Sådan modstår vi falsk information

En vejledning til offentlige myndigheder og private virksomheder

Desinformation er en betegnelse for falsk information, der udbredes af fjendtlige aktører med *intention* om at forvirre og mislede befolkningen. Det er afgørende for sammenhængskraften og tilliden i vores samfund, samt kvaliteten af vores demokratiske processer, at offentlige myndigheder er i stand til at modstå desinformation. Derfor har Rådet for Digital Sikkerhed udviklet fem trin som jeres organisation med fordel kan strukturere arbejdet efter.

Udfordringen

Danmark er blandt verdens førende nationer i den digitale udvikling. Det medfører afgørende gevinster for samfundet i form af økonomisk vækst, bedre sundhed, uddannelse samt nye smarte tjenester og produkter. Samtidig afføder digitaliseringen en øget sårbarhed over for digitale trusler, hvorfor det er nødvendigt, at vi kan beskytte os tilstrækkeligt. Forsvarets Efterretningstjeneste vurderer, at cybertruslen mod Danmark er meget høj både hvad angår cyberspionage, cyberkriminalitet og det forhold, at fremmede stater anvender cyberangreb til at påvirke den offentlige meningsdannelse.

Desinformation er ikke noget nyt fænomen. Det har som minimum eksisteret siden pressen begyndte at trykke aviser. Det til trods, betyder et medielandskab i hastig forandring, at desinformation kan spredes mere effektivt og nå et større publikum. Dertil kommer det forhold, at information af falsk karakter har en betydelig større rækkevidde end korrekt information[1]. Våbenliggørelsen af information kan udgøre en trussel mod sammenhængskraften i vores samfund, tilliden til offentlige myndigheder og medier, hindre økonomisk fremgang og global indflydelse samt forringe kvaliteten af vores demokratiske processer. Derfor skal vi handle hurtigt og effektivt. Det skal vi gøre på en sådan vis, at vi fortsat omfavner de muligheder, vi har for at interagere som offentlighed i en online digital verden.

Med denne vejledning ønsker Rådet for Digital Sikkerhed (RfDS) at bidrage med et konkret værktøj målrettet kommunikationsansatte, politikudviklere og politiske rådgivere i den offentlige sektor, samt marketing- og PR-ansvarlige i den private sektor. De fem trin, der foreslås i denne vejledning, hjælper jeres organisation med at udvikle en effektiv respons, når desinformation påvirker udførelsen af jeres kerneopgaver eller repræsenterer en trussel mod den offentlige sikkerhed.

[1] I 2018 konkluderede MIT Media Lab i en rapport, at "*falsehood diffused significantly farther, faster, deeper, and more broadly than the truth in all categories of information.*" Samtidig er sandheden, "*about six times as long as falsehood to reach 1,500 people,*" mens falsk information er "70% more likely to be retweeted than the truth." Kilde: Vosoughi Soroush, Roy Deb, Aral Sinan. (2018). "The spread of true and false news online," Science 359, 1146-1151. https://science.sciencemag.org/content/359/6380/1146

Fem trin til at modstå desinformation

Rådet for Digital Sikkerhed foreslår, at de fem nedenstående trin anvendes:

1. Lær kendetegnene ved desinformationen
2. Vær på forkant
3. Situationel indsigt
4. Risikovurdering
5. Strategisk kommunikation

1. Identificer desinformation

Desinformation handler om indflydelse. De aktører, der spreder den, ønsker ikke, at offentligheden foretager informerede og fornuftige beslutninger. Det mål forsøges opnået ved at forkorte den kognitive beslutningsproces hos den enkelte borger. De teknikker, der benyttes, er forholdsvist basale og kan forstås gennem følgende principper:

- **Fabrikering:** Manipulering af indhold. F.eks. forfalskning af dokumenter eller dygtigt redigerede billeder.
- **Identitet:** Skjuler kilden til information eller benytter sig af en falsk kilde. F.eks. falske konti på sociale medier.
- **Retorik:** Anvender falske og ofte polariserende argumenter. F.eks. bots og trolde, der promoverer bestemte narrativer for at skabe online debat og øge populariteten og rækkevidden af desinformationen.
- **Symbolik:** Udnytter bestemte begivenheder. F.eks. terrorangreb.
- **Teknologi:** Drager fordel af teknologiske kapabiliteter. F.eks. botnets der automatisk spreder desinformation gennem brugen af hashtags og delinger.

Disse principper kombineres ofte af fjendtligtsindede aktører for at skabe den størst mulige effekt gennem følgende strategi:

1. Finder et følsomt samfundsproblem der har symbolsk værdi.
2. Opretter to eller flere konti på sociale medier under falsk identitet.
3. Udarbejder indhold der har til formål at fremprovokere en respons.
4. Udgiver indholdet fra den ene konto og kritiserer det gennem de andre.
5. Anvender bots til at sprede det manipulerede eller falske indhold til andre netværk.
6. Anvender memes og trolling for at give indtryk af en polariseret negativ offentlig debat.

En sådan strategi har potentiale til at underminere tilliden til beslutningstagere, skabe splid mellem forskellige sociale grupper i samfundet, bidrage til politisk polarisering, skabe profit gennem et højt antal visninger eller øge sandsynligheden for, at den falske information går viralt og i værste fald når ud til større traditionelle medier.

2. Vær på forkant

Når I er blevet bekendt med, hvordan I identificerer desinformation, kan det være et nyttigt udgangspunkt at vurdere, hvilke emner af interesse for din organisation fjendtligtsindede aktører kan have interesse i at målrette deres desinformation mod. Det bør give et fornuftigt afsæt til at lave en strategi for overvågning af digitale medier. Ved at besvare spørgsmålene i skemaet herunder kan I fokusere jeres indsats.

	Prioriteter	**Holdninger**
Policy mål	Hvilke policyområder prioriterer jeres organisation, og hvad er jeres målsætninger?	Hvilke dominerende holdninger inden for de policyområder er sårbare over for brug af desinformation?
Meningsdannere	Hvem er de største meningsdannere, der har indflydelse på jeres policyområder?	Hvilke holdninger har de til jeres organisation og/eller jeres målsætninger, som kan blive udnyttet gennem brug af desinformation?
Publikum	Hvem består jeres hovedpublikum af?	Hvilke holdninger har de til jeres organisation og/eller jeres målsætninger, som kan blive udnyttet gennem brug af desinformation?

Din digitale medieovervågning kan med fordel lade sig styre af besvarelsen af disse spørgsmål og dermed hjælpe dig til at identificere relevante indikatorer på potentielle trusler i et tidligt stadie.

3. Situationel indsigt

Din digitale medieovervågning bliver først værdifuld for dig og din organisation, når den bliver omdannet til en situationel indsigt. En sådan indsigt opnås, når den indsamlede data stilles over for spørgsmålet ”og hvad så?” og dermed gøres til data, der kan handles på. Formålet er at udarbejde en analyse baseret på de indledende faresignaler afspejlet i din digitale medieovervågning og præsentere den for de nødvendige mennesker i din organisation. Som et minimum bør jeres analyse indeholde:

- Et overordnet resume af den indsamlede data med en kort forklaring af spørgsmålet ”og hvad så?” efterfulgt af dine anbefalinger til næste skridt.
- Herefter bør du behandle de vigtigste emner, der vedrører din organisation, og du kan med fordel strukturere arbejdet, således:

1. Undersøg relevante kommunikative produkter, der er udgået fra jeres organisation om prioriterede emner. F.eks. ministerielle annonceringer eller pressemeddelelser.
2. Find derefter eksempler på desinformation der relaterer sig til disse kommunikative produkter med en dertilhørende analyse af, hvor og hvordan de florerer på internettet.
3. Undersøg udviklingen i holdninger over tid (her kan du med fordel benytte dig af tilgængelige meningsmålinger).
4. Afslutningsvist bør du inddrage dine anbefalinger til, hvordan organisationen bedst udformer en respons.

4. Risikovurdering

I tilfælde af, at ovenstående i tilstrækkelig grad tyder på, at desinformationen har en negativ effekt på jeres organisation, bør I nu foretage en analyse af desinformationens mål, påvirkningsgrad og rækkevidde. Det kan I gøre ved at besvare nedenstående spørgsmål, der vejleder til at vurdere, hvorvidt der bør reageres på desinformationen eller ej.

Påvirker desinformationen din organisations evne til at udføre jeres job?	**Har desinformationen indflydelse på de mennesker, der er afhængige af jeres services?**	**Udgør desinformationen en betydelig trussel for den generelle offentlighed?**
Levering af services	Stakeholders	National sikkerhed
Omdømme	Primære modtagere	Offentlighedens sikkerhed
Policy områder/målsætninger	Niche modtagere	Offentlighedens helbred
Medarbejdersikkerhed	Sårbare modtagere	Intensiteten af debatten

Du bør også vurdere i hvor høj grad, der vil blive interageret med desinformationen. Er det sandsynligt, at den vil forsvinde inden for et par timer, eller har den potentiale til at skabe overskrifter i morgenaviserne?

Rækkevidde	**Sandsynlighed**
Lille interesse: Meget begrænset antal delinger, hashtags, kommentarer mm.	
Filterboble: Lidt interaktion blandt nichemodtagere med holdninger, der i forvejen placerer sig tæt op af desinformationen	
Trender: En del diskussion online, som kan afspejle en åben debat med argumenter for og imod	
Mindre historie: Lidt rapportering i større traditionelle medier	
Hovedoverskrifter: Får stor indflydelse på organisationens kortsigtede arbejde	

Du bør nu være i stand til at vurdere, i hvor høj grad desinformationen skal prioriteres. Nedenfor er et eksempel på tre prioriteringskategorier: Høj, middel og lav. Det er sandsynligt, at jeres organisation selv skal udvikle en række kriterier, der passer bedre i jeres vurdering af, hvor presserende opgaven er. Princippet er dog fortsat, at mål, påvirkningsgrad og rækkevidde er afgørende for dit prioriteringsniveau.

	Trusselsniveau	**Handling**	**Aktører**	**Værktøjer**
Høj	Desinformationen kan true den nationale sikkerhed og har stor sandsynlighed for at skabe overskrifter. Kræver omgående handling.	Gør den siddende regering opmærksom på truslen og dets prioriteringsniveau. Del viden.	Højtstående embedsmænd, regering	Underretninger, vidensdeling, prioriter kortsigtet kommunikation
Middel	Desinformationen kan have negativ indflydelse på relevante policy områder, omdømme eller en stor gruppe af interessenter. Trender online og kræver en respons.	Gør ledelsen og politiske rådgivere opmærksom på situationen. Del viden inden for organisationen. Undersøg nærmere og forbered en pressemeddelelse baseret på fakta.	Ledelsen, politiske rådgivere	Underretninger, vidensdeling, pressemeddelelser, prioriter kort og mellemlangsigtet kommunikation
Lav	Desinformationen kan have indflydelse på intensiteten af debatten og har en begrænset rækkevidde. Debatten bør følges, men indgriben er unødvendig.	Del viden inden for kommunikationsafdelingen. Undersøg nærmere og forbered narrativer baseret på fakta. Udarbejd en analyse af debatten og følg op på ændringer af debattens intensitet.	Kommunikationsafdelingen	Vidensdeling, analyse, prioriter mellem og langsigtet kommunikation

5. Strategisk kommunikation

Efter risikovurderingen er foretaget og prioritetsniveauet er fastlagt, bør det nu overvejes, hvilke kommunikative værktøjer I skal anvende. I denne vejledning er kategorierne inddelt i kortsigtet/reaktivt, mellemlangsigt/proaktivt og langsigtet/strategisk. Des højere prioritetsniveauet er, jo mere fokus bør I have på en kortsigtet reaktiv respons. Bemærk at det afhængigt af trusselsniveauet kan være nødvendigt at kombinere den kortsigtede, mellemlangsigtede og langsigtede tilgang.

	Handling	**Målgruppe**	**Værktøjer**
Kortsigtet/reaktivt	Desinformationen kræver omgående handling. Kommuniker modargumenter, korriger fejlinformation, afklar muligheden for at blokere eller modarbejd desinformationen i overensstemmelse med fakta.	Traditionelle medier (journalister og redaktører), meningsdannere, SoMe platforme	Pressemeddelelser, ministerudtalelse, underret journalister, Q&A, betalt annoncering, SEO, meningsdannere
Mellemlangsigt/proaktivt	Desinformationen kræver i et vist omfang en respons. Kommuniker jeres egne værdier. Sammenflet proaktive metoder med jeres hverdagskommunikation og samarbejd med ledelsen om at etablere konsensus om jeres position.	Traditionelle medier (journalister og redaktører), meningsdannere, SoMe platforme, bredt publikum	Kampagner, udvikling af organisationens narrativ og omdømme, dialog, facilitering af netværk, meningsdannere, workshops
Langsigtet/strategisk	Desinformationen kræver en vedvarende og sammenhængende respons for at skabe langsigtede forandringer. Udarbejd strategiske narrativer omkring emnet ved at forme informationsmiljøet til at fremme jeres position og afskrække andre aktører.	Traditionelle medier (journalister og redaktører), talenter, meningsdannere, SoMe platforme, bredt publikum	Kampagner, udvikling af organisationens narrativ(er) og omdømme, finansiering af talentprogrammer, facilitering af netværk, workshops, beredskabsplanlægning

På bestyrelsens vegne

Henning Mortensen
Formand, Rådet for Digital Sikkerhed