

Mikkel Storm Jensen og Jens Svensson  
**Danmarks beredskab mod påvirkningsoperationer: minimalistisk tilgang til kompleks udfordring**

Påvirkningsoperationer fra fjendtlige stater er en stigende trussel, som kræver et stående beredskab til at forebygge og imødekomme. Skiftende danske regeringer har siden 2018 valgt en minimalistisk tilgang i rammen af sektoransvarsprincippet til håndteringen af denne trussel: en task force bestående af embedsmænd fra en række ministerier støttet af Forsvarets Efterretningstjeneste, som skal imødekomme denne udfordring ved siden af deres primære opgaver. Denne artikel argumenterer for, at truslen fra påvirkningsoperationer er et såkaldt *wicked problem* – en kompleks problemstilling, der ikke kan løses af en enkelt aktør alene, og som fordrer en mere netværksbaseret tilgang med bred inddragelse fra offentlige og private organisationer og civile borgere. Artiklen undersøger den nuværende indsats og vejer den op imod de teoretiske anbefalinger i håndteringen af komplekse problemer. Til sidst drages paralleller til Sveriges tilgang, hvor der er oprettet en organisation udelukkende dedikeret til håndtering af truslen.

**Nøgleord:** påvirkningsoperationer, sektoransvar, komplekse problemer, hybride trusler

Selvom DK indtil nu har været forskånet for større, koordinerede påvirkningsforsøg, tages truslen alvorligt på det politisk-strategiske niveau. Danmark valgt at håndtere trusler i rammen af sektoransvarsprincippet. Det er en tilgang, som Danmark deler med Sverige i forhold til lignende trusler, fx på cyberområdet (Jensen, 2019). Men selvom principperne bag tilgangene er ens, har Danmark i modsætning til Sverige valgt en meget minimalistisk løsning.

Sektoransvarsprincippet er en naturlig tilgang til trusler, som store dele af samfundet kan komme i direkte kontakt med, fordi det principielt åbner mulighed for et bredt engagement med både offentlige og private aktører, dvs. virksomheder, organisationer, og i nogle tilfælde inddrage den enkelte borger. Disse aktører kan fungere som sensorer for at varsle om kommende trusler og være med til at overkomme dem lokalt i samvirke med eller støttet af centrale myndigheder. Sverige har af samme årsager også valgt at håndtere påvirkningsoperationer i rammen af sektoransvarsprincippet og har, ligesom fx Storbritannien, oprettet en dedikeret og højt profileret organisation af anseelig størrelse og

uden andre opgaver. Her adskiller den danske tilgang sig markant ved at være minimalistisk: en taskforce bestående af embedsmænd fra en række ministerier overvåger, støttet af Forsvarets Efterretningstjeneste (FE), påvirkningsoperationer ved siden af deres primære opgaver. Taskforcen skal udgøre kernen i de ad hoc-organisationer, der skal imødegå erkendte hændelser, afhængigt af hvor de opstår.

Artiklen undersøger, hvordan den danske indsats mod påvirkningsoperationer er organiseret, og hvordan teoretiske overvejelser i rammen af litteraturen om kompleksitet kan bidrage til forståelsen af påvirkningsoperationers natur og staters muligheder for at imødegå dem.

Artiklen demonstrerer med udgangspunkt i resiliens- og kompleksitetsteori, at sektoransvarsprincippet principielt er en hensigtsmæssig implementering af offentligt-privat samarbejde med inddragelse af offentlige, private og civile aktører, der kan samarbejde om at identificere, attribuere og modsvare forøg på påvirkning. Herefter analyserer artiklen den danske implementering af indsatsen ift. imødegåelse af påvirkningsoperationer og sammenligner med den svenske for at identificere væsentlige udfordringer ift. en netværksbaseret indsats i rammen af sektoransvarsprincippet.

Et par definitioner af emnet er på sin plads til at begynde med: Denne artikel beskæftiger sig med påvirkningsoperationer baseret på desinformation. Påvirkningsoperationer benytter sig af desinformation for at opnå et formål gennem bevidst spredning af ”forkerte, fejlagtige eller ufuldstændige meddelelser der umiddelbart forekommer at være reel information”. På dansk bruges desinformation (der kommer af russisk *dezinformatsia*) indimellem synonymt med ”misinformation” og det engelske ”disinformation”. På engelsk skelnes mellem desinformation (*disinformation*) og misinformation: Misinformation kan være uforsætlig viderebringelse af fejlagtige oplysninger, mens desinformation sker bevidst og med forsæt (Andersen, 2021). Der er ikke nogen fast definition på misinformation. For eksempel definerer EU ikke begrebet i sit materiale, men giver i stedet en række eksempler på misinformation (EU, 2020). De britiske myndigheder har en klar definition af disinformation: “Disinformation is the deliberate creation and dissemination of false and/or manipulated information that is intended to deceive and mislead audiences, either for the purposes of causing harm, or for political, personal or financial gain” (GCS, 2019). Denne artikel anvender begrebet desinformation, da det er den teknisk korrekte betegnelse for den aktivitet, som den engelske definition beskriver. I daglig tale og dansk nyhedsformidling bruges den engelske betegnelse disinformation dog oftest – ordet optræder også regeringens handlingsplan fra 2018 – men desinformation er altså det korrekte begreb (Justitsministeriet, 2018).

## Litteraturen om imødegåelse af påvirkningsoperationer

Den emergerende litteratur om wicked problems (på dansk: komplekse problemer) peger på, at sådanne udfordringer bedst håndteres i netværksstrukturer. Camillus beskriver i artiklen ”Strategy as a wicked problem” (2008) nødvendigheden af inddragelse af alle relevante aktører, når denne type problemer skal håndteres. Huggins og Hilvert beskriver i ”Tackling ’wicked problems’ takes resident management” (2013), hvordan det civile samfund bør aktiveres i håndteringen af komplekse, samfundsmæssige problemer. Koppenjan og Klijs *Managing uncertainties in networks* (2004) er ligeledes enige i, at wicked problems kræver netværk og inddragelse. Der er dog kun en begrænset litteratur, der knytter udfordringen fra desinformation til øvrig resilienslitteratur, der behandler statens rolle – som fx Dunn-Cavelty og Suter i ”Public-private partnerships are no silver bullet” (2009). Det er således karakteristisk for både den britiske regerings vejledning i imødegåelse af desinformation, det amerikanske RANDs 2017-anbefalinger om emnet og Europa-Kommissionens vejledning om styrkelse af adfærdskodeksen om desinformation, at disse tre vejledninger kun i begrænset omfang refererer til den akademiske litteratur på området (Bodine-Baron et al., 2018; European Commission, 2021; GCS, 2019). Den britiske regerings og Kommissionens vejledning henviser dog begge til *The debunking handbook*, en kort, lavpraktisk håndbog der ikke adresserer statens rolle specifikt, men mere retter sig mod borgere og virksomheder. Denne håndbog er et resultat af et transnationalt samarbejde mellem en lang række universiteter, og dens referenceliste giver et godt overblik over den akademiske litteratur på området (Lewandowsky, Cook og Lombardi, 2020).

Så vidt forfatterne ved, findes der ikke dansk litteratur, der specifikt laver koblingen mellem påvirkningsoperationer, komplekse problemer og netværks-tilgang. En samlet kortlægning af håndteringen af påvirkningsoperationer er så vidt vides heller ikke tilgængelig for nuværende. Det er netop fraværet af denne litteratur og forskning, der har motiveret forfatterne til denne artikel. Det er vores håb at skabe denne kobling og give et samlet overblik over den nuværende indsats i Danmark.

## Påvirkningsoperationer er et komplekst problem

I en stadig mere forbundet og digitaliseret verden, forekommer statsligt organiserede påvirkningsoperationer ofte subtilt og med anvendelse af blandt andet sociale medier. Hensigten med operationerne er sandsynligvis at styrke egen position i relation til modstandere ved at skabe splittelse og udnytte eksisterende skel eller konflikter og skade sammenhængskraften i et land eller en alliance, undergrave tillid til myndigheder eller blot at skabe forvirring for derved at

lamme beslutningstagning i tilfælde af, eller forud for, en konflikt. Denne type påvirkningsforsøg er en alvorlig trussel, da tilliden imellem befolkningsgrupper og til myndighederne er afgørende for, at moderne, demokratiske samfund kan fungere. Påvirkningsoperationer indgår i Ruslands strategiske doktriner, og Rusland har op gennem 2010'erne demonstreret både vilje og evne til at sprede målrettet desinformation (Jensen, 2021). Metoden er relativt billig og forbundet med begrænset risiko i forhold til andre former for angreb: Påvirkningsoperationer går ofte "under radaren" og har historisk kun medført en lille risiko for et samlet modsvar fra fx NATO. Den russiske cyberspionage og efterfølgende offentliggørelse af materiale fra Demokraterne gennem Wikileaks ved det amerikanske præsidentvalg i 2016 er formentlig det hidtil mest vellykkede eksempel på, at russisk påvirkning og desinformation har skabt strategiske resultater. Operationerne medførte indenrigspolitisk splittelse og påvirkede USA's politiske handlekraft og forhold til sine allierede gennem hele Trumps præsidentperiode 2016-2020 (Jensen, 2021). Påvirkningsoperationer skal have en række egenskaber for at opnå succes. De skal tjene afsenderens formål og samtidig finde en historisk, kulturel, politisk eller ideologisk klangbund, der engagerer den befolkning eller større grupper i den, der er mål for operationerne og gør, at den kan sprede sig videre blandt dem. Afsenderen af desinformationen skal fremstå som troværdig, eller, hvis operationen gennemføres i hemmelighed, camoufleres eller ligefrem skjules eller forfalskes (for en detaljeret gennemgang af russiske midler og metoder i påvirkningsoperationer, se Kragh og Åsberg, 2017). Hvis desinformation er plantet med succes, står offeret over for en kompleks udfordring. Desinformationen kan sprede sig i åbne eller skjulte fora og dukke op igen og igen i nye sammenhænge og med nye mellemlid mellem afsender og modtager, og myndighedernes forsøg på at bekæmpe desinformationen vil ofte bekræfte de mennesker, der accepterer den som sand, i deres mistillid til de etablerede autoriteter, samtidig med at den spreder sig hurtigere, end den kan bekæmpes (Lewandowsky og van der Linden, 2021: 349, 351, 356). Opgaven med at imødegå bliver dermed kompleks.

Et komplekst problem har blandt andre følgende karakteristika (Rittel og Webber, 1973; Snowden og Boone, 2007; Stacey, 2012; Trillingsgaard, 2015):

- Der er ingen klar sammenhæng mellem årsag og virkning.
- Der er et stort antal aktører, humane og non-humane, der gensidigt påvirker hinanden på uforudsigelige måder.
- Der er mange forskellige og konkurrerende opfattelser af problemet.
- Problemet er dynamisk, dvs. det udvikler sig konstant. Situationer opstår uventet eller "emergerer".
- Det er kun muligt at se mønstre i retrospekt.

- Komplekse problemer kan ikke løses – kun håndteres.
- Håndtering af komplekse problemer kræver uddelegering, innovation og kreativitet gennem inddragelse af aktører på alle niveauer.

Påvirkningsoperationer kan kendetegnes ved lav eller ingen grad af linearitet og orden og rummer karakteristika, der kendetegner komplekse problemer (Verstraete, Bambauer og Bambauer, 2021: 22). Det er ikke umiddelbart muligt at se en sammenhæng mellem årsag og virkning. Vi forstår først påvirkningsoperationens sande natur i retrospekt, og det er ikke muligt til fulde at forudse konsekvenserne af ens handlinger, mens man forsøger at imødegå den. Der er desuden mange aktører involveret blandt målgrupper og afsendere, som gensidigt påvirker hinanden på uforudsigelige måder. Koppenjan og Klijn beskriver i deres bog *Managing uncertainties in networks* (2004), at hierarkiske organisationer eller enkelte aktører alene ikke er egnede til at håndtere komplekse, samfundsmæssige problemer og anbefaler i stedet en netværksbaseret tilgang for at imødekomme disse.

Overført til statsniveauet kan man se kompleksitetslitteraturens anbefalede tilgange afspejlet i sektoransvarsprincippet. Princippet betyder, at den myndighed, virksomhed eller institution, som til daglig har ansvaret for et område, også har ansvaret for kriseplanlægning og opretholdelse af funktionerne under en krise (Beredskabsstyrelsen, 2006: 22). Her fastholder staten ansvaret for, og faciliterer i muligt omfang, opgavens løsning, men delegerer selve udførelsen til de berørte sektorer, der har den nødvendige indsigt og ekspertise i egne forhold.

Helt konkret betyder det, at staten bør inddrage aktører med forskellige fagligheder og opfattelser i et netværk til håndtering af komplekse problemer. I tilfældet med imødegåelse af påvirkningsoperationer kunne dette være aktører fra fx Forsvaret, Politiet, efterretningstjenesterne, undervisningssektoren, journalister og private virksomheder, fx sociale medier. Statens opgave er at facilitere informationsudvekslingen på tværs mellem aktørerne med så få friktioner som muligt.

## Statens vanskelige rolle

Hvor den ovenstående litteratur har beskæftiget sig med, hvad der med fordel kan gøres, har den i mindre grad beskrevet, hvem der bør gøre det. Udgangspunktet for denne del af analysen er Hobbes statsmodel, hvor staten har en basal forpligtelse over for sine borgere og virksomheder i form af en social kontrakt: Staten har monopol på anvendelsen af magt og yder beskyttelse til gengæld for skat (Hobbes, 1965: 133). Beskyttelsesforpligtelsen er i Danmark med forsvarsforliget i 2018 blevet udvidet til også at omfatte påvirkningsoperationer

(Regeringen, 2018: 10). Overført til det moderne samfund, hvor mange vitale opgaver varetages af private aktører, betyder Hobbes statsmodel, at staten kan uddelegere opgaver til andre aktører, men ikke ansvaret for opgaveløsningen (Dunn-Cavelty og Suter, 2009: 184). Det er væsentligt i forhold til påvirkningsoperationer, fordi den teknologiske og økonomiske udvikling har betydet, at staten har mistet en stor del af den direkte kontrol med mulighederne for at kontrollere og styre udbredelsen af desinformation (Hemsley, 2021: 263). I de "analoge gamle dage" kunne staten kontrollere informationsspredning gennem medier i æteren og på skrift med lovgivning, der holdt redaktørerne ansvarlige for indholdet. Herved kom redaktørerne til at fungere som "dørvogtere" for desinformation. Udenlandske aktører var derfor begrænset til at påvirke gennem egne medier eller gennem relativt let genkendelige kanaler. I Sovjetunionens tilfælde fx gennem det kommunistiske danske dagblad *Land og Folk* (Sohn, 2011).

I dag kan alle med adgang til internettet med få midler, lave omkostninger og en høj mulighed for at sløre sin identitet udbrede information, der gennem sociale mediers algoritmer billigt og effektivt kan rettes direkte mod de mest modtagelige eller velvillige modtagere. Dermed har informationsudbredelsen i samfundet udviklet sig fra i de gamle analoge dage at være et kompliceret, men overskueligt system af primært nationale æterbårne og skriftlige platforme, der hver havde en redaktør, som stod til ansvar for indholdet. Det analoge system er nu erstattet af et komplekst og konstant skiftende og gensidigt informationsudvekslende netværk af internetbaserede platforme, hvoraf mange har ingen eller meget lidt redaktionel kontrol, og hvor den redaktionelle kontrol ofte befinder sig i udlandet, fx for Facebook i USA eller for TikTok i Kina.

Udfordringen med at imødegå desinformation og påvirkningsoperationer er vanskelig. Dels fordi det kan være svært at skelne mellem sand og falsk information i en tid, hvor mange får serveret nyheder på få sekunder gennem sociale medier, og fordi problemet potentielt rammer mange forskellige målgrupper og spænder mange forskellige ressortområder, herunder forsvar og sikkerhed, uddannelse, retsvæsenet m.m. Dertil kommer, at det er vanskeligt at attribuere forsøg på påvirkning og spore omfanget og effekten af dem i tide. De samfundsundergravende halve sandheder og hele løgne kan have spredt sig – bogstaveligt talt være gået viralt – før angrebet er identificeret, og modforanstaltninger kan iværksættes. Samtidig kan tiltag for at imødegå påvirkningsoperationer som beskrevet af Lewandowski og van der Linden (2021) udlægges som forsøg på at begrænse ytringsfriheden og skjule "sandheden" og dermed komme til at indgå i kommende cyklusser af påvirkningsoperationer.

Udviklingen har betydet, at opgaven med at indsamle og bearbejde tilstrækkelig information til at identificere og reagere hensigtsmæssigt på påvirkningsoperationer er blevet helt uoverskuelig, hvis en central myndighed skulle kunne løfte den opgave alene. Et samfund som det danske kan derfor ikke længere organisere sig ud af udfordringen ved at gøre det umuligt for påvirkningsoperationer at trænge ind. I stedet må samfundet gøres resilient, dvs. sættes i stand til at erkende, reagere på og overkomme negative påvirkninger (Walker og Cooper, 2011: 10, 17). For at opnå resiliens må løsningen være en variant af sektoransvarsprincippet, hvor de enkelte sektorer identificerer, rapporterer om og imødegår påvirkningsoperationer. Dunn-Cavelty og Suter har analyseret problemstillingen om moderne, komplekse samfund i forhold til beskyttelse af kritisk infrastruktur. Problemstillingen i forhold til påvirkningsoperationer er den samme: ”Den spidse ende” af samfundets sektorer er det eneste sted, hvor der er tilstrækkelig viden til at erkende problemer og reagere hurtigt. Sektorerne kan med den rette kombination af organisation og incitamenter fungere som selvorganiserende netværk, der bidrager til samfundets resiliens. Staten spiller stadig en væsentlig rolle, men fra at være den centrale overvåger og kontrollant bliver rollen nu en blanding af facilitator, motivator og understøttende rammesætter, fx gennem lovgivning (Dunn-Cavelty og Suter, 2009).

## Usikkerhed og håndtering af påvirkningsoperationer

Målgrupperne for påvirkningsoperationer kan være mangeartede og vidt forskellige. Ruslands kampagner i USA op til valget i 2016 spillede forskellige målgrupper ud mod hinanden ved at udnytte eksisterende stridigheder: Elementer fra den yderste højre- og venstrefløj blev påvirket med henblik på at skabe splittelse og optøjer (Barnes og Goldman, 2020). Andre målgrupper kan være brede befolkningsgrupper med fælles økonomiske, sociale eller politiske bekymringer (fx globalisering, pandemier, indvandring, opbrydning af sociale normer om køn og familieformer), beslutningstagere eller unge, ukritiske medieforbrugere. Det er ikke en realistisk ambition at identificere og overvåge alle potentielle målgrupper og deres indflydelse på hinanden: Deres gensidige påvirkning giver uforudsigelige interaktioner, der igen skaber uforudsigelige konsekvenser. Derfor er det først muligt at forstå effekterne af påvirkningsoperationen på bagkant. Det kræver en undersøgende tilgang med henblik på at finde mønstre, der kan guide kommende indsatser med inddragelse af mange fagligheder og kompetencer fra forskellige ressortområder, eksempelvis i et horisontalt netværk med vide rammer for opgaveløsningen (Snowden og Boone, 2007). Forsøg på at topstyre eller centralisere en planlægningsproces til imødegåelse af komplekse problemer vil ofte fejle, da det ikke er muligt på forhånd at vide, hvilke input



der er mest værdifulde, eller hvilken aktør der i sidste ende bliver udslagsgivende for problemets håndtering. Topstyring og hierarki kan endvidere skabe friktion for problemhåndtering ved at dæmpe nytænkning og kreativitet. Dertil kommer, at det er en udfordring i sig selv at erkende påvirkningsoperationer, da der er så mange forskellige platforme at overvåge.

Incitamentsstrukturen vigtig for, at en netværksbaseret løsningsmodel som sektoransvarsprincippet kan fungere. Derfor er det en udfordring, at imødegåelsen af påvirkningsoperationer er i alles interesse, men de færrestes kerneopgave, endsigte indtjeningsgrundlag. Dermed bliver incitamentet for både individer og organisationer til at forlade sig på, at andre løser den fælles opgave, meget stor – et klassisk *free rider*-problem (Savigny, 2022). Dissonansen mellem statens interesse i at imødegå påvirkningsoperationer og borgernes, virksomhedernes og de enkelte sektorer manglende individuelle interesse i at afsætte ressourcer til opgaven gør, at staten må afsætte ressourcerne eller give inddragne aktører incitament til at gøre det (Dunn-Cavelty og Suter, 2009: 184). Oven i incitamentsudfordringerne kommer indholdsmæssig, strategisk og institutionel usikkerhed (Koppenjan og Klijn, 2004). Tilliden mellem aktørerne kan udfordres af fx inddragelse af efterretningstjenester, der arbejder uden offentlig indsigt, eller private, der primært er motiveret af overskud på bundlinjen.

Manglende gennemsigtighed i beslutningsprocesser og sløret ansvarsfordeling kan også true legitimiteten i samarbejdet. Dette er en udfordring i demokratiske samfund, hvor sektoransvarsprincippet benyttes, fordi sektoransvarsprincippet delegerende natur gør det sværere at placere ansvaret for beslutninger. Alene opgaven at definere desinformation og påvirkningsoperationer i forhold til lovgivning og administrere imødegåelse på et legalt og demokratisk grundlag er vanskelig (Verstraete, Bambauer og Bambauer, 2021). I et offentligt baseret netværk til identifikation, analyse og imødegåelse af forsøg på ondsindet påvirkning bør der således være gennemsigtighed, da beslutninger truffet i netværket kan have vidtrækkende konsekvenser for samfundet. Opgaven er kompleks, omkostningsbehæftet og i sagens natur knyttet til politisk følsomme sager, der kan vække offentlighedens opmærksomhed og engagement.

Endvidere er der politisk incitament til at undgå klar ansvarsfordeling i forhold til opgaven, herunder allokering af ressourcer, fordi klare ansvarsfordelinger er ansvarspådragende og udstiller manglende indsats. Der kan samtidig være et incitament til at have en juridisk frem for operativ tilgang til styringen, fx ved at have en strategi eller et formelt beredskab uden egentligt operativt indhold eller afsatte ressourcer, fx i form af øvelsesaktivitet: At være i juridisk compliance er ikke det samme som at have opnået en operativ effekt (Jensen, 2018: 6-7, 11-14).



For at imødekomme disse udfordringer peger Sørensen og Torfing (2005) på tre metoder til at regulere et ellers selvregulerende, horisontalt netværk: netværksdesign, netværksdeltagelse og netværksframing. Sørensen og Torfing betegner denne form for regulering som "meta-governance", her gengivet med staten i rollen som beslutningstager.

- Netværksdesign: Staten kan befale specifikke aktører til deltagelse og opfordre andre.
- Netværksdeltagelse: Ved selv at deltage i netværket får staten direkte viden om arbejdet og mulighed for at påvirke beslutninger, især i de tidlige faser af arbejdet.
- Netværksframing: Staten sætter rammer for arbejdet i netværket gennem allokering af ressourcer, formulering af overordnede mål og gennem anvendelse af diskursive praksis til at skabe mentale modeller for mulige problemstillinger, løsninger samt normer og værdier, der bør opretholdes i samarbejdet blandt aktørerne.

Design, deltagelse og framing kan også læses ind i Dunn-Cavelty og Suters analyse af netværks rolle i offentligt-privat samarbejde om resiliens i den kritiske infrastruktur. Dunn-Cavelty og Suter bruger begrebet meta-governance af netværk som den gennemgående tilgang til udfordringerne. Den anbefaler, at statens primære fokus frem for direkte styring bliver at koordinere og facilitere selvregulerende netværk gennem tildeling af mål, rammer (fx budgetter og lovgivning) og informationsdeling på tværs af netværkene. Statens opgave bliver derfor at erkende trusler og udfordringer, fastsætte og kommunikere strategiske mål for en tilfredsstillende tilstand på området, vælge de rigtige værktøjer til at organisere og facilitere en (netværksbaseret) løsning, evaluere effekten – og så starte cyklussen forfra. De erkender ligesom Sørensen og Torfing en række udfordringer, primært med udspring i incitamentsforskelle og asymmetrisk informationsadgang hos staten, der har ansvaret for opgavens løsning og de aktører, der skal udføre det i praksis (Dunn-Cavelty og Suter, 2009: 182-184).

## Den danske tilgang: et minimalt beredskab, der til daglig løser andre opgaver

Man kan nedbryde den danske tilgang analytisk i forhold til de teoretiske modeller: Indledningsvis skal truslen erkendes: Årene op til den danske regerings beslutning i 2018 om at styrke Danmarks muligheder for at erkende og imødegå udenlandske påvirkningsoperationer var præget af en række, især russiske, påvirknings- og desinformationskampagner: Den russiske cyberspionage og efterfølgende læk af oplysninger fra Demokraternes præsidentvalgskampagne

i 2016 i USA var den mest spektakulære og fik stor indflydelse. Men også Storbritanniens folkeafstemning om fortsat medlemskab af EU i 2016, det tyske parlamentsvalg i 2017 og det franske præsidentvalg samme år var udsat for russiske påvirkningsoperationer (Jensen, 2021: 349-351).

Herefter skal der fastsættes og kommunikeres strategiske mål og vælges værktøj til at implementere dem: I lyset af denne udvikling valgte den danske regering i september 2018 at implementere sektoransvarsprincippet for at håndtere truslen ved at etablere ”den tværministerielle task force til imødegåelse af påvirkningsoperationer” bestående af Justitsministeriet (formand), Udenrigsministeriet, Forsvarsministeriet, Politiets Efterretningstjeneste (PET) og FE (Justitsministeriet, 2018). Taskforcen, som til daglig omtales som ”task force Påvirkning”, arbejder således: Den mødes jævnligt og forholder sig til aktuelle begivenheder og forhold, der relaterer sig til påvirkningsoperationer rettet mod Danmark. Overvågningen og analysen ligger i FE, PET og Udenrigsministeriet, men de øvrige deltagere byder ind, hvis der er erkendt relevante forhold inden for deres ressortområder. Taskforcens opbygning kan således sidestilles med et begrænset governance-netværk designet af regeringen (jf. Sørensen og Torfing, 2005). Taskforcens fokus skifter afhængigt af aktuelle debatter og begivenheder. Under de seneste års pandemi har opmærksomheden fx været særligt rettet mod covid- og vaccinerelateret desinformation, og påvirkningskampagner været genstand for særlig opmærksomhed. Taskforcens opgave var og er stadig ”at koordinere den danske indsats mod statslige påvirkningskampagner og sikre, at myndighederne samlet agerer effektivt og velkoordineret mod påvirkningskampagner ud fra en tværgående og helhedsorienteret tilgang, truslens karakter og omfang samt sårbarheden i samfundet.” Taskforcens mandat blev afgrænset til statslige påvirkningskampagner (UPN, 2020: 2). Opgaven med at erkende og varsle om påvirkningsoperationer blev endvidere placeret ved FE i det forsvarsforlig, der blev vedtaget januar 2018 (Regeringen, 2018: 10). Som forberedelse til folketingsvalget i 2019 besluttede regeringen i september 2018 at styrke indsatsen yderligere gennem en handlingsplan. Den indeholdt nye opgaver til Udenrigsministeriet om at monitorere desinformation samt ordre til FE og PET om at styrke overvågningen og i samarbejde med Økonomi- og Indenrigsministeriet at sikre udarbejdelse af risiko- og trusselsvurderinger. Regeringen tilbød samtidig de øvrige partier orientering om og uddannelse i at imødegå truslen og indbød pressen og de sociale medier til samarbejde på området. Det kan tolkes som et forsøg på at udvide netværket til også at inddrage private/civile aktører (Folketinget, 2019b; Runge, 2019). Regeringen fremsatte endvidere lovforslag for at sikre, at det strafferetlige værn mod fremmede efterretningstjenesters påvirkningskampagner mod Danmark var opdateret i forhold til den aktuelle

trussel (Justitsministeriet, 2018). Straffelovens § 108 om samvirke med fremmede efterretningstjenester blev samme år ændret, så det tydeligt fremgik, at påvirkningsoperationer var omfattet på linje med spionage o.a. (Folketinget, 2019a). I forbindelse med forberedelserne til folketingsvalget gennemførte FE en række klassificerede og ikkeklassificerede (afhængigt af publikum) briefinger om truslen fra påvirkningsoperationer med såvel de opstillingsberettigede partier som pressen. Partierne erklærede samtidig fælles front mod illegitim påvirkningsvirksomhed (FE, 2019b: 50; Folketinget, 2019b). Briefingerne blev godt modtaget af politikerne.<sup>1</sup> Endvidere udgav FE en ikkeklassificeret trusselvurdering forud for valget (FE, 2019a). FE og PET har siden 2017 varslet om truslen fra påvirkningsoperationer i ikkeklassificerede publikationer med særlig vægt på truslen fra Rusland (FE, 2022: 29).

Det forhold, at overvågning og varsling ligger ved FE i forhold til Rigsfællesskabet, er en potentiel svaghed, der er særegen for det samlede kongerige i forhold til andre stater: FE's opgaver er reguleret i lov om Forsvarets Efterretningstjeneste (FE-loven). Loven gælder ikke for Færøerne og Grønland, men vil ved kongelig anordning helt eller delvis kunne sættes i kraft for Færøerne og Grønland med de ændringer, som de færøske og grønlandske forhold tilsiger (Forsvarsministeriet, 2019). Uden at forklejne den risiko, den administrative og ansvarsmæssige sprække udgør, har det i praksis hidtil ikke været et problem: Samarbejdet mellem de grønlandske og danske myndigheder fungerede fx i forbindelse med, at et falsk brev, der skulle så splid mellem Danmark og Grønland, dukkede op på sociale medier i 2019, og i 2020 gennemførte PET briefinger om påvirkningstrusler i Grønland (PET, 2020: 32; Turnowski, 2019). Men ud over det forfalskede brev og en begrænset kampagne rettet mod det russiske hjemmepublikum om, at Danmark skulle være hjemsted for dyrebordeller, har der ikke været rapporteret om større målrettede russiske desinformations- og påvirkningskampagner mod Danmark baseret på falske nyheder og sociale medier (Redder, 2017; UPN, 2020: 3; se dog Jeanette Serritzlevs kronik om russiske påvirkningsoperationer i Danmark i dette nummer). Den russiske ambassadør tweetede ikke uden ironi i 2018, at siden der ikke var forskel på den danske regerings og oppositionens "russofobi", var der slet ingen grund til at blande sig i de danske valg (Embassy of Russia, DK [@RusEmbDK], 2018).

Det er dog et åbent spørgsmål, om der er tale om underrapportering, der kan skjule betydelige mørketal. Denne artikels forfattere er bekendt med, men har ikke videnskabeligt belæg for at vurdere omfanget af, en række russiske desinformations- og propagandabudskaber, der flourer på dansk i grupper på sociale medier som Facebook, fx om Ruslands krig i Ukraine. Disse omfatter budskaber, som at den ukrainske præsident foranstalter bombardementer af

befolkningen i Donbas, at ukrainske frivillige er fascistiske krigsforbrydere, og at USA havde biologiske laboratorier i Ukraine (European Commission, 2023). Man kan få fænomenet demonstreret ved selvsyn ved et besøg på danske mediers kommentarspor om emner som krigen i Ukraine og vaccineskepsis: Der finder man hurtigt ”troldebudskaber”.

En anden potentiel udfordring ved at lade en efterretningstjeneste selvstændigt forestå overvågning og varsling er, at én enkelt aktør alene har svært ved at overskue og imødegå komplekse problemstillinger. Imødegåelse af påvirkningsoperationer er en udfordring, der berører mange aktører, og som overskrider grænserne mellem sektorer og organisationer i samfundet. Der er derfor behov for en bred involvering fra såvel offentlige som private aktører. Desuden vil et netværk med en efterretningstjeneste i centrum udfordres af, at enkelte aktører har adgang til vigtige informationer, der ikke kan deles med andre. Dette kan øge de indholdsmæssige usikkerheder samt potentielt være skadeligt for tilliden i netværket. Staten har derfor behov for at motivere større dele af samfundet til at fungere som sensorer gennem privat-offentligt samarbejde – måske helt ned på borgerniveau – og facilitere muligheden for informationsdeling mellem staten og sensorerne (Dunn-Cavelty og Suter, 2009: 183).

Til den danske indsats føjer sig supplerende aktiviteter fra EU, der begyndte at tage initiativer til imødegåelse af desinformation i 2018. EU intensiverede indsatsen i forbindelse med coronaepidemien og følger russisk desinformation om krigen i Ukraine (EU, 2018, 2020; European Commission, 2023).

Dunn-Cavelty og Suters model for resiliens anbefaler, at indsatsen evalueres med henblik på at justere i forhold til opgaveløsningens effekt: En kort evaluering af taskeforcens indsats fra 2020 til Udenrigspolitisk Nævn og Retsudvalget er reelt mere en beskrivelse af dens funktion og resultater indtil da (Dunn-Cavelty og Suter, 2009: 185; UPN, 2020). Den samlede indsats blev mere omfattende evalueret i forbindelse med udarbejdelsen af Justitsministeriets omfattende betænkning fra 2020, *Ytringsfrihedens rammer*. Kommissionen finder, at de iværksatte foranstaltninger, herunder oprettelsen af taskeforcen og ændringen af straffelovens § 108, er tilstrækkelige til at håndtere truslen på nuværende tidspunkt (Justitsministeriet og Ytringsfrihedskommissionen, 2020: 47). Kommissionen vurderer, at der for det første ikke er belæg for, at problemet med desinformation i en snæver dansk sammenhæng ikke kan håndteres inden for rammerne af de eksisterende initiativer. Kommissionen vurderer endvidere, at den nationale modstandskraft er stærk på grund af et generelt højt uddannelsesniveau og en høj grad af troværdighed hos den professionelle danske mediebranche (Justitsministeriet og Ytringsfrihedskommissionen, 2020: 48).

Konkluderende kan det siges, at i princippet følger den danske tilgang Dunn-Cavelty og Suters anbefalinger om etablering af netværk med inddragelse af forskellige sektorer: Der er etableret et begrænset netværk, der kan skaleres efter opgavens omfang, der er fastsat et strategisk og afgrænset mål, der er etableret rammer i form af lovgivning, og informationsdeling faciliteres dels gennem taskforcens møder, hvor deltagerne hver især kan bidrage med den viden, de har fra deres egne netværk. Dertil kommer efterretningstjenesternes specielle mulighed for at bidrage med deres særlige muligheder for fx at identificere afsendere af desinformation eller få indsigt i intentionerne bag. Og endelig er indsatsen formelt blevet evalueret.

I praksis kan man dog rejse spørgsmålet, om indsatsen er tilstrækkelig. Som den teoretiske gennemgang har vist, er der stærke incitamentter til at være i formel overensstemmelse med de formulerede strategier uden nødvendigvis at opnå den tiltænkte effekt. Fraværet af en dedikeret officiel dansk indsats til imødegåelse af mytedannelse og misinformation i forbindelse med Ukraine-krigen kan undre i lyset af eksistensen af dansksprogede fora, der formidler de russiske budskaber. Der foregår ikke engang en systematisk officiel dansk promovering af de EU-ledede forsøg på at imødegå desinformationen.

## Sveriges alternative tilgang

For bedre at forstå den danske tilgang kan det være nyttigt at sammenligne med Sverige. Den svenske regering deler ikke den danske ytringsfrihedskommissionens vurdering af, hvilke tiltag der er tilstrækkelige, men vurderede, at der skulle en dedikeret enhed med et betydeligt budget til at løfte opgaven (MSB, 2020: 3-10). Ansvar for beredskabet i Sverige har siden 2009 ligget hos Myndigheten för Samhällskydd och Beredskap (MSB), men opgaverne har været fordelt på en lang række myndigheder fra kommunalt til statsligt niveau (Vilmer, 2021: 10-14). Fra 1. januar 2022 er hele opgaven blevet samlet i en selvstændig statslig myndighed, Myndigheten för Psykologiskt Försvar (MPF), der udelukkende er dedikeret til den opgave. Det fremgår ikke af de tilgængelige oplysninger, hvor stor en organisation MPF er, men den er betydeligt større end den danske taskforce og har ikke andre opgaver. I betænkningen om oprettelse af enheden er budgetteret med 100 mio. SEK (ca. 73 mio. DKK) om året (MSB, 2020: 11). Til sammenligning har den danske indsats ikke en selvstændig post i det forsvarsbudget, hvor opgaven blev oprettet (Regeringen, 2018). MPF ledes af en generaldirektør med tre afdelingschefer under sig for hhv. administration, operationer (erkendelse, analyse og imødegåelse af desinformation) og *förmågehöjande* (groft oversat ”evneforøgelse”). Den sidstnævnte står for fx udvikling, uddannelse og øvelser, der skal øge andre relevante samfundsinstitutioners –

offentlige såvel som private – evne til at modstå påvirkningsoperationer (MPF, 2022). Sverige er kommet frem til den meget anderledes løsning på baggrund af samme trusselsbillede som det danske, nemlig under indtryk af det stigende antal påvirkningsoperationer siden 2010. Sverige har ikke været mål for betydelige kampanjer, men der er dog rapporteret om betydeligt mere russisk desinformation, der har involveret Sverige. Således har EU's East Stratcom Task Force, der blev oprettet i 2015 som reaktion på russiske desinformationskampanjer frem til april 2023 identificeret 28 aktiviteter der er rettet mod eller handler om Danmark, mens der for Sverige er identificeret 228 aktiviteter (East Stratcom Task Force, u.å.; Kragh og Åsberg, 2017: 790-808; Vilmer, 2021: 10).

### Dansk minimalløsning eller svensk ressourcetildeling: Hvad er bedst? Det kommer an på ...

Den danske model er ikke nødvendigvis utilstrækkelig, blot fordi den er tildelt betydeligt færre ressourcer end den svenske. Taskforcen har ikke indtil nu haft anledning til nogen særlig udadvendt virksomhed, da Danmark ikke har været fokus for omfattende påvirkningskampanjer. Fra et deltagerperspektiv byder den danske tværministerielle taskforcemodell på både fordele og ulemper i forhold til at håndtere udfordringerne fra påvirkningsoperationer. I den danske model har deltagerne i vidt omfang opgaven som ”skræstregsfunktion”, dvs. en opgave ved siden af eller supplerende deres normale opgaveportefølje. Det kan ses som udtryk for en lavere prioritering af opgaven end den svenske, hvor der er oprettet særlige organisationer, der udelukkende arbejder med varsling og imødegåelse af påvirkningsoperationer. Samtidig er deltagerne generelt embedsmænd og chefer på lavere niveauer, hvilket igen kan opfattes som mangel på prioritet. Taskforcen, eller netværket, kunne med fordel udvides til også at inkludere et bredere udsnit af aktører fra andre sektorer samt offentlige og private organisationer, der har eller måtte komme i berøring med problemstillingen. Endelig viser de sidste to årtiers kriseøvelser i Danmark, at koordination af fælles indsatser på tværs af sektorer er en stående udfordring under sektorsvarsningsprincippet (Beredskabsstyrelsen, 2017: 2-5, 2019: 35). På den anden side tillader den brede sammensætning på relativt lavt organisatorisk niveau en løbende og uformel gensidig orientering, med hurtig adgang til de højere lag i kommandostrukturen helt op til ministre og det politiske niveau, hvis det skulle blive nødvendigt. Det er endvidere sandsynligt, at bemanningen i en krisesituation relativt hurtigt ville kunne blive udvidet med udgangspunkt i taskforcen i de relevante sektorer.

De potentielle trusler fra større påvirkningsoperationer har, i modsætning til andre ”hybride” trusler, især fra statslige og kriminelt motiverede cyberan-

greb, som beskrevet ovenfor, endnu ikke manifesteret sig mod Danmark. Det er derfor også et spørgsmål om prioritering af begrænsede ressourcer, om der skal oprettes selvstændige organisationer dedikeret til opgaven, sådan som det er sket i fx Sverige og Storbritannien. Så længe opgaven ikke bliver negligeret, er der også et vægtigt ressourceargument for at fastholde overvågning og opmærksomhed gennem en mindre, tværministeriel taskforce støttet af efterretningstjenesterne og med mulighed for ekspansion ved behov.<sup>2</sup>

## Konklusion

Artiklen startede med at stille spørgsmålet, hvordan indsatsen ift. imødegåelse af påvirkningsoperationer ser ud i Danmark, og hvor de væsentligste udfordringer er ift. en netværksbaseret indsats i rammen af sektoransvarsprincippet. Analysen har vist, at opgavens natur og de strukturer, samfundets informationsudbredelse finder sted i, er så komplekse, at en netværksbaseret tilgang – i Danmark og Sverige implementeret gennem sektoransvarsprincippet – er velegnet. I Danmark har man valgt en minimalistisk tilgang, hvor opgaven til daglig løses som ”skråstregsfunktion” af en lille gruppe ministerielle embedsmænd støttet af efterretningstjenesterne, der så i tilfælde af en krise skal udgøre kernen i en ad hoc-organisation, der skal håndtere den opståede situation. Fordelen ved denne tilgang er, at der kun tilføres ressourcer, når der er en krise. Blandt de sandsynlige ulemper er, at gruppens outreach til hverdag er begrænset, og de dele af samfundet, der skal aktiveres under en krise, ikke har erfaring med opgaveløsningen. Derfor bliver reaktionstiden og risikoen for at begå fejl sandsynligvis højere på grund af manglende øvelse og beredskab. Samtidig har Danmark ikke et naturligt sted for borgerne at henvende sig, hvis de mener at have erkendt påvirkningsmateriale, fx på de sociale medier. Dermed udnytter den danske tilgang ikke muligheden for at engagere hele befolkningen som indhentningsplatform og varslingsplatform.

Over for den danske løsning står den svenske med en relativt stor, stående og højtprofileret organisation. Ulempen ved den er naturligvis, at der dermed afsættes ressourcer, der kunne være brugt andetsteds, så længe der ikke er en krise. Blandt fordelene er, at statens centrale ansvar i opgavens løsning tydeliggøres, at der er et større outreach, en højere grad af specialisering og professionalisme og dermed beredskab, samt ikke mindst at alle, inklusive befolkningen, har et centralt sted at henvende sig med mistanke om påvirkningsoperationer.

Man kan konkludere, at både den danske og den svenske tilgang bygger på principperne for netværksbaseret imødegåelse af komplekse udfordringer, men at den danske er udtryk for en større risikovillighed end den svenske. Den svenske tilgang kræver til gengæld langt flere ressourcer. I Danmarks udenrigs- og



sikkerhedspolitiske strategi fra 2022 beskrives truslen fra påvirkningsoperationer som stor og stigende (Regeringen, 2022: 26). Truslen har dog som beskrevet endnu ikke materialiseret sig. Der har derfor ikke været lejlighed til at teste, om den danske minimalistiske tilgang er tilstrækkelig. Artiklens teoretiske modeller for resiliens og håndtering af komplekse problemer ville formentlig anbefale den danske tilgang at udvide netværket og styrke det privat-offentlige samarbejde, fx ved at facilitere borgernes mulighed for at indrapportere forhold, som de mistænker for at være desinformation. Risikoen ved den danske tilgang er, grundet den lave prioritering og de begrænsede ressourcer, at problemets omfang og kompleksitet først erkendes for sent. Man risikerer således, at en kompleks situation bliver kaotisk, fordrer topstyring og hastige beslutninger og får mere karakter af brandslukning end forebyggelse (Snowden og Boone, 2007).

## Noter

1. Interview om påvirkningsoperationsbriefing foretaget af Mikkel Storm Jensen.
2. Task force påvirkning dagligt virke. Interview med FMN foretaget af Mikkel Storm Jensen.

## Litteratur

- Andersen, Margrethe Heidemann (2021). Desinformation, disinformation, misinformation og fake news – DSN. *Dansk sprognævn*. <https://dsn.dk/nyt-fra-sproгнаevnet/januar-2021/desinformation-disinformation-misinformation-og-fake-news/>
- Barnes, Julian E. og Adam Goldman (2020). Russia trying to stoke U.S. racial tensions before election, officials say. *The New York Times*, 10. marts. <https://www.nytimes.com/2020/03/10/us/politics/russian-interference-race.html>
- Beredskabsstyrelsen (2006). *National Sårbarhedsrapport 2006*. [https://www.brs.dk/globalassets/brs---beredskabsstyrelsen/dokumenter/krisestyling-og-beredskabsplanlagning/2020/-national\\_saarbarhedsrapport\\_2008-.pdf](https://www.brs.dk/globalassets/brs---beredskabsstyrelsen/dokumenter/krisestyling-og-beredskabsplanlagning/2020/-national_saarbarhedsrapport_2008-.pdf)
- Beredskabsstyrelsen (2017). *Evaluering af KRISOEV 2017*. <https://www.brs.dk/globalassets/brs---beredskabsstyrelsen/dokumenter/krisestyling-og-beredskabsplanlagning/2020/-evaluering-af-kriso-ev-2017-.pdf>
- Beredskabsstyrelsen (2019). *Evaluering af KRISØV 2019*. <https://www.brs.dk/globalassets/brs---beredskabsstyrelsen/dokumenter/krisestyling-og-beredskabsplanlagning/2020/ovelseskoncept/-krisov-19---evaluering-af-krisov-2019-til-kriseberedskabsgruppen---godke...2551-.pdf>
- Bodine-Baron, Elizabeth, Todd C. Helmus, Andrew Radin og Elina Treyger (2018). *Countering Russian social media influence*. Santa Monica: RAND Corporation. <https://doi.org/10.7249/RR2740>

- Camillus, John C. (2008). Strategy as a wicked problem. *Harvard Business Review*. <https://hbr.org/2008/05/strategy-as-a-wicked-problem>
- Dunn-Cavelty, Myriam og Manuel Suter (2009). Public-private partnerships are no silver bullet: An expanded governance model for critical infrastructure protection. *International Journal of Critical Infrastructure Protection* 2 (1): 179-187. <https://doi.org/10.1016/j.ijcip.2009.08.006>
- East Stratcom Task Force (u.å.). *DISINFO DATABASE*. EUvsDisinfo. <https://euvsdisinfo.eu/disinformation-cases/> (14. april 2023)
- Embassy of Russia, DK [@RusEmbDK] (2018). *Since there is no difference in russophobic approach between #DK Government and opposition, meddling into DK elections makes no sense* <https://b.dk/nationalt/danmark-forbereder-sig-paa-russisk-paavirkning> [Tweet], 24. juli. Twitter. <https://twitter.com/RusEmbDK/status/1021688735677734912>
- EU (2018). *Action Plan on disinformation: Commission contribution to the European Council (13-14 December 2018)* [Text]. European Commission. [https://ec.europa.eu/info/publications/action-plan-disinformation-commission-contribution-european-council-13-14-december-2018\\_en](https://ec.europa.eu/info/publications/action-plan-disinformation-commission-contribution-european-council-13-14-december-2018_en)
- EU (2020). *Bekæmpelse af misinformation om coronavirusudbruddet* [Text]. European Commission. [https://ec.europa.eu/info/live-work-travel-eu/coronavirus-response/fighting-disinformation/tackling-coronavirus-disinformation\\_da](https://ec.europa.eu/info/live-work-travel-eu/coronavirus-response/fighting-disinformation/tackling-coronavirus-disinformation_da)
- European Commission (2021). *Europa-Kommissionens vejledning om styrkelse af adfærdskodeksen om desinformation*. <https://eur-lex.europa.eu/legal-content/da/TXT/?uri=CELEX%3A52021DC0262>
- European Commission (2023). *Twelve myths about Russia's War in Ukraine exposed*. Representation in Cyprus. [https://cyprus.representation.ec.europa.eu/news/twelve-myths-about-russias-war-ukraine-exposed-2023-03-08\\_en](https://cyprus.representation.ec.europa.eu/news/twelve-myths-about-russias-war-ukraine-exposed-2023-03-08_en)
- FE (2019a). *Ikke-klassificeret trusselvurdering for folketingsvalget 2019*. [https://fe-ddis.dk/globalassets/fe/dokumenter/2019/situations--og-trusselvurderinger/pavirkningskampagner/STVpaavirkningskampagner\\_14042019](https://fe-ddis.dk/globalassets/fe/dokumenter/2019/situations--og-trusselvurderinger/pavirkningskampagner/STVpaavirkningskampagner_14042019)
- FE (2019b). *INDBLIK, FE beretning 2017-18*. <https://www.fe-ddis.dk/globalassets/fe/dokumenter/2019/fe-beretning-2017-18-2019.pdf>
- FE (2022). *UDSYN 2021*. <https://www.fe-ddis.dk/globalassets/fe/dokumenter/2021/udsyn/-fe-udsyn-pages-.pdf>
- Folketinget (2019a). *Forslag til Lov om ændring af straffeloven (Ulovlig påvirkningsvirksomhed)*. <https://www.retsinformation.dk/eli/ft/201813L00095>
- Folketinget (2019b). *Værn mod illegitim påvirkningsvirksomhed*. <https://www.ft.dk/aktuelt/nyheder/2019/04/gentlemanagreement>
- Forsvarsministeriet (2019). *FOU, Alm.del—2018-19 (1. Samling)—Endeligt svar på spørgsmål 56: MFU spm. Om, de danske efterretningstjenester, herunder Forsvarets Efterretningstjeneste, har tilstrækkelig lovhjælp til at operere på Færøer-*

- ne, til forsvarsministeren. <https://www.ft.dk/samling/20181/almdel/fou/spm/56/svar/1563229/2026428/index.htm>
- GCS (2019). *RESIST Counter-disinformation Toolkit*. UK Government Communication Service. <https://3x7ip91ron4ju9ehf2unqrm1-wpengine.netdna-ssl.com/wp-content/uploads/2020/03/RESIST-Counter-Disinformation-Toolkit.pdf>
- Hemsley, Jeff (2021). The role of middle-level gatekeepers in the propagation and longevity of misinformation, pp. 263-273 i Brian G. Southwell, Emily A. Thorson og Laura Sheble (red.), *Misinformation and mass audiences*. Austin: University of Texas Press. <https://doi.org/doi:10.7560/314555>
- Huggins, Mike og Cheryll Hilvert (2013). Tackling wicked problems takes resident engagement. *Public Management*. <https://icma.org/articles/article/tackling-wicked-problems-takes-resident-engagement>
- Jensen, Mikkel Storm (2018). Sector responsibility or sector task? New cyber strategy occasion for rethinking the Danish sector responsibility principle. *Scandinavian Journal of Military Studies* 1 (1): 1-18. <https://doi.org/10.31374/sjms.3>
- Jensen, Mikkel Storm (2019). Cyberresiliens, sektorprincip og ansvarsplacering – nordiske erfaringer. *Internasjonal Politikk* 77 (3): 266-277. <https://doi.org/10.23865/INTPOL.V77.1369>
- Jensen, Mikkel Storm (2021). Rusland og cyber: Spionage, sabotage og evig kamp om sandheden, pp. 331-358 i Niels Bo Poulsen og Jørgen Staun (red.), *Rusland som militær stormagt*. Djøf Forlag.
- Justitsministeriet (2018). *Styrket værn mod udenlandsk påvirkning af danske valg og demokrati*. Justitsministeriet. <https://www.justitsministeriet.dk/pressemeddelelse/styrket-vaern-mod-udenlandsk-paavirkning-af-danske-valg-og-demokratiet/>
- Justitsministeriet og Ytringsfrihedskommissionen (2020). *Betænkning om ytringsfrihedens rammer og vilkår i Danmark*. Justitsministeriet. [https://www.justitsministeriet.dk/sites/default/files/media/Pressemeddelelser/pdf/2020/betaenkning\\_nr.\\_1573\\_2020\\_del\\_2.pdf](https://www.justitsministeriet.dk/sites/default/files/media/Pressemeddelelser/pdf/2020/betaenkning_nr._1573_2020_del_2.pdf)
- Koppenjan, Joop og Erik-Hans Klijn (2004). *Managing uncertainties in networks*. Routledge. <https://doi.org/10.4324/9780203643457>
- Kragh, Martin og Sebastian Åsberg (2017). Russia's strategy for influence through public diplomacy and active measures: The Swedish case. *Journal of Strategic Studies* 40 (6): 773-816. <https://doi.org/10.1080/01402390.2016.1273830>
- Lewandowsky, Stephan, John Cook og Doug Lombardi (2020). *Debunking handbook 2020* [Data set]. Databrary. <https://doi.org/10.17910/B7.1182>
- Lewandowsky, Stephan og Sander van der Linden (2021). Countering misinformation and fake news through inoculation and prebunking. *European Review of Social Psychology* 32 (2): 348-384. <https://doi.org/10.1080/10463283.2021.1876983>

- MPF (2022). *Om oss*. Myndigheten för psykologiskt försvar. <https://www.mpf.se/om-organisationen/>
- MSB (2020). *Msb-remissvar-en-ny-myndighet-for-att-starka-det-psykologiska-forsvaret-sou-2020-29.pdf*. <https://www.msb.se/siteassets/dokument/om-msb/vart-uppdrag/remissvar-fran-msb-till-regeringen/2020/msb-remissvar-en-ny-myndighet-for-att-starka-det-psykologiska-forsvaret-sou-2020-29.pdf>
- PET (2020). *Årlig redogørelse 2020*. <https://www.pet.dk/Nyheder/2021/-/media/Aarsberetninger/AR2020/PET2020AARLIGREDEGOERELSEANSKpdf.ashx>
- Pogson Smith, W. G. (1965). *Hobbes's Leviathan. Reprinted from the edition of 1651 with an essay by the late W.G. Pogson Smith*. Clarendon Press.
- Redder, Anders (2017). "EU-enhed: Russiske medier spreder fake news om dyresex i Danmark". *Altinget.dk*, 9. september. <https://www.alinget.dk/artikel/eu-enhed-russiske-medier-spreder-fake-news-om-dyresex-i-danmark>
- Regeringen (2018). *Forsvarsforlig 2018*. <https://www.regeringen.dk/nyheder/2018/forsvarsforlig-2018/>
- Regeringen (2022). *Danmarks udenrigs- og sikkerhedspolitiske strategi*. <https://www.regeringen.dk/nyheder/2022/regeringen-praesenterer-ny-udenrigs-og-sikkerhedspolitisk-strategi/>
- Rittel, Horst og Melvin Webber (1973). Dilemmas in a general theory of planning. *Policy Sciences* 4 (2): 155-169. <https://doi.org/10.1007/BF01405730>
- Runge, Troels (2019). Fake news er en del af valgkampen – sådan undgår du at blive snydt. *Forskerzonen*. <https://videnskab.dk/kultur-samfund/fake-news-er-en-del-af-valgkampen-saadan-undgaar-du-at-blive-snydt>
- Savigny, Heather (2022). *Free riding | social science | Britannica*. Encyclopedia Britannica. <https://www.britannica.com/topic/free-riding>
- Snowden, David og Mary Boone (2007). A leader's framework for decision making. *Harvard Business Review*. <https://hbr.org/2007/11/a-leaders-framework-for-decision-making>
- Sohn, Ole (2011). DKP-tiden var en fejl. *Berlingske.dk*. <https://www.berlingske.dk/content/item/587485>
- Stacey, Ralph D. (2012). *Tools and techniques of leadership and management: Meeting the challenge of complexity*. Routledge.
- Sørensen, Eva og Jacob Torfing (2005). Network governance and post-liberal democracy. *Administrative Theory og Praxis* 27 (2): 197-237. <https://doi.org/10.1080/10841806.2005.11029489>
- Trillingsgaard, Anders (2015). Chefens nye kerneopgave: Professionel forsimpning. *Væksthus for Ledelse*. <https://www.lederweb.dk/media/2591/vh-artikel2-trillingsgaard-161215.pdf>

- Turnowski, Walter (2019). *Falskt brev: Snusfornuft er det bedste forsvar mod fake news angreb*. Sermitsiaq.AG. <https://sermitsiaq.ag/node/217428>
- UPN (2020). *Evaluering af den tværministerielle task force til imødegåelse af påvirkningsoperationer*. <https://www.ft.dk/samling/20201/almdel/UPN/bilag/5/2261444.pdf>
- Verstraete, Mark, Derek E. Bambauer og Jane R. Bambauer (2021). Identifying and countering fake news. *Hastings Law Journal* 73. <https://doi.org/10.2139/ssrn.3007971>
- Vilmer, Jean-Baptiste (2021). *Effective state practices against disinformation: Four country case studies*. Hybrid Centre of Excellence. [https://www.hybridcoe.fi/wp-content/uploads/2021/07/20210709\\_Hybrid\\_CoE\\_Research\\_Report\\_2\\_Effective\\_state\\_practices\\_against\\_disinformation\\_WEB.pdf](https://www.hybridcoe.fi/wp-content/uploads/2021/07/20210709_Hybrid_CoE_Research_Report_2_Effective_state_practices_against_disinformation_WEB.pdf)
- Walker, Jeremy og Melinda Cooper (2011). Genealogies of resilience: From systems ecology to the political economy of crisis adaptation. *Security Dialogue* 42 (2): 143-160.