



Informationspåvirkning som demokratisk udfordring

Desinformation, Danmark og tre
præmisser for det liberale demokrati

Christiern Santos Rasmussen

November 2019

Kolofon

Informationspåvirkning som demokratisk udfordring

Denne rapport er en del af Center for Militære Studiers forskningsbaserede myndighedsbetjening for Forsvarsministeriet og de politiske partier bag forsvarsforliget. Formålet med rapporten er at undersøge fænomenet informationspåvirknings karakteristika og identificere, hvordan det udfordrer demokratiet. På den baggrund præsenterer rapporten den danske stats initiativer for at imødegå informationspåvirkning og kommer slutteligt med en række anbefalinger til, hvordan Danmark kan beskytte sit demokrati mod informationspåvirkning i fremtiden.

Center for Militære Studier er et forskningscenter på Institut for Statskundskab på Københavns Universitet. På centret forskes der i sikkerheds- og forsvarspolitik samt militær strategi. Forskningen danner grundlag for forskningsbaseret myndighedsbetjening af Forsvarsministeriet og de politiske partier bag forsvarsforliget.

Denne rapport er et analysearbejde baseret på forskningsmæssig metode. Rapportens konklusioner er ikke et udtryk for holdninger hos den danske regering, det danske forsvar eller andre myndigheder.

Læs mere om centret og dets aktiviteter på: <http://cms.polsci.ku.dk/>.

Forfatter:

Videnskabelig assistent, cand.scient.pol. Christiern Santos Rasmussen

Masthead

Disinformation as democratic challenge

This report is a part of Centre for Military Studies' policy research services for the Ministry of Defence and the political parties to the Defence Agreement. The purpose of the report is to examine the characteristics of information influence activities and identify how they challenge democracy. Building on this, the report presents the initiatives of the Danish state to counter information influence activities and formulates a number of recommendations on how Denmark could protect its democracy against information influence activities in the future.

The Centre for Military Studies is a research centre at the Department of Political Science at the University of Copenhagen. The Centre undertakes research on security and defence issues as well as military strategy. This research constitutes the foundation for the policy research services that the Centre provides for the Ministry of Defence and the political parties to the Defence Agreement.

This report contains an analysis based on academic research methodology. Its conclusions should not be understood as a reflection of the views and opinions of the Danish Government, the Danish Armed Forces or any other authority.

Read more about the Centre and its activities at <http://cms.polsci.ku.dk/>.

Author:

Research assistant, MSc. Christiern Santos Rasmussen

ISBN: 978-87-7393-842-3

Indholdsfortegnelse

Dansk resumé og anbefalinger	1
Abstract and recommendations.....	3
1. Introduktion.....	5
1.1 Rapportens metode.....	6
1.2 Rapportens formål og struktur.....	6
2. Informationspåvirkning – hvorfor, hvordan og gennem hvem?..	9
2.1 Hvordan: Strategiske narrativer.....	11
2.2 Gennem hvem: Informationskanaler.....	13
3. Et demokratisk dilemma.....	17
3.1 Den danske regerings balancegang	22
4. Anbefalinger.....	28
Noter	32
Litteraturliste.....	45

Dansk resumé og anbefalinger

Informationspåvirkning er en strategisk udfordring for Vestens liberale demokratier. Det står klart efter Ruslands indblanding i det amerikanske præsidentvalg i 2016, som er et af de senere års tydeligste eksempler på, hvordan en fremmed magt har benyttet information strategisk til at påvirke en demokratisk stats indenrigspolitiske anliggender med henblik på at realisere egne udenrigs- og sikkerhedspolitiske mål. En sådan påvirkning er ikke et nyt fænomen, men i takt med at den teknologiske udvikling og digitale revolution har reduceret omkostninger ved at producere og distribuere vildledende og falske historier, er det sket en genkomst i informationspåvirkningens potentielle som strategisk, sikkerhedspolitisk redskab og i dens udbredelse.

Denne rapport undersøger derfor informationspåvirkningens karakteristika – rationalet bag, hvordan den virker og gennem hvilke kanaler – og identificerer på den baggrund tre grundpræmisser for det liberale demokrati, som bliver udfordret af informationspåvirkning. Det gælder hhv. den demokratiske funktion, den demokratiske selvbestemmelse og den demokratiske inklusion. Rapporten argumenterer i forlængelse heraf for, at informationspåvirkning stiller staten over for et demokratisk dilemma, når den vil forsøre de tre præmisser: Bestræbelser på at værne om den demokratiske funktion og selvbestemmelse kan være på bekostning af den demokratiske inklusion og vice versa. På den baggrund præsenterer rapporten den danske stats initiativer for at imødegå informationspåvirkning – regeringens valghandlingsplan fra 2018 – og diskuterer, hvordan den forsøger at finde en balance i demokratiske dilemma. Sluttligt kommer rapporten med række anbefalinger til, hvordan Danmark kan beskytte sit demokrati mod informationspåvirkning under henvisningen til at skabe en passende balance mellem de tre demokratiske præmisser. Rapportens anbefalinger falder på tre niveauer:

Principielle anbefalinger:

- Sikre, at den danske stats dialog med civilsamfundet er tydelig, ved at formulere principper herfor.
- Genoverveje formuleringen af straffelovens § 108 vedrørende påvirkningsvirksomhed, og hvorvidt denne overskridt grænserne for statens interaktion med civilsamfundet. For at sikre et grundlag for sådanne overvejelser, kunne Justitsministeriet bede Ytringsfrihedskommissionen om at evaluere loven med inddragelse af de tre demokratiske præmisser og sikkerhedspolitiske bekymringer forbundet med informationspåvirkning.

Ministerielle anbefalinger:

- Hæve de politiske omkostninger ved brugen af informationspåvirkning, fx ved at Danmark, via Udenrigsministeriet, spiller en aktiv rolle i internationale samarbejder og arbejder for at fremme økonomiske og politiske sanktioner mod udenrigspolitiske aktører, der benytter informationspåvirkning.

- Begrænse digital informationspåvirkning ved at arbejde for yderligere EU-regulering af det digitale marked.
- Bevare Danmarks robuste offentlige debat ved at styrke danske mediers rolle i dialogen mellem stat og samfund, og gøre den nye strategiske virkelighed gældende for både Kulturministeriets mediestøtte og mediernes publicistiske selvforståelse.
- Styrke borgerne i den offentlige debat ved at prioritere fag omhandlende bearbejdning og indsamling af information på uddannelsesområdet.

Myndighedsbårne anbefalinger:

- Fastholde efterretningstjenesternes fokus på informationspåvirkning og de bagvedstående udenrigspolitiske aktører, så Danmarks evne til at identificere informationspåvirkning styrkes.
- Fastholde den danske stats fokus på informationspåvirkning ved at styrke den tværministerielle taskforce og mediescreeningsenheden samt videreføre deres funktioner.
- Styrke det danske beredskab på lang sigt ved at samle indsatsen mod informationspåvirkning i én enhed. Dette vil kunne sikre, forankre og styrke Danmarks beredskab med hensyn til og viden om informationspåvirkning samt følge udviklinger inden for området. Enheden kan evt. etableres i en femårig testperiode med efterfølgende evaluering og have følgende opgaver:
 - Agere kontaktpunkt for statens kommunikation med civilsamfundet.
 - Bygge offentlig kommunikation i krisesituationer på verificerbarhed og transparens.
 - Inkludere et varslingssystem bestående af kontaktpunkter i alle myndigheders kommunikationsafdelinger, herunder også efterretningstjenesterne.
 - Fortsætte valghandlingsplanens rådgivning af de politiske partier og andre aktører i civilsamfundet.
 - Udvikle en håndbog for kommunikatører og udbyde kurser i håndtering af informationspåvirkning til aktører og ansatte i både staten og civilsamfundet.
 - Styrke samarbejdet med efterretningstjenesterne om at udveksle efterretninger om informationsoperationer.
 - Samarbejde med allierede internationale organisationer, der fokuserer på informationspåvirkning.
 - Samarbejde med digitale medier såsom Google og Facebook om fx fælles kriseøvelser og udvikle offentlige goder, som styrker borgernes position i forhold til informationspåvirkning.
 - Trods de sikkerhedspolitiske og efterretningsmæssige dimensioner kunne en sådan enhed oplagt placeres under Beredskabstyrelsen, der har erfaring med transparent samfundskommunikation og krisekommunikation og er vant til at operere mellem civilsamfund og sikkerhedshensyn.
 - Overvejelser om tilsyn bør være et centralt indgå i oprettelsen af en sådan enhed.

Abstract and recommendations

Information influence activities is a strategic challenge for Western liberal democracies. This is evident after the Russian interference in the U.S. presidential election in 2016, which is one of the clearest examples in recent years of how a foreign power has used information strategies to influence a democratic state's internal affairs in order to realise its own foreign and security policy objectives. Such an interference is not a new phenomenon, but as the technological development and digital revolution have reduced the costs of producing and distributing misleading information and fake news, information influence activities have gained renewed potential as a strategic foreign and security policy instrument.

This report examines the characteristics of information influence activities – the rationale behind, how they work and through what channels – and identifies three fundamental premises for liberal democracies that are challenged by information influence activities: the democratic function, the democratic self-determination and the democratic inclusion. The report argues that information influence activities confront the state with a democratic dilemma when it seeks to defend its three democratic premises, since efforts to protect the democratic function and self-determination can come at the expense of democratic inclusion and vice versa. Building on this argument, the report presents the initiatives of the Danish state to counter information influence activities – the Government's electoral action plan of 2018 – and discusses how these initiatives try to balance the democratic dilemma. Finally, the report formulates a number of recommendations on how Denmark could protect its democracy against information influence activities, taking the balance between the three democratic premises into consideration. The recommendations are formulated on three levels:

Principle recommendations:

- Secure that the dialogue of the Danish state with civil society is clear by formulating a set of principles for this dialogue.
- Reconsider the phrasing of § 108 in the criminal code regarding illegal influence activities and whether it gives the state too much authority in its interaction with civil society. These considerations should build on a factual basis, and the Ministry of Justice could therefore ask the Commission of Freedom of Expression to evaluate the law in the light of the three democratic premises and security policy concerns related to information influence activities.

Ministerial recommendations:

- Increase the political costs of using information influence activities, e.g. through the Ministry of Foreign Affairs by playing an active role in international efforts to promote economic and political sanctions against foreign policy actors who carry out information influence activities.

- Limit digital information influence activities by promoting further EU regulation of the digital market.
- Preserve the robustness of Denmark's public debate by strengthening the role of the Danish media in the dialogue between state and society and by considering this new strategic reality, both in connection with government media subsidies and in relation to the self-perception of Danish media publicists.
- Empower the citizens in the public debate by promoting courses on the processing and collection of information in schools.

Government agency-level recommendations:

- Maintain the intelligence agencies' focus on information influence activities and the responsible foreign policy actors, so Denmark will strengthen its ability to identify information influence activities.
- Maintain the Danish state's focus on information influence activities by strengthening the inter-ministerial task force as well as the media-screening unit and continuing their functions.
- Strengthen the Danish preparedness in the long term by merging the different efforts to counter information influence activities in one unit. That would ensure, anchor and strengthen Danish preparedness and knowledge about information influence activities and ability to follow recent developments. This unit could be established for a five year test-period with subsequent evaluation. It could have the following tasks:
 - Be the overall contact point for the state's communication with civil society.
 - Base public communication in crisis situations on verifiability and transparency.
 - Include an early warning system consisting of contact points from the communications branches of all state agencies, including the intelligence agencies.
 - Continue the counselling of political parties and other civil society actors initiated by the Government's electoral action plan.
 - Develop a handbook for communicators and develop courses in management of information influence activities to actors and employees in both state and civil society.
 - Strengthen the cooperation with the intelligence agencies regarding exchange of intelligence on information operations.
 - Cooperate with allied international organisations that focus on information influence activities.
 - Cooperate with digital media such as Google and Facebook about e.g. joint crisis exercises and developing public goods that will empower citizens against information influence activities.
 - Despite dimensions of security and intelligence, this unit could be established under the Danish Emergency Management Agency, which is experienced in transparent public communication, crisis communication and in navigating between civil society and considerations of safety.
 - Considerations about oversight should be a key element in the establishment of such a unit.

1

Introduktion

I efterdønningerne fra Ruslands indblanding i det amerikanske præsidentvalg i 2016¹ står det klart for vestlige beslutningstagere, at den internationale sikkerhedspolitik i dag er kendetegnet ved en mere omfattende strategisk brug af information. Ved at spredte vildledende informationer gennem et økosystem af informationskanaler har Rusland formået at påvirke holdninger og adfærd blandt borgere i Vesten.² Dermed er informationspåvirkning igen blevet en strategisk udfordring for de liberale demokratier.³

For at imødegå denne udfordring iværksatte den danske regering i løbet af 2018 og foråret 2019 en række initiativer for at sikre det kommende folketingsvalg mod fremmede magters påvirkning. Valget den 5. juni 2019 forløb ifølge regeringen uden påvirkning.⁴ Det var der til gengæld ifølge EU-Kommissionen ved europaparlamentsvalget to uger tidligere.⁵ Fraværet af konkrete anslag ved folketingsvalget gør ikke den mere generelle udfordring med hensyn til informationspåvirkning mindre relevant. Udfordringen er drevet dels af forhold i international sikkerhedspolitik, dels af teknologiske udviklinger, som gør, at vi må forvente, at informationspåvirkning i lang tid fremover fortsat vil være en væsentlig udfordring for liberale demokratier og herunder det danske. Det er naturligt, hvis de danske myndigheder efter valget overvejer, hvordan Danmark fremadrettet skal forholde sig til det strategiske problem, som informationspåvirkning udgør. Rapporten søger at bidrage til denne refleksion.

Informationspåvirkning udgør et problem for særligt liberale demokratier, fordi det potentielt kan undergrave fundamentale demokratiske processer for borgerdeltagelse, demokratiske valg og den offentlige debat. Det er processer, som er essentielle for liberale demokratier. En særlig udfordring er, at i forsøget på at värne om disse processer kan staten, ved at blive for indgribende og sætte for rigide rammer, risikere at skade det, den vil forsøre. Informationspåvirkning stiller dermed liberale demokratier i et dilemma, hvor tiltag og modforanstaltninger må balanceres mellem at gøre for lidt og for meget.

Informationspåvirkning er ikke et nyt fænomen, hverken i stormagtspolitik eller i politik mere generelt.⁶ Vinkling af information (også kaldet *framing* på engelsk) er allestedsnærværende i politik.⁷ Men afgørende for graden af informationspåvirkningens alvor er ikke bare vinklingen, men udsigten til, at fremmede magter grüber ind i andre landes indenrigspolitik. Genkomsten af denne strategiske brug af information skyldes i stor grad den digitale revolution, der har sænket omkostningerne ved produktion, vinkling og distribution af information.

Denne nye strategiske virkelighed vil stå mere tydeligt frem, efterhånden som flere fremmede magter opdager informationspåvirkningens særlige anvendelighed, og i takt med at den digitale tidsalder udfoldes. Det berører også Danmark, hvor både Politiets Efterretningstjeneste (PET) og Forsvarets Efterretningstjeneste (FE) tidligere har advaret om russisk indblanding.⁸ Når regeringens strategi mod informationspåvirkning i forbindelse med folketingsvalget den 5. juni 2019 skal evalueres, så står danske beslutningstagere dermed også over for at skulle navigere mellem skærene, der udgøres af strategiske

og demokratiske hensyn. Den navigation fordrer en forståelse af både informationspåvirkningens karakter og de demokratiske dilemmaer. Denne rapport bidrager til en sådan forståelse ved at beskrive informationspåvirkning og identificere de demokratiske risici forbundet hermed.

1.1

Rapportens metode

Under udarbejdelsen har forfatteren brugt videnskabelige metoder, herunder undersøgt, analyseret og anvendt akademisk litteratur, nyere policyrapporter og åbne kilder, interviewet eksperter i den danske centraladministration samt deltaget i internationale seminarer. Rapportens analyse har gennemgået intern og ekstern kvalitetssikring, herunder i form af fagfællesbedømmelse, i pagt med Center for Militære Studiers procedurer for kvalitetssikring. Metodisk bygger rapporten på et længerevarende *desk-study* og en række interviews, der har givet væsentlige input til analysen.

1.2

Rapportens formål og struktur

Rapporten har to formål: at beskrive informationspåvirkningens karakter og at diskutere de demokratiske udfordringer, der følger heraf. Hensigten er at informere beslutningstagere og den bredere offentlighed om emnet og dets problemstillinger. Udfordringen har en generel karakter, blandt andet drevet af forandringer i international sikkerhedspolitik generelt (øget stormagtsrivalisering) samt af den teknologiske udvikling og dennes tilgængelighed. Udfordringen kan derfor ikke reduceres til et enkelt land. Rusland har længe bedrevet informationspåvirkning i de lande, som Rusland anser som en del af landets *indflydelsessfædre*.⁹ Informationspåvirkning er imidlertid en stigende tendens i den internationale sikkerhedspolitik, som ikke er forbeholdt Rusland. Andre autokratiske regimer, herunder Kina, bedriver aktivt informationspåvirkning mod sin egen befolkning.¹⁰ Selvom Ruslands informationspåvirkning generelt er mere raffineret og aggressiv, så forfines disse andre aktørers operationer konstant. Operationerne finder også sted som del af andre aktørers udenrigs- og sikkerhedspolitik, hvor særligt Iran har gjort sig bemærket.¹¹ Derfor vil udfordringen fra informationspåvirkning fra fremmede magter sandsynligvis blive en mere almindelig del af Danmarks sikkerhedsmiljø i det 21. århundrede.

Rapporten tager udgangspunkt i udfordringen fra Ruslands sofistikerede informationspåvirkning, redegjort for i kapitel 2, som et eksempel, der også kan tjene til at forstå, hvordan andre fremmede magter kan bedrive informationspåvirkning. Herefter beskrives de demokratiske dilemmaer i kapitel 3.

Ruslands strategiske brug af information bør forstås som et krydsprodukt mellem først den langvarige og multidimensionelle konflikt, som Rusland ser sig selv være i med Vesten, og dernæst behovet for regimesikkerhed, som den russiske regering søger at opnå gennem kontrol af sit nationale informationsrum (afsnit 2.1.). Siden murens fald har Rusland haft behov for at opveje sin underlegne position i forhold til vestlig militær og økonomisk magt. Det har ført til genkomsten af gamle doktriner, der opererer i andre dimensioner, som supplerende modspil. I kraft af at være et autoritært regime har Kreml altid haft et behov for at sikre regimeoverlevelse ved at kontrollere information i sit samfund.¹² Det behov har ført til udviklingen af en række digitale represionsmidler. Disse redskaber er sidenhen blevet anvendt udenrigspolitisk. Det strategiske instrument informationspåvirkning tillader dermed Kreml både at forfølge sine udenrigspolitiske mål og at dæmme op for spredningen af demokrati til Rusland.

Et kerneaspekt i forbindelse med al politisk kommunikation er ideen om at påvirke modtagerens virkelighedsopfattelse gennem et meningsgivende narrativ.¹³ Derfor er narrativer, der fordrejer modtagerens virkelighedsopfattelse også centrale for informationspåvirkning. I Ruslands informationspåvirkning anvendes fire temaer af narrativer, der har til formål at i) undergrave Vesten som internationalt fællesskab, ii) undergrave nationale og demokratiske fællesskaber i Vesten, iii) legitimere Rusland og iv) afskrække Kreml-kritiske stemmer (afsnit 2.2.). I en digital tidsalder kan informationspåvirkningens narrativer i stigende grad tilpasses eksisterende narrativer i modtagerlandets offentlige debat og specifikke målgruppers allerede eksisterende holdninger.¹⁴

For at kunne nå modtagerlandets offentlige debat kræver informationspåvirkning adgang til forskellige informationskanaler og aktører, der kan videreforsmide ovennævnte narrativer. Her benytter Rusland et sofistikeret økosystem, der forsøger at maskere sig i modtagerlandets civilsamfund og spredte fornævnte narrativer ud i modtagerlandets offentlige debat (afsnit 2.3.). Ved at give direkte adgang til andre landes offentlige debat har de digitale medier sänket omkostningerne ved at bedrive informationspåvirkning markant. Dette gør de digitale medier til den primære arena for informationspåvirkning.

Informationspåvirkning er særligt problematisk for de liberale demokrater, fordi centrale demokratiske processer bliver objekter for udenrigspolitik (kapitel 3).¹⁵ Særligt brugen af vildledende information og maskering i modtagerlandets civilsamfund og offentlige debat er demokratisk udfordrende. Analysens bidrag er at identificere tre fundamentale præmisser for det liberale demokrati og beskrive, hvordan disse udfordres af informationspåvirkning:

Den første præmis, som rapporten identificerer, er den *demokratiske funktion*, det vil sige, at den offentlige debat føres på et grundlag af retvisende og pålidelige informationer. Her undergraver spredningen af vildledende informationer den generelle tillid til både information og afsendere. Tillid til, at den fælles samtale overhovedet kan føres ordentligt, er generelt afgørende for det deliberative liberale demokratis funktion.

Den anden præmis, som rapporten identificerer, er den *demokratiske selvbestemmelse*, det vil sige, at konkurrencen om vælgernes opbakning er fri, fair og national. Her betyder fremmede magters indblanding, at de nationale eliter nu også konkurrerer mod udenlandske aktører eller deres proxyer, hvilket undergraver demokratisk selvbestemmelse.

Den tredje præmis, som rapporten identificerer, er den *demokratiske inklusion*, hvor de basale rettigheder såsom ytrings- og opinionsfrihed garanterer, at borgerne har adgang til den demokratiske offentlige debat og de politiske beslutningsprocesser. Her betyder misbrugen af retten til deltagelse i den offentlige debat, at forsøg på at imødegå informationspåvirkningens illegitime deltagelse kan risikere at undergrave borgernes legitime deltagelse i den offentlige debat.

Informationspåvirkning udfordrer disse præmisser og stiller staten i et dilemma, når den søger at forsøre dem. I bestræbelserne på at sikre den demokratiske funktion og selvbestemmelse kan staten risikere at sætte rammerne for den offentlige debat for rigidt og dominere civilsamfundet for meget, hvilket både kan gå ud over den demokratiske inklusion og have autoritatiske undertoner. Af hensyn til det frie samfund og den offentlige debat er det derfor vigtigt, at de liberale demokrater finder den rette balance mellem aktiv indblanding og en mere tilbageholdende stillingtagen. En for tilbagelænet tilgang risikerer at lade fremmede magter undergrave det danske demokrati og en for aggressiv tilgang risikerer at udøve selvkade på det.

Den 7. september 2018 fremlagde den daværende VLAK-regering sit bud på, hvordan en sådan balance kan findes, i form af valghandlingsplanen.¹⁶ Informationspåvirkningens virkemidler og herunder maskering i civilsamfundet har mange ligheder med efterretningsvirksomhed, hvilket gør dem svære at identificere. Endvidere er informationspåvirkning en langsigtet strategi, hvor valgkampe er særlige lejligheder til at påvirke borgere, men langt fra de eneste.¹⁷ Informationspåvirkning er fortsat en udfordring for Danmark. For at bidrage til den opsamlende og fremadrettede vurdering af regeringens indsats mod informationspåvirkning behandler afsnit 3.1. valghandlingsplanen i forhold til det demokratiske dilemma.

Rapportens centrale observationer opsummeres i kapitel 4. På dette grundlag uddrages rapportens anbefalinger om, hvordan regering, offentlighed og private aktører kan navigere i denne nye strategiske virkelighed og finde den rette balance i beskyttelsen af det danske liberale demokrati.

2

Informationspåvirkning – hvorfor, hvordan og gennem hvem?

Informationspåvirkning er udenlandske aktørers anvendelse af informationsoperationer med det formål at påvirke og manipulere modtagerlandets offentlige debat, beslutningsprocesser og politiske handlinger for at opnå strategiske mål. Informationsoperationer er koordinerede forsøg på at påvirke og vildlede målgruppens virkelighedsopfattelse ved hjælp af strategiske narrativer, der spredes gennem både digitale og analoge informationskanaler. Aktiviteterne er illegitime, men efterligner legitim demokratisk deltagelse og debat. Denne brug af manipulation og bedrag adskiller informationspåvirkning fra aktive foranstaltninger og gråzoneredskaber, hvis magtlogik også kan inkludere tvang.¹⁸ Endelig er det vigtigt at skelne mellem det overordnede virkemiddel (informationspåvirkning som strategisk instrument) og den specifikke brug af information i konkrete operationer.

Informationspåvirkning benyttes i stigende grad af både statslige og ikke-statslige aktører med udenrigs- og sikkerhedspolitiske formål. Blandt disse har særligt russiske informationsoperationer gjort sig bemærket ved både mængde og rækkevidde. Derfor tager dette kapitel udgangspunkt i Rusland for at præsentere informationspåvirkningens karakter, og hvordan den opererer. Kapitlet analyserer den bagvedliggende intention (hvorfor anvender Rusland informationspåvirkning?), beskriver information som strategisk redskab (hvordan vildledes modtagere af informationspåvirkning?) og klarlægger den anvendte struktur (gennem hvem spredes den vildledende information?).

Siden den russiske annektering af Krim i 2014 er relationen mellem Rusland og Vesten forværret. Kreml anser Rusland for at være i en multidimensional og langvarig konflikt med Vesten.¹⁹ Carl von Clausewitz' beskrivelse af krig som 'fortsættelsen af politik med andre midler'²⁰ understreger, at den militære sfære er konfliktenes mest udtrykte form, men langt fra den eneste. Konflikter har altid opereret på tværs af mange dimensioner, og det er ikke givet, at alle konflikter fører til konventionel krigsførelse. Hvor konflikt i vestlig optik som regel ses som separat fra fredstid, ser Rusland konflikt som en integreret del af kontinuummet mellem krigs- og fredstid. Det gælder særligt forholdet til Vesten.²¹ Derfor betød murens fald i 1989 i russisk optik ikke en afslutning på konflikten med Vesten, men snarere, at den fortsatte med en vestlig konventionel overmagt, samtidig med at de økonomiske og normative dimensioner fik en større rolle. Her opfattedes særligt udvidelsen af EU som en måde at bruge disse dimensioner til at skubbe Rusland ud af sin historiske indflydelsessfære i Østeuropa.²²

At definere legitime handlinger, aktører og forståelser af konflikten har altid været en central dimension af konflikt. Ifølge Rand Waltzman fra RAND Corporation er informationspåvirkning en integreret del af Ruslands multidimensionelle konfliktforståelse.²³ Informationspåvirkning tillader Rusland at kompensere for sin underlegne position i forhold til de militære, økonomiske

og normative dimensioner med relativt lave omkostninger. Samtidig er denne konfliktdimensions virkemidler velkendte for Rusland. I den sovjetiske æra indgik der i udenrigs- og sikkerhedspolitikken informationsdoktriner, hvis formål var at undergrave modstanderens sammenhængskraft og prædeterminere modstanderens afgørelser gennem strategisk brug af information.²⁴

Eksistensen af sådanne offensive doktriner i Rusland – og andre autokratier – harmonerer samtidig med den autokratiske opfattelse af, at fri information er en trussel mod deres stabilitet.²⁵ I takt med udviklingen af moderne informationsteknologi blev det sværere at kontrollere, hvilken information der var tilgængelig i samfundet. Det stod tidligt klart for de russiske efterretnings-tjenester, der i 90’erne havde forsøgt at håndtere den digitale revolution uden held.²⁶ Samtidig voksede begrebet ”informationsrummet”²⁷ frem blandt russiske sikkerhedssekspertes, og det kan betegnes som det abstrakte rum, hvori information produceres og spredes mellem enheder. Begrebet indgik i den officielle informationssikkerhedsdoktrin fra 2000, hvis formål blandt andet var suverænitethåndhævelse i det russiske informationsrum.²⁸ I de efterfølgende år udviklede Rusland en række digitale repressionsmidler til at begrænse oppositionen eller styrke landets position i informationsrummet,²⁹ hvilket blandt andet blev brugt i forbindelse med de prodemokratiske protester i 2011.³⁰ Ifølge lektor Mette Skak blev protesterne set som et produkt af en udefra-kommende demokratisk dominoeffekt. Efterfølgende blev kontrollen med det russiske medilandskab og de digitale virkemidler derfor også intensiveret og videreført. Samme digitale virkemidler, der nu også anvendes til at bedrive informationspåvirkning.

For Rusland tilbyder informationspåvirkning dermed en velkendt løsning på et dobbelt pres – dels eksternt ved den perciperede multidimensionelle og langvarige konflikt med Vesten, dels internt ved den digitale revolutions demokratiske potentiale og eksistentielle trussel mod regimet.

Informationspåvirkningen har dermed tre formål. i) Svække Vestens handleevne og indflydelse ved at kunne undergrave sammenhængskraften i Vesten, både som internationalt fællesskab og i de enkelte lande. Her gør det danske EU- og NATO-medlemskab og landets opbakning til den regelbundne verdensorden Danmark til et integreret medlem af Vesten. Dermed er Danmark også i skudlinjen for Ruslands informationsoperationer. ii) Skabe manøvrerum til at forfølge geopolitiske interesser og igen dominere sin indflydelses-sfære ved at undergrave vestlig handleevne. iii) Undergrave demokratiske strømninger i Rusland, der ser Vesten som et forbillede, ved at miskreditere og destabilisere vestlige liberale demokratier. Ved at destabilisere og eksponere splid i liberale demokratier mister demokratiske oppositioner deres moralske forspring og det russiske ”suveræne demokrati”³¹ sin ideologiske konkurrent. Fordi Danmark er et demokratisk foregangsland, kan Rusland ved at fremhæve danske politiske gridninger potentielt sende et effektfuldt signal om demokratiets og Vestens mangler til en hjemlig opposition og til publikummer i Østeuropa.

Opsamlende kan man sige, at informationspåvirkning er et strategisk redskab, der opstår ud af et krydspress mellem udenrigspolitisk konflikt og indenrigspolitisk regimeoverlevelse. Informationspåvirkningen sigter mod at balancere vestlig overmagt, skabe manøvrerum for den russiske regering og bremse demokratiets spredning til Rusland (jf. tekstdoks 1).

Tekstboks 1:
Ruslands
informationspåvirkning

Ruslands informationspåvirkning sigter mod:

1. At modbalance Vesten
2. At skabe manøvrerum
3. At begrænse og forhindre den demokratiske styreforms spredning til Rusland

2.1

Hvordan: Strategiske narrativer

Formålet med informationspåvirkningen er derfor at påvirke modtagerens virkelighedsopfattelse i en ønsket retning. Al politisk information kræver en meningsgivende kontekst, hvilket også kaldes for et ”strategisk narrativ”³². Til forskel fra anden politisk kommunikation er formålet med informationspåvirkningens narrativer at promovere en samlet og ofte forvrænget fortolkning af virkeligheden, der passer til de udenrigspolitiske mål. For at vildlede og påvirke modtagerne bruges forskellige retoriske kneb – men centralt er desinformation og misinformation.³³ For at påvirke målgrupper tilpasses disse strategiske narrativer modtagerlandets offentlige debat og absorberer dem i narrativer, der allerede findes lokalt.³⁴ Tilpasningen øger chancerne for, at desinformationen påvirker modtagerne i modtagerlandet, og at de videresender denne information – men nu som misinformation (jf. tekstboks 2). Desinformationens ypperste formål er derfor at blive omsat til misinformation.

Tekstboks 2:
Forskellen på desinformation og
misinformation

Hvad er forskellen mellem desinformation og misinformation?

Desinformation – er vildledende information, som afsenderen bevidst har designet til at forbreje modtagerens opfattelse af virkeligheden.

Misinformation – er vildledende information, der ubevidst for afsenderen forbrejer modtagerens opfattelse af virkeligheden.

Den digitale tidsalder giver adgang til andre landes offentlige debatter og de inndejrede narrativer. Denne adgang har også betydet, at de strategiske narrativers effekt nemmere kan evalueres, og at tilpasningen kan korrigeres ved at kortlægge andre landes debatter og narrativer.³⁵ Eksempelvis fandt de to svenske forskere Sebastian Åsberg og Martin Kragh, at Rusland har forsøgt at skævvride den svenske offentlige NATO-debat ved at blandt andet udnytte en eksisterende svensk NATO-skeptis.³⁶ Skandalerne omkring Cambridge Analytica viste dertil, at adgangen til personlige data kan bruges til at skræddersy narrativer og desinformation til enkelte individers og marginaliserede gruppers allerede eksisterende holdninger og frustrationer.³⁷

Det ville være en forsimpling at stemple al information fra den russiske stat som falsk. Dels fordi virkeligheden kan passe med Ruslands interesser og mål, dels fordi de strategiske narrativer og desinformationen opererer mellem, hvad der er sandsynligt og muligt. Denne brug af gråzonen mellem sandt og falsk udfordrer den traditionelle antagelse om informations sandhedsværdi, hvor påstande enten er sande eller falske.³⁸

Samtidig betyder de seneste års teknologiske udvikling, at ”virkelighedsstro” beviser nu kan masseproduceres for at bakke op om desinformationens påstande (jf. tekstboks 3). Ifølge forskerne Robert Chesney og Daniella Citron udgør såkaldte ”deepfakes” et potent redskab i forbindelse med informationspåvirkning som i fremtiden vil komme til at udgøre et mareridt for demokratiet.³⁹ Der udvikles konstant software til at beskytte autentiske data og identificere ”deepfakes”, men dette medfører en risiko for, at konkurrencen mellem ondsindede og venligtsindede softwareudviklere vil intensiveres.⁴⁰

Tekstboks 3:
”Deepfakes” udfordring af demokratiet

Hvorfor er ”Deepfakes” problematiske for demokratiet?

De informationsteknologiske udviklinger er en drivende faktor for informationspåvirkning ved at sænke omkostninger for informationsproduktion og -distribution.

En særlig bekymrende udvikling er **deepfake**-teknologien, hvis manipulation af audiovisuelle data i dag har opnået et stadie, hvor de forfalskede data fremstår så autentiske, at de er troværdige. Det er med andre ord relativt nemt og forbundet med lave omkostninger at fremstille og spredte eksempelvis videoklip, hvor øvrighedspersoner såsom ministre eller embedsmænd tillægges falske udtalelser. Sådanne ”deepfakes” kan undergrave borgernes tillid til demokratisk debat og udfordrer centrale komponenter i bevisføring.

Ruslands narrativer

De mest fremtrædende narrativer, som Rusland bruger, kan groft opdeles i fire temae, som alle direkte og indirekte bidrager til de tre ovenstående strategiske mål.

Det første tema søger at få Vesten og vestlige institutioner til at fremstå som destruktive, amoralske og hykleriske. Formålet er at undergrave opbakningen til Vesten som helhed, dennes institutioner og værdisæt.⁴¹ Dette tema går særligt ud over EU og NATO, som jævnligt portrætteres som dysfunktionelle, undertrykkende eller undergravende for sine medlemmers nationale værdier.⁴² Ifølge forskerne Aleksander Król og Ben Nimmos har Kreml spredt falske historier om tyske NATO-soldaters voldtægt af en litauisk kvinde i januar 2017 for at miskreditere NATO’s fremskudte tilstedeværelse i Baltikum.⁴³ Endvidere konkluderede en rapport fra det britiske parlament, at Kreml-kontrollerede medier aktivt promoverede anti-EU-bias ved brexit-afstemningen i 2016 i et forsøg på at påvirke afstemningen.⁴⁴

Det andet tema tilstræber at undergrave de nationale fællesskaber i Vesten. Det gøres ved at designe narrativerne til at udnytte eksisterende skel og gnidningspunkter i samfundet for derved at polarisere og vende samfundet mod staten.⁴⁵ Ifølge den særlige anklager Robert Muellers rapport havde Rusland konkurrerende informationsoperationer på hver sin side af politiske spørgsmål for at polarisere det amerikanske samfund.⁴⁶ To af disse blev ifølge en rapport fra Lunds universitet og Myndigheten för samhällsskydd och beredskap særligt populære og anvendtes til at orkestre en række demonstrationer og samtidige moddemonstrationer.⁴⁷ Narrativerne genbruges ofte i forskellige modtagerlande, og særligt immigration vurderes af FE som relevant i

en dansk kontekst.⁴⁸ Konklusionerne i Jacek Kucharczyks rapport om russiske påvirkningskampagner i Polen indikerer, at de strategiske narrativer lige så enkelt kan tilpasses specifikke samfundskontekster. Kucharczyk beskriver, hvordan Rusland bruger konspirationsteorierne omkring Smolensk-styret – hvor den polske præsident Lech Kaczyński omkom – til at anklage forskellige partier for at stå i ledet med russiske efterretningstjenester, hvilket kan anses for at være forsøg på at skabe yderligere splid i polsk politik.⁴⁹

I det tredje tema bruges de to fornævnte temae som bagtæppe for at få Rusland til at fremstå som en attraktiv modpol til Vesten.⁵⁰ Disse prorussiske narrativer rettes mod både et hjemligt og et udenlandsk publikum.⁵¹ Ofte bruges termen ”russofobi”⁵² til at beskrive vestlig kritik af Rusland. Gennem at få Rusland (og russere) til at fremstå som offer for vestlig chikane delegimeres al vestlig kritik af Rusland. Eksempelvis udgav den russiske ambassade i Washington i kølvandet på Mueller-rapportens offentliggørelse en 120 siders rapport, som affærdigede alle Muellers påstande som russofobiske.⁵³ I 2018 afføgte udtalelser fra Danmarks forsvarsminister og chefen for FE om risiko for russisk informationspåvirkning ved det danske valg anklager om antirussisk hysteri fra den daværende russiske ambassadør Mikhail Vanin.⁵⁴

I forlængelse af de prorussiske narrativer formes det sidste tema af forsøg på at afskrække individer og organisationer fra at kritisere Kreml eller på andre måder udgøre en politisk modstand. Siden 2014 er den finske journalist Jessikka Arro eksempelvis blevet af udsat for smædekamprænge og har modtaget dødstrusler for at have dokumenteret russiske troldefarme og påvirkningskamprænge.⁵⁵

2.2

Gennem hvem: Informationskanaler

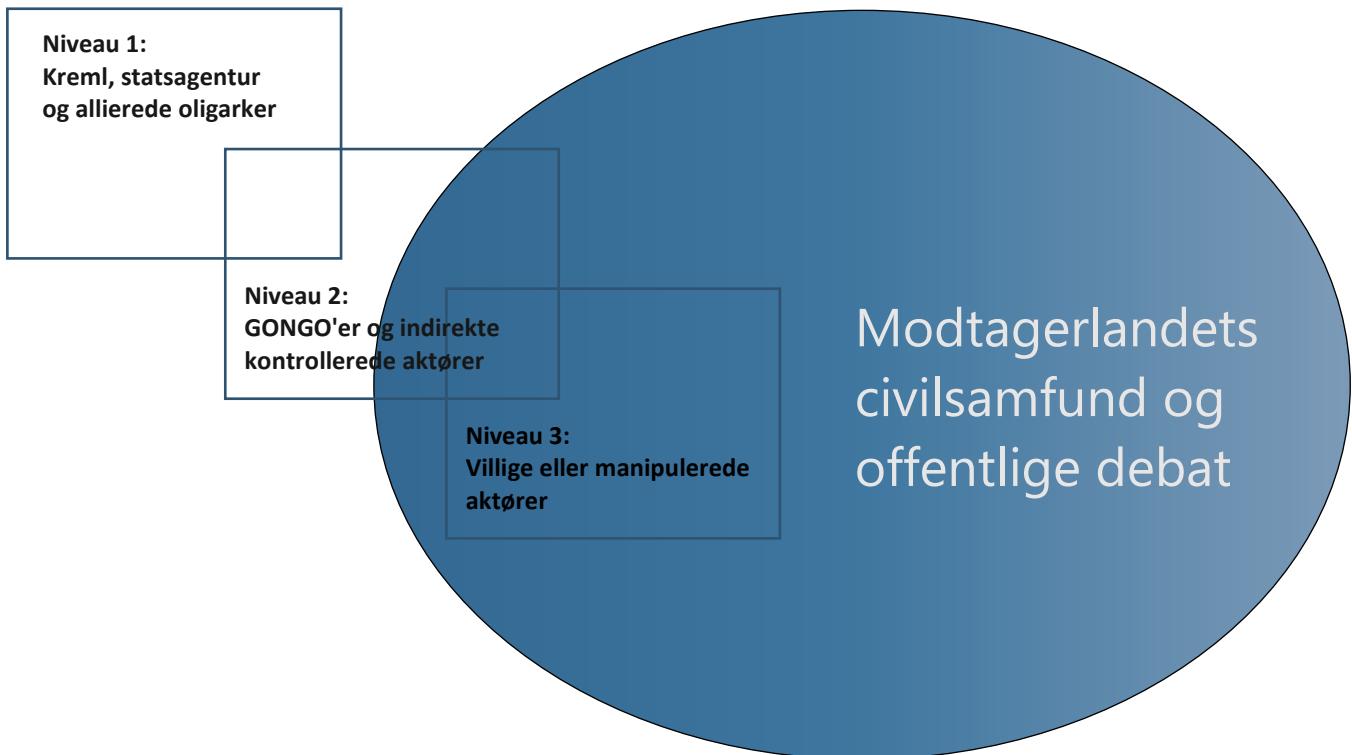
Det foregående afsnit beskrev, hvordan strategiske narrativer og desinformation bruges til at påvirke og skævvride modtagernes virkelighedsopfattelse. For at kunne påvirke modtagerlandets offentlige debat kræves et netværk af informationskanaler, der kan sprede desinformationen og de strategiske narrativer. I dette afsnit beskrives det løse økosystem af informationskanaler bestående af både analoge og digitale aktører, Rusland benytter.

Et økosystem

Ifølge Orysia Lutsevych fra Chatham House har det økosystem, som benyttes af Rusland, en struktur, der består af tre niveauer med forskellige grader af tilknytning til Kreml.⁵⁶ Økosystemet er designet til at maskere sig i modtagerlandets civilsamfund og udvande skellet mellem desinformation og misinformation. Denne maskering giver en særlig adgang til modtagerlandets offentlige debat, da narrativerne spredes af stemmer fra civilsamfundet (jf. figur 1).

Figur 1: Informationspåvirkningens maskering i civilsamfundet:

Illustration af, hvordan informationspåvirkningens økosystem forsøger at påvirke modtagerlandets offentlige debat ved at lade de tre niveauer gradvist maskere sig i modtagerlandets civilsamfund



Det første niveau af kanaler udgøres af statslige agenturer, ambassader, efterretningstjenester og Kreml-venlige oligarker. Aktører på dette niveau understøtter det omkringliggende økosystem gennem blandt andet økonomiske bidrag.⁵⁷ Disse aktører bør ikke nødvendigvis opfattes som en enhedsaktør. Ruslandseksperten Mark Galleotti har eksempelvis beskrevet, hvordan russiske efterretningstjenester befinner sig i en aggressiv konkurrence om Kremls gunst.⁵⁸ De russiske informationsoperationer er derfor ikke nødvendigvis koordineret mellem aktører eller detailstyret af Kreml.

På økosystemets andet niveau finder man aktører, som kontrolleres af det ovenstående niveau. Disse har til formål at fremstå som legitime medlemmer af civilsamfundet og den offentlige debat for derved at kommunikere fornævnte strategiske narrativer og desinformation. Aktørerne varierer i høj grad, og der indgår for eksempel organisationer såsom den selvudnævnte antifascistiske organisation 'Nochnoi Dozor' (Nattevagten), der ifølge eksperterne i påvirkningskampagner Edward Lucas og Peter Pomerantsev blev grundlagt med hjælp fra den russiske ambassade i Tallinn, og som var aktive i organiseringen af optøjerne omkring bron zestatuen i Estland i 2008;⁵⁹ den tjekkiske tænk tank Det Russiske Center for Videnskab og Kultur, der ifølge en rapport af Ivana Smolenová et al. er en del af Russotrudnichestvo (et føderalt agentur under det russiske udenrigsministerium), og som jævnligt holder foredrag på tjekkiske universiteter;⁶⁰ en ombudsmand i Estland, hvis fokus er på den russiske diasporas rettigheder, og som ifølge Buklah et al. fra the International Centre for Defence Studies i Tallinn er finansieret af den russiske stat;⁶¹ de statskontrollerede nyhedsmedier RT og Sputnik, der generelt anses for at være Kremls flagskibe i dets informationspåvirkning af Vesten, og som fungerer som platform for vestlige konspirationsteoretikere.⁶²

På økosystemets tredje niveau finder man aktører, der enten villigt eller ubevidst bidrager til informationspåvirkningen. Modsat økosystemets andet niveau har disse aktører ikke et over- eller underordnet forhold til aktørerne på det første niveau. Ved at være vokset ud af modtagerlandets civilsamfund og gennem den ekstra afstand til Rusland fremstår dette niveaus aktører som mere legitime deltagere i den offentlige debat. Derved er de særligt effektive til at sprede desinformation og misinformation i civilsamfundet, da de ikke nødvendigvis er bevidste om deres deltagelse i informationsoperationerne.⁶³ Samtidig bidrager dette niveau også til at holde informationspåvirkningens strategiske narrativer opdaterede ved at producere indhold og narrativer, som økosystemets andet niveau kan absorbere og udnytte.

Digitale virkemidler

Den digitale revolution har grundlæggende ændret forudsætningerne for informationskanaler ved kraftigt at reducere omkostningerne for informationsproduktion og -distribution samt en forbedret mulighed for at være anonym.⁶⁴ Informationsoperationer kan gennem digitale virkemidler interagere direkte med udvalgte målgrupper og manipulere eksponeringen af specifikt indhold – alt til en langt billigere pris end de analoge informationskanaler.⁶⁵ Som følge deraf er de digitale medier blevet en central arena for informationspåvirkning i det 21. århundrede. De digitale virkemidler består af alt fra trolde, *bots*, alternative medier og platforme for konspirationsteoretikere til større medieselskaber, der opererer på forskellige digitale platforme, såsom YouTube, Facebook, Twitter, Telegram osv. Særligt trolde og bots spiller en stor rolle og er definerede i tekstboksen ovenfor. Trolde benyttes til blandt andet at forstyrre onlinediskussioner og levere en mere menneskelig påvirkning end bots – og dermed en mere effektfuld påvirkning.⁶⁶ *Botnets* kan bruges til at skabe kunstig aktivitet omkring specifikt indhold og kan derved manipulere algoritmer, der baserer sig på trafik og adfærd, såsom søgeresultater, *newsfeeds* osv. Derigennem kan visse emner i debatten få mere eksponering og fremstå mere presserende eller populære.⁶⁷

Tekstboks 4: Digitale virkemidler

Den digitale revolution medførte nye måder at distribuere information på. For moderne informationspåvirkning har dette skabt tre særligt vigtige digitale virkemidler:

Trolde – betalte kommentatorer på de sociale medier.

Sociale bots (*bots*) – automatiserede profiler på de sociale medier, der emulerer menneskelig adfærd.

Botnets – koordineret netværk af bots.

Mindre sofistikerede bots kan på grund af deres mekaniske adfærd fjernes ved hjælp af filtreringsalgoritmer på sociale medier. Som følge deraf er der en konkurrence mellem bot- og softwareudviklere om at overgå hinanden.⁶⁸ En konkurrence, der ifølge flere undersøgelser har skabt et frodigt sort marked, hvor botnets og hele informationsoperationer sælges af private aktører til højestbydende.⁶⁹ På grund af de lave omkostninger ved oprettelsen af bots og

profiler samt dette marked risikerer effekten af de sociale mediers fjernelser at være midlertidige.

Ved gradvist at maskere sig i civilsamfundet, manipulere borgerne og udnytte de digitale medier forsøger et digitalt og analogt økosystem af informationskanaler at sprede de strategiske narrativer og påvirke den offentlige debat. På denne måde kan informationspåvirkningens strategiske narrativer og desinformation fremstå som legitime dele af den offentlige debat.

3

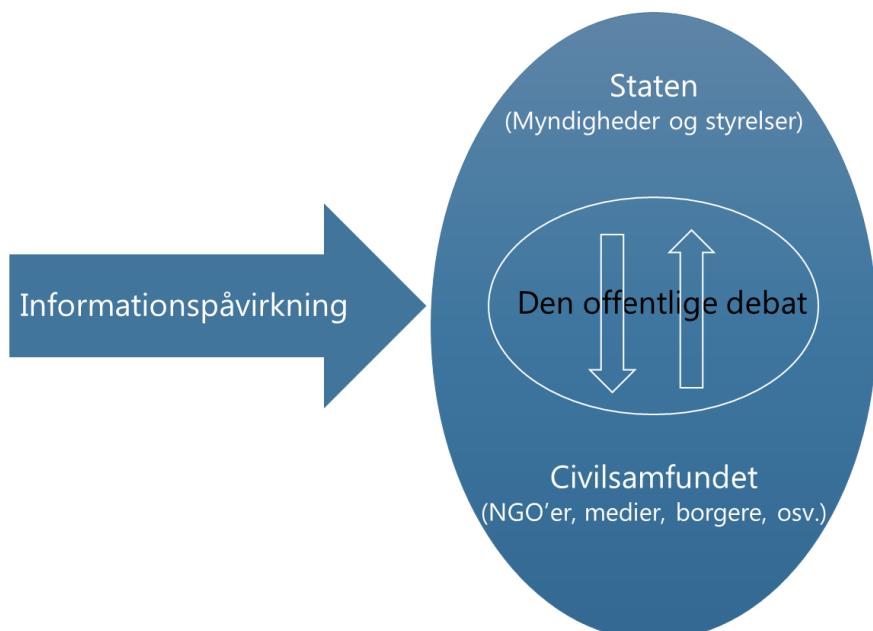
Et demokratisk dilemma

Kapitel 2 beskrev informationspåvirkningen som et strategisk redskab, der bygger på skjult påvirkning af den offentlige debat. I dette kapitel identificeres tre demokratiske præmisser, som udfordres af denne skjulte påvirkning. Dertil diskuteses, hvordan informationspåvirkning skaber et dilemma for liberale demokratier, og hvordan den danske stat har forholdt sig til dette dilemma.

Det liberale demokrati bygger på borgernes medbestemmelse og inklusion. Det muliggøres af den offentlige debat. Ifølge demokratiteoretikeren Jürgen Habermas bidrager offentlig debat (det at *deliberere*) til, at borgerne oplyses, og i fællesskab gennem fornuftig samtale finder frem til de bedste beslutninger.⁷⁰ For politologen David Easton har den offentlige debat en mere strukturel rolle ved at oplyse både borgerne og staten. Ifølge Easton formidler den offentlige debat kommunikationen mellem civilsamfundet og staten. Ved at formidle oplysninger om samfundsbehov, politiske beslutninger og folkelig opbakning guides staten, og civilsamfundet gives medbestemmelse.⁷¹ Dermed bliver den offentlige debat det liberale demokratis evne til at bearbejde information. Det er denne bearbejdningsevne og responsivitet, som forskerne Barry Buzan og George Lawson mener, er de liberale demokratiers styrke, da informationer og samfundsbehov kommunikeres til staten.⁷²

Ved at maskere sig i civilsamfundet og fordreje virkelighedsopfattelser vender informationspåvirkning imidlertid den offentlige debat mod demokratiet og forstyrre derved dialogen mellem civilsamfund og stat. Figur 2 illustrerer, hvordan udefrakommende informationspåvirkning spredt vildledende oplysninger i civilsamfundet og dermed forstyrre dialogen mellem stat og samfund.

Figur 2:
Informationspåvirkningens
inblanding i den offentlige debat.
I et liberalt demokratisk samfund
står den offentlige debat for
kommunikationen mellem civil-
samfund og stat.



I forsøget på at beskytte den offentlige debat kan staten hurtigt ende med at sætte rammerne for den for rigtigt og blande sig for meget i civilsamfundet. Er tiltag for indgribende, kan civilsamfundets frihed indskrænkes, og borgere ekskluderes fra debatten. Det er netop sådanne træk, der adskiller demokratier og mere autokratiske styreformer. Dermed må liberale demokratier, herunder også den danske stat, finde en balance mellem at lade udefrakommende magter undergrave det liberale danske demokrati og at udøve selvskade på det. Dette demokratiske dilemma kan forstås gennem at se på den rolle, (des)information spiller i den liberale-demokratiske styreform, og ved at se på præmisserne for det liberale demokratis funktion, selvestemmelse og inklusion.

Den offentlige debat må forventes at blive ført på et grundlag af retvisende information og af troværdige deltagere. Dette kalder vi *præmissen om demokratisk funktion*.

Den offentlige debats rolle for demokratiets funktionsevne består konkret i at oplyse borgerne og det øvrige civilsamfund om statens og politikernes beslutninger. Dermed er den nødvendig for både borgernes evne til at evaluere beslutningstagerne, politikerne og andre borgers bekymringer. Omvendt oplyser den offentlige debat også beslutningstagerne om de udfordringer og behov, der findes i samfundet, hvilket gør den nødvendig for deres opgave med at varetage borgernes ønsker.

Kommunikationen mellem civilsamfundet og staten avler tillid ved at vise, at politikerne varetager deres opgaver ordentligt,⁷³ men den forudsætter også tillid. Tillid til, at debatten føres på et grundlag af retvisende information, og at de, som leverer informationen, er troværdige og sandfærdige, det vil sige en demokratisk præmis om tillid.

Det er denne tillid, som informationspåvirkningens strategiske narrativer undergraver ved at forurene debatten med vildledende informationer,⁷⁴ ved at miskreditere medier og myndigheder⁷⁵ og ved at manipulere borgere og civilsamfundsaktører til at sprede misinformation.

Demokratiet fordrer i forvejen, at almindelige borgere skal have evnen til at navigere i den offentlige debat og afgøre, hvorvidt informationer er ret eller misvisende, om afsenderen er troværdig, og om myndighederne egentlig varetager folkets ønsker. At navigere i den offentlige debat er blevet særligt besværligt på grund af den digitale tidsalders overflod af information.⁷⁶ Konsekvenserne af et skævt forhold mellem den billige masseproduktion af information og den tidskrævende evaluering af information fører til en overbelastning af den enkelte borgers. En overbelastning, der gør det svært at danne sig det nødvendige overblik af den tilgængelige information og evaluere myndigheder og beslutningstagere.

I mødet med sådan en overbelastning med hensyn til information bruger mennesker *heuristiske smutveje*,⁷⁷ hvor information evalueres på baggrund af andre parametre end dens sandhedsværdi.⁷⁸ Ifølge forskerne Arthur Lupia, Elihu Katz og Paul Lazarsfeld er en særligt vigtig smutvej uddelegeringen af selve indsamlingen og evalueringen af information til aktører, som både kan stoles på og anses for at være mere indsatt i det konkrete emne.⁷⁹ Sådanne aktører, såsom eksperter og medier, kan bruges som markører og tillade borgere at træffe semiinformede valg. Rollen som markør gør disse aktører – og særligt nyhedsmedierne – vigtige for den offentlige debats evne til at formidle information mellem stat og samfund. Men dette kræver, at de anses for at være troværdige og kompetente af de borgere, som bruger dem.

I en tid, hvor digitale medier sluger annoncementtægter og hurtigt leverer nyheder,⁸⁰ er det i stigende grad svært for de traditionelle medier både at være kompetente og følge journalistiske standarder. Ifølge John Watts fra the Atlantic Council og Gordon Ramsay og Sam Robertshaw fra Kings College London vil de strukturelle konsekvenser af denne krise begrænse mediernes evne til at identificere og håndtere misinformation.⁸¹ Dette pres er en bidragende faktor til den langvarige tillidskrise, som både de vestlige institutioner og de vestlige medier længe har befundet sig i.⁸² Ved at miskreditere myndigheder, eksperter og medier udnytter informationspåvirkningen denne eksisterende tillidskrise. Mistilliden udnyttes til at øge utilfredsheden blandt borgere, skævvride deres opfattelse af staten og polarisere samfundet. Det er gennem denne direkte og indirekte undergravning af tillid, at informationspåvirkning også undergraver demokratiets sammenhængskraft.

Informationspåvirkning kan dermed bidrage til en øget mistillid, hvilket kan risikere at skabe en tilstand i modtagerlandet, hvor ingen stoler på nogen i samfundet og betivler al information. Opnås denne tilstand, er der yderligere risiko for, at den offentlige debat eroderer og med den det liberale demokratis evne til at bearbejde information. På denne måde medfører informationspåvirkning en udfordring for det liberale demokratis funktionsevne.

Den anden præmis bygger på en antagelse om, at konkurrencen om vælgernes opbakning er fri, fair og national. Den kalder vi *præmissen om demokratisk selvbestemmelse*.

I demokratiteoretikerne Joseph Schumpeters og Elmer E. Schattschneiders demokratiforståelse koges demokratiet ned til en lige og fair konkurrence mellem eliter om borgernes opbakning.⁸³ Denne løsning reducerer vigtigheden af den offentlige debat til fordel for folketingsvalg, hvor konkurrencen om borgene (vælgerne) er mest udtalt. Men denne konkurrence – og særligt valghandlingen – er ikke meningsfuld, medmindre den er afgrænset til det politiske fællesskab, den omhandler. I demokratiteoretikeren Robert A. Dahls diskussion om ”de berørte interesser” er et minimumskrav, at de interesser, som skal have indflydelse på politikken, udspringer af landets eget folk og samfund.⁸⁴ På denne måde er der tale om en præmis om demokratisk selvbestemmelse. En præmis, der også er grunden til, at FN’s Verdenserklæring om Menneskerettighederne fra 1948 erklærer, at staters legitimitet udspringer fra folket og ikke udefrakommende interesser.⁸⁵

Informationspåvirkning undergraver denne præmis ved at lade udefrakommende aktører træde ind i konkurrencen. Fremmede aktørerne kan blive indirekte deltagere i den nationale konkurrence, ved at udnytte politiske skel og mobilisere sit økosystem til fordel for særligt udvalgte politiske eliter.⁸⁶ Gennem brugen af digitale virkemidler kan samtaler om demokratiske valg påvirkes uafhængigt af det analoge økosystem og geografi. Det forsøgte russiske informationsoperationer at gøre ved brexitafstemningen, ifølge det britiske parlament, og det amerikanske præsidentvalg i 2016, ifølge den særlige anklager Robert Mueller.⁸⁷ Informationspåvirkningen kan ligeført demobilisere andre politiske eliters opbakning hos folket ved at sprede sensitiv information, som Rusland gjorde mod præsidentkampagnerne for Hillary Clinton i 2016 og Emanuel Macron i 2017, ifølge forskerne Marine Guillaume og Jean-Baptiste J. Vilmer.⁸⁸ Dette gælder imidlertid ikke kun ved valg; eksempelvis har Alliance for Securing Democracy dokumenteret, at russiske botnets i 2018 blev mobiliseret i USA både mod Robert Mueller-undersøgelsen og for yderfløjene i debatten om våbenlovgivning, der fulgte efter store skole-/masseskyderier samme år.⁸⁹

I konkurrencen om vælgerne og borgerne kan de nationale eliter dermed ende med at stå over for ikke kun andre nationale modstandere, men også fremmede magter, som agerer gennem informationsoperationer. På denne måde kan informationspåvirkningen forhindre den nationale konkurrence i at være lige og fair. Dette kan have negative konsekvenser for konkurrencens integritet og statens legitimitet, da den politiske magt ikke længere er forankret i borgernes (frie) vilje. Dette legitimetsproblem har blandt andet dannet grundlag for debat i løbet af den amerikanske præsident Donald Trumps embedsperiode, da hans kampagne er mistænkt for at have samarbejdet med den russiske stat ved præsidentvalget 2016.

På denne måde medfører informationspåvirkning for modtagerlandet en vis risiko med hensyn til den demokratiske selvbestemmelse og integriteten af demokratiske valg.

Den tredje præmis tager udgangspunkt i de basale rettigheder såsom ytrings- og opinionsfrihed og garanterer, at borgere har adgang til den demokratiske offentlige debat og til de politiske beslutningsprocesser. Det kalder vi *præmissen om demokratisk inklusion*.

En forudsætning for både det liberale demokratis offentlige debat og det minimalistiske demokratis nationale konkurrence er borgerinddragelse i de politiske beslutningsprocesser. For den offentlige debat gælder det særligt at lade borgeren komme til orde. Det er formålet med ytrings- og pressefriheden – der i Danmark garanteres i grundlovens § 77.⁹⁰ Det er gennem disse rettigheder, at civilsamfundet kan kommunikere med staten, og borgere kan oplyses. Ytrings- og pressefriheden er centrale og kan ikke tilskidesættes uden også at tilskidesætte det liberale demokrati.

Men som det fremgår af de to foregående afsnit, kan denne præmis om demokratisk inklusion også misbruges af informationspåvirkning og risikere demokratiets funktion og selvbestemmelse.

I en fællesrapport fra Lunds universitet og den svenska Myndigheten för samhällsskydd och beredskap sondres der mellem *illegitim* og *illegal* deltagelse i den offentlige debat.⁹¹ Rapporten definerer informationspåvirkning som illegitim på baggrund af sit vildledende formål og indblandingen i den nationale konkurrence. Men på grund af de redskaber, som informationspåvirkningen benytter – det vil sige at aktører i civilsamfundet (informationskanaler) offentliggør politiske holdninger (strategiske narrativer) – deltager informationspåvirkningen i den offentlige debat på en legal måde.

Udfordringen for særligt de liberale demokratier ligger i at ekskludere informationspåvirkningen uden at ekskludere borgerne og civilsamfundet fra de politiske beslutningsprocesser. At gøre specifik demokratisk deltagelse illegal er demokratisk problematisk. I det nødstilfælde, dette gøres, bør en sådan lovgivning kun tilstræbe at forbyde illegitim demokratisk deltagelse. Men selv det forudsætter, at man kan sondre mellem legitim og illegitim demokratisk deltagelse. Denne sondring er praktisk og objektivt udfordrende, fortsat demokratisk problematisk og noget, informationspåvirkningen er designet til at modvirke.

Udfordringen ved at skelne informationspåvirkning fra borgeres legitime demokratiske deltagelse gør sig gældende på tre måder:

- At sondre mellem den illegitime og legitime deltagelse på baggrund af påstandes sandhedsværdi er problematisk. Selve det at tage patent på sandheden har stærke autokratiske undertoner.⁹² Men denne sondring kræver, at man kan placere information og narrativer på en skala mellem

ret- og misvisende. At undgå, at sådan en placering sker subjektivt og ikke er tilfældig, er ifølge forskerne Joseph Uscinski og Ryden Butler yderst besværligt.⁹³ Dermed er det nuancer af sandhed og usikkerhed, der gør sådan en sondring praktisk udfordrende.

- At sondre mellem illegitim og legitim demokratisk deltagelse på baggrund af forstærkelsen af strategiske narrativer er også problematisk. Informationsoperationer forsøger at polarisere samfundet ved at forstærke og skabe opmærksomhed over for eksisterende politiske skel. Disse skel er imidlertid en del af indlejrede narrativer og kan være borgeres legitime holdninger, såsom prorussiske holdninger. Dermed er det kun forstærkelsen af holdningen, der er illegitim, og ikke holdningen i sig selv. Men at identificere koordineret falsk forstærkelse af narrativer er også problematisk. Det kræver praktiske og objektive definitioner af både forstærkelse af politiske narrativer og falsk forstærkelse. Igen bliver sådan en sondring demokratisk problematisk og praktisk udfordrende.
- At sondre mellem den illegitime deltagelse og et patron-klient-forhold eller samarbejde med statsaktøren bag informationsoperationer – også kaldet for attribuering – kan virke som den sidste løsning. Attribuering forudsætter imidlertid, at man kan skelne mellem uvidende og kontrollerede informationskanaler/aktører, hvilket informationspåvirkningen er designet til at modvirke. Særligt økosystemets andet og tredje niveau tilstræber at udviske relationer mellem Kreml og de manipulerede aktører, som spredet misinformation. Ignoreres denne udfordring, risikerer borgere med relation eller kontakt til fjendtlige statsaktører at blive ekskluderet fra den offentlige debat, hvilket igen har stærke autokratiske undertoner. Det er derfor nødvendigt at attribueringen også inkluderer beviser for aktørens bevidste deltagelse og viden om informationsoperationens formål. Denne bevisførelse tilfører yderligere omkostninger til den allerede ressourcekrævende attribuering, og den anklagede kan let undsige sig et bevidst samarbejde.

Ovenstående viser, hvor praktisk besværligt det er at adskille illegitim informationspåvirkning og legitim demokratisk deltagelse. At lovgive på dette usikre grundlag vil derfor altid risikere at medføre autokratiske undertoner til fare for det liberale demokrati.

Samtidig vil en offentlig stempling af specifikke aktører som illegitime også have demokratiske konsekvenser. Sådan en stempling vil fortsat være plaget af de ovenstående tre udfordringer med at sondre mellem legitim/illegitim og kan risikere at føre til indirekte censur. De tre hollandske medier GS Media, TPO og De Persgroep sagsøgte sidste år EU's faktatjekkende organisation "EU vs Disinfo" for at have stemplet dem som misinformerende medier.⁹⁴ Ud over at mene, at stemplingen var uberettiget, påpegede de tre medier, at nyhedsmedier frit skal kunne stille kritiske spørgsmål uden frygt for repressialer. Derfor bør en offentlig stempling af illegitim deltagelse og anklager om informationsoperationer ske med omtanke og på et forsvarligt grundlag. Det kræver tid og forsigtighed, hvilket står i kontrast til den digitale tidsalders hastige informationsstrømme. Dette tilfører et tidspres med hensyn til håndteringen af informationspåvirkning og komplicerer den demokratiske balancegang yderligere.

Dette afsnits fund opsamles i tabel 1, der beskriver, hvordan de tre præmisser for det liberale demokrati undermineres og skaber tre demokratiske

risici. Gennem disse præmisser har afsnittet redegjort for det dilemma, liberale demokratier stilles i, når de konfronteres af informationspåvirkning.

Tabel 1: Beskrivelse af, hvordan informationspåvirkning udfordrer de tre demokratiske præmisser.

Demokratisk præmis	Informationspåvirkningens udfordringer	Demokratisk risiko	Mekanisme
Funktion	Spredning af misinformation/desinformation	Mistillid	Undergraves tilliden i den offentlige debat, risikerer det liberale demokratis evne til at bearbejde information og dermed dets funktionsevne også at blive undergravet.
Selvbestemmelse	Indblanding i national konkurrence	Integritet	Indgår udenlandske aktører i den nationale konkurrence om vælgernes opbakning, risikerer det at indskrænke de nationale eliters indflydelse og konkurrencens integritet.
Inklusion	Maskering i civilsamfundet	Eksklusion	Begrænses informationsoperationers adgang til den offentlige debat, risikerer staten at ekskludere borgers legitime demokratiske deltagelse på grund af informationspåvirkningens maskering i civilsamfundet.

3.1

Den danske regerings balancegang

Den 7. september 2018 fremlagde den danske regering en valghandlingsplan. I takt med den gradvise afdækning af de russiske informationsoperationer rettet mod det amerikanske præsidentvalg i 2016 og det franske præsidentvalg i 2017 indså den danske regering, at også Danmark kunne trues af informationspåvirkning. Bekymringen lå særligt i, at potentielle russiske informationsoperationer kunne forsøge at påvirke danske vælgere til det kommende folketingsvalg i 2019. Efter en række overvejelser, med inddragelser af udenlandske erfaringer, formulerede regeringen i foråret 2018 en national strategi for at modvirke informationspåvirkning, baseret på 11 generelle tiltag.⁹⁵

Tiltagene varetages af en række arbejdsgrupper fordelt mellem Justitsministeriet, Udenrigsministeriet, Forsvarsministeriet samt Økonomi- og Indenrigsministeriet og forsøger både at indføre modforanstaltninger hos danske myndigheder og at mobilisere aktører i civilsamfundet. Blandt de tiltag, der fokuserer på statens myndigheder, blev en tværministeriel taskforce oprettet for at koordinere de øvrige arbejdsgrupper, bestående af repræsentanter fra både Justitsministeriet, Udenrigsministeriet og Forsvarsministeriet samt PET og FE (tiltag 1). Dertil har man styrket den danske stats evne til at identificere informationsoperationer ved at oprette en mediescreeningsenhed i Udenrigsministeriet og styrke efterretningstjenesterne (tiltag 2 og 3). Særligt PET blev styrket ved at få yderligere juridiske beføjelser gennem ændringen af straffelovens § 108. (tiltag 11). Foranstaltninger vedrørende de tekniske aspekter af valghandlingen varetages af Økonomi- og Indenrigsministeriets valgenhed, der er ansvarlig for valghandlingen, og Center for Cybersikkerhed (tiltag 4 og 5). Derimod forsøger de øvrige tiltag at engagere aktører i civilsamfundet ved at tilbyde politiske partier rådgivning (tiltag 6 og 7) og dele oplysninger med medier. Alt dette med respekt for pressefriheden og det frie samfund (tiltag

8-10). På denne måde forsøger man at skabe et bredt værn, der sammentænker både statslige tiltag og civilsamfundets styrke. Det efterfølgende vil nu uddybe opgaverne for disse arbejdsgrupper for at give et overblik over den samlede danske indsats.

Taskforcen

Informationspåvirkningens brug af forskellige politiske skel og miskreditering af myndighederne gør, at alle politiske emneområder er sårbare. Det bør enhver indsats tage højde for ved at skabe et overblik på tværs af politiske ressortområder. Derfor oprettede regeringen den tværministerielle taskforce, der skal styrke kommunikation mellem myndighederne og mellem de øvrige arbejdsgrupper og sammentænke et dansk værn mod informationspåvirkning. Dermed udgør taskforcen et samlingspunkt for overblikket over indsatsen i Danmark, som også suppleres af udenlandske erfaringer og efterretninger, ved at medlemmerne også er kontaktpunkter til alliance og netværk, hvor oplysninger om attribuering deles.⁹⁶ Dette samarbejde kan også bidrage til at sænke de omkostninger ved attribuering og identificering af informationsoperationer, som blev diskuteret i det foregående afsnit.

For at forhindre, at taskforcen skulle blive for dominerende eller træffe forhastede beslutninger inden for statens område, valgte man en decentraliseret struktur, så de øvrige arbejdsgrupper kunne bringe deres fagspecifikke viden i spil. Dette valg tillader modforanstaltninger at blive tilpasset hvert ansvars- og emneområdes specifikke forhold. Dertil har bekymringer om forhastede beslutninger og en for dominerende rolle i den offentlige debat også været grund til, at taskforcen har valgt en ad hoc-baseret responsprocedure med udgangspunkt i at varsiko de berørte ressortministerier. Dette lader til at skyldes et ønske om at trække på den faglige viden, som ressortministerierne har for bedst at kunne svare på informationsoperationer og rette eller påpege deres vildledende informationers skævvridning af virkeligheden.

Men dette valg af en decentral tilgang og en ad hoc-baseret responsprocedure kan imidlertid risikere Task Forcens evne til at danne sig et hurtigt overblik af både indsatsen og potentiel informationspåvirkning. At have flere led fra identificeringen af potentielle informationsoperationer til en faglig vurdering og til, at en respons vælges og udformes, kan blive tidskrævende og tager ikke højde for den digitale tidsalders hastige informationsstrømme. For dertil at begrænse informationsoperationers påvirkning af vælgerne kræves det, at de vildledende påstande afsløres, og at afsløringen hurtigt når ud til vælgerne. Det forudsætter en vis forberedelse, infrastruktur og en eksisterende kontaktflade med berørte borgere, som det kan tænkes, at de enkelte ressortministerier ikke har. Dermed kan taskforcens valg af en decentral struktur og manglen på en klar og fælles kommunikationsstrategi medføre en risiko med hensyn til indsatsens reaktionsevne og overblik.

Denne tilbageholdenhed i taskforcen lader til at udspringe fra bekymringen om indsatsens konsekvenser for præmissen om demokratisk inklusion. Men selvom denne forsigtighed er vigtig, kan det også have konsekvenser for præmisserne om den demokratiske funktion og selvbestemmelse.

Identifikation af informationsoperationer

At kunne identificere den trussel, som et værn skal afskærme mod, er en prioritet for ethvert værn. Derfor oprettedes Udenrigsministeriets mediescreeningsenhed, der skal identificere desinformation og strategiske narrativer i og

uden for Danmark. Dertil tildelte regeringen yderligere ressourcer til efterretningstjenesterne, for at disse skal kunne have et fokus på påvirkningsaktivitet⁹⁷ og kortlægge Ruslands økosystem af aktører.⁹⁸ Denne styrkelse af den danske stats evne til at identificere informationsoperationer lader til at lægge vægt på efterretningstjenesterne, der har flere redskaber og ressourcer til rådighed, for at kunne identificere aktører og informationskanaler i det russiske økosystem. Imidlertid virker det ikke til, at samme prioritering også gælder mediescreeningsenheden, selvom denne spiller en stor rolle for indsatsens samarbejde med medierne og træning af myndigheders kommunikatører.

Mediescreeningsenhedens beskedne størrelse kan have konsekvenser ved at begrænse indsatsens evne til at identificere nye strategiske narrativer rettet mod Danmark. I løbet af vinteren kunne mediescreeningsenheden, efter screening af kendte Kreml-kontrollerede medier, rapportere, at russisk informationspåvirkning ikke benytter Danmark-specifikke narrativer. Imidlertid var screeningen baseret på narrativer, som ekstern forskning allerede havde knyttet til de russiske informationskanaler, og der var således ikke fund af nye narrativer.⁹⁹ Ifølge Rebecca Adler-Nissen et. al. fra Københavns Universitet er denne type research og forskning primært udenlandsk.¹⁰⁰ Dermed vil en afhængighed af sådanne kilder, der ikke har et dansk fokus, kunne risikere at begrænse mediescreeningsenheden evne til at identificere nye strategiske narrativer tilpasset Danmark.

Mediescreeningsenheden har dertil valgt at fokusere på at identificere forekomsten af digitale virkemidler på Facebook, og her har man identificeret omkring 206 danske facebookgrupper, der aktivt spreder misinformation. De identificerede grupper lader ikke til at være knyttet til Rusland, og deres aktivitet¹⁰¹ på Facebook er langt mindre end de danske mediers, men overstiger derimod alle danske politikeres og partiers enkeltaktiviteter. Valget af Facebook skyldes platformens dominans i det danske medielandskab, hvilket vil gøre den central for enhver informationsoperation rettet mod Danmark.¹⁰² Imidlertid kan dette fokus på længere sigt risikere at blive en hæmsko. På den ene side har Facebook annonceret, at man vil end-to-end-kryptere sine beskedservicestørrelser, hvilket vil begrænse mediescreeningsenhedens evne til at identificere informationsoperationer.¹⁰³ Men samtidig er andre sociale medier også begyndt at vinde frem og kan dermed udgøre alternativer til Facebook¹⁰⁴ og vil i stigende grad bruges af informationsoperationer til at omgå overvågning på Facebook.

Nedprioriteringen af mediescreeningsenheden kan også have konsekvenser for dennes opgave med at træne kommunikatører i offentlige myndigheder, beskrevet i valghandlingsplanens tiltag 2. Ifølge EU-Kommissionens handlingsplan vil træning af myndigheders kommunikatører styrke enhver indsats' evne til at identificere og håndtere informationspåvirkning.¹⁰⁵ Sådan en træning af kommunikatører forudsætter imidlertid en introduktion til informationsoperationer, deres operation, mål og strategier samt træning i brugen af relevante digitale redskaber. Det tyder imidlertid på, at mediescreeningsenhedens møder med kommunikatører ansat i danske myndigheder har været mere opmærksomhedsskabende end uddannende i sin natur. Økonomi- og Indenrigsministeriet har afholdt lignende møder med sine frivillige valgtilsynsforordnede, dog har disse været begrænset af hensyn til rekruttering af frivillige.

Dermed lader det til, at en fortsat nedprioritering af mediescreeningsenheden er forbundet med en risiko for indsatsens evne til at identificere informationsoperationer og dermed også muligheden for at gøre noget ved dem.

Engagere civilsamfundsaktører

Mediescreeningsenheden lader også til at spille en stor rolle for valghandlingsplanens aktivering af medierne. For at modvirke informationsoperationers undergravning af den offentlige debat har enheden inviteret repræsentanter fra de danske medier til netværksmøder forud for folketingsvalget, hvor man har redegjort for ovenstående fund for at opmuntre medierne til at have et fokus på informationspåvirkning og øge befolkningens bevidsthed. På samme måde er FE begyndt at træde mere frem i den offentlige debat gennem interviews og pressemødelelser.¹⁰⁶ Ved at give medier og borgere mere adgang sæknes offentlighedens usikkerhed i forhold til efterretningstjenesterne, der derved virker mere troværdige, og selvom der er ikke en udbredt skepsis over for efterretningstjenesterne i Danmark, kan en mere transparent tilgang fortsat begrænse informationspåvirkningens forsøg på at undergrave tilliden til statens myndigheder. Derfor bør FE roses for at trodse sin lyssky natur og opmuntres til at fortsætte denne gradvise åbning, så vidt det er muligt.¹⁰⁷

Ved at indtage en mere rådgivende rolle og dele svært tilgængelige oplysninger med civilsamfundet lader det til, at den danske indsats forsøger at aktivere civilsamfundet og øge borgernes bevidsthed, men uden at dette går ud over pressefriheden.

Imidlertid spiller de digitale medier en stigende rolle for både den offentlige debat og informationspåvirkningen. Derfor har taskforce og repræsentanter fra udvalgte arbejdsgrupper etableret kommunikationsveje til de sociale medier, hvor det ser ud til, at Udenrigsministeriets techplomacy-initiativ og tech-ambassadør har vist sig brugbare til at få adgang til Facebook. Disse kommunikationsveje vil tillade taskforceen at gå i dialog med de sociale medier om eksempelvis at fjerne botnets og begrænse spredningen af misinformation. Men disse kommunikationsveje er kun dele af løsningen, som også kræver, at de digitale medier selv spiller en aktiv rolle i at nægte informationspåvirkning adgang til de digitale medier. Det ser ud til at den danske indsats har valgt at læne sig op af EU-Kommissionens aftale med repræsentanter fra digitale medier fra september 2018, kaldet Code of Practice.¹⁰⁸ Aftalen har til formål at igangsætte en række frivillige initiativer, der skal begrænse informationspåvirkningens adgang til de digitale medier og styrke brugernes evne til at modstå misinformation.¹⁰⁹ Aftalen, der i høj grad var et udtryk for goodwill fra Kommissionens side, afhænger af de digitale mediers frivillige engagement.¹¹⁰ Imidlertid var Kommissionens første rapporter kritiske over for de digitale mediers engagement og mindede om tidligere kritik af de digitale mediers mangelfulde indsats mod misinformation, der er blevet beskrevet som *reaktive*¹¹¹ og *krise-PR*.^{112, 113}

Selvom Code of Practice er mere specifik end tidligere forordninger, spiller EU og den danske stat fortsat en passiv rolle og risikerer en fortsat utilstrækkelig håndtering af digital informationspåvirkning.

Ud over et fokus på medierne har valghandlingsplanen også tilstræbt at styrke sikkerheden og bevidstheden blandt de opstillingsberettigede partier og partiledere for at sikre valgets integritet og den offentlige debat. Derfor har efterretningstjenesterne gennem efteråret rådgivet partierne og partilederne om informationspåvirkning og cybersikkerhed i samarbejde med Folketingets Præsidium.¹¹⁴ Dette samarbejde virker til også at have fået Folketingets formand til at indgå en gentlemanaftale med folketingspartierne om at udveksle oplysninger om lækager eller hacking og være påpasselige med ikke at videregive misinformation.¹¹⁵

Den danske indsats synes derfor at ville sikre integriteten af det danske valg ved også at styrke og rådgive de nationale eliter. Statens rådgivende rolle heri tyder igen på en prioritering af den demokratiske inklusion.

Valghandlingens integritet

Bekymringer for hacking af selve valghandlingen og cybersikkerheden omkring de relevante it-systemer lader til at være en prioritering for den danske indsats.¹¹⁶ Derfor har Økonomi- og Indenrigsministeriets valgenhed sammen med Center for Cybersikkerhed i løbet af efteråret gennemført en 360-graders trusselsvurdering, der er blevet brugt til at identificere og udbedre svagheder. Rapportens rolle for valghandlingens integritet taget i betragtning har valgenheden valgt ikke at offentliggøre vurderingen. Den danske valghandling er fortsat relativt manuel,¹¹⁷ og de anvendte it-systemer decentrale, hvilket i et vist omfang kan begrænse hackeres adgang til valghandlingen. I midlertid betyder indførelsen af det nye elektroniske valgsystem, at dette ændres. Det nye system vil integrere en række administrative procedurer i et fælles system, men fortsat beholde den fysiske stemmeafgivelse.¹¹⁸ Selv uden stemmeafgivelsen behøver ondsindede hackere dermed fortsat kun at hacke ét system for at tilgå vigtige procedurer og processer af betydning for valgets integritet. Af denne grund udvikles det nye elektroniske system i dialog med Center for Cybersikkerhed.¹¹⁹

Nye juridiske virkemidler

Indtil nu lader indsatsen til at have været kendtegnet ved en vis tilbageholdenhed, hvor indblanding kommer i form af oplysning og rådgivning. I midlertid er ændringen af straffelovens § 108 valghandlingsplanens mest indgribende tiltag i forhold til den offentlige debat. Lovændringen indførte et forbud mod at "samarbejde [med udenlandske efterretningstjenester] om at udøve påvirkningsvirksomhed med henblik på at påvirke beslutningstagning eller den almene meningsdannelse"¹²⁰, og dertil hævedes straffen til 12 års fængsel, hvis påvirkningsvirksomheden sker i forbindelse med en valghandling.¹²¹ Selve lovændringen skyldtes manglende præcedens og tvivlsspørgsmål i forhold til eksisterende lovgivning. Lovændringen var derfor et forsøg på at styrke PET's og Rigspolitiets evne til at retsforfølge informationsoperationers illegitime deltagelse i den offentlige debat.¹²² Ændringen af § 108 kan ses som en prioritering af den demokratiske selvbestemmelse på bekostning af præmissen om demokratisk inklusion.

Af den grund mødte lovforslaget også en del kritik for de konsekvenser, det vil have for ytringsfriheden. Særligt det oprindelige lovforslag blev kritiseret,¹²³ hvor en manglende sondring mellem desinformation (bevidst påvirkningsvirksomhed) og misinformation (ubevidst påvirkningsvirksomhed) lader til at have været udslagsgivende. Lovforslaget blev udbedret ved andenbehandling – hvis formulering er den samme som lovændringens.¹²⁴ Trods udbedringer lider loven fortsat af en vag definition af samarbejde – ifølge tænkertanken Justitia, der også anser lovændringen for at være en generel indskrænkning af ytringsfriheden i Danmark.¹²⁵

Ud over de demokratiske implikationer, § 108 kan have, lader det til, at man kan sætte spørgsmålstegn ved lovens afskrækende effekt på fjendtlige statsaktører. Eksempelvis har FE påpeget, at Ruslands påvirkningsagenter fortsat vil forsøge at skævvride den danske offentlige debat trods lovændringen.¹²⁶ Samtidig ser det ud til, at lovens formulering også kan føre til problemer med hensyn til lovens anvendelighed. Eksempelvis kan lovens fokus på

fremmede efterretningstjenester føre til, at lige så potente og aktive aktører overses, såsom statskontrollerede medier og oligarker, der ikke samarbejder med efterretningstjenesterne, men alligevel bedriver påvirkningsvirksomhed.¹²⁷ Dertil kan forbuddets specifikation om bevidst samarbejde medføre, at loven fortsat vil møde problemer vedrørende attribuering og informationspåvirkningens design diskuteret i kapitel 3. Dermed er der en risiko for, at § 108 vil have negative konsekvenser for borgernes legitime demokratiske deltagelse og dermed for Danmarks liberale demokrati.

Dette afsnit har behandlet den danske stats forsøg på at finde balancen i det demokratiske dilemma, som informationspåvirkning skaber. Indsatsen lader til at være kendtegnet ved en decentral struktur, en forsigtighed i forhold til en for dominerende stat i den offentlige debat og et fokus på Rusland. Valghandlingsplanen har givet Danmark ressourcer og kapaciteter til at imødegå informationsoperationer. Ressourcer og kapaciteter, som fremover kan ligge til grund for et solidt og afbalanceret værn om det danske demokrati. Valghandlingsplanens mål var at sikre det danske folketingsvalg i 2019, og der er derfor lagt op til en diskussion om indsatsens fremtid.

Informationspåvirkning vil fortsat være en udfordring for liberale demokratier. Dette skyldes delvist, at de beskrevne forhold i international politik og teknologiske udviklinger fortsat er til stede. Ydermere betyder en maskering i civilsamfundet og manglende transparens på de digitale medier, at informationspåvirkning fortsat er svær at identificere. Dertil er informationsoperationer ikke kun aktive ved valg, men indgår i en langsigtet strategi, der også er aktiv mellem valg. Her har FE i en trusselsvurdering også påpeget informationspåvirkningens fortsatte udfordring, hvor fjendtlige aktører opportunistisk kan udnytte særlige begivenheder.¹²⁸ Dermed er der fortsat et behov for, at Danmark er opmærksom på udfordringen og formulerer en langsigtet politik for at værne om det danske demokrati.

4

Anbefalinger

De foregående kapitler har redegjort for den strategiske udfordring, som Danmark står over for (kapitel 2), og de demokratiske udfordringer, der følger heraf (kapitel 3). Dette kapitel vil bidrage til diskussionen om et fortsat værn om det danske demokrati og den danske offentlige debat og herunder identificere en række anbefalinger, der kan bidrage til balancede tiltag. Anbefalingerne inddeltes i tre niveauer: principielle, ministerielle og myndighedsbårne.

Danmark står relativt stærkere end visse andre lande og har særlige fordele i kampen mod informationspåvirkning. I forhold til de særligt udsatte østeuropæiske lande har Danmark en relativt veluddannet befolkning, relativt kompetente medier og relativt stor social tillid.¹²⁹ Dette er begrænsende faktorer for informationspåvirkningens mål om at forstyrre dialogen mellem civilsamfund og stat. Dertil har Danmark fordelen af at være et lille sprogområde, hvilket øger omkostningerne ved informationsoperationer. For at kunne føre informationsoperationer kræves danske sprogfærdigheder og en vis kulturståelse, hvilket kan påføre for store omkostninger i forhold til udkommet, en sådan informationspåvirkning vil have.

Imidlertid kan det danske medlemskab af Vesten og klubben af liberale demokratier være bidragende årsager til, at særligt Rusland vil rette informationsoperationer mod Danmark. Dertil er informationspåvirkning langvarigt, og selvom informationsoperationer vil være særligt aktive under valg, er der fortsat risiko for opportunistisk udnyttelse af kriser mellem valg. Andre udenrigspolitiske aktører kan også søge at udøve informationsoperationer i Danmark.

Endelig betyder en stigende brug af fremmedsprog i det danske samfund, at Danmark i stigende grad indgår i et mere internationalt sprogområde. Dette betyder flere sproglige indfallsveje til danske borgere og den danske debat. Dermed kan omkostningerne sænkes for fjendtlige udenrigspolitiske aktører, som fremover kunne tænkes at bruge informationspåvirkning over for Danmark.

Dermed vil der fortsat være et behov for en dansk indsats, der går ud over valghandlingsplanen, trods manglende dokumentation for russisk påvirkning af folketingsvalget 2019.

At værne om den offentlige debat og dialogen mellem stat og civilsamfund betyder at værne om demokratiets evne til frit at bearbejde information. Det kræver en bevidsthed om grænserne for statens interaktion med civilsamfundet.

De principielle anbefalinger er derfor:

- Sikre, at den danske stats dialog med civilsamfundet er tydelig, ved at formulere principper herfor. Informationspåvirkning forsøger blandt andet at erodere tilliden mellem civilsamfund og stat. Dette kan sådanne principper modvirke ved at skabe en tillidsvækkende adfærd ved eksempelvis at bygge på transparens, demokratiske værdier, demokratisk inklusion og krav om tydelig, faglig og saglig oplysning.

- Genoverveje formuleringen af straffelovens § 108 vedrørende påvirkningsvirksomhed, og hvorvidt denne overskridt grænserne for statens interaktion med civilsamfundet. For at sikre, at regeringen har et grundlag for sådanne overvejelser, kunne Justitsministeriet bede Ytringsfrihedskommissionen om at evaluere loven med inddragelse af de tre demokratiske præmisser og sikkerhedspolitiske bekymringer forbundet med informationspåvirkning.

At værne mod informationspåvirkning kræver en sammentænkt indsats, der inkluderer både internationale tiltag, støtte til det danske civilsamfund og en styrkelse af de danske borgere.

De ministerielle anbefalinger er derfor:

- Hæve de politiske omkostninger ved brugen af informationspåvirkning. I denne henseende er Danmark afhængig af bred international opbakning og bredt internationalt samarbejde. Derfor kunne den danske stat, via Udenrigsministeriet, spille en aktiv rolle i internationale samarbejder og arbejde for at fremme økonomiske og politiske sanktioner mod udenrigspolitiske aktører, der benytter informationspåvirkning.
 - Bekymringen om informationspåvirkning kan ligeledes indgå i overvejelserne af EU's eksisterende sanktionsregime mod Rusland.
- Begrænse digital informationspåvirkning ved at arbejde for EU-regulering af det digitale marked. Persondataforordningens (GDPR's) globale effekt vidner både om EU's rolle med hensyn til dette marked og EU's potentiale for at begrænse informationsoperationers adgang til og brug af digitale medier og virkemidler. Tager danske beslutningstagere føringen i EU-regi, kan man sikre, at en sådan lovgivning vil lægge vægt på demokratiske rettigheder, digital transparens og individets privativ. Dette kunne gøres, ved at Danmark i Det Europæiske Råd eller danske medlemmer af Europa-Parlamentet støtter op om lovgivning om det digitale marked med udgangspunkt i Code of Practice og GDPR.¹³⁰
- Bevare Danmarks robuste offentlige debat ved at styrke danske mediers rolle i dialogen mellem stat og samfund. Dermed gør den nye strategiske virkelighed sig gældende for både Kulturministeriets mediestøtte og mediernes publicistiske selvforståelse. Her kunne informationspåvirkning indgå i Kulturministeriets overvejelser vedrørende mediestøtten og sikre, at danske medier fortsat kan varetage public service-roller. Hertil kommer mediernes publicistiske selvforståelse, som fremover må tage højde for informationspåvirkning fra udenrigspolitiske aktører ved at prioritere korrekt oplysning og bekämpelsen af misinformation og desinformation.¹³¹
- Styrke borgerne i den offentlige debat ved at prioritere fag omhandlende bearbejdning og indsamling af information på uddannelsesområdet. En prioritering af klassiske færdigheder, der omfatter kildekritik, statistik og argumentationsteknik samt digitale færdigheder, det vil sige forståelse af dynamikker og mekanismer på de digitale medier,¹³² kan styrke borgernes kritiske sans og evne til at modstå informationspåvirkning. Dette kunne særligt Undervisningsministeriet adressere ved at

sikre, at bekendtgørelser og vejledninger rettet mod de gymnasiale ud-dannelser afspejler udfordringen med informationspåvirkning.¹³³ Da forskning viser, at særligt ældre borgere er tilbøjelige til at sprede digital misinformation, kan lignende uddannelsestilbud til disse borgere også overvejes.¹³⁴

At værne om det danske demokrati er en vedvarende opgave, der kræver en vedvarende indsats fra de relevante myndigheder.

De myndighedsbårne anbefalinger er derfor:

- Fastholde efterretningstjenesternes fokus på informationspåvirkning og de bagvedstående udenrigspolitiske aktører, så Danmarks evne til at identificere informationspåvirkning styrkes.
- Fastholde den danske stats fokus på informationspåvirkning ved at styrke den tværministerielle taskforce og mediescreeningsenheden samt videreføre deres funktioner.
- Styrke det danske beredskab på lang sigt ved at samle indsatsen mod informationspåvirkning i én enhed. Dette vil kunne sikre, forankre og styrke Danmarks beredskab med hensyn til og viden om informations-påvirkning samt kunne følge udviklinger inden for området. Her kan en sådan enhed mod informationspåvirkning starte med en femårig testperiode med efterfølgende evaluering og have følgende opgaver:
 - Agere kontaktpunkt for statens kommunikation med civilsam-fundet, i tilfælde af at informationsoperationer rettes mod den danske stat. Her med inspiration fra den svenske Myndigheten för samhällsskydd och beredskap.
 - Bygge offentlig kommunikation i krisesituationer på principper om verificerbarhed og en vis transparens. Erfaringer fra de britiske myndigheders håndtering af Skripal-mordet viste, at hurtig og verificerbar kommunikation er vigtig for at begrænse infor-mationsoperationer i at opbygge momentum og få succes. Dette kan enheden sikre ved at være inkluderende og transpar-ent i sin kommunikation med offentligheden, så danske medier kritisk kan dække identificerede informationsoperationer.
 - Inkludere et varslingsssystem bestående af kontaktpunkter i alle myndigheders kommunikationsafdelinger, herunder også for efterretningstjenesterne, for at sikre hurtig og saglig kommu-nikation om informationsoperationer. Et sådant varslingsssystem kunne med fordel inddrage erfaringer fra EU's Rapid Alert Sy-tem, der fik sin ilddåb ved europaparlamentsvalget i 2019.
 - Fortsætte valghandlingsplanens rådgivning af de politiske par-tier og andre aktører i civilsamfundet om informationspåvirk-ning.
 - Udvikle en håndbog for kommunikatører og udbyde kurser i håndtering af informationspåvirkning til aktører og ansatte i både staten og civilsamfundet.¹³⁵

- Fortsætte samarbejdet med efterretningstjenesterne om at udveksle efterretninger om informationsoperationer og holde enheden opdateret.
- Samarbejde med allierede internationale organisationer, der fokuserer på informationspåvirkning, såsom NATO Strategic Communication Center of Excellence, EU's Hybrid Fusion Cell og East StratCom Task Force.
- Samarbejde med digitale medier såsom Google og Facebook¹³⁶ om at afholde fælles krisøvelser og udvikle offentlige goder, som styrker borgernes position i forhold til informationspåvirkning. Sidstnævnte kunne inkludere udviklingen af digitale redskaber til at identificere informationsoperationer, digitale virkemidler og audiovisuel manipulation, der er offentligt og frit tilgængelige for borgerne.
- Trods de sikkerhedspolitiske og efterretningsmæssige dimensioner kunne en sådan enhed oplagt placeres i Beredskabsstyrelsen, der har erfaring med transparent samfunds-kommunikation og krisekommunikation og er vant til at operere mellem civilsamfund og sikkerhedshensyn.
- Overvejelser om tilsyn bør også indgå i oprettelsen af en sådan enhed. Tilsynet kunne baseres på principper om demokratisk kontrol, tavshedspligt og vægtning af de tre demokratiske præmisser med vægt på borgerens legitime demokratiske deltagelse. I dansk kontekst kunne en sådan tilsynsopgave ligge hos Tilsynet med Efterretningstjenesterne, som allerede fører aktivt tilsyn med de tre efterretningstjenester, der offentliggøres i frit tilgængelige rapporter. Alternativt vil en dansk tilpasning af de svenske *insynsråd* kunne benyttes som model, hvor medlemmer både er folkevalgte og inkluderer repræsentanter fra forsvar og civilsamfund.

I kraft af at være et vestligt, digitalt og liberalt demokratisk samfund er det i Danmarks klare interesse at have en grundlæggende forståelse af både informationspåvirkning i en digital tidsalder og de demokratiske udfordringer, det medfører. Denne rapport har leveret en sådan forståelse af informationspåvirkning i en digital tidsalder og udforsket, hvilke effekter dette kan have for demokratiets funktion, selvbestemmelse og inklusion. At tage de nødvendige forbehold derefter kræver både et fremsyn og en forståelse af den komplekse problemstilling, Danmark står over for.

Noter

- 1 Mueller, Robert S. *Report on the Investigation into Russian Interference in the 2016 Presidential Election*. U.S. department of Justice (March 2019); Select Committee on Intelligence. *Russian Intervention in European Elections*. No. HRG 115-105. The United States Senate. (Washington: June 28 2017); Adam Badawy et al., "Characterizing the 2016 Russian IRA Influence Campaign". (Under udgivelse); Matthew Hindman, and Vlad Barash, *Disinformation, 'Fake News' and Influence Campaigns on Twitter*, John S. and James L. Knight Foundation (4 October 2018); Renee DiResta et al., *The Tactics & Tropes of the Internet Research Agency*, Knew Knowledge (1 December 2018).
- 2 Ud over påvirkningsforsøgene i forbindelse med det amerikanske valg har der også været indikationer på lignende påvirkningsforsøg i Storbritannien se Digital, Culture, Media and Sport Committee. *Disinformation and 'Fake News': Final Report*. House of Commons, UK (14 February 2019) Men også i forbindelse med andre europæiske valg: Select Committee on Intelligence, *Russian Targeting of Election Infrastructure During the 2016 Election: Summary of Initial Findings and Recommendations*. The United States Senate. (Washington: 8 May 2018); Committee on Foreign Relations. *Putin's Asymmetric Assault on Democracy in Russia and Europe: Implications for U.S. National Security*. The United States Senate, (Washington: 10 January 2018).; Laura Galante and E. E Shaun. "Defining Russian Election Interference: An Analysis of Select 2014 to 2018 Cyber Enabled Incidents". (11 September 2018) ; Philip N. Howard et al., *Junk News and Bots During the French Presidential Election: What Are French Voters Sharing Over Twitter?*, Oxford Internet Institute (22 April 2017); Jean-Baptiste Jeangène Vilmer. "Successfully Counteracting Russian Electoral Interference – 15 Lessons Learned from the Macron Leaks". *CSIS Briefs* (June 2018).
- 3 Garrett M. Graff, "A guide to Russias high tech tool box for subverting US democracy," *Wired*, (13 September 2017); Richard Shultz and Roy Godson, *Dezinformatsia. Active Measures in Soviet Strategy*. United States of America Pergamon. (New York: 1984) Begrebet bruges også i James Pamment et al., *Countering Information Influence Activities The State of the Art*, Department of Strategic Communication, Lund University & MSB (1 July 2018).
- 4 Jens Beck Nielsen, "Hjort slog alarm – men Forsvaret har ikke fundet ét eneste eksempel på russisk påvirkning af valget," *Berlingske* (5. juni 2019).
- 5 European Commission, *Report on the implementation of the Action Plan Against Disinformation*, High Representative of the Union for Foreign Affairs and Security Policy (Brussels: 14 June 2019).
- 6 Eksempler er kejser Augustus' smudskastning på Markus Antonius: L. Powell and K. Galinsky, *Augustus at War : The Struggle for the Pax Augusta*. (Great Britain Pen & Sword Military, 2016) Andre eksempler er fra førsteverdenskrig hvor de europæiske stormagter brugte propaganda til rekruttere USA til deres

respektive side Ian F. W. Beckett, *The Making of the First World War*. Yale University Press. (JSTOR, www.jstor.org/stable/j.ctt32bpn0: 2012)

- 7 Robert M. Entman, "Media framing biases and political power: Explaining slant in news of Campaign 2008." *Journalism: Theory, Practice & Criticism* 11, no. 4 (2010): 389-408 (2010).
- 8 Forsvarets Efterretningstjeneste, *Efterretningsmæssig Risikovurdering 2018* (2018). Politiets Efterretningstjeneste, "Årlig redegørelse 2017," (2018).
- 9 Indflydelsessfærer: Dette drejer sig primært om de postsovjetiske lande: Keir Giles et al., *The Russian Challenge*, The Royal Institute of International Affairs (2015); Mette Skak, "Russias new Monroe Doctrine," in *Russias foreign policy in the 21st Century*, ed. Roger E. Kanet Palgrave MacMillan (2011). Se i øvrigt: Mike Winnerstig et al., *Tools of Destabilization Russian Soft Power and Non-military Influence in the Baltic States*, Försvarsanalys, Swedish Defence Ministry (2014); Edward Lucas and Peter Pomeranzev, *Winning the Information War: Techniques and Counter-Strategies in Russian Propaganda*, Center for European Policy Analysis (Washington DC: August 2016); Ivana Smolenová et al., *United We Stand, Divided We Fall: The Kremlin's Leverage in the Visegrad Countries*. Prague Security Studies Institute (November 2017); Jonáš Syrovatka et al., *Information Warfare in the Internet – Countering Pro-Kremlin Disinformation in the Cee Countries*. Centre For International Relations & Partners (2017).
- 10 Peter Pomerantsev et al., *Information at War: From China's Three Warfares to NATO's Nartives*, Legatum Institute (2015); Jeanne L. Wilson, "Russia and China Respond to Soft Power: Interpretation and Readaptation of a Western Construct," *Politics* 35, no. 3-4 (2015); X. Qiang, "The Rise Of China As A Digital Totalitarian State.,," *New Perspectives Quarterly* 35, no. 2 (2018); Karrie J. Koesel and Valerie J. Bunce, "Diffusion-Proofing: Russian and Chinese Responses to Waves of Popular Mobilizations against Authoritarian Rulers," *Perspectives on Politics*, 11, no. 3 (2013).
- 11 Jack Watling, *Iran's Objectives and Capabilities Deterrence and Subversion*, Royal United Services Institute (2019); Kanishk Karan et. al. "TrollTracker: Outward Influence Operation From Iran," *Medium* (31. January 2019). Andre lande, som kan nævnes, er Saudi-Arabien, se Donara Barojan, "BotSpot: Journalist's Death Followed by Fake Accounts," *Medium* (25 October 2018); John Watts, *Whose Truth? Sovereignty, Disinformation, and Winning the Battle of Trust*, Atlantic Council (September 2018), Blandt ikke-statslige aktører kan terrororganisationen Islamisk Stat nævnes se Charlie Winter *The Virtual 'Caliphate': Understanding Islamic State's Propaganda Strategy*, NATO Stratcom COE (July 2015).
- 12 Kier Giles. *Countering Russian Information Operations in the Age of Social Media*. Council on Foreign Relations (21. November 2017).; V. S. Ovchinsky, E. S. Larina, and S.A. Kulik, *Russia and the Challenges of the Digital Environment*, Russian International Affairs Council (2014); H. Akin Unver, "Digital Challenges to Democracy: Politics of automation, attention and engagement.,," *Journal of International Affairs* 71, no. 1 (2017); Koesel and Bunce, "Diffusion-Proofing: Russian and Chinese Responses to Waves of Popular Mobilizations against Authoritarian Rulers."; Regina Smyth and Sarah

Oates, "Mind the Gaps: Media Use and Mass Action in Russia," *Europe-Asia Studies* 67, no. 2 (2015).

- 13 Joanna Szostek, "The Power and Limits of Russia's Strategic Narrative in Ukraine: The Role of Linkage," *Perspectives on Politics* 15, no. 02 (2017);; Laura Roselle, Alister Miskimmon, and Ben O'Loughlin, "Strategic narrative: A new means to understand soft power," *Media, War & Conflict* 7, no. 1 (2014).
- 14 Lili Bayer et al., *Responding to Cognitive Security Challenges*. NATO Stratcom COE (2019).
- 15 Arch Puddington, *Breaking Down Democracy: Goals, Strategies, and Methods of Modern Authoritarians*. Freedom House (June 2017).
- 16 Justitsministeriet, "Styrket værn mod udenlandsk påvirkning af danske valg og demokratiet". Pressemeldelse , (7. september 2018).
- 17 Richard Shultz' og Roy Godsons studier viser, at sovjetisk informationspåvirkning af den amerikanske offentlighed var aktiv i mere end 20 år. Se Richard Shultz and Roy Godson, *Dezinformatsia- Active Measures in Soviet Strategy* (1984). Ligeledes indikerer nyere studier, at denne tidshorisont ikke er blevet mindre i en digital tidsalder, se Andres Dawson and Martin Innes, *The Internet Research Agency in Europe 2014-2016*. Cardiff University, Crime and Security Research Institute (May 2019).
- 18 Se videre om gråzonekonflikter i André Ken Jakobsson, *Når Hydra angriber – Hybrid afskrækkelser i gråzonens mellem krig og fred*, Center for Militære Studier, Københavns Universitet (oktober 2019).
- 19 Kapitel 3 i Henrik Ø. Breitenbauch et al., *Orden og afskrækkelser – Vestens håndtering af Rusland efter annekteringen af Krim*, Center for Militære Studier, Københavns Universitet (juni 2017).
- 20 von Clausewitz, Carl. *On War*. Translated by Michael Howard and Peter Paret. Oxford University Press, (Oxford: 2007), s. 28-29
- 21 Bobo Lo, "Two Worlds" in *Russia and the New World Disorder* Brookings Institution Press (Washington D.C: 2015).
- 22 Skak, "Russias new Monroe Doctrine.", Keir Giles et al., *The Russian Challenge*.
- 23 Rand Waltzman *The Weaponization of Information The Need for Cognitive Security*, Senate Armed Services Committee (27. April 2017). s. 4
- 24 Steve Abrams, "Beyond Propaganda: Soviet Active Measures in Putin's Russia." *Connections: The Quarterly Journal* 15, no. 1 (2016): 5-31; Kier Giles, *Handbook of Russian Information Warfare*, NATO Defense College (Rome: NATO, November 2016); Shultz and Godson, *Dezinformatsia. Active Measures in Soviet Strategy*. Katri Pynnöniemi and András Rácz, *Fog of Falsehoods – Russian Strategy of Deception and the Conflict in Ukraine*, The Finnish Institute of International Affairs (Helsinki, Finland: 2016). Can Kasapoglu, "Russia's Renewed Military Thinking: Non-Linear Warfare and Reflexive Control," *NATO Defense College, Research*, 121 (25 November 2015).
- 25 Kapitel 2 i Pynnöniemi and Rácz, *Fog of Falsehoods – Russian Strategy of Deception and the Conflict in Ukraine*. Vladim Kononenko and Arkady

Moshes, *Russia as a Network State: What Works in Russia When State Institutions Do Not*, Palgrave Macmillan (London: 2011). Olesya Zakharova, "Vladimir Putin Loves Civil Society (As Long As He Controls It)," *Foreign Policy*, (12. October, 2016). Koesel and Bunce, "Diffusion-Proofing: Russian and Chinese Responses to Waves of Popular Mobilizations against Authoritarian Rulers." Andrei Soldatov and Irina Borogan, *The Red Web: The Struggle Between Russia's Digital Dictators and the New Online Revolutionaries*, Public Affairs (New York, N.Y.: 2015).

- 26 Her tænkes særligt på den anden tjetjenske krig i 1999, se Keir Giles, *Russia's 'New' Tools for Confronting the West*. Chatham House The Royal Institute of International Affairs (March 2016); The Russian Federation, Doctrine of Information Security of the Russian Federation, 646 (2016). Gennem 00'erne forsøgte de russiske efterretningstjenester at kontrollere russiske internetudbydere og myndigheder ansvarlige for telekommunikation, se Mark Galeotti, *Putin's Hydra: Inside Russia's Intelligence Services*. (11 May 2016); Joshua Yaffa, "The Double Sting", *The New Yorker* (27 July 2015); Gordon Bennett, *FPS & FAPSI – RIP*, Conflict Studies Research Centre (17. March 2003).
- 27 Overblik over den teoretiske diskussion kan findes i Natalya Kovaleva, "Russian Information Space, Russian Scholarship, and Kremlin Controls". *Defence Strategic Communications* 4 (2018)..
- 28 § 1, kaldet Information Sphere, se Vladimir Putin, "Information Security Doctrine of the Russian Federation Approved by President of the Russian Federation" (2000).
- 29 Sergey Sanovich, *Computational Propaganda in Russia: The Origins of Digital Misinformation*, Oxford University Computational Propaganda Project. (2017).
- 30 BBC News, "Moscow protest: Thousands rally against Vladimir Putin," *BBC*, (25 December 2011); BBC News, "Russian election: Biggest protests since fall of USSR " (10 December 2011). Stephen White and Ian McAllister, "Did Russia (Nearly) have a Facebook Revolution in 2011? Social Media's Challenge to Authoritarianism," *Politics* 34, no. 1 (2013); Koesel and Bunce, "Diffusion-Proofing: Russian and Chinese Responses to Waves of Popular Mobilizations against Authoritarian Rulers."
- 31 Vladimir Putins beskrivelse af sin autokratiske styreform, for gennemgang, se Puddington, *Breaking Down Democracy: Goals, Strategies, and Methods of Modern Authoritarians*. Kapitel 7
- 32 Roselle, Miskimmon, and O'Loughlin, "Strategic narrative: A new means to understand soft power."
- 33 Ben Nimmo har identificeret en række strategier brugt af Kreml: Dismiss (benægte alle anklager), Distort (forstyrre og mudre tilgængelig information), Distract (ligesom whataboutism drages ofte falske sammenligninger for at lede opmærksomheden væk fra Kreml, ofte med brugen af konspirationsteorier) og Dismay (true og skræmme modstandere fra specifik handling), se Ben Nimmo, "Anatomy of an Info-War: How Russia's Propaganda Machine Works, and How to Counter It," *StopFake*, 19 May 2015.

- 34 Peter Pomerantsev and Michael Weiss, *The Menace of Unreality: How the Kremlin Weaponizes Information, Culture and Money*, The Institute of Modern Russia & The Interpreter (New York: 2014); Winnerstig et al., *Tools of Destabilization Russian Soft Power and Non-military Influence in the Baltic States*. Smolenčová et al., *United We Stand, Divided We Fall: The Kremlin's Leverage in the Visegrad Countries*.
- 35 Waltzman, *The Weaponization of Information The Need for Cognitive Security*.
- 36 Kragh and Åsberg, "Russia's strategy for influence through public diplomacy and active measures: the Swedish case."
- 37 Bayer et al., *Responding to Cognitive Security Challenges*; Carole Cadwalladr, "I made Steve Bannon's psychological warfare tool': meet the data war whistleblower," *The Guardian*, (18 March 2018).
- 38 For en grundig diskussion af de epistemologiske problemer ved denne tankegang kan findes i Joseph E. Uscinski and Ryden W. Butler, "The Epistemology of Fact Checking," *Critical Review* 25, no. 2 (2013).
- 39 Robert Chesney and Danielle Citron, "Deepfakes and the New Disinformation War The Coming Age of Post-Truth Geopolitics," (11 December 2018).
- 40 Lily Hay Newman. "A New Tool Protects Videos from Deepfakes and Tampering". *Wired*, (11 February 2019); W. Knight, The Defense Department Has Produced the First Tools for Catching Deepfakes". *MIT Technology Review*. (7 August 2018).
- 41 Pomerantsev et al., *Information at War: From China's Three Warfares to NATO's Narratives*; Syrovatka et al., *Information warfare in the Internet – countering pro-kremlin disinformation in the CEE Countries*; Pomerantsev and Weiss, *The Menace of Unreality: How the Kremlin Weaponizes Information, Culture and Money*; Lange-Ionatamishvili, *Redefining Euro-Atlantic Values: Russias Manipulative Techniques*, NATO StratCom Center of Excellence (2017); Kragh and Åsberg, "Russia's strategy for influence through public diplomacy and active measures: the Swedish case." ; Lange-Ionatamishvili et al., *Russias Footprint in the Nordic-Baltic Informations Environment*, NATO StratCom Centre of Excellence (Riga: January 2018); Smolenčová et al., *United We Stand, Divided We Fall: The Kremlin's Leverage in the Visegrad Countries.*; Lucas and Pomeranzev, *Winning the Information War: Techniques and Counter-Strategies in Russian Propaganda*. Gordon Ramsay and Sam Robertshaw, *Weaponising news: RT, Sputnik and targeted disinformation*, Communication & Power Centre for the Study of Media, King's College London (London: January 2019).
- 42 Ben Nimmo, Donara Barojan, and Nika Aleksejeva, Russian Narratives on NATO's Deployment, *Medium* (1 April 2017); James Headley, "Challenging the EU's claim to moral authority: Russian talk of 'double standards'," *Asia European Journal* 13, no. 3 (2015); Christopher Walker et al., *Sharp Power – Rising Authoritarian Influence*, National Endowment for Democracy (5 December 2017); Syrovatka et al., *Information warfare in the Internet – countering pro-kremlin disinformation in the CEE Countries*.

- 43 Ben Nimmo, Donara Barojan, and Nika Aleksejeva, *Russian Narratives on NATO's Deployment*; Aleksander Król, "Russian Information Warfare in the Baltic States". *The Warsaw Intitute Review*, (20 July 2017)
- 44 Digital, Culture, Media and Sport Committee, House of commons UK, *Disinformation and 'fake news': Final Report*.
- 45 Pomerantsev et al., *Information at War: From China's Three Warfares to NATO's Nartives*; Syrovatka et al., *Information warfare in the Internet – countering pro-kremlin disinformation in the CEE Countries*; Jakub Janda and Ondřej Kundra, *Mechanisms of Influence of the Russian Federation into Internal Affairs of the Czech Republic*; Pomerantsev and Weiss, *The Menace of Unreality: How the Kremlin Weaponizes Information, Culture and Money*; Avaaz, *Yellow Vests Flooded by Fake News*. Avaaz (12 March 2019); Hindman & Barash , *Disinformation, 'Fake News' and Influence Campaigns on Twitter*. John S. and James L. Knight Foundation (4 October 2018); Pomerantsev and Weiss, *The Menace of Unreality: How the Kremlin Weaponizes Information, Culture and Money*. Smolenová et al., *United We Stand, Divided We Fall: The Kremlin's Leverage in the Visegrad Countries*; Ramsay and Robertshaw, *Weaponising news: RT, Sputnik and targeted disinformation*.
- 46 Mueller, Robert S."Indictment: United States of America v. Internet Research Agency" Case 1:18-cr-00215-ABJ. Special Council and U.S. Department of Justice. (13 July 2018).
- 47 Pamment et al., *Countering Information Influence Activities The State of the Art*.
- 48 Forsvarets Efterretningstjeneste, *Efterretningsmæssig Risikovurdering 2018*.
- 49 Kucharczyk i Walker et al., *Sharp Power – Rising Authoritarian Influence*.
- 50 Ramsay and Robertshaw, *Weaponising news: RT, Sputnik and targeted disinformation*.
- 51 Headley, "Challenging the EU's claim to moral authority: Russian talk of 'double standards'."; Vincent Charles Keating and Katarzyna Kaczmarska, "Conservative soft power: liberal soft power bias and the 'hidden' attraction of Russia," *Journal of International Relations and Development* (May 2017); Yulia Kiseleva, "Russia's Soft Power Discourse: Identity, Status and the Attraction of Power," *Politics* 35, no. 3-4 (2015).
- 52 Der skal forstås som irrationel angst eller had til alt russisk med stærke racistiske undertoner.
- 53 Sputnik, "Russia Releases Big 120-Page Report on Russophobia, Russiagate Hysteria in US", (20 April 2019); Den russiske rapports påstande modbevises i Ben Nimmo, *Russian Interference: The Evidence*, Medium (25 April 2019).
- 54 M. Vanin, "Statement by H.E. Ambassador of the Russian Federation to the Kingdom of Denmark Mr. M.Vanin," Pressemeldelse, (24 Juli 2018).
- 55 Cherilyn Ireton and Julie Posetti, *Journalism, fake news & disinformation: handbook for journalism education and training* (Paris: United Nations Educational, Scientific and Cultural Organization, 2018); Todd C. Helmus et

al., *Russian Social Media Influence Understanding Russian Propaganda in Eastern Europe*, RAND (2018).

- 56 Orygia Lutsevych, *Agents of the Russian World Proxy Groups in the Contested Neighbourhood*, Chatham House, The Royal Institute of International Affairs (London: 2016).
- 57 Lutsevych, *Agents of the Russian World Proxy Groups in the Contested Neighbourhood*; Winnerstig et al., *Tools of Destabilization Russian Soft Power and Non-military Influence in the Baltic States*; Smolenová, *The Pro-Russian Disinformation Campaign in the Czech Republic and Slovakia Types of Media Spreading Pro-Russian Propaganda, Their Characteristics and Frequently Used Narratives*. Prague Security Studies Institute (June 2015).; Pomerantsev and Weiss, *The Menace of Unreality: How the Kremlin Weaponizes Information, Culture and Money*. Helmus et al., *Russian Social Media Influence Understanding Russian Propaganda in Eastern Europe*.
- 58 Galeotti, *Putin's Hydra: Inside Russia's Intelligence Services*.
- 59 Estonian Internal Security Service, *Security Police of the Republic of Estonia Annual Review 2008* (Tallinn: 2008); Winnerstig et al., *Tools of Destabilization Russian Soft Power and Non-military Influence in the Baltic States*. Lucas and Pomeranzev, *Winning the Information War: Techniques and Counter-Strategies in Russian Propaganda*.
- 60 Smolenová et al., *United We Stand, Divided We Fall: The Kremlin's Leverage in the Visegrad Countries*.
- 61 Buklah et. al. i Winnerstig et al., *Tools of Destabilization Russian Soft Power and Non-military Influence in the Baltic States*.
- 62 For seneste grundige analyse, se Ramsay and Robertshaw, *Weaponising news: RT, Sputnik and targeted disinformation*.
- 63 Nimmo, "Anatomy of an Info-War: How Russia's Propaganda Machine Works, and How to Counter It"; Hindman & Barash, *Disinformation, 'Fake News' and Influence Campaigns on Twitter*; Andrew Foxhall, *Putin's Useful Idiots: Britain's Left, Right and Russia* Russia Studies Centre at The Henry Jackson Society (London: 2016); Kragh and Åsberg, "Russia's strategy for influence through public diplomacy and active measures: the Swedish case."; Pynnoniemi and Rácz, *Fog of Falsehoods – Russian Strategy of Deception and the Conflict in Ukraine*; Helmus et al., *Russian Social Media Influence Understanding Russian Propaganda in Eastern Europe*.
- 64 Hermann, "The nine links in the Chain: the weaponized narrative, Sun Tzu, and the Essence of War." *The Strategy Bridge*, (27 July 2017); Vincent Hendricks and Pelle G. Hansen, *Infostorms – How to take information punches and save democracy*. Springer (New York: 2014); J.G. Webster, "User Information Regimes: How Social Media Shape Patterns of Consumptions." *North Western University Law Review* 104, no. 2 (2010): 593-612. Waltzman, *The Weaponization of Information The Need for Cognitive Security*.
- 65 Radek Tadajewski, "Hybrid War" (presentation at the NATO StratCom COE: "Emerging Trends in Social Media", (Riga, 25 March 2018). Andrew Dawson and Martin Innes, "How Russia's Internet Research Agency Built its Disinformation Campaign," *The Political Quarterly* (6 Maj 2019); Helmus et

- al., *Russian Social Media Influence Understanding Russian Propaganda in Eastern Europe*; Samantha Bradshaw and Philip N. Howard, *Troops, Trolls and Troublemakers: A Global Inventory of Organized Social Media Manipulation*, Computational Propaganda Research Project (2017).
- 66 Bradshaw and Howard, *Troops, Trolls and Troublemakers: A Global Inventory of Organized Social Media Manipulation*; Lee Rainie, Janna Anderson, and Jonathan Albright, *The Future of Free Speech, Trolls, Anonymity and Fake News Online*, Pew Research Center (March 2017).
- 67 Vladimir Barash and John Kelly, *Salience vs. Commitment Dynamics of Political Hashtags in Russian Twitter*, The Berkman Center for Internet & Society Research (Harvard University: 2012); Emilio Ferrara et al., "The Rise of Social Bots," *Communications of the ACM* 59, no. 7 (2016); Marco T. Bastos and Dan Mercea, "The Brexit Botnet and User-Generated Hyperpartisan News." *Social Science Computer Review* 37, no. 1 (2017): 38-54.
- 68 Ferrara et al., "The Rise of Social Bots."; Robert Gorwa and Douglas Guilbeault, "Understanding Bots for Policy and Research: Challenges, Methods, and Solutions," Presented at ICA 2018. (21 January 2018).
- 69 NATO StratCom Center of Excellence, *The Black Market for Social Media Manipulation*. (Riga, 2018).
- 70 Jürgen Habermas, *Between Facts and Norms: Contributions to a Discourse Theory of Law and Democracy*, Polity Press (Cambridge: 1995).
- 71 David Easton, *A Systems Analysis of Political Life* (New York: John Wiley, 1965);
- 72 Barry Buzan and George Lawson, "Capitalism and the emergent world order," *International Affairs* 90, no. 1 (2014).
- 73 Kenneth Newton, "Trust, Social Capital, Civil Society, and Democracy.," *International Political Science Review* 22, no. 2 (2001).
- 74 Aric Toler, "The Weird World of MH17 Conspiracy Theories," *Bellingcat* (August 7, 2015); Alya Shandra, "The most comprehensive guide ever to MH17 conspiracies," *Stopfake.org* (July 18 2016).
- 75 Ifølge Kenneth Newton er tillid til myndigheder afhængigt af tredjeparter, hvilket gør medier og autoriteter i civilsamfundet (såsom tænketanke) vigtige for statens interaktion med borgerne. Newton, "Trust, Social Capital, Civil Society, and Democracy".
- 76 Hendricks and Hansen, *Infostorms – How to take information punches and save democracy*.
- 77 Daniel Kahneman, Paul Slovic, and Amos. Tversky, *Judgment under Uncertainty, Heuristics and Biases*, Cambridge University (Cambridge: Press., 1982); Hajo Boomgaarden, "Interpersonal and mass mediated political communication," in *Political Communication*, ed. Carsten Reinemann De Gruyter (Berlin: 2014).
- 78 Dette inkluderer præ-eksisterende holdninger eller gruppertilhørsforhold for at afgøre troværdigheden af politiske budskaber. Kahneman, Slovic, and Tversky, *Judgment under Uncertainty, Heuristics and Biases*.

- 79 Arthur Lupia, "Shortcuts versus Encyclopedias: Information and Voting Behavior in California Insurance Reform Elections", *The American Political Science Review* 88, no. 1 (1994); Elihu Katz and Paul F. Glencoe Lazarsfeld, *Personal Influence*, The Free Press (Glencoe Illinoise: 1955).
- 80 Nic Newman et al., *Reuters Institute Digital News Report 2018*, Reuters Institute for the Study of Journalism (2018).; Lisbeth Knudsen, *Globalisering af den danske mediebranche*, Slots og Kulturstyrelsen (2017).
- 81 Hvilket fører til det, Ramsay og Robertshaw beskriver som "churnalism". Ramsay and Robertshaw, *Weaponising news: RT, Sputnik and targeted disinformation; Watts, Whose Truth? Sovereignty, Disinformation, and Winning the Battle of Trust.*
- 82 Ifølge Reuters Institut for Study of Journalism er tilliden til medier i vestlige lande på 44 %. Newman et al., *Reuters Institute Digital News Report 2018*. Dog udskiller danske institutioner og medier sig ved at nyde en relativt stor folkelig opbakning, se Ida Willig et al., *Journalistiske kvaliteter 1999-2014*, Kulturstyrelsen (2015)
- 83 J. A. Schumpeter, *Capitalism, Socialism and Democracy*. Unwin University Books., (London:1974); E. E. Schattschneider, *The Semisovereign People: a Realist's View of Democracy in America* (Chicago: Holt, Rinehart & Winston, 1983)
- 84 Robert A. Dahl, *Democracy and Its Critics*. (New Haven:: Yale University Press, 1989).
- 85 Artikel 21, stk. 3, se "Universal Declaration of Human Rights," United Nations (1948).
- 86 Winnerstig et al., *Tools of Destabilization Russian Soft Power and Non-military Influence in the Baltic States*; Pomerantsev & Weiss, *The Menace of Unreality: How the Kremlin Weaponizes Information, Culture and Money*.
- 87 Digital, Culture, Media and Sport Committee, *Disinformation and 'fake news': Interim Report*, House of Commons (4 juli 2017). S. Mueller, *Report On The Investigation Into Russian Interference In The 2016 Presidential Election*.
- 88 Mueller, "Indictment: United States of America v. Internet Research Agency".; Vilmer, "Successfully Countering Russian Electoral Interference – 15 Lessons Learned from the Macron Leaks".; Marine Guillaume, *Combating the Manipulation of Information – a French Case*. Hybrid CoE (2019).
- 89 Bret Schaffer, *A view from the Digital Trenches – Lessons from Year One of Hamilton*. 68, Alliance for Securing Democracy (2018).
- 90 "Enhver er berettiget til på tryk, i skrift og tale at offentliggøre sine tanker, dog under ansvar for domstolene. Censur og andre forebyggende forholdsregler kan ingensinde påny indføres". Se grundlovens § 77.
- 91 Pamment et al., *Countering Information Influence Activities The State of the Art*.
- 92 At tage patent på sandheden og bruge den politisk har altid været benyttet af totalitære styrer. Hannah Arendt, *Origins of Totalitarianism*, World Publishing Company (Cleveland and NY: 1962).

- 93 Ifølge Joseph Uscinski og Ryden Butlers studie af faktatjekkende procedurer, hvor særligt problemer med nuanceforskelle, afhængighed af eksisterende viiden og mål af sociale fænomener gør sig gældende. Uscinski and Butler, "The Epistemology of Fact Checking."
- 94 Årsagen var blandt andet, at man havde citeret den russiske producent af den type missil, der skød det malaysiske passagerfly MH-17 ned i 2014. Men også, at man havde spurgt ind til fascistiske bevægelser i Ukraine. Daniel Funke, "Three publications are suing the EU over fake news allegations," *Poynter* (2018).
- 95 Justitsministeriet, "Styrket værn mod udenlandsk påvirkning af danske valg og demokratiet."
- 96 Eksempelvis er Udenrigsministeriet kontaktpunkt for EU's *Rapid Alert System* et europæisk netværk af ansvarlige myndigheder, se European Commission, "Action Plan against Disinformation," news release, (5 december, 2018). Der til er Forsvarsministeriet et kontaktpunkt for NorDef og Northern Group. For et overblik over danske militære samarbejdspartnere, se Henrik Ø. Breitenbauch et al., *Options for Enhancing Nordic-Baltic Defence and Security Cooperation An Explorative Survey*, Centre for Military Studies, Copenhagen University (May 2017).
- 97 Begrebet bruges i valghandlingsplanen og lader til at referere til mere end blot den strategiske brug af information. Justitsministeriet, "Styrket værn mod udenlandsk påvirkning af danske valg og demokratiet."
- 98 PET fik 43 mio. kroner årligt frem til 2022 i finansloven for 2018, Finansministeriet, "Forslag til finanslov for finansåret 2019," (2018). Både PET og FE fik fra foråret 2018 tildelt flere ressourcer som del af den nationale strategi for cyber- og informationssikkerhed, der imidlertid har et større fokus på cybersikkerhed end på informationspåvirkning. Regeringen, "National strategi for cyber- og informationssikkerhed," (15. maj).
- 99 Enheden består af tre fuldtidsansatte og en studentermedhjælper.
- 100 Rebecca Adler-Nissen, Frederik Hjort, and Yevgeniy Golovchenko, "Digital misinformation: Hvordan virker det egentlig?," *Puzzle Piece* nr. 6, Oktober, PIA – Political Ideas and Analysis (2018). s. 8
- 101 Aktivitet forstået som likes, shares, kommentarer osv.
- 102 Lisbeth Knudsen, *Globalisering af den danske mediebranche*.
- 103 Mark Zuckerberg "A Privacy-Focused Vision for Social Networking". News release, (6 March 2019), <https://www.facebook.com/notes/mark-zuckerberg/a-privacy-focused-vision-for-social-networking/10156700570096634/>.
- 104 Nina Angelovska, "Facebook Losing Users To Pinterest, Youtube And Twitter (Market Share By Region)," *Forbes* (7 Januar 2019); Pew Research Center, "Teens, Social Media & Technology 2018," (2018); Lisbeth Knudsen, *Globalisering af den danske mediebranche*.
- 105 European Commission, "Action Plan against Disinformation," news release, (5 December, 2018).

- 106 Marianne Fajstrup. "FE: Straf til påvirkningsagenter kan ikke stoppe Rusland," *Berlingske*. (9. december 2018); Marianne Fajstrup, "FE-chef: Sådan kæmper vi imod Ruslands troldehær," *Berlingske* (10. december, 2018); Jesper Kongstad, "Dansk spionchef skærper tonen over for Putin og truslerne fra Rusland," *Jyllands-Posten* (5. december 2018); Marianne Fajstrup "FE: Påvirkningskampagner er en gråzone". *Berlingske*. (10. december 2018)..
- 107 Selvom tillid forudsætter en grad af uvidenhed, mener Kenneth Newton, at adgang til oplysninger og transparens er tillidsskabende, da det sænker potentiel usikkerhed i samarbejdet. Newton, "Social and Political Trust in Established Democracies." In *Critical Citizens*, edited by Pippa Norris, 169-87: (Oxford University Press, 1999)
- 108 European Commission, "EU Code of Practice on Disinformation." News release (26 September 2018).
- 109 Dette inkluderer i) indførelsen af policies og processer, der begrænser det økonomiske incitamentet i forbindelse med spredning af misrepræsenterende information, ii) at styrke transparensen af politisk reklame og udvælgelsen af publikum, iii) at styrke integriteten af det digitale økosystem ved at identificere bots og fjerne desinformationsspredende bots, iv) at styrke brugernes kildekritiske sans gennem udvikling af digitale redskaber, prioritere relevant information i feeds og søgeresultater samt samarbejde med faktatjekkende institutioner, og v) at styrke forskningsmiljøet omkring desinformation.
- 110 Aftalen var i tråd med Kommissionens princip om selv- og medregulering. European Commission "*The Principles for better self- and co-regulation*" (2018).
- 111 Emily Taylor, Stacie Walsh, and Samantha Bradshaw. *Industry Responses to the Malicious Use of Social Media*. NATO StratCom CoE (November 2018) s.8 & 14.
- 112 Sam Levin, "'They don't care': Facebook factchecking in disarray as journalists push to cut ties", *The Guardian* (13 December 2018).
- 113 European Commission, "Code of Practice against disinformation: Commission calls on signatories to intensify their efforts " news release, 29 January, 2019. Senere rapporter var mere milde i deres kritik, men engagementet har fortsat manglet. Se European Commission, *Report on the implementation of the Action Plan Against Disinformation*, High Representative of the Union for Foreign Affairs and Security Policy (Brussels: 14 June 2019).
- 114 Forsvarets Efterretningstjeneste, "Rådgivning om cyberangreb og trusler til partierne forud for valget," pressemeldelse, (20. februar, 2019).
- 115 Pia Kjærsgaard, "Pia Kjærsgaard: Pressen og politikerne må danne fælles værn mod falske nyheder," *Altinget* (3. januar 2019).
- 116 US Senate Select Committee on Intelligence. *Russian Targeting of Election Infrastructure During the 2016 Election: Summary of Initial Findings and Recommendations*. The United States Senate. (Washington: 8 May 2018).
- 117 Selve stemmeafgivelsen foregår stadig analogt, med pen og papir.
- 118 Man vil eksempelvis sammenkøre procedurer vedrørende opstillingslister, kandidatlister og indsamling af navne og cpr-numre i et fælles system. Dog vil produktionen af stemmesedler fortsat foregå separat. KOMBIT, "VALG sender

udbudsmateriale til print af valgkort i høring hos leverandører”, (17. april 2019).

- 119 KOMBIT, ”Projekt VALG afholder workshops ”, (14. december 2016).
- 120 Straffeloven, § 108, stk. 1.
- 121 Folketinget. ”Vedtaget af Folketinget ved 3. behandling den 19. marts 2019. Forslag til lov om ændring af straffeloven (ulovlig påvirkningsvirksomhed)”. Folketingstidende, tillæg C, (2019).
- 122 § 108 har kun været relevant for videregivelse af information to gange før, ved Arne Herløv Petersen-sagen, se Heiberg Morten, *KGB'S Kontakt og Agentnet i Danmark*, Justitsministeriet (Juni 2009), og ved sagen om professor Timo Kiwimäki, se Søren Astrup and Bo Maltesen, ”Professor får fem måneders fængsel for spionage,” *Politiken* (31. maj 2012). I lovforslagets bestemmelser fremlægges derfor argumenter om en usikkerhed i den juridiske litteratur.
- 123 Kritikken gik blandt andet på en indskrænkning af grundlovens § 77, på uforholdsmæssig straf, på at give staten for vide beføjelser og på for vagt formuleringer, der underminerede retssikkerheden. Justitsministeriet ”Forslag til lov om ændring af straffeloven (ulovlig påvirkningsvirksomhed)”, (13. september 2018). For kritik, se Ulrik Dahlin, ”Nyt lovforslag fra Pape skaber ‘kolossal retsuzsikkerhed’, mener kritikere,” *Dagbladet Information* (10. oktober 2018); Ole Hasselbalch, Bjørn Elmquist, and Ole Stig Andersen, ”Juraprofessor, forsvarsadvokat og tidl. PET-chef i fælles opråb: Regeringens forslag om ændring af straffelovens § 108 presser ytringsfriheden,” *Politiken* (21. februar 2019); Justitia, *Bemærkninger til udkast til forslag til lov om ændring af straffeloven (ulovlig påvirkningsvirksomhed)*. (2019); Beck Nielsen, Jens, and Jens Anton Bjørnager. ”Nul eksempler fra regeringen på russisk påvirkning”. *Berlingske*. (24. november 2018).; Aia Fog, ”Regeringens nye påvirkningslov er en glidebane mod det totalitære,” *Trykkefrihed.dk* (15. februar 2019); Jonas Stenbæk Christoffersen and Jens Beck Nielsen, ”Dansk Folkeparti vil hellere »håne« end lovgive mod påvirkning fra fremmede magter,” *Berlingske* (27. november 2018). Ulrik Dahlin, ”Dommere og Amnesty kritiserer Papes lovforslag om ulovlig påvirkning,” *Dagbladet Information* (25. Oktober 2018).
- 124 Folketingets Retsudvalg. *Lov om ændring af straffeloven (ulovlig påvirkningsvirksomhed)*. 2018-19, L95.
- 125 Jacob Mchangama and Birgitte Arent Eiriksson, ”Ytringsfriheden under V- og VLAK-regeringerne,” *Justitia*, (2019).; Jacob Mchangama, ”Den offentlige debat bør være frontlinjen mod propaganda. Ikke lovgivning,” *Berlingske* (23. marts 2019).
- 126 Fajstrup. ”FE: Straf til danske påvirkningsagenter vil ikke stoppe Rusland.”
- 127 Lovforslaget ændrede ordlyden til, at et ulovligt samarbejde er et samarbejde med en fremmed efterretningstjeneste. I bemærkningerne inkluderes dog indirekte samarbejde, det vil sige samarbejde med myndigheder og organisationer, der samarbejder med en fremmed efterretningstjeneste.
- 128 Forsvarets Efterretningstjeneste, *Ikke-klassificeret trusselsvurdering for folketingsvalget 2019* (14. april 2019).

- 129 Danskernes tillid til politikere og medier har været faldende gennem de seneste ti år. RADIUS, *Troværdighedsanalysen 2018*, (2019).
- 130 En sådan EU-regulering bør være opmærksom på de potentielle konsekvenser, en global standard kan have for regimekritikeres og aktivisters virke og sikkerhed i autokratiske regimer, hvis arbejde sikres af anonymiteten på og tilgængeligheden til de sociale medier. Ligeledes bør man være opmærksom på de signaler, anti-desinformations-love kan sende til fx autokratiske lande, der i dag allerede bruger disse love som begrundelse for statscensur, jf. Bradshaw, Samantha, Lisa Maria Neudert, and Philip N. Howard. *Government Responses to Malicious Use of Social Media*. NATO StratCom COE (2018).
- 131 Jf. de presseetiske regler: Dansk Journalistforbund og Danske Medier, *Guide til De presseetiske regler* (2013).
- 132 Flemming Splidsboel-Hansen fra Dansk Institut for Internationale Studier har allerede udgivet undervisningsmateriale om påvirkningskampagner, se Flemming Splidsboel Hansen, *Trolde i dit feed – russisk desinformation*. (DIIS, 2018). Dog er der også behov for en generel forståelse af dynamikkerne på de digitale medier, hvilket Center for Information og Boblestudier har forsøgt i centerets lærebog *Like*, red. Camilla Mehlsen and Vincent F. Hendricks. Center for Information og Boblestudier (CIBS), Københavns Universitet, (2019).
- 133 Dette kunne gøres ved at udvide Undervisningsministeriets vejledning om digitale kompetencer med et separat afsnit med de klassiske færdigheder vedrørende informationsbearbejdning, og hvordan dette appliceres i en digital tidsalder. Se Undervisningsministeriet, Digitale kompetencer: Vejledning til lov og bekendtgørelse – Lov om de gymnasiale uddannelser, § 29, (august 2018).
- 134 Guess, Andrew, Jonathan Nagler, and Joshua A. Tucker, "Less than you think: Prevalence and predictors of fake news dissemination on Facebook," *Science Advanced* (2019); Rebecca Adler-Nissen and Frederik Hjort, "Ideological Asymmetry in the Reach of Pro-Russian Digital Disinformation to United States Audiences," *Journal of Communication* 69, no. 2 (2018). Dette kunne eksempelvis komme i form af samarbejde med landets biblioteker og folkeuniversiteter om at udbyde kurser for denne aldersgruppe, se SIRI-Kommissionen, *AI, medier og demokrati: Sådan styrker vi vores demokratiske immunforsvar*, SIRI-Kommissionen (februar 2019).
- 135 Den svenska Myndigheten för samhällsskydd och beredskap har skrevet en håndbog for kommunikatører og tilbyder kurser i at håndtering af informationspåvirkning. Myndigheten för samhällsskydd och beredskap (MSB), *Att möta informationspåverkan. Handbok för kommunikatörer*, MSB (December 2018). Britiske myndigheder har udarbejdet lignende materiale, se Government Communication Service, *RESIST – Counter-Disinformation Toolkit* (2019).
- 136 Disse to er særligt vigtige i en dansk kontekst, og man bør inkludere andre platforme, som disse to medier ejer, såsom Instagram og YouTube i et samarbejde, da disse også bruges i forbindelse med informationsoperationer.

Litteraturliste

Abrams, Steve. "Beyond Propaganda: Soviet Active Measures in Putin's Russia". *Connections: The Quarterly Journal* 15, no. 1 (2016): 5-31.

Adler-Nissen, Rebecca, and Frederik Hjort. "Ideological Asymmetry in the Reach of Pro-Russian Digital Disinformation to United States Audiences". *Journal of Communication* 69, no. 2 (2018): 168-92.

Adler-Nissen, Rebecca, Frederik Hjort, and Yevgeniy Golovchenko. "Digital misinformation: Hvordan virker det egentlig?". *Puzzle Piece* nr. 6, Oktober, PIA – Political Ideas and Analysis (2018).

Angelovska, Nina. "Facebook Losing Users to Pinterest, Youtube and Twitter (Market Share by Region)". *Forbes*. (7 January 2019).

Arendt, Hannah. *Origins of Totalitarianism*. Cleveland and New York: World Publishing Company, (1962).

Astrup, Søren, and Bo Maltesen. "Professor får fem måneders fængsel for spionage". *Politiken*. (31. maj 2012).

<https://politiken.dk/indland/art5389181/Professor-f%C3%A5r-fem-m%C3%A5neders-f%C3%A6ngsel-for-spionage>

AVAAZ. *Yellow Vests Flooded by Fake News*. Avaaz (12 March 2019).

Badawy, Adam, Aseel Addawood, Kristina Lerman, and Emilio Ferrara. "Characterizing the 2016 Russian IRA Influence Campaign". (Under udgivelse).

Barash, Vladimir, and John Kelly. *Salience vs. Commitment Dynamics of Political Hashtags in Russian Twitter*. The Berkman Center for Internet & Society Research, Harvard University (2012).

Baroian, Donara. "Botspot: Journalist's Death Followed by Fake Accounts". *Medium*. (25 October 2018).

Bastos, Marco T., and Dan Mercea. "The Brexit Botnet and User-Generated Hyperpartisan News". *Social Science Computer Review* 37, no. 1 (2017): 38-54.

Bayer, Lili, Giorgio Bertolin, Nora Biteniece, Edward H. Christie, Anton Dek, Rolf Fredheim, John Gallacher, Kateryna Kononova, and Tetiana Marchenko. *Responding to Cognitive Security Challenges*. NATO Stratcom COE (2019).

BBC News. "Moscow Protest: Thousands Rally against Vladimir Putin". *BBC*. (25 December 2011).

<https://www.bbc.com/news/world-europe-16324644>

BBC News. "Russian Election: Biggest Protests since Fall of USSR". *BBC*. (10 December 2011).

<https://www.bbc.com/news/world-europe-16122524>

Beck Nielsen, Jens. "Hjort slog alarm – men forsvaret har ikke fundet ét eneste eksempel på russisk påvirkning af valget." *Berlingske*. (5. juni 2019).

Beck Nielsen, Jens, and Jens Anton Bjørnager. "Nul eksempler fra regeringen på russisk påvirkning". *Berlingske*. (24. november 2018).

Beckett, Ian F. W. *The Making of the First World War*. JSTOR, www.jstor.org/stable/j.ctt32bpn0. (Yale University Press: 2012).

Bennett, Gordon. *FPS & FAPSI – RIP*. Conflict Studies Research Centre (17 March 2003).

Boomgaarden, Hajo. "Interpersonal and Mass Mediated Political Communication." In *Political Communication*, edited by Carsten Reinemann, 469-88. Berlin: De Gruyter, (2014).

Bradshaw, Samantha, and Philip N. Howard. *Troops, Trolls and Troublemakers: A Global Inventory of Organized Social Media Manipulation*. Computational Propaganda Research Project (2017).

Breitenbauch, Henrik Ø., Niels Byrjalsen, Mark Winther, and Mikkel Broen Jakobsen. *Orden og afskrækkelse – Vestens håndtering af Rusland efter annektationen af Krim*. Center for Militære Studier, Københavns Universitet (Juni 2017).

Breitenbauch, Henrik Ø., Kristian Søby Kristensen, Gary Schaub Jr., André Ken Jakobson, and Mark Winther. *Options for Enhancing Nordic-Baltic Defence and Security Cooperation an Explorative Survey*. Centre for Military Studies, Copenhagen University (Maj 2017).

Buzan, Barry, and George Lawson. "Capitalism and the Emergent World Order". *International Affairs* 90, no. 1 (2014): 71-91.

Cadwalladr, Carole "I Made Steve Bannon's Psychological Warfare Tool": Meet the Data War Whistleblower". *The Guardian*. (18 March 2018). <https://www.theguardian.com/news/2018/mar/17/data-war-whistleblower-christopher-wylie-facebook-nix-bannon-trump>

Chesney, Robert, and Danielle Citron. "Deepfakes and the New Disinformation War: The Coming Age of Post-Truth Geopolitics". (11 December 2018).

von Clausewitz, Carl. *On War*. Translated by Michael Howard and Peter Paret. Oxford: Oxford University Press, (2007).

Committee on Foreign Relations. *Putin's Asymmetric Assault on Democracy in Russia and Europe: Implications for U.S. National Security*. The United States Senate, (Washington: 10 January 2018).

Dahl, Robert A. *Democracy and Its Critics*. New Haven: Yale University Press, (1989).

Dahlin, Ulrik. "Dommere og Amnesty kritiserer Papes lovforslag om ulovlig påvirkning". *Dagbladet Information* (25. Oktober 2018).

Dahlin, Ulrik. "Nyt lovforslag fra Pape skaber 'kolossal retsusikkerhed', mener kritikere". *Dagbladet Information* (10. oktober 2018).

Dansk Journalistforbund og Danske Medier. *Guide til de presseetiske regler*. (2013).

Dawson, Andres, and Martin Innes. *The Internet Research Agency in Europe 2014-2016*. Cardiff University, Crime and Security Research Institute (May 2019).

Dawson, Andrew, and Martin Innes. "How Russia's Internet Research Agency Built Its Disinformation Campaign". *The Political Quarterly* (6 May 2019).

Digital, Culture, Media and Sport Committee. *Disinformation and 'Fake News': Final Report*. House of Commons, UK (14 February 2019).

Digital, Culture, Media and Sport Committee. *Disinformation and 'Fake News': Interim Report*. House of Commons, UK (4 July 2017).

DiResta, Renee, Kris Shaffer, Becky Ruppel, David Sullivan, Robert Matney, Ryan Fox, Jonathan Albright, and Ben Johnson. *The Tactics & Tropes of the Internet Research Agency*. Knew Knowledge (1 December 2018).

Easton, David. *A Systems Analysis of Political Life*. New York: John Wiley, (1965).

Estonian Internal Security Service. *Security Police of the Republic of Estonia Annual Review 2008*. (Tallinn: 2008).

Entman, Robert M.. "Media Framing Biases and Political Power: Explaining Slant in News of Campaign 2008". *Journalism: Theory, Practice & Criticism* 11, no. 4 (2010): 389-408.

European Commission, "EU Code of Practice on Disinformation." News release (26 September 2018).

European Commission. "Action Plan against Disinformation". News release, (5 december 2018).

European Commission. "Code of Practice against Disinformation: Commission Calls on Signatories to Intensify Their Efforts". News release, (29 January 2019).

European Commission. "The Principles for Better Self- and Co-Regulation". 2018.

<https://ec.europa.eu/digital-single-market/sites/digital-agenda/files/CoP%20-%20Principles%20for%20better%20self-%20and%20co-regulation.pdf>

European Commission. *Report on the Implementation of the Action Plan against Disinformation*. High Representative of the Union for Foreign Affairs and Security Policy (Brussels: 14 June 2019).

Fajstrup, Marianne. "FE: Påvirkningskampagner er en gråzone". *Berlingske* (10. december 2018).

Fajstrup, Marianne. "FE-chef: Sådan kæmper vi imod Ruslands troldehær". *Berlingske*. (10. december 2018).

Fajstrup, Marianne. "FE: Straf til danske påvirkningsagenter vil ikke stoppe Rusland". *Berlingske*. (9. december 2018).

Ferrara, Emilio, Onur Varol, Clayton Davis, Filippo Menczer, and Alessandro Flammini. "The Rise of Social Bots", *Communications of the ACM* 59, no. 7 (2016): 96-104.

Finansministeriet. "Forslag til finanslov for finansåret 2019". 2018.

Fog, Aia. "Regeringens Nye Påvirkningslov Er En Glidebane Mod Det Totalitære". *Trykkehed.dk*. (15. februar 2019).

Folketinget. "Vedtaget af Folketinget ved 3. behandling den 19. marts 2019. Forslag til lov om ændring af straffeloven (ulovlig påvirkningsvirksomhed)". Folketingstidende, tillæg C, (2019).

Folketinget. "Grundlovens paragraf 77". Folketinget. Tilgået 4. marts 2019, <https://www.ft.dk/da/dokumenter/bestil-publikationer/publikationer/mingrundlov/min-grundlov/kapitel-8/paragraf-77>.

Forsvarets Efterretningstjeneste. *Ikke-klassificeret trusselsvurdering for folkestingsvalget 2019*. (14. april 2019).

Forsvarets Efterretningstjeneste. *Efterretningsmæssig Risikovurdering 2018*. (2018).

Forsvarets Efterretningstjeneste. "Rådgivning om cyberangreb og trusler til partierne forud for valget". Presse meddelelse, 20. februar 2019.

Folketingets Retsudvalg. *Lov om ændring af straffeloven (ulovlig påvirkningsvirksomhed)*. 2018-19, L95.

Foxhall, Andrew. *Putin's Useful Idiots: Britain's Left, Right and Russia*. Russia Studies Centre at The Henry Jackson Society (London: 2016).

Funke, Daniel. "Three Publications Are Suing the EU over Fake News Allegations". Poynter, 2018.

Galante, Laura, and Shaun E. E. "Defining Russian Election Interference: An Analysis of Select 2014 to 2018 Cyber Enabled Incidents". (11 September 2018).

Galeotti, Mark. *Putin's Hydra: Inside Russia's Intelligence Services*. (11 May 2016).

Giles, Keir. *Countering Russian Information Operations in the Age of Social Media*. Council on Foreign Relations (21 November 2017). <https://www.cfr.org/report/countering-russian-information-operations-age-social-media>

Giles, Keir. *Handbook of Russian Information Warfare*. NATO Defense College (Rome: NATO, November 2016).

Giles, Keir. *Russia's 'New' Tools for Confronting the West*. Chatham House The Royal Institute of International Affairs (March 2016).

Giles, Keir, Philip Hanson, Roderic Lyne, James Nixey, James Sherr, and Andrew Wood. *The Russian Challenge*. The Royal Institute of International Affairs (City Print, 2015).

Gorwa, Robert, and Douglas Guilbeault. "Understanding Bots for Policy and Research: Challenges, Methods, and Solutions". Presented at ICA 2018. (21 January 2018).

Government Communication Service. *RESIST – Counter-Disinformation Toolkit*. (2019).

Graff, Garrett M. "A Guide to Russias High Tech Tool Box for Subverting US Democracy". *Wired*, 13 September 2017.

<https://www.wired.com/story/a-guide-to-russias-high-tech-tool-box-for-subverting-us-democracy/>

Guess, Andrew, Jonathan Nagler, and Joshua A. Tucker. "Less Than You Think: Prevalence and Predictors of Fake News Dissemination on Facebook". *Science Advanced* (2019).

Guillaume, Marine. *Combating the Manipulation of Information – a French Case*. Hybrid CoE (2019).

Habermas, Jürgen. *Between Facts and Norms: Contributions to a Discourse Theory of Law and Democracy*. Polity Press (Camebridge: 1995).

Hasselbalch, Ole, Bjørn Elmquist, and Ole Stig Andersen. "Juraprofessor, forsvarsadvokat og tidl. PET-chef i fælles opråb: Regeringens forslag om ændring af straffelovens paragraf 108 presser ytringsfriheden". *Politiken* (21. februar 2019).

Hay Newman, Lily. "A New Tool Protects Videos from Deepfakes and Tampering". *Wired*, (11. February 2019).

<https://www.wired.com/story/amber-authenticate-video-validation-block-chain-tampering-deepfakes/>

Headley, James "Challenging the EU's Claim to Moral Authority: Russian Talk of 'Double Standards'". *Asia European Journal* 13, no. 3 (2015): 297–307.

Heiberg, Morten. *KGB's kontakt- og agentnet i Danmark*. Justitsministeriet (juni 2009).

Helmus, Todd C., Elizabeth Bodine-Baron, Andrew Radin, Madeline Magnusson, Joshua Mendelsohn, William Marcellino, Andriy Bega, and Zev Winkelmann. *Russian Social Media Influence Understanding Russian Propaganda in Eastern Europe*. RAND (2018).

Hendricks, Vincent, and Pelle G. Hansen. *Infostorms – How to Take Information Punches and Save Democracy*. Springer. (New York: 2014).

Hermann, Jon. "The Nine Links in the Chain: The Weaponized Narrative, Sun Tzu, and the Essence of War". *The Strategy Bridge*, (27 July 2017).

Hindman, Matthew and Vlad Barash. *Disinformation, 'Fake News' and Influence Campaigns on Twitter*. John S. and James L. Knight Foundation (4 October 2018).

Howard, Philip N., Samantha Bradshaw, Bence Kollanyi, Clementine Desigaud, and Gilian Bolsover. *Junk News and Bots During the French Presidential Election: What Are French Voters Sharing over Twitter?* Oxford Internet Institute (22 April 2017).

Ireton, Cherilyn, and Julie Posetti. *Journalism, Fake News & Disinformation: Handbook for Journalism Education and Training*. Paris: United Nations Educational, Scientific and Cultural Organization, (2018).

Jakobsson, André Ken, *Når Hydra angriber – Hybrid afskrækkelse i gråzonen mellem krig og fred*, Center for Militære Studier, Københavns Universitet (oktober 2019).

Janda, Jakub, and Ondřej Kundra. *Mechanisms of Influence of the Russian Federation into Internal Affairs of the Czech Republic*. European Values (4 September 2016).

Justitia, Bemærkninger til udkast til forslag til lov om ændring af straffeloven (ulovlig påvirkningsvirksomhed). (2019)

<http://justitia-int.org/wp-content/uploads/2018/10/H%C3%88ringssvar-til-ulovlig-p%C3%A5virkningsvirksomhed.pdf> (tilgået 20. februar 2019)

Justitsministeriet. "Styrket værn mod udenlandsk påvirkning af danske valg og demokratiet". Pressemeldelse , (7. september 2018).

Justitsministeriet. "Forslag til lov om ændring af straffeloven (ulovlig påvirkningsvirksomhed)". (13. september 2018).

Kahneman, Daniel, Paul Slovic, and Amos Tversky. *Judgment under Uncertainty, Heuristics and Biases*. Cambridge: Cambridge University Press (1982).

Kasapoglu, Can."Russia's Renewed Military Thinking: Non-Linear Warfare and Reflexive Control". *NATO Defense College Research*, 121, (25. November 2015).

Katz, Elihu, and Paul F. Glencoe Lazarsfeld. *Personal Influence*. The Free Press. (Glencoe Illinoise: 1955).

Karan, Kanishk, Donara Barojan, Melissa Hall & Graham Brookie. "Trolltracker: Outward Influence Operation from Iran". *Medium*. (31 January 2019).

<https://medium.com/dfrlab/trolltracker-outward-influence-operation-from-iran-cc4539684c8d>

Keating, Vincent Charles, and Katarzyna Kaczmarska. "Conservative Soft Power: Liberal Soft Power Bias and the 'Hidden' Attraction of Russia". *Journal of International Relations and Development* (May 11 2017).

Kiseleva, Yulia. "Russia's Soft Power Discourse: Identity, Status and the Attraction of Power". *Politics* 35, no. 3-4 (2015): 316-29.

Kjærsgaard, Pia. "Pia Kjærsgaard: Pressen og politikerne må danne fælles værn mod falske nyheder". *Alttinget*. (3. januar 2019).

Knight, W. "The Defense Department Has Produced the First Tools for Catching Deepfakes". *MIT Technology Review*. (7 August 2018).

<https://www.technologyreview.com/s/611726/thedefense-department-has-produced-the-first-tools-for-catching-deepfakes/> (Accessed 4. february)

Knudsen, Lisbeth. *Globaliseringen Af Den Danske Mediebranche*. Slots og Kulturstyrelsen (2017).

Koesel, Karrie J., and Valerie J. Bunce. "Diffusion-Proofing: Russian and Chinese Responses to Waves of Popular Mobilizations against Authoritarian Rulers". *Perspectives on Politics*, 11, no. 3 (2013): 753-68.

KOMBIT. "Valg sender udbudsmateriale til print af valgkort i høring hos leverandører". (17. april 2019).

<https://www.kombit.dk/nyheder/valg-sender-udbudsmateriale-til-print-af-valgkort-i-høring-hos-leverandører>

KOMBIT. "Projekt valg afholder workshops". (14. december 2016).
<https://www.kombit.dk/nyheder/projekt-valg-afholder-workshops>.

Kongstad, Jesper. "Dansk spionchef skærper tonen over for Putin og truslerne fra Rusland". *Jyllands-Posten*. (5. december 2018).

Kononenko, Vladimir, and Arkady Moses. *Russia as a Network State: What Works in Russia When State Institutions Do Not*. Palgrave Macmillan. London: 2011.

Kovaleva, Natalya. "Russian Information Space, Russian Scholarship, and Kremlin Controls". *Defence Strategic Communications* 4 (2018).

Kragh, Martin, and Sebastian Åsberg. "Russia's Strategy for Influence through Public Diplomacy and Active Measures: The Swedish Case". *Journal of Strategic Studies* 40, no. 6 (2017): 773-816.

Król, Aleksander. "Russian Information Warfare in the Baltic States". *The Warsaw Intitute Review*, (20 July 2017).

Lange-Ionatamišvili, Elīna. *Redefining Euro-Atlantic Values: Russias Manipulative Techniques*. NATO StratCom Center of Excellence (2017).

Lange-Ionatamišvili, Elīna, Ieva Bērziņa, Māris Cepurītis, Diana Kaljula, and Ivo Juurvee. *Russias Footprint in the Nordic-Baltic Informations Environment*. NATO StratCom Centre of Excellence (Riga: January 2018).

Levin, Sam. "'They Don't Care': Facebook Factchecking in Disarray as Journalists Push to Cut Ties". *The Guardian*. (13 December 2018).

Lo, Bobo "Two Worlds". In *Russia and the New World Disorder*, 38-67. Brookings Institution Press (Washington D.C.: 2015).

Lucas, Edward, and Peter Pomeranzev. *Winning the Information War: Techniques and Counter-Strategies in Russian Propaganda*. Center for European Policy Analysis (Washington DC: August 2016).

Lupia, Arthur "Shortcuts Versus Encyclopedias: Information and Voting Behavior in California Insurance Reform Elections". *The American Political Science Review* 88, no. 1 (1994): 63-76.

Lutsevych, Orysia. *Agents of the Russian World Proxy Groups in the Contested Neighbourhood*. Chatham House, The Royal Institute of International Affairs (London:2016).

Mchangama, Jacob. "Den offentlige debat bør være frontlinjen mod propaganda. Ikke lovgivning". *Berlingske* (23. marts 2019).

- Mchangama, Jacob, and Birgitte Arent Eiriksson. "Ytringsfriheden under V-Og VLAK-regeringerne". *Justitia*. (2019).
- Mehlsen, Camilla and Hendricks, F. Vincent. *Like*. Center for Information og Boblestudier (CIBS), Københavns Universitet, (2019).
- Mueller, Robert S. "Indictment: United States of America v. Internet Research Agency". Case 1:18-cr-00215-ABJ. Special Council and U.S. Department of Justice. (13 July 2018).
- Mueller, Robert S. *Report on the Investigation into Russian Interference in the 2016 Presidential Election*. U.S. department of Justice (March 2019).
- Myndigheten för samhällsskydd och beredskap (MSB). *Att möta informationspåverkan. Handbok för kommunikatörer*. MSB (December 2018).
- NATO StratCom Center of Excellence. *The Black Market for Social Media Manipulation*. (Riga, 2018).
- Newman, Nic, Richard Fletcher, Antonis Kalogeropoulos, David A. L. Levy, and Rasmus Kleis Nielsen. Reuters Institute Digital News Report 2018. *Reuters Institute for the Study of Journalism* (2018).
- Newton, Kenneth. "Social and Political Trust in Established Democracies". In *Critical Citizens*, edited by Pippa Norris, 169-87: Oxford University Press, 1999.
- Newton, Kenneth. "Trust, Social Capital, Civil Society, and Democracy". *International Political Science Review* 22, no. 2 (2001): 201-214.
- Nimmo, Ben. "Anatomy of an Info-War: How Russia's Propaganda Machine Works, and How to Counter It". *StopFake*, 19 May 2015.
<http://www.stopfake.org/en/anatomy-of-an-info-war-how-russia-s-propaganda-machine-works-and-how-to-counter-it/>
- Nimmo, Ben. "Russian Interference: The Evidence." *Medium*. (25 April 2019).
- Nimmo, Ben, Donara Barojan, and Nika Aleksejeva. "Russian Narratives on Nato's Deployment". *Medium* (1 April 2017).
<https://medium.com/dfrlab/russian-narratives-on-natos-deployment-616e19c3d194>
- Ovchinsky, V. S., E. S. Larina, and S. A. Kulik. *Russia and the Challenges of the Digital Environment*. Russian International Affairs Council (2014).
- Pamment, James, Howard Nothhaft, Henrik Agardh-Twetman, and Alicia Fjällhed. *Countering Information Influence Activities the State of the Art*. Department of Strategic Communication, Lund University & MSB (1 July 2018).
- Pew Research Center. "Teens, Social Media & Technology 2018". (2018).
- Politiets Efterretningstjeneste. "Årlig redegørelse 2017." (2018).
- Pomerantsev, Peter, Laura Jackson, Timothy Thomas, Mark Laity, and Ben Nimmo. *Information at War: From China's Three Warfares to Nato's Narratives*. Legatum Institute (2015).
- Pomerantsev, Peter, and Michael Weiss. *The Menace of Unreality: How the Kremlin Weaponizes Information, Culture and Money*. The Institute of Modern Russia & The Interpreter (New York: 2014).

- Powell, L., and K. Galinsky. *Augustus at War: The Struggle for the Pax Augusta*. Great Britain Pen & Sword Military, 2016.
- Puddington, Arch. *Breaking Down Democracy: Goals, Strategies, and Methods of Modern Authoritarians*. Freedom House (June 2017).
- Putin, Vladimir. "Information Security Doctrine of the Russian Federation Approved by President of the Russian Federation" (2000).
- Pynnoniemi, Katri, and András Rácz. *Fog of Falsehoods – Russian Strategy of Deception and the Conflict in Ukraine*. The Finnish Institute of International Affairs. Helsinki: Grano Oy, 2016.
- Qiang, X. "The Rise of China as a Digital Totalitarian State". *New Perspectives Quarterly* 35, no. 2 (2018): 37-39.
- RADIUS. *Troværdighedsanalysen 2018*. (2019).
- Rainie, Lee, Janna Anderson, and Jonathan Albright. *The Future of Free Speech, Trolls, Anonymity and Fake News Online*. Pew Research Center (March 2017).
- Ramsay, Gordon, and Sam Robertshaw. *Weaponising News: RT, Sputnik and Targeted Disinformation*. Communication & Power Centre for the Study of Media, King's College London (London: January 2019).
- Regeringen. "National Strategi for cyber- og informationssikkerhed". (15. maj 2018).
- Roselle, Laura, Alister Miskimmon, and Ben O'Loughlin. "Strategic Narrative: A New Means to Understand Soft Power". *Media, War & Conflict* 7, no. 1 (2014): 70-84.
- Sanovich, Sergey. *Computational Propaganda in Russia: The Origins of Digital Misinformation*. Oxford University Computational Propaganda Project (2017).
- Schaffer, Bret. *A View from the Digital Trenches – Lessons from Year One of Hamilton*. 68. Alliance for Securing Democracy (2018).
- Schattschneider, E. E. *The Semisovereign People: A Realist's View of Democracy in America*. Holt, Rinehart & Winston. (Chicago: 1983).
- Schumpeter, J. A. *Capitalism, Socialism and Democracy*. Unwin University Books. (London: 1974).
- Select Committee on Intelligence. *Russian Intervention in European Elections*. No. HRG 115-105. The United States Senate. (Washington: June 28 2017).
- Select Committee on Intelligence. *Russian Targeting of Election Infrastructure During the 2016 Election: Summary of Initial Findings and Recommendations*. The United States Senate. (Washington: 8 May 2018).
- Shandra, Alya. "The Most Comprehensive Guide Ever to MH17 Conspiracies." *Stopfake.org*. (18 July 2016).
- Shultz, Richard, and Roy Godson. *Dezinformatsia – Active Measures in Soviet Strategy*. United States of America Pergamon, (New York: 1984).

SIRI-Kommisionen. *AI, medier og demokrati: Sađan styrker vi vores demokratiske immunforsvar.* (Februar 2019).

Skak, Mette. "Russia's New Monroe Doctrine". In *Russia's Foreign Policy in the 21st Century*, edited by Roger E. Kanet, 138-54: Palgrave MacMillan, (2011).

Smolenčová, Ivana. *The Pro-Russian Disinformation Campaign in the Czech Republic and Slovakia Types of Media Spreading Pro-Russian Propaganda, Their Characteristics and Frequently Used Narratives.* Prague Security Studies Institute (June 2015).

Smolenčová, Ivana, Barbora Chrzová, Iveta Várenyiov, Dušan Fischer, Dániel Bartha, András Deák, András Rácz, and Andrzej Turkowski. *United We Stand, Divided We Fall: The Kremlin's Leverage in the Visegrad Countries.* Prague Security Studies Institute (November 2017).

Smyth, Regina, and Sarah Oates. "Mind the Gaps: Media Use and Mass Action in Russia". *Europe-Asia Studies* 67, no. 2 (2015): 285-305.

Soldatov, Andrei and Irina Borogan. "The Red Web: The Struggle between Russia's Digital Dictators and the New Online Revolutionaries". *Public affairs* (New York, N.Y. 2015).

Splidsboel Hansen, Flemming. *Trolde i dit feed – russisk desinformation.* DIIS, (2018).

Sputnik. "Russia Releases Big 120-Page Report on Russophobia, Russiagate Hysteria in Us." (20 April 2019).

Straffeloven §108, Retsinformation,
<https://www.retsinformation.dk/Forms/R0710.aspx?id=202516>

Stenbæk Christoffersen, Jonas, and Jens Beck Nielsen. "Dansk Folkeparti vil hellere »håne« end lovgive mod påvirkning fra fremmede magter". *Berlingske.* (27. november 2018).

Syrovatka, Jonáš, Daniel Bartha, Botond Feledy, András Rácz, Petru Macovei, Antoni Wierzejski, Dusan Fischer, and Margo Gontar. *Information Warfare in the Internet – Countering Pro-Kremlin Disinformation in the Cee Countries.* Centre For International Relations & Partners (2017).

Szostek, Joanna. "The Power and Limits of Russia's Strategic Narrative in Ukraine: The Role of Linkage". *Perspectives on Politics* 15, no. 02 (2017): 379-95.

Tadajewski, Radek. "Hybrid War". Presentation at the NATO StratCom COE: "Emerging Trends in Social Media", (Riga: 25 March 2018).

Taylor, Emily, Stacie Walsh, and Samantha Bradshaw. *Industry Responses to the Malicious Use of Social Media.* NATO StratCom CoE (November 2018).

The Russian Federation. *Doctrine of Information Security of the Russian Federation,* 2016.

Toler, Aric. "The Weird World of MH17 Conspiracy Theories". *Bellingcat.* (7 August 2015).

Undervisningsministeriet. *Digitale Kompetencer: Vejledning til lov og bekendtgørelse – Lov om de gymnasiale uddannelser*, § 29, (august 2018).

United Nations. "Universal Declaration of Human Rights". (1948).

Unver, H. Akin. "Digital Challenges to Democracy: Politics of Automation, Attention and Engagement". *Journal of International Affairs* 71, no. 1 (2017): 127-46.

Uscinski, Joseph E., and Ryden W. Butler. "The Epistemology of Fact Checking". *Critical Review* 25, no. 2 (2013): 162-80.

Vanin, M. "Statement by H.E. Ambassador of the Russian Federation to the Kingdom of Denmark Mr. M.Vanin". Pressemeldelse, (24. juli 2018).

Vilmer, Jean-Baptiste Jeangène. "Successfully Countering Russian Electoral Interference – 15 Lessons Learned from the Macron Leaks". *CSIS Briefs* (June 2018).

Walker, Christopher, Jessica Ludwig, Jacek Kucharczyk, Juan Pablo Cardenal, Grigorij Mesežnikov, and Gabriela Pleschová. *Sharp Power – Rising Authoritarian Influence*. National Endowment for Democracy (5 December 2017) <https://www.ned.org/sharp-power-rising-authoritarian-influence-forum-report/>

Waltzman, Rand. *The Weaponization of Information the Need for Cognitive Security*. Senate Armed Services Committee (27 April 2017).

Watling, Jack. *Iran's Objectives and Capabilities Deterrence and Subversion*. Royal United Services Institute (2019).

Watts, John. *Whose Truth? Sovereignty, Disinformation, and Winning the Battle of Trust*. Atlantic Council (September 2018).

Webster, J. G. "User Information Regimes: How Social Media Shape Patterns of Consumptions". *North Western University Law Review* 104, no. 2 (2010): 593-612.

White, Stephen, and Ian McAllister. "Did Russia (Nearly) Have a Facebook Revolution in 2011? Social Media's Challenge to Authoritarianism". *Politics* 34, no. 1 (2013): 72-84.

Wilson, Jeanne L. "Russia and China Respond to Soft Power: Interpretation and Readaptation of a Western Construct". *Politics* 35, no. 3-4 (2015): 287-300.

Winnerstig, Mike, Gudrun Persson, Anna Bulakh, Julian Tupay, Karel Kaas, Emmet Tuohy, Kristiina Visnapuu, et al. *Tools of Destabilization Russian Soft Power and Non-Military Influence in the Baltic States*. Försvarsanalys, Swedish Defence Ministry (2014).

Winter, Charlie. *The Virtual 'Caliphate': Understanding Islamic State's Propaganda Strategy*. NATO Stratcom COE (July 2015).

Yaffa, Joshua. ""The Double Sting"". *The New Yorker*. (27 July 2015). www.newyorker.com/magazine/2015/07/27/the-double-sting

Zakharova, Olesya. "Vladimir Putin Loves Civil Society (as Long as He Controls It)". *Foreign Policy*, (12 October, 2016).

Zuckerberg, Mark. "A Privacy-Focused Vision for Social Networking". News release, (6 March 2019).

<https://newsroom.fb.com/news/2019/03/vision-for-social-networking/>