till exempel genom spamming och trollning på sociala medier eller genom att sprida desinformation på social medier. Målet är att tränga ut tillförlitlig information.

DEL III
Att möta informations-påverkan

Hur kan jag förbereda organisationen?

Hur väljer jag rätt respons?

Hur tar jag till vara lärdomar?

I det här avsnittet berättas hur man kan möta informationspåverkan.

FÖRBEREDA
Skapa medvetenhet
Bygg förtroende
Bedöm risker

AGERA
Välj lämplig motåtgärd
Gör faktakoll
Nyttja sociala medier

LÄRA
Beskriv
Reflektera
Dela

3.1 Hur kan organisationen förbereda sig?

Den viktigaste delen för att bygga beredskap är förberedelser och att utveckla och etablera fungerande strukturer. God beredskap skapar en grund för att förebygga, identifiera och möta informationspåverkan.

Förberedelserna består av att öka medvetenheten om informationspåverkan, att utveckla budskap och narrativ och att förbättra förståelsen för på vilket sätt olika grupper är sårbara samt att genomföra en risk- och sårbarhetsanalys av organisationen.

Skapa medvetenhet

Ett första steg i beredskapen för informationspåverkan är att öka medvetenheten om de hot och sårbarheter som samhället och organisationen står inför. Med tanke på samhället är det bästa försvaret att problem och hotbilder hanteras på ett öppet och konstruktivt sätt. För detta behövs omfattande nätverk och rutiner som överskrider samhällsgränserna, där exempelvis ledare, journalister, företrädare för sociala medieplattformar, forskare och medborgare kan utbyta kunskap och bästa praxis.

Som kommunikatör finns det även saker du kan göra för att bygga upp beredskap.

- Du kan vara en viktig kontaktpunkt genom din kunskap inom området. I ditt arbete är det viktigt att du diskuterar frågan med ledningen och kommunicerar internt med kollegor.
- I händelse av att organisationen utsätts för informationspåverkan måste du veta hur agera. I den förberedande fasen ingår här att kartlägga behov av och möjligheter till utbildning.
- Du bör bygga nätverk bestående av experter även utanför din organisation som baseras på ömsesidigt stöd och utbyte av erfarenheter.
- En ökad transparens och kännedom om din organisations verksamhet kan förebygga spridningen av felaktiga uppgifter.

Bygg förtroende genom strategisk kommunikation

Ett av målen med informationspåverkan är att undergräva människors förtroende för samhällets institutioner. Man kan möta denna typ av verksamhet genom åtgärder som bygger och främjar förtroende. Anseende förtjänas. Det uppkommer genom förtroende. Därför är anseende och förvaltningens legitimitet mycket viktiga delar i alla strategier för att möta informationspåverkan.

Förbereda kommunikation

Det viktigt att förbereda generiska budskap som enkelt kan anpassas till specifika händelser. Dessa budskap bör stödja organisationens värderingar.

För att öka medvetenheten kan organisationen informera om påverkansförsök som den utsatts för.

Förbereda budskap

Lyckad kommunikation i snabb takt och i rätt tid möjliggörs, om färdiga budskap tagits fram och godkänts i förväg. Ett gott exempel är Londonpolisen som skickade sin första tweet endast sju minuter efter terrorattacken i Westminster i mars 2017. Meddelandet innehöll noggrann information om den pågående situationen, men var baserat på en kommunikationsmall som tagits fram för liknande scenarion.

När budskapet utformas är det viktigt att ta hänsyn till vad det talas om din organisation och vilka narrativ det genererar. Narrativen hänger samman med målgruppens uppfattningar. Man ska bedöma hur enskilda meddelanden bidrar till den eftersträvade identiteten, värderingarna och narrativet med hänsyn till olika målgrupper. Budskap som stöder ett positivt narrativ kan i avsevärd grad förbättra organisationens motståndskraft mot falsk information.

Vilken är vår berättelse?

Budskap ska ligga i linje med det önskade narrativet.

Ett starkt narrativ kommer ur en tydlig förståelse för organisationens identitet, värderingar och mål.

Analys och förståelse för vilka faktorer som bidrar till narrativen skapar samtidigt en förståelse för sårbarheter med tanke på anseende.

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

Lär känna din målgrupp

När kärnvärden, budskap och önskade narrativ fastställs, ska man kartlägga de grupper som bör nås i krissituationer. Samtidigt ska man utreda hur sårbara målgrupper och intressenter är för informationspåverkan.

Målgruppsanalysen syftar till att kartlägga gruppernas sårbarheter och anledningen till sårbarheten. Målet är att identifiera vilka delar av samhället som kan bli föremål för informationspåverkan och vilken typ av skadlig kommunikation de kan vara mottagliga för. På detta sätt kan det fastställas hur man kan nå ut till dessa målgrupper med motbudskap (counter-messaging) och förebyggande kommunikation.

Målgruppsanalys

Målgrupper uppstår inte i ett vakuum

Interaktion mellan människor, delade åsikter, uppfattningar och intressen ”skapar” publik och sociala sammansättningar. Det är viktigt att förstå vad som förenar medlemmar i en målgrupp.

Kartlägg intressenterna

Informationspåverkan skadar inte enbart den organisation som är utsatt, utan även samhällets mest sårbara grupper. Därför är det viktigt att identifiera dessa grupper och att förstå hur utsatta de är för skadliga narrativ. Samtidigt är det viktigt att förstå relationen mellan dessa grupper och den egna organisationen.

Kartlägg era narrativ

Eventuella egna narrativ måste identifieras för att möta informationspåverkan. Samtidigt bör det kartläggas hur dessa narrativ kan förmedlas till målgrupper och vilka kommunikatörer som har hög trovärdighet hos en viss målgrupp.

Det bra att beakta de metoder som anges ovan i organisationens olika beredskaps- och kommunikationsplaner. Metoderna stöder åtgärder för att möta avsiktlig, illasinnad verksamhet som används för att undergräva förtroendet och därigenom anseendet. Målet med metoderna är att bidra till att återställa det skadade förtroendet så snabbt som möjligt.

I metoderna ingår också att förbereda budskap och narrativ som kan riktas till olika målgrupper. Därför är det viktigt att förstå hur olika målgrupper kan påverkas av falsk information och hur de egna budskapen kan utformas för olika grupper.

Känn till risker och sårbarheter

Organisationen bör även göra en bedömning av vilka konsekvenser informationspåverkan kan ha för dess verksamhet. Samtidigt bör man överväga hur de egna värderingarna, budskapen och narrativen kan kommuniceras till olika målgrupper i olika situationer. Kartläggningen och analyseringen av olika publiker och målgrupper samt sårbarheter och risker skapar en god grund för att möta informationspåverkan. Risk- och sårbarhetsanalysen bör vara ett led i organisationens strategiska planering.

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 att 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 scenarion bör bedömas i relation till organisationens krishanteringsförmåga?

Vilka förebyggande åtgärder bör vidtas?

Steg 3: Sårbarhetsbedömning

Hur påverkas din organisation av olika scenarion, om de blir verklighet?

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

Steg 4: Riskhantering

Vad gör man om informationspåverkan upptäcks?

Se avsnittet nedan för exempel.

3.2 Hur beslutar jag om de rätta motåtgärderna?

Det finns ingen färdig lösning för alla problem i samband med informationspåverkan. Informationspåverkan förekommer i olika former.

Bedömning, kommunikation, förespråkande (advocate)

Motåtgärderna bör stå i proportion till hur allvarlig situationen och hotet är. Åtgärderna kan delas in i fyra steg där varje steg har sina metoder.

Först ska situationen bedömas. Detta är samtidigt en signal till motparten om att problemet har upptäckts.

Därefter informeras allmänheten och intressenterna generellt om situationen och om fakta.

I det tredje steget argumenteras till exempel mot den falska information som förmedlats. Teknikerna kan vara retoriskt övertygande och PR. Dessa åtgärder syftar till att främja organisationens sak och stödja dess budskap.

I det fjärde steget försvaras organisationen genom att insatser riktas mot angriparen.

I det första och andra steget ageras neutralt. Stegen utgör grunden för faktabaserade motåtgärder. På den tredje och fjärde nivån försvarar man genom argumentation. Dessa argumenterande motåtgärder är nyttiga, men bör användas med eftertanke beroende på situationen.

3.3 Faktabaserad motåtgärd

Bedömning och kommunikation är de två första nivåerna för att möta informationspåverkan. De kan användas i de flesta situationer.

STEG 1: BEDÖM

Det behövs en bedömning av situationen för att man ska veta vad det är som pågår. Vad är det som händer? Vilka är de centrala aktörerna? Vilka är deras motiv?

Kartlägg och bedöm situationen ur så många olika synvinklar som möjligt.

KARTLÄGG SITUATIONEN

Orientera dig i situationen för att skapa en tydlig bild av situationen. Använd de verktyg som presenteras i del I och II för att bedöma situationen.

FAKTAKOLL

Kontrollera den information som finns tillgänglig – vad är sant?

TRANSPARENT UTREDNING

Informera externa aktörer, till exempel medier, om frågan.

STEG 2: INFORMERA

Efter bedömningen av situationen kan du informera dina målgrupper om de fakta du bedömt och ditt agerande. Dra nytta av målgruppsanalysen när du kommunicerar med olika grupper.

UTARBETA ETT UTTALANDE

Ange din syn på vad som är fakta.

KORRIGERA

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

HÄNVISA

Om externa aktörer och experter kan verifiera dina fakta, kan ditt synsätt stärkas.

BETONA VÄRDEGRUNDEN

Påminn målgruppen om vad din organisation står för.

MEDDELA BERÖRDA PARTER

Berätta om situationen för de berörda parterna så snabbt som möjligt.

PUBLICERA ETT PRELIMINÄRT UTTALANDE

Informera om att situationen/frågan utreds. Förmedlingen av preliminär information visar att frågan utreds. Samtidigt ger det tid att utarbeta en mer genomgripande beskrivning av situationen.

3.4 Argumentbaserad motåtgärd

Att förespråka (advocate) och försvara är åtgärder på den tredje och fjärde nivån. Dessa steg innehåller en del åtgärder som endast är lämpliga i mer allvarliga situationer där informationspåverkan tydligt kan identifieras. Dessa två kategorier kan grupperas ihop som argumentbaserade motåtgärder.

STEG 3: FÖRESPRÅKA (ADVOCATE)

Att förespråka sin position och verksamhet är en upptrappning från att neutralt informera. Det innebär mer aktiv och utåtriktad kommunikation. I detta steg är det viktigt att alltid försäkra sig om behörighet och ansvarsområden samt kommunikationspraxis och organisationens värdegrund.

FÖR DIALOG

För dialog med målgrupper och företrädare för viktiga intressentgrupper.

UNDERLÄTTA

Försäkra dig om att informationen når målgruppen. Organisera tillfällen där din organisation kan tydliggöra sina åsikter för intressenter.

SAMARBETA

Samarbeta med nyckelaktörer. Genom att delaktiggöra aktörer kan ni stärka ert budskap till målgrupperna.

PÅHÄNG

Använd olika händelser, initiativ eller debatter för att nå ut med fakta till andra.

PAKETERA

Sätt ihop ett informationspaket om händelsen som presenterar händelseförloppet och lägger fram fakta. Detta stöder er verksamhet och stärker er position. Att detta baseras på fakta och verifierad information är viktigt.

STORYTELLING

Relatera händelsen till ett bredare narrativ om exempelvis din organisation och era värderingar. Argumentation som ingår i berättelsen (advocacy-based storytelling) gör det lätt för målgruppen att förstå situationen.

STEG 4: FÖRSVARA

Att försvara innefattar direkta motåtgärder mot angriparen. Åtgärderna kan vara kontroversiella och ska därför endast användas i extrema situationer. Se till att med kollegor och chefer på förhand säkerställa att sådana åtgärder inte överskrider ditt mandat eller riskerar att förvärra situationen.

IGNORERA

Ibland är det bäst att inte göra något alls. Att ignorera frågan är en lämplig lösning, om angreppet inte fått stor uppmärksamhet eller om en reaktion från din organisation skulle stödja angriparen.

RAPPORTERA

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

BLOCKERA

Aktörer måste alltid vara medvetna om vad yttrandefriheten innebär och vikten av att respektera yttrandefriheten. Aktiviteter som stör verksamheten kan till exempel motivera av den som stör blockeras eller avstängs från en plattform. Varje blockering bör basera sig på gällande regelverk. Att slippa svåra diskussioner är ingen grund för blockering.

AVSLÖJA

En mer strategisk åtgärd för att möta informationspåverkan kan vara att avslöja den aktör som ligger bakom till exempel ett falskt konto. I regel rekommenderas detta dock inte och det ska inte göras lättvindigt. Avslöjande måste föregås av en konsekvensanalys som beaktar vilka konsekvenser det får för organisationen, intressenterna och för den som exponeras.

Motåtgärderna bör vägas mot hur allvarlig situationen är. Aktivitet som verkar vara småskalig bemöts bäst så att man först bedömer situationen och sedan informerar allmänheten. Vid mer aggressiv informationspåverkan kan samma metoder användas och även kombineras med verktyg från de två sista kategorierna av motåtgärder, dvs. med kommunikation som stöder den egna positionen och verksamheten och med försvarande metoder. Dessa argumentbaserade metoder bör dock användas med försiktighet. Se till att du har mandat från ledningen och beakta också demokratiska principer, yttrandefrihet och övriga regelverk och instruktioner.

Vidta en faktabaserad motåtgärd

I de två första kategorierna av motåtgärder (att bedöma och informera) är det viktigt att din kommunikation är neutral och faktabaserad. Detta utgör en grund för faktabaserade motåtgärder. En kommunikativ motåtgärd som stöder den egna positionen och verksamheten går längre än så. Om felaktig information sprids utan att den korrigeras, kan det bidra till att uppfattningar om din organisation, dina målgrupper eller frågor inom ditt verksamhetsområde baseras på felaktigheter. Därför ska man bedöma situationen och informera målgrupperna innan några åtgärder vidtas.

Vid faktakollen ska man också bedöma vilka konsekvenser den felaktiga informationen kan ha. Man måste alltså bedöma vilka betydelsefulla berättelser det berättas om din organisation. Vem som sprider informationen, hur stor spridning den fått och vad den berör. Organisationer kan till exempel söka citat från organisationens representanter, inlägg som blir virala och får stor spridning online eller påståenden om den egna organisationen och dess verksamhetsområde. För bedömningen av fakta föreslås följande angreppssätt:

Utvärdering

- ☑ **Inhämta utomstående expertomdömen och/eller data från relevanta och pålitliga källor.**
- ☑ **Efterfråga mer information av den person eller organisation som gjort påståendet.**
- ☑ **Leta upp det falska påståendets originalkälla.**

Om påståendet bedöms vara felaktigt, ska man svara med en rättelse. Många experter anser att desinformation bäst bemöts med korrekt information. Andra menar dock att rättelsen enbart får en effekt bland de som är intresserade av att ta reda på sanningen. Målgruppsanalysen och utredningen av narrativ på förhand förbättrar möjligheterna att välja de lämpligaste åtgärderna.

Vidta en faktabaserad motåtgärd

- ☑ **Be den som publicerat felaktigheten att rätta eller ta tillbaka publiceringen.**
- ☑ **Ta fram en sammanställning över fakta 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

På sociala medier interagerar användare med varandra. Sociala medier är ett av verktygen inom informationspåverkan. Sociala medier har sin egen logik som måste beaktas vid planeringen av motåtgärder.

Ofta kan man inte få reda på vem som ligger bakom ett konto på sociala medier, varifrån informationen kommer och om åsikterna är representativa. Kommunikation på sociala medier är också utmanande, eftersom den bör ske snabbt, men att man samtidigt måste ta hänsyn till exempel till *taggar, namnetiketter (name calls), länkar och bifogade filer*. Ett typiskt inlägg på sociala medier innehåller ett eller flera av dessa element som dessutom kopplar samman budskapet med ett större nätverk av konton, idéer och debatter.

TAGGAR (*TAGS*)

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

NAMNETIKETTER (*NAME CALLS*)

Används för att länka till en organisations 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

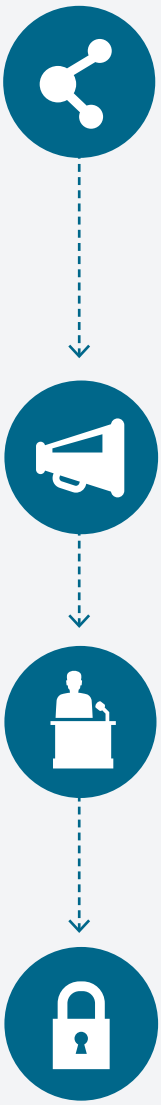
Bifogade filer kan förändra ett inläggs innebörd. De kan till exempel vara olika bilder eller videoklipp.

Proaktiv och initiativtagande aktivitet på sociala medier gör det lättare att nå olika publiker. Detta innebär att bygga nätverk och utveckla olika taggar. Budskap kan utarbetas och godkännas på förhand och sedan utnyttjas snabbt i överraskande situationer. Sociala medier gör det också möjligt för en organisation att i realtid upptäcka eventuella hot eller sårbarheter som rör organisationens anseende.

Sociala medier kan utöver debatter, interaktion och kommunikation också användas både för att inhämta information via öppna källor och för analys.

3.5 Motåtgärder på sociala medier

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



BEDÖM

Bedöm situationen. Handlar det om informationspåverkan eller medborgardebatt? Om du misstänker att informationspåverkan försiggår, utred situationen så noggrant som möjligt. Vilka är de som kommunicerar med dig? Är de fientliga mot din sak? Handlar det om en reaktion på ett budskap 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 av situationen skapar bättre förutsättningar för att besluta om rätt tillvägagångssätt.

INFORMERA

Utforma ditt budskap baserat på din bedömning. Välj målgrupper, användare och taggar noggrant.

Fokusera på att klarlägga din organisations uppfattning och betona organisationens värderingar i de kanaler du anser lämpliga.

FÖRESPRÅKA

Om situationen kräver det, kan du positionera dig tydligare i debatten, till exempel genom förberedda budskap eller videoklipp. Dessutom kan det vara motiverat att delta mer aktivt i debatten och skapa ett bredare engagemang för frågan hos dina målgrupper. Involvering av följare i debatten kan tjäna dina syften.

FÖRSVARA

Om situationen eskalerar så att konstruktiv diskussion inte är möjlig och den hederliga kommunikationen trängs undan av spam och destruktiva inlägg, kan det vara motiverat att gå i försvarsställning. Beroende på din organisations riktlinjer och plattformens regler kan du ha rätt att blockera eller ignorera fientliga användare. Rådgör alltid med chefer innan du agerar. Yttrandefriheten är ett av samhällets kärnvärden. En öppen och fri demokratisk debatt ska alltid främjas och upprätthållas. Om du bestämmer dig för att blockera eller ignorera en användare, se till att grunderna för ditt beslut är transparenta och hållbara.

3.6 Hur tar jag till vara lärdomar?

Att samla in och dokumentera exempel och observationer är viktigt för att förstå problemet bättre. En beskrivning och utvärdering att det egna agerandet bidrar till att utveckla verksamheten. Kunskapen kan även användas för att utveckla utbildningsmaterial och den kan bidra till organisationens och samhällets beredskap. Det lönar sig att dela informationen med experter i liknande uppgifter. Det lönar sig också att förmedla information till myndigheter och i vissa fall även till allmänheten.

I Finland är varje aktör ansvarig för sin beredskap. Detta gäller också beredskap för fientlig informationspåverkan. Av samhällets vitala funktioner kan speciellt mental kristålighet och ledning vara föremål för fientlig informationsverksamhet. De vitala funktionerna är funktionshelheter som är nödvändiga för samhällets funktionsduglighet och som ska upprätthållas i alla situationer. (Se Säkerhetsstrategin för samhället 2017.)

Samarbete har en avgörande betydelse när det gäller beredskap, insatser och återhämtande. I den finländska samarbetsmodellen för övergripande säkerhet baserar sig säkerheten på samarbete mellan myndigheter, näringsliv, organisationer och medborgare. Myndigheter har en lagstadgad skyldighet att förbereda sig inom varje uppgiftsområde. Den behöriga myndigheten svarar för beredskapen tillsammans med sina samarbetspartner. Dagens beredskap gäller ofta flera myndigheter samt gemensamma tjänster och därigenom också tjänsteleverantörer, såsom företag och organisationer. Därför är det viktigt att dra nytta av samarbetsforum för beredskap på alla olika verksamhetsnivåer. Exempelvis Säkerhetskommittén, som samordnar utvecklingen av beredskapen på statsrådsnivå, behandlar månatligen beredskapsfrågor på initiativ av medlemmarna[2]. Beredskapscheferna, som stöder kanslicheferna, kan i störningssituationer sammanträda för att söka metoder för att andra myndigheter ska kunna stödja det förvaltningsområde som ansvarar för ledningen i lösningen av krisen. I problem som hänger samman med kommunikation är de viktigaste samarbetsforumen mötena för statsrådets kommunikationsdirektörer och kriskommunikatörer samt de informella mötena för nätverket för informationspåverkan. Olika samarbetsorgan för beredskap i statsförvaltningen kan tjäna som exempel också för andra aktörer. Samverkan behövs alltid när störningssituationen eskalerar. Därmed skapar regelbundna, mer permanenta arrangemang kontinuitet i verksamheten och förbättrar dess kvalitet. Genom regelbundet samarbete byggs det förtroende mellan aktörer, vilket är nödvändigt i krisledning.

På nästa sida finns några exempel på uppgifter som det lönar sig att samla in i syfte att lära sig.

2 Medlemmar är ministeriernas kanslichefer, säkerhetsmyndigheterna och företrädare för näringslivet och organisationer.

Lärdomar

BESKRIV

- Beskriv händelsens bakgrund.
- Vilka aktörer var inblandade? (Undvik spekulation)
- 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?

DELA

- Spara de uppgifter 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.
- Dela med dig av dina kunskaper och erfarenheter inom och utanför din egen organisation genom exempelvis utbildning och möten.

3.7 Strategisk bedömning

Motåtgärderna begränsas av det faktum att de alltid svarar på någon annans intentioner. En initiativtagande angripare bestämmer vad organisationen kan göra eller låta bli att göra. Då *agerar* den motsatta sidan, medan den egna sidan endast *reagerar*. Den utsatta organisationen ligger hela tiden steget efter motståndaren.

Med tanke på samhället är det viktigt att upprätthålla och stödja en öppen och fri debatt samt demokratiska värderingar, såsom yttrandefriheten och åsiktsfriheten. Uppdraget är att skydda den opinionsbildande processen genom att minimera effekten av sårbarheter i t.ex. mediesystemet. Vi rekommenderar att man utnyttjar kraftiga, men samtidigt väl avvägda faktabaserade motåtgärder.

Arbetet med att möta informationspåverkan får aldrig leda till att den offentliga debatten tystas ner. Det skulle enbart leda till ökad polarisering och till att samhällets funktioner undermineras och skulle därmed motverka sitt syfte. Öppen och demokratisk debatt måste alltid skyddas och uppmuntras. Vi rekommenderar följande angreppssätt:

- **Höj tröskeln för fientlig informationspåverkan genom att bidra till medvetenhet och genom beredskap.**
- **Utveckla proaktiva, rätt dimensionerade och förnuftiga kommunikativa motåtgärder som riktar sig till målgruppen (snarare än motståndaren) och som kan bidra till att försvara samhällets gemensamma värderingar.**
- **Upprätthåll din förmåga att vidta faktabaserade motåtgärder. Under vissa omständigheter lönar det sig att genomföra argumenterande och förespråkande motåtgärder på högre nivå.**
- **Dela med dig av metoder som fungerar till kollegor och lär av varandra.**
- **Var vaksam men inte paranoid!**

4 Ordlista

Botar (bots) – Datorprogram som utför automatiserade uppgifter.

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

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

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

Tystnadsspiralen (spiral of silence) – Personer som upplever sig vara i minoritet är återhållsamma eller försiktiga med att dela med sig av sina åsikter.

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.

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

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

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

Ekokammare och filterbubblor (echo chambers and filter bubbles) – Naturliga grupperingar online eller offline där människor kommunicerar med andra som delar samma åsikter och uppfattningar.

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

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

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

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

Bandwagon-effekten (bandwagon effect) – Personer som upplever sig vara en del av en majoritet är mer benägna att dela med sig av sin åsikt.

Whataboutism – Att ta fokus från ett argument genom att lyfta fram ett liknande, mindre betydelsefullt fenomen som inte är riktigt relevant i frågan.

Statsförvaltningens kommunikation styrs av olika författningar, anvisningar och rekommendationer.

De viktigaste av dem är:

Grundlagen (731/1999)

Förvaltningslagen (434/2003)

Lagen om offentlighet i myndigheternas verksamhet (621/1999)

Förordningen om offentlighet och god informationshantering i myndigheternas verksamhet (1030/1999)

Statsrådets förordning om informationssäkerheten inom statsförvaltningen (681/2010)

Diskrimineringslagen (1325/2014)

Informationssamhällsbalken (917/2014)

Lagen om samarbete inom statens ämbetsverk och inrättningar (1233/2013)

Lagen om integritetsskydd i arbetslivet (759/2004).

Lagen om elektronisk kommunikation i myndigheternas verksamhet (13/2003)

Personuppgiftslagen (523/1999)

Språklagar

Språklagen (423/2003)

Samiska språklagen (1086/2003)

Teckenspråkslagen (359/2015)

Upphovsrätt och yttrandefrihet

Upphovsrättslagen (404/1961)

Lagen om yttrandefrihet i masskommunikation (460/2003)

Lagar som reglerar störningssituationer och undantagsförhållanden

Beredskapslagen (1552/2011)

Lagen om försvarstillstånd (1083/1991)

Lagen om varningsmeddelanden (466/2012)

Lagen om Rundradion Ab (1380/1993)

Lagen om smittsamma sjukdomar (583/1986)

Lagen om säkerhetsutredning av olyckor och vissa andra händelser (525/2011)

Anvisningar och rekommendationer

Rekommendation om statsförvaltningens kommunikation, statsrådets kansli (2016)

Statsförvaltningens kommunikation i störningssituationer och under undantagsförhållanden, statsrådets kansli (2013)

Handbok om varningsmeddelanden, inrikesministeriet (2013)

Ministerns handbok(2015)

Statsrådets kanslis meddelande om minister, statssekreterare och specialassistent samt valkampanj (2015)

En tjänsteman i de sociala medierna, rekommendation från statens tjänstemannaetiska delegation (2016) Praktiska anvisningar om tillämpningen av språklagstiftningen i webbtjänster, justitieministeriets rekommendation (2015)

Klart myndighetsspråk – ett handlingsprogram, undervisnings- och kulturministeriets arbetsgruppspromemorior och utredningar (2014)

Användarrättighet för öppen data, JHS rekommendation 189 (2014)

Riktlinjer för utformning av tillgängligt innehåll på webben (WCAG) 2.0 (2008)

Anvisningar om etisk kommunikation, delegationen för etisk kommunikation VEN (2015)

Redogörelser, strategier och principbeslut

Principbeslut om den övergripande säkerheten, statsrådets principbeslut (2012)

Strategin för den inre säkerheten, statsrådets principbeslut (2017)

Strategin för cybersäkerheten i Finland, statsrådets principbeslut (2013)

Statsrådets försvarsredogörelse, statsrådets kansli (2017)

Statsrådets utrikes- och säkerhetspolitiska redogörelse, statsrådets kansli (2016)

Säkerhetsstrategi för samhället, statsrådets principbeslut (2017)

Andra publikationer

Finlands nationella riskbedömning 2018, inrikesministeriet

Turvallinen Suomi – Tietoja Suomen kokonaisturvallisuudesta (2018), Säkerhetskommittén

STATSRÅDETS KANSLI

SNELLMANSGATAN 1, HELSINGFORS
PB 23, 00023 STATSRÅDET
tfn. 0295 16001
info@vnk.fi
vnk.fi/julkaisut

ISSN PDF 2490-1164
ISBN PDF 978-952-287-731-4