

# Når Rusland fører krig i det kognitive domæne

Temanummer: Det moderne Rusland i krig

*Denne artikel præsenterer et indblik i den russiske tænkning om informationsoperationer, som denne kommer til udtryk politisk og forskningsmæssigt. Baggrunden er en forståelse i Rusland af en igangværende "informationskrig", ført an af Vesten mod Rusland, og meget af den præsenterede tænkning skal hjælpe Rusland til at håndtere denne påståede krig.*

*Artiklen ser nærmere på forholdet mellem afsender og modtager, platforme, kommunikationsformer og typer af information. Russiske informationsoperationer forbindes ofte – og med god grund – med desinformation, men der er tillige en omfattende*

*brug af regulær information, som blot præsenteres i en tendentiøs form. Der er stor variation i operationerne, men formålet er altid det samme: At påvirke en modtager.*

*Der er betydelig usikkerhed om effekten af operationerne. Flere af de russiske forskere udtrykker skepsis ift. en effekt. De anbefaler f.eks., at Ruslands informationspolitik skal koordineres meget mere, end tilfældet er i dag, og at området skal tilføres flere midler og mere forskningsbaseret viden. Der er dog generel enighed om, at informationsoperationer byder på så stort et potentiale, at vi i fremtiden vil se stater engagere sig endnu mere i dette.*

*"Udenlandske politikere tilskriver Rusland indblanding i valg og afstemninger over hele kloden. I virkeligheden er sagen endnu mere alvorlig – Rusland foretager indgreb i deres hjerner, og de ved ikke, hvad de skal stille op med deres egne forandrede bevidstheder" (Surkov, 2019).<sup>1</sup>*

"Russerne fucker med vores hjerner", lød en dramatisk overskrift i Politiken (2017). Artiklen kom som reaktion på den hastigt voksende offentlige debat om påstået russisk indblanding i forskellige valg i vestlige demokratier og især i det amerikanske præsidentvalg i 2016. Som et bagtæppe til denne debat er der naturligvis et stort antal videnskabelige felter, som hvert især og sammen bidrager til en dybere forståelse af relevante mekanismer. Det er bl.a. psykologi, lingvistik, informations- og medievidenskab og krigsstudier. Meget af denne viden fra disse felter er samtidig med til at informere forskellige aktører om relevante mekanismer, og på den måde tjener den et dobbelt formål: At muliggøre og forklare.

I denne artikel præsenterer jeg et lille indblik i den nuværende russiske forskning i og tænkning om påvirkningsoperationer med særligt fokus på informationsoperationer. "Informationskrig" er det mest anvendte begreb i den russiske litteratur for operationer af denne type, og i de seneste år er der blevet talt meget mere om "informationskrig" i Rusland end tidligere (Gnesdilova, 2018: 109). Det gælder i politik, journalistik og forskning. Den offentlige rammesætning for russisk indenrigs- og udenrigspolitik tager nu som hovedregel

**FLEMMING SPLIDSBOEL  
HANSEN**

Seniorforsker, Ph.d.  
Dansk Institut for Internationale  
Studier  
fsha@diis.dk

udgangspunkt i en igangværende informationskrig med Vesten og med Rusland som offer (Gnesdilova, 2018: 109).

Artiklen falder i fem dele. Jeg starter med at skitsere baggrunden og definere centrale begreber, herunder især information, påvirkning og læring. Herefter præsenterer jeg de domæner, hvor informationen flyder, og påvirkningen og læringen sker, inden jeg åbner den russiske værktøjskasse og lægger forskellige redskaber frem. Jeg vil her diskutere brugen af forskellige typer af information og af midler, som de ses i den russiske tænkning, til at påvirke modtagere af informationen. Efter dette vurderer jeg effekten af de russiske informationsoperationer, inden jeg afslutningsvis opridses grundelementerne i den fremtidige informationskamp.

## Information og påvirkning

I februar 2013 leverede general Valerij Gerasimov, chef for den russiske generalstab, et nyt og autoritativt bidrag til den russiske forståelse af nutidens og fremtidens krig. Gerasimov beskrev bl.a., hvorledes hele udviklingen fra en konflikts opståen til dens fredelige afslutning, ifølge ham udfoldet i seks separate faser, er ledsaget af en informationskamp. Informationsoperationerne forbinder de ”militære” og ”ikke-militære” (kinetiske og ikke-kinetiske, hhv.) operationer ved bl.a. at støtte samtænkningen af disse såvel som deres dimensionering (Gerasimov, 2013).

F.eks. vil en aktør kunne forsøge at legitimere en hurtig overgang til kinetiske operationer med henvisning til en form for ”nødvendighed” eller alternativt – og det er den aktuelle forsknings primære fokus – at forsøge at opnå de identificerede mål *uden* brug af kinetiske virkemidler. Ifølge Gerasimov (2013) viste Det arabiske Forår, at ”informationskampen åbner omfattende asymmetriske muligheder for at svække en modstanders potentiale for kamp”. I en senere artikel refererede Gerasimov (2017) mere specifikt til disse processer som ”mulighederne for mobilisering via sociale netværk”.

Gerasimovs artikel fra 2013 er i høj grad blevet set som en skabelon for Ruslands besættelse af Krim i februar 2014 og efterfølgende engagement i krigen i Østukraine, men den bør også ses som en erkendelse i toppen af det russiske forsvar af udviklingen på informationsområdet. Russiske forskere (f.eks. Labusj, 2018: 286) har beskrevet og beklaget, hvor uforberedt Rusland var på informationsområdet under den russisk-georgiske krig om Sydossetien i 2008, og hvorledes ”de russiske medier slet ikke formåede at overbevise (...) den vestlige offentlighed [om legitimiteten af Ruslands politik]”. De finder dog også, som en bl.a. formulerer det, at ”det var en anden situation på tidspunktet for genforeningen af Krim” (Labusj, 2018: 286). I den mellemliggende periode, må vi forstå, skete der en betydelig erfaringsindhentning og læring i hele det russiske apparat, så informationsoperationerne i 2014 blev vurderet til at have haft langt større effekt.

Gerasimov (2013) betonede særligt ”de asymmetriske muligheder” i informationsoperationerne, hvilket i denne sammenhæng knytter an til den svagere parts muligheder for at mindske forskellen i kapabiliteter mellem sig selv og den stærkere part (Tjekinov og Bogdanov, 2016). Informationsværktøjerne kan på denne måde kompensere for mangler på andre områder, herunder især de kinetiske redskaber. Senere har der dog også været stort fokus på, hvorledes den stærkere part kan benytte informationsoperationer til at styrke sin overlegenhed – en anden form for asymmetri – og argumentet i denne del af den russiske litteratur er oftest, at Rusland er mål for påvirkning fra vestlig og især amerikansk side.

Informationsværktøjerne kan mest umiddelbart opfylde helt simple logistiske behov som f.eks. at muliggøre en samlet koordination af en demonstration. Dette er i stigende grad en udfordring for ikke-demokratiske styre, som derfor i stadig større omfang både teknologisk og lovgivningsmæssigt forsøger at forhindre denne form for koordination via sociale medier. Den russiske stats planer om udviklingen af et suverænt russisk internet – det bliver almindeligvis refereret til som RuNet – fortolkes også ofte i denne ramme (Hansen, 2019a og 2019b; også Kolnosjenko og Kolnosjenko, 2019).

Kritikere (f.eks. Ruslands internetombudsmand Dmitrij Marinitjev i Ekspert, 2019: 16) hævder, at det russiske styre ønsker sit eget internet for derved bedre at kunne styre kommunikationsstrømme og i givet fald afspore eller helt blokere for dem. F.eks. krævede Roskomnadzor (2019), Ruslands statslige tjeneste for bl.a. massekommunikation, i august 2019 i et åbent brev til Google, at fildelingstjenesten Youtube (som er ejet af Google) skulle stoppe push-notifikationer om såkaldte usanktionerede demonstrationer til brugere af Youtube. Roskomnadzor reagerede på baggrund af de omfattende regeringskritiske demonstrationer, som var i Moskva især i august 2019, og som i stort omfang blev organiseret via sociale medier. Youtube var et logistisk værktøj i denne forbindelse – brugere fik beskeder om planlagte demonstrationer – og Roskomnadzor ønskede at deaktivere det. I sit brev til Google hævdede tjenesten, at udenlandske aktører stod bag notifikationerne, som derfor blev stemplet som uacceptabel indblanding i Ruslands indre anliggender.

 **Jeg definerer påvirkningskampagner som operationer, som skal resultere i en kognitiv effekt. De skal med andre ord resultere i en læringsproces**

I et bredere perspektiv kan informationsværktøjerne benyttes til at påvirke enkelte modtagere eller større modtagergrupper. Det er her, den helt store interesse er (f.eks. Kunakova, 2012). Omdrejningspunktet for tænkning om og brug af værktøjerne er påvirkning. Jeg definerer påvirkningskampagner som operationer, som skal resultere i en kognitiv effekt. De skal med andre ord resultere i en læringsproces. Skematisk vil det se således ud:

Afsender → operation → modtager → evt. umiddelbar kognitiv effekt → endelig kognitiv effekt

Den sidste del af den skitserede proces er naturligvis den vanskeligste. Russiske forskere (f.eks. Novikov og Gerasimov, 2019: 18) forklarer, at afsenderen kan maksimere sandsynligheden for effekt ved at levere information, som er ”ny, vigtig og aktuel”. Hvis modtageren forbliver upåvirket af den information, som afsenderen har viderebragt ud fra et ønske om at opnå en særlig effekt, er operationen mislykkedes, og den afbrydes ved modtageren (dvs. afsender → operation → modtager). Vi kan beskrive nøglen til den fortsatte proces som en situationalitet, dvs. en kontekstrelevant afsendelse af information.

Centralt i dette er en forståelse af modtageren. Afsenderen skal have et såvel bredt som dybt vidensgrundlag om modtageren og skal kunne besvare spørgsmål som ”hvad, hvornår, hvor og hvorfor?” (Popova og Fedorinov, 2018: 18). Det er kulturelle efterretninger i bred forstand, og en russisk forsker (Akhatova, 2019: 244, 249) opsummerer det som ”interkulturelle kompetencer” eller en viden om ”mentalitet, kultur og særtræk i omgangsformen hos repræsentanter for andre lande”.

Det skal tilføjes, at afsenderen tillige skal have en forståelse af sin egen rolle i processen. Informationen kan meget vel være ”ny, vigtig og aktuel”, men hvis afsenderen blokerer for den ønskede effekt hos modtageren, vil processen blive afbrudt. Den statskontrollerede russiske nyhedsplatform RT (indtil 2008 benævnt Russia Today) har meget bevidst gennemført en national forankring af sine fremmedsprogede udsendelser ved at ansætte journalister og værter fra de pågældende sprogområder (Korneev 2019, ingen sideangivelse). En russisk medieforsker (Korneev, 2019, ingen sideangivelse) forklarer, at det er gjort for at give platformen en højere grad af tillid hos forbrugerne, da nyhederne så ikke bliver præsenteret af repræsentanter for ”de andre”, men af repræsentanter for [forbrugernes] eget mediemiljø”. Tillid kan defineres som en tro på, at relevante aktører ”har integritet og handler etisk, hvilket vil sige, at de er pålidelige, troværdige og moralsk ansvarlige” (Feldman, 2000: 27). RT har forsøgt at fjerne nogle af de barrierer, som har stået i vejen for et mere tillidsfuldt forhold mellem platformen og modtagerne af dens kommunikation.

Der er i den ovenfor skitserede proces en intentionalitet. Afsenderen ønsker, at operationen skal have en kognitiv effekt i modtageren. Intentionaliteten er grundlaget for den såkaldte våbenliggørelse. Det er et forholdsvis nyt begreb, som refererer til den bevidste anvendelse af ikke-kinetiske redskaber til at opnå opsatte mål, herunder via læringsprocesser hos en modtager eller modtagergruppe. Et eksempel er de russiske myndigheders frigivelse af en optaget samtale fra 2014 mellem USA's daværende viceudenrigsminister for europæiske forhold, Victoria Nuland, og USA's daværende ambassadør i Ukraine. De to havde en fortrolig samtale om den politiske udvikling i Ukraine og om, hvilke parter der burde inddrages i udformningen af denne udvikling. EU dukkede op i samtalen som en mulig aktør, men Nuland afviste ideen med

et kort "Fuck the EU!". Frigivelsen af optagelserne er et eksempel på en operation, hvor et stykke information anvendes i håbet om at opnå en kognitiv effekt hos en eller flere modtagergrupper (f.eks. hos ukrainske vælgere eller hos borgere i EU). Det er også et eksempel på en våbenliggørelse af information; afsenderen har givetvis nøje vurderet de mulige gevinster og tab ved en offentliggørelse og har på den baggrund besluttet at iværksætte en kort, men potentielt meget effektiv operation.<sup>2</sup>

Modtageren kan blive påvirket via ubevidste såvel som bevidste processer. Og den eventuelle læring kan være simpel eller kompleks, hvilket vil sige, at modtagerens adfærd er drevet hhv. af et overfladisk ønske om blot at optimere sit udbytte eller af en dybere overbevisning om, at det er "det rigtige" at gøre.<sup>3</sup> En russisk forsker beskriver den komplekse læring som overgangen "fra et verdensbillede til et andet" (Gnesdilova, 2018: 108). For afsenderen er den optimale kognitive effekt en ubevidst og kompleks læring hos modtageren. I disse tilfælde kan afsenderen håbe at påvirke modtageren til at gøre, som afsenderen gerne vil, og uden at modtageren opdager påvirkningen. Afsenderen vil normalt også have velbegrandede forventninger om, at effekten af netop den ubevidste og komplekse læring er mere langtidsholdbar hos modtageren. Det kan f.eks. dreje sig om operationer, som skal påvirke større vælgergrupper til at stemme på en måde, som svarer til afsenderens interesser. Vælgerne bliver ikke lokket med belønninger eller truet med straf – de stemmer af egen fri vilje og overbevisning, men på baggrund af en ubemærket operation, som har fået dem til at anskue problemstillingen som beskrevet af afsenderen.

Det er naturligvis dramatisk at tale om "krig" i denne sammenhæng, som jeg gør det i titlen. Vi bliver jo alle intentionelt påvirket af mange forskellige afsendere stort set dagligt, og det får os ikke til at føle, at vi er ofre for "krig". Det skyldes jo bl.a., at den dominerende forståelse af krig er, at det kinetiske element er nødvendigt og muligvis endog primært (f.eks. Speller og Tuck, 2009: 1 og Kaldor, 1999). Uden det kinetiske element – uden "krudt og kugler" – er der ingen krig. Men i Rusland anvendes begrebet i stigende grad løsere og med fokus på det ikke-kinetiske element. Der er helt oplagt en politisk dagsorden bag en del af denne udvikling; det gør det f.eks. meget lettere for de russiske myndigheder at hævde, at Vesten fører "krig" mod Rusland (f.eks. Bartosj, 2018a: 10-13), selvom ingen bliver dræbt, og intet bliver sprængt i luften. Det er, som det ofte fremføres i den russiske debat, en ny type af krig. Talsmanden for Ruslands præsident Vladimir Putin, Dmitrij Pesjkov (2018), forklarede i et interview, at

*"Det er mere krig, end det ikke er krig. Det er helt sikkert krig (...) Når massemedierne udbreder løgne, og det ikke bare er tilfældige løgne, det er ondsindede løgne. Man møder dem særligt ofte i forbindelse med vores land. Når massemedierne bliver brugt i forsøget på at dæmonisere vores land. Er det så ikke krig? Det er krig."*

I forlængelse af dette er der faktisk en igangværende diskussion om og udvikling af begrebet ”krig” i det russiske forsvar (Gerasimov, 2017). Gerasimov forklarer, at der er forslag om ”grundlæggende at revurdere synet på indholdet og essensen af begrebet ’krig’ under de nuværende forhold”. Og han tilføjer, at tilhængere af denne tilgang argumenterer for, at ”væbnet kamp ikke [længere] er et nødvendigt element [af krig]. I dag kan man støde på definitioner som informationskrig, økonomisk krig, hybridkrig og mange andre varianter”. Russiske kritikere af denne fortolkning anfører, at ”den voksende rolle for andre typer af kamp (økonomisk, ideologisk, psykologisk, informationsmæssigt m.m.) ændrer ikke ved essensen af fremtidens krig, den afgørende rolle for væbnet kamp vil forblive bevaret” (Tjekinov og Bogdanov, 2017: 32). Disse kritikere medgiver dog deres mere reformvillige kolleger, at der er kommet en ”principielt ny form for kamp – en informationskamp, hvis handlinger ligger til grundlag for begrebet bevidsthedskrig” (Tjekinov og Bogdanov, 2017: 38).

I forhold til denne artikel er det værd at hæfte sig ved, at der således er en konceptuel udvikling af begrebet ”krig” undervejs i Rusland, hvor det kinetiske element skubbes tilbage og tildeles en sekundær rolle. En mere vidtgående fløj i diskussionen er tilsyneladende klar til ikke blot at tildele det kinetiske element en sekundær rolle i vores forståelse af ”krig”, men også at skrive det helt ud af definitionen. Uanset det endelige udfald synes alle enige om, at alt peger i retning af en stadig mere central rolle for informationsoperationerne. Derudover er det vigtigt at pointere, at ”informationskrig” er et særdeles veletableret begreb i såvel den tidligere sovjetiske som den nuværende russiske forskning, herunder i høj grad i den militært styrede forskning (f.eks. Savadskij, 1996; Potjeptsov, 2000; Kunakova, 2012; Markov, 2018 og Krasovskaja et al., 2019; for en diskussion se Muratova, 2018). Det er dette begreb, der har fundet vej til titlen på denne artikel.

Det skal tilføjes, at begrebet ”informationskrig” i Rusland ofte også indeholder et teknologisk aspekt (Savadskij, 1996; Dilevskij et al., 2014; Gerasimov og Sjakirova, 2017; Kapralov og Tjernjajkov, 2018; Nikulin, Sidorin og Ivanov, 2018; Muratova, 2018). Fokus i denne forbindelse er da på infrastrukturen, som gør det muligt at indsamle, lagre, behandle og videresende data. Det er med udgangspunkt i såvel offensive som defensive operationer udført i såvel militære som civile systemer. Forskningen i anvendelsen af teknologi foregår uafhængigt af kognitive effekter, men som nævnt er der en stor interesse i fællesmængden mellem de to områder.

## Domæner

Hvis en informationsoperation har en effekt – hvilket jo slet ikke er givet, at den vil have – så finder denne sted i det kognitive domæne. Tidligere studier har visualiseret en verden med tre domæner – et fysisk, et digitalt og et kognitivt – hvor såvel stater som mennesker agerer (Hansen, 2018).<sup>4</sup>

Det kognitive domæne er den arena, hvor tænkningen sker. Det er her, vi træffer beslutninger om så forskellige forhold som f.eks. indkøb, fritidsaktiviteter og stemmeafgivelse. Som sociale væsener og med begrænset rationalitet (Tversky og Kahneman, 1974; Kahneman, 2011) er vi relativt letpåvirkelige af ydre forhold og træffer ofte suboptimale beslutninger. Vi har f.eks. behov for at føle os set og anerkendte og for at indgå, på baggrund af forskellige givne statusser, i sociale sammenhænge. Samtidig er vi nødt til at analysere verden med de redskaber, vi nu engang har fået, og vores kognitive kapacitet er begrænset; vi kan kun overskue en vis mængde information, og når vi så behandler den information, som vi kan rumme, bliver vi påvirket af bl.a. en mængde ikke-erkendte bias, som truer med at forringe kvaliteten af vores beslutningsprocesser (Kahneman, 2011; Haselton, Nettle og Andrews, 2016).

Vores sociale behov og begrænsede rationalitet er velkendte faktorer, og begge forhold kan udnyttes af aktører, som ønsker at påvirke os. De får hjælp af f.eks. psykologer med speciale i social adfærd eller kognition – psykologer som er gået over på ”den sorte side” – og derfor finder vi bogtitler som f.eks. ”Manipulation af bevidstheden” (Kara-Mursa, 2018), ”Propagandaens teknologier” (Novikov og Gerasimov, 2019) og ”Rygter: Teknologier for deres styring” (Ignatjuk, 2018). De nævnte bogtitler er alle russiske, men det er naturligvis et universelt forskningsfelt, som ikke er særegent for Rusland.

Dernæst er det digitale domæne. Denne betegnelse bliver benyttet for at fremhæve, at det er her, vi finder den digitale infrastruktur, og at forholdsvis højt digitaliserede stater som f.eks. Danmark har investeret meget, herunder afhængighed og muligvis sårbarhed, i dette domæne. Det er i dette domæne, stater iværksætter cyberoperationer, og domænet omtales da også ofte som cyberdomænet. Operationer i det digitale domæne kan være begrænset til dette domæne – det kan f.eks. være hacking af data eller angreb på styresystemer – men de kan også have deres endelige effekt i det fysiske domæne og/eller det kognitive domæne. Det digitale domæne er jo forholdsvis nyt, men alle stater er aktive der, og i 2018 nåede verden et gennembrud i brugen af internettet, da det blev rapporteret, at flere end 50 pct. af alle mennesker i verden nu har adgang til internettet.

Tidligere studier (f.eks. Hansen, 2018) har skrevet om et igangværende ”Big Bang” i det digitale domæne (primært) og i det kognitive domæne (sekundært). Med det menes, at domænets rammer bevæger sig væk og udad. Vi ser det tydeligst i det digitale domæne, hvor rammerne hastigt bliver skubbet udad af bl.a. kvantecomputere og kunstig intelligens (”Artificial intelligence”, AI). Men vores viden om kognitive processer er også vokset betragteligt i de seneste årtier, og vi ved derfor også mere om f.eks. beslutningsprocesser. De to domæner byder hver især og isoleret set på væsentlige udviklinger, som forskellige aktører kan benytte i håbet om at nå deres mål. Men *kombinationen* af udviklingerne i såvel det digitale som det kognitive domæne byder også på meget store muligheder – og det er især brugen af det digitale domæne som

nøgle til det kognitive domæne, som er væsentlig i denne sammenhæng (f.eks. Buntovskij og Tonjan, 2019).

Til sidst er så det fysiske domæne. Det er det domæne, som traditionelt forbindes med krig, og som vi lettest kan forholde os til. Informationsoperationer ses i dag primært i forbindelse med det digitale domæne – ovenfor omtalte jeg det som fællesmængden mellem det teknologiske og det kognitive – men de kan naturligvis også gennemføres i det fysiske domæne. Det kan f.eks. ske i form af demonstrationer. ”Lisa-sagen” fra 2016 er et eksempel, da repræsentanter for det russiske samfund i Tyskland i stort tal gik på gaden for at kræve, at den russisk-fødte og dengang blot 13-årige Lisa blev reddet fra påståede seksuelle overgreb begået af arabiske migranter. I Moskva blev budskabet forstærket af pressekonferencer med bl.a. udenrigsminister Sergej Lavrov og andre højtstående politikere (Ejdelman 2018, 56-9). Et andet eksempel er russiske diplomaters påståede organisering af demonstrationer i Athen i 2018 *imod* et forlig mellem Grækenland og Republikken Nordmakedonien om navnet på sidstnævnte (Hansen, 2018). Forliget banede vejen for Nordmakedonien til at blive medlem af NATO.

Operationer i det fysiske domæne kan efterfølgende viderebringes som operationer i det digitale domæne – f.eks. i form af nyheder understøttet af optagelser fra demonstrationerne og af interviews med deltagere – som derefter rammer det kognitive domæne. Operationerne i det fysiske domæne har bl.a. den fordel, at billeder fra begivenhederne kan øge sandsynligheden for, at den tilsigtede effekt bliver opnået. Forskning indikerer, at forekomsten af billeder – fotos eller video – i en nyhedshistorie kan forstærke modtagerens interesse (Novikov og Gerasimov, 2019: 85), følelsesmæssige respons og derefter prægningen af vedkommendes politiske præferencer (Soroka et al., 2016; også Domke, Perlmutter og Spratt, 2002). En aktør vil i sidste ende kunne skaffe billeder ved at iscenesætte operationer i det fysiske domæne eller ved at producere dem som deep fakes, dvs. digitalt manipulerede billeder (Resnick, 2018).

Aktuelt bliver der brugt mange ressourcer på forskning, drevet i f.eks. politisk og militært øjemed, om udviklingen i de tre skitserede domæner og om samtænkningen mellem dem. Det sker med henblik på bedre at forstå de muligheder, som domænerne bringer, men også for at kunne forsvare sig mod trusler som kan opstå. F.eks. rummer det nuværende danske forsvarsforlig (2018-2023) elementer fra alle tre domæner – det er f.eks. en ny udsendelsesbar brigade, nye missiler og midler til ubådsbekæmpelse (det fysiske domæne), yderligere udbredelse af sensornetværk og etablering af et situationscenter (det digitale domæne) foruden en indsats mod desinformation (det kognitive domæne). Samtænkningen gælder såvel offensive som defensive operationer; i forhold til sidstnævnte foregår indsatserne ofte under overskriften ”resiliens” (eller robusthed), dvs. opbygning og fastholdelse af fysisk, digital og kognitiv resiliens.

I den russiske forskning dækker betegnelsen ”hybridkrig” oftest over en sam-tænkning af operationer i de tre domæner; det er typisk med udgangspunkt i lavintense operationer, som er under niveauet for direkte konfrontation, men som alligevel over tid og i koordination med andre lignende operationer svækker en modstander. En af Ruslands førende eksperter i hybridkrig, Aleksandr Bartosj (2018b), argumenterer for, at nutidens krig er defineret ved en øget anvendelse af ikke-militære (dvs. ikke-kinetiske) virkemidler i staters forsøg på at opnå deres mål; han peger på politiske, økonomiske og informationsmæssige værktøjer og tilføjer så, at kampen også foregår i andre arenaer – ”diplomatiske, forskningsmæssige, sportslige, kulturelle, den er faktisk blevet total” (Bartosj, 2018b: 5). Et konstant og stadig mere dominerende bagtæppe til denne udvikling er informationsoperationerne, som kan afvikles inden for og til støtte for operationer i alle de nævnte arenaer. Det er en vigtig lære fra Gerasimov (2013).

Statens operationer i de tre domæner dimensioneres bl.a. af dens strategiske kultur. Jeg følger Alastair Johnston og beskriver kort strategisk kultur som ”det idemæssige miljø, som begrænser adfærdsvalg” (Lantis og Howlett, 2010: 88). Den strategiske kultur siger os noget om, hvor langt staten er villig til at gå, og om hvad den betragter som acceptabel adfærd. Den strategiske kultur beskrives ofte som mere eller mindre robust – en eufemisme for ”aggressiv” – og stater med robuste strategiske kulturer går ofte helt til stregen eller endog et skridt videre.

Traditionel tænkning om strategisk kultur har bundet denne til det fysiske domæne, f.eks. til brugen af atomvåben (Lantis og Howlett, 88-89), men statens operationer i de digitale og kognitive domæner er også dimensioneret af bl.a. dens strategiske kultur. I visse tilfælde bør vi identificere domænespecifikke strategiske kulturer og derefter samle disse i en overordnet strategisk kultur. En dybere forståelse af de domænespecifikke strategiske kulturer vil sandsynligvis også bidrage til at formulere mere effektive modsvar inden for hvert domæne. Et modsvar kan f.eks. komme i form af afskrækkelse (Morgan, 2019). Dette begreb er blevet udvidet i de senere år, bl.a. via en mere nuanceret forståelse af ”afskrækkelse via afvisning” (som modsætning til ”afskrækkelse via straf”), hvilket har givet aktører bedre værktøjer til at målrette deres modsvar.

Et hurtigt kig på de senere års statskontrollerede informationsoperationer fra Rusland vidner om en særdeles robust strategisk kultur i det kognitive domæne. Enkelte nedslagspunkter kan være Ruslands invasion af Krim i februar 2014, landets engagement i krigen i det østlige Ukraine siden foråret 2014, dets rolle i nedskydningen af det malaysiske fly MH17 i juli 2014 og i drabsforsøget på den russiske eksspion Sergej Skripal i marts 2018 foruden dets forsøg på at påvirke de amerikanske vælgere under præsidentvalget i USA i 2016. Fælles for alle eksempler er, at det officielle Rusland, understøttet af de statskontrollerede russiske medier, har afvist alle beskyldninger om disse aktiviteter, enten fuldstændigt eller i en periode. Eksemplerne rummer såvel offensive som defensive informationsoperationer; hvor sidstnævnte ofte blot

tager sigte på at minimere skaden for Rusland – og typisk har en panikagtig karakter over sig – er målet for førstnævnte at vinde indflydelse i et nulsums-spil, og disse operationer afspejler typisk en anden strategisk tænkning om den ønskede effekt.

## Værktøjerne

Som nævnt i indledningen er der et stort antal videnskabelige felter, som bidrager til at muliggøre og forklare informationsoperationerne. En russisk forsker gør det klart, at vi er nødt til at anlægge en ”poliparadigmatisk tilgang til undersøgelsen af informationskrig som et af aspekterne af nutidige social-politiske aktiviteter” (Kunakova, 2012: 95). Denne kompleksitet gør det vanskeligt, hvis ikke umuligt, at præsentere en fuldstændig liste over de anvendte værktøjer. Det kan være nyttigt at se informationsoperationerne som et læringskapløb mellem offensive og defensive aktører – der bliver konstant tænkt nyt for hhv. at udnytte og udbedre sårbarheder (f.eks. af psykologisk, teknologisk, juridisk og dannelsesmæssig art). Afsenderen vil konstant forsøge at optimere blandingen af platforme og kommunikation for at opnå den ønskede kognitive effekt hos modtageren. Som udgangspunkt vil den rationelle afsender have interesse for operationer, hvor den forventede gevinst er større end de forventede omkostninger. Inden for denne ramme bliver der tænkt nyt – det kan f.eks. være produktionen af spillefilm og serier (Petrova, 2018), udviklingen af bloggere (Gontjarov, 2018) eller oprettelse og redigering af opslag på Wikipedia (Garifullin, 2018).

I Rusland kan afsenderen f.eks. være statslige myndigheder, herunder efterretningstjenesterne (United States Senate, 2019, II: 7-8), statskontrollerede medier og private firmaer, som opererer i overensstemmelse med styrets interesser eller sågar efter kontrakt med staten (Letunovskij og Nikonorov, 2018 om outsourcing) eller individuelle bloggere på kontrakt (Gontjarov, 2018). Afsenderen kan tillige være en ikke-russisk aktør, herunder enkeltpersoner (The Guardian, 2017 og Straffeloven, 2019). Platformene er f.eks. de traditionelle medier, webbaserede medier og sociale medier. Den russiske litteratur (f.eks. Gratjev og Baranova, 2018 og Gontjarov, 2018) ser de sociale medier som fremtidens altdominerende platform, i Rusland såvel som i Vesten, men blandt en del af forskerne er der kritik af, at de russiske operationer ikke tilstrækkeligt rettidigt og effektivt er blevet orienteret i denne retning (f.eks. Astakhov, 2018 og Manoilo, 2018).

Mellem afsender og modtager står en del af teknologien som en forstærkende faktor. Det gælder f.eks. brugen af bots, dvs. computerprogrammer som kan videresende information i kaskader og interagere med rigtige brugere online. De kan benyttes som en forstærker til meget hurtigt at nå ud til en meget stor gruppe af modtagere. AI vil f.eks. kunne benyttes til at høste stadig mere data fra det kognitive domæne (via det digitale domæne hvor den enkelte bruger gør udtryk for forskellige typer af præferencer), behandle det i det digitale domæne og derefter sende det i stadig mere modtagerorienteret form tilbage i

det kognitive domæne. Afsenderne vil med ny teknologi vide meget mere om modtagerne, og de vil kunne sammensætte en stadig mere optimal blanding af kommunikation og platforme for at opnå deres mål. Teknologien vil muliggøre en langt bedre forståelse af den enkelte situationalitet og dermed også en kommunikation, som er stadig mere skræddersyet til individniveauet, dvs. mikromålrettet (se f.eks. Meduza, 2019b).

Det er en væsentlig forudsætning for den russiske stats aktiviteter i det kognitive domæne, at medierne i høj grad er statskontrollerede. Det har i første omgang betydning for muligheden for at gennemføre informationsoperationerne, men det medfører også, at der er en endog meget svag debat om den russiske stats aktiviteter og dens forsøg på at påvirke forskellige modtagere. Det putinistiske styre bliver af og til betegnet ”neautoritært” (f.eks. Becker, 2004), hvilket refererer til den manipulerende og kontrollerende brug af medierne i dagens Rusland. Den internationale NGO *Reporters without Borders* (2019) skønner, at Rusland i 2019 har en pressefrihed på 50,3 (på en skala hvor 0 er mest frit, og 100 er mindst frit), hvilket placerer landet på en 149. plads ud af i alt 180 undersøgte lande og mellem Venezuela og Bangladesh.



**Der er ikke som i sovjettiden direkte censur med medierne. Det er snarere en form for selvcensur, hvor redaktører og journalister pålægger sig selv en lang række begrænsninger, fordi de ikke vil eller tør rapportere kritisk**

Dette russiske medielandskab kan visualiseres som en enorm boble af statskontrollerede medier med en ultratynd periferi af frie medier udenom (Hansen 2019c). De statskontrollerede medier er enten ejet af staten, af virksomheder som er ejet af staten, eller af privatpersoner, som af forskellige årsager gerne vil være tæt på Kreml og derfor villigt lægger sendetid og spaltepads til de accepterede nyheder og fortolkninger. Der er ikke som i sovjettiden direkte censur med medierne. Det er snarere en form for selvcensur, hvor redaktører og journalister pålægger sig selv en lang række begrænsninger, fordi de ikke vil eller tør rapportere kritisk. Denne selvcensur i medieverden gør, at den russiske stat kan bringe et stort antal virkemidler i brug, og at den kan gå ganske langt i sin anvendelse af disse. Risikoen for at blive afsløret og udskammet af de russiske medier er forsvindende lille.

En af de mest kendte statsejede nyhedsplatforme i Rusland i dag er RT. Chefredaktøren er Margarita Simonjan, og hun gav i 2012 et bemærkelsesværdigt interview om platformens rolle og om sit syn på journalistik (Kommersant, 2012). Det skal bemærkes, at interviewet blev givet *efter* den russisk-georgiske krig om Sydossetien i 2008 men *før* Ruslands invasion og annektering af Krim i 2014. Simonjan er i øvrigt enig i den tidligere anførte kommentator om, at Rusland tabte informationskampen i 2008, og hun forklarer derefter, at

*”Nu kæmper vi ikke med nogen. Men vi kæmpede i 2008. Forsvarsministeriet kæmpede med Georgien, men vi førte informationskrigen, og med hele den vestlige verden. Men det er umuligt først at begynde at producere våben, når krigen er startet! Forsvarsministeriet er ikke i kamp med nogen, men de er klar til kamp. Sådan er vi også”.*

Intervieweren spørger derefter Migranjan, om RT er ”et forsvarsministerium, bare på TV?”, hvortil hun svarer, at ”når Rusland kæmper, er vi naturligvis på Ruslands side” (Kommersant, 2012). Det skaber selvsagt fordelagtige forhold for de russiske politikere at agere under, ikke mindst fordi ”kampen”, igen med hybridkrigsforskeren Bartosjs ord, ”faktisk [er] blevet total”. De amerikanske myndigheder tvang i 2017 RT Americas produktionsselskab T&R til at registrere sig som ”fremmed agent” hos USA’s justitsministerium, hvilket betyder, at RT America nu officielt betragtes som den russiske stats forlængede arm i USA.

Vi forbinder ofte Ruslands virkemidler på informationsområdet med desinformation, defineret her som ”intentionelt forkert information”. Det er med andre ord løgn, og afsenderen er bevidst om dette. Hvis desinformationen efterfølgende videreformidles af andre, som er uvidende om løggen, taler vi om misinformation. Intentionaliteten er afgørende i denne sontring. Den kan være væsentlig at fastholde, hvis man ønsker at analysere en bagvedliggende motivation. Desinformationen tiltrækker stor opmærksomhed, fordi den er grænseoverskridende i forhold til en udbredt opfattelse af, hvorledes politiske aktører og medier kan agere. Dertil kommer de simple forhold, at løggen spredes ”længere, hurtigere, dybere og bredere” end sandheden (Vosoughi, Roy og Aral, 2018), og at den ofte virker. Den russiske propagandaforsker Tamara Ejdelman forklarer (2018: 59), at ”hvis du i lang tid, med detaljer og mange forklaringer skaber et velsagtens virkelighedstro billede, vil folk tro mindre på det end på en simpel, men fræk løgn”.



**Vi forbinder ofte Ruslands virkemidler på informationsområdet med desinformation, defineret her som ”intentionelt forkert information”. Det er med andre ord løgn, og afsenderen er bevidst om dette. Hvis desinformationen efterfølgende videreformidles af andre, som er uvidende om løggen, taler vi om misinformation**

Desinformationen er beskrevet som en integreret og sofistikeret del af nyhedsformidlingen hos de russiske statskontrollerede medier (f.eks. Ramsay og Robertshaw, 2019 og Nemr og Gangware, 2019; også Antifake og East Stratcom). Det er især nogle af de mest højtprofilerede sager, som synes at være genstand for omfattende desinformationskampagner. Et eksempel er sagen om Skripal. Russiske statskontrollerede medier havde allerede på et tidligt tidspunkt fremført et stort antal tydeligvis falske og gensidigt inkompatible historier om

drabsforsøget – herunder at der slet ikke var tale om et drabsforsøg, såvel som at det var et drabsforsøg udført af en vestlig efterretningstjeneste (Hansen, 2018b). Denne sag er et eksempel på en defensiv operation, og som nævnt har de ofte en lidt panikagtig karakter over sig. Det eneste konstante element i mylderet af forklaringer var afvisningen af Ruslands skyld.

Desinformation forbindes typisk med *indholdet*, men det kan tillige være afsenderen og formen. Det kan f.eks. dreje sig om falske repræsentanter for en myndighed eller en befolkningsgruppe, falske eksperter, falske medier, falske profiler på sociale medier eller falske breve. Blandt de mere velkendte teknikker er falske profiler på sociale medier, som benyttes til at formidle egne opslag eller kommentere på nyhedshistorier eller på andre brugeres opslag. Det er især den meget omtalte ”Troldefabrik” i Sankt Petersborg (Novaja Gazeta, 2013, 2015), hvis aktiviteter er blevet beskrevet som ”industriel politisk krigsførelse” (Linwill og Warren, 2018), som er blevet symbol på denne form for påvirkning (United States Senate, 2018: 44-6). Virksomheden bag ”Troldefabrikken” er Agenturet for Internetforskning (Internet Research Agency, IRA). Efterretningsudvalget i USA’s senat (United States Senate, 2019, II: 5) har konkluderet, at IRA gennemførte sine aktiviteter efter ordre fra Ruslands regering.

I september 2019 offentliggjorde den russiske avis Argumenti i fakti (2019) en liste over kandidater til valget til Moskvas Duma, som den kendte russiske skuespiller Vasilij Lanovoj skulle have udarbejdet. ”Lanovojs liste” indeholdt 45 kandidater, en for hver valgkreds, som Lanovoj anbefalede at stemme på. Alle kandidater var pro-Putin. I Argumenti i fakti (2019) blev Lanovoj citeret for at erklære, at ”[når det gælder valget], ved jeg bare en ting: Jeg kommer til at stemme for dem 100 pct. Fordi jeg ved, at de her mennesker arbejder for landet, for hovedstaden, for Moskva.”

Lanovoj dementerede hurtigt historien, men ”Lanovojs liste” fortsatte sit eget liv på en lang række platforme, som avisen Meduza (2019a) senere kunne forbinde til et vidtforgrenet økosystem af stats- og Moskva-kontrollerede medier og virksomheder. Kampagnens formål var tydeligvis at benytte Lanovojs navn til at understøtte styrets kandidater og miskreditere oppositionen. Meduza (2019a) beskrev det som det nyeste inden for informationsoperationer, men celebrity endorsements i politik er velkendte (Pease og Brewer, 2008; O’Regan, 2014), og de russiske vælgere har tidligere set det i mere vidtgående form, f.eks. når celebrities har meldt sig ind i det magtbærende parti Det Forenede Rusland og endog er blevet valgt til Dumaen.<sup>5</sup> Men her var det altså et falsk endorsement, og det giver naturligvis sagen en anden karakter. Den væsentligste lære fra ”Lanovojs liste” er måske, at der bliver tænkt kreativt og kynisk i forsøget på at påvirke modtagernes politiske præferencer. Og så hører det med til historien, at ”Lanovojs liste” givetvis har haft langt større spredning end ”Lanovojs dementi”.

Desinformationen tiltrækker stor opmærksomhed, men de russiske statskontrollerede nyhedsplatforme domineres af regulær information, som er vinklet meget skarpt eller ensidigt. I det føromtalte læringskapløb kan den ensidige nyhedsdækning – som modsætning til den egentlige desinformation – være en fordel, da det er vanskeligere for udenlandske pressenævn at identificere klare brud på god presseskik. Der er dog eksempler på dette. F.eks. advarede det britiske pressenævn Ofcom (2018) i december 2018 såvel RT UK som det statskontrollerede russiske nyhedsbureau Sputnik om, at deres dækning i flere tilfælde havde været for ensidig. Det gjaldt bl.a. dækningen af sagen om Skripal, hvor, med Ofcoms ord, ”the viewpoint of the UK Government was not adequately represented within this programme and the programme had not included and given due weight to an appropriately wide range of significant views” (Ofcom, 2018: 39). Den ensidige nyhedsdækning viser populært sagt alle fordelene ved X og, måske i endnu højere grad, alle ulemperne ved Y, og så er det op til den enkelte nyhedsforbruger at træffe et valg mellem de to alternativer. Novikov og Gerasimov (2019: 55) forklarer, at hvis man vil have en modtager til at følge ens prædefinerede kurs, skal man bare videregive information om, at alternativerne ikke er farbare.

Ifølge Simonjan, chefredaktøren for RT, er der ”ingen objektivitet” i medieverden (Kommersant, 2012). Med dette udsagn ønsker hun ikke at henlede opmærksomheden på RT, men snarere på de vestlige medier, som hævder at repræsentere objektiviteten. Den statskontrollerede russiske informationspolitik italesættes i Rusland som en del af en perspektivistisk nyhedsstrøm. Eftersom medieverden ikke indeholder objektivitet – og i sin natur ikke kan gøre dette – er alle nyheder konstrueret af afsenderne. Nyhederne repræsenterer alle forskellige fortolkninger af forskellige begivenheder eller forskellige ”virkeligheder”, og det er op til den enkelte modtager at vælge mellem dem. Det sker i et nationalt eller internationalt nyhedsrum, hvor de forskellige fortolkninger konkurrerer med hinanden om opmærksomhed og om at have den ønskede effekt på modtageren.



**Målet for afsenderen er at ændre forholdet mellem virkelighed og forestilling som oplevet af modtageren – og jo større diskrepansen mellem virkelighed og forestilling, jo mere ustabil er systemet**

Den russiske forskning indeholder et meget stort antal teorier om, hvorledes en afsender bedst opnår effekt. Et fremtrædende eksempel er Novikov og Gerasimov (2019), som i deres arbejde fokuserer på, hvorledes man kan destabilisere ellers stabile systemer. De forklarer, at et system i balance skal have tilført energi for at blive sat i bevægelse og dermed blive ustabil. Energin leveres i form af information. Målet for afsenderen er at ændre forholdet mellem virkelighed og forestilling som oplevet af modtageren – og jo større diskrepansen mellem virkelighed og forestilling, jo mere ustabil er systemet (Novikov og Gerasimov, 2019: 50-1).

Det er en afgørende pointe, at virkeligheden skabes af den afsendte information, som samtidig fortrænger forestillingen, dvs. modtagerens oprindelige verdensbillede. Den nye information skal få modtageren til at erkende, at virkeligheden ikke er, som hun ellers troede. Ideen om destabilisering genfindes i litteraturen om hybridkrig, hvor informationsoperationer er et helt afgørende ikke-kinetisk redskab, som dog ofte anvendes sammen med mindre kinetiske indsatser. Russiske hybridkrigsforskere (f.eks. Bartosj, 2015) taler om at påføre en modstander en tilstand af ”kontrolleret kaos”, og teorien af Novikov og Gerasimov indeholder samme tanke, her blot gennemført via information alene.

Som nævnt skal informationen helst indeholde viden, som er ”ny, vigtig og aktuel”. Novikov og Gerasimov (2019: 92 og 51) tilføjer, at informationen bør appellere til følelserne, herunder til spørgsmålet ”hvem er den skyldige?”, og derudover være vanskeligt verificerbar (også Letunovskij og Nikonorov, 2018). Disse elementer genfindes ofte i konspirationsteorier. Studier (NN og Yablokov, 2015) har indikeret en omfattende udbredelse og anvendelse af konspirationsteorier i det russiske politiske system, hvorfra de kan finde vej til medierne. Fx har forskere fra universitetet King’s College (Ramsay og Robertshaw, 2019: 31-3) påvist, hvorledes RT UK og Sputnik begge har benyttet en række konspirationsteorier i forsøget på at så tvivl om de britiske myndigheders konklusioner i sagen om Skripal. Det er fx stærke antydninger af, at de britiske myndigheder faktisk selv stod bag angrebet i et forsøg på at tilsværte Rusland. Antydninger om mørke kræfter og skjulte årsagssammenhænge bærer i sig spørgsmålet om – og måske også svaret på – ”hvem er den skyldige?”. På den måde er konspirationsteorierne også oplagte redskaber, når en ny virkelighed skal skabes og en tidligere forestilling punkteres.

Novikov og Gerasimov (2019: 39) forklarer, at modtagere af information generelt ønsker at håndtere denne så økonomisk som muligt. Det styrende spørgsmål vil være ”hvilken type af hændelse er dette?”, og modtageren vil forsøge at matche spørgsmålet med så lille et katalog af svar og dermed kategorier som muligt. RT’s slogan – ”Question more” – er en tilskyndelse til modtagerne af RT’s nyheder til at åbne og anvende nye kategorier, og måske lukke eksisterende, til at deponere viden i. En kategori kan f.eks. være ”staten står bag”, og svaret inden da kan fortælle modtageren, at hændelsen er af den type, hvor en stat A gør noget fordækt for at kunne skyde skylden på stat B.

Ejdelman (2018: 56-58) illustrerer brugen af kategorier med sagen om Lisa. Desinformationen fra Rusland havde først som mål at appellere til en kategori, som kombinerede migranter og kriminalitet, men da denne med succes blev lukket fra tysk side, forsøgte de russiske politikere og medier sig derefter med en kategori, som kobledede mistillid til de tyske myndigheder. En kommentar i et russisk nyhedsprogram konkluderede, at ”der har været chikane af de russiske journalister i stedet for en omhyggelig undersøgelse”, og det blev fulgt af en opfordring til at få gennemført en ”objektiv undersøgelse” af sagen om Lisa (Ejdelman, 2018: 57). Svaret på spørgsmålet ”hvem er den skyldige?”, skiftede

således fra ”migranterne”, som skulle have begået overgreb på en mindreårig pige, til ”de tyske myndigheder”, som blev beskyldt for at fortie sandheden og forhindre den i at komme til offentlighedens kendskab.

## Effekt

Russiske forskere er generelt enige om, at informationsoperationerne virker, og at fremtiden entydigt vil byde på mere offensive, sofistikerede og effektfulde operationer. Ny teknologi gør, at ”mulighederne er ubegrænsede” (Gnesdilo, 2018: 110). En repræsentativ artikel (Popova og Fedorinov, 2018) i et russisk militært tidsskrift opsummerer status på denne måde:

*”den nutidige informationskrig kan man føre vedvarende, anonymt og ubemærket, i ethvert informationsrum, herunder på fremmed territorium. Objektet for angrebet er modstanderens kulturelle rum, hans bevidsthed, og det er muligt, at han i lang tid slet ikke erkender, at han er blevet genstand for et angreb eller styring udefra. Alt dette sikrer en betydelig effekt af påvirkningsmetoderne under en minimering af ”aggressorens” tab, samtidig med at det tillader denne at bevare udseende af at være en fredelig og civiliseret stat.”*

En anden forsker (Tsimbal, 2018: 69) supplerer ved at slå fast, at i informationskrigen er ”aggressoren, hans sande mål og de anvendte våben omhyggeligt skjult, og selv offeret for informationsangrebet ser ikke altid sig selv i denne rolle, hvilket gør en forudsigelse om informationsangreb umulig og vanskeliggør en effektiv planlægning af forsvarsforanstaltninger”.

Samtidig er det i russiske akademiske kredse en udbredt opfattelse, at Rusland er under massivt pres på informationsområdet, og at landet lider under dette pres. Dette er på trods af de mange tiltag, som er gjort af de russiske myndigheder. Den dominerende fortolkning hævder, at ”informationskrigen har ikke nogen afslutning – der er ingen årsag, som vil få aggressoren til at indstille sin påvirkning af offeret” (i Popova og Fedorinov, 2018: 19). I denne fortolkning er informationsoperationer således noget, som bare finder sted. Det ligger i forlængelse af opfattelsen af hybridkrig og – mere specifikt – den såkaldte ikke-lineære krig, at operationerne ikke på noget tidspunkt indstilles (Surkov/Dubovitskij, 2014). Det er en fortsat og konstant kamp om indflydelse, hvor information spiller en central rolle og hvor, med Surkovs ord, ”vi vinder. Eller vi går til grunde. Der er ingen tredje vej” (Surkov/Dubovitskij, 2014).

Det er vigtigt at huske på, at denne fortolkning af informationsoperationerne og Ruslands rolle i disse afspejler et stærkt russisk metanarrativ om Rusland som offer for Vestens politik (Hansen, 2016). Ifølge dette metanarrativ er Rusland låst i en konflikt med Vesten, og denne konflikt strækker sig flere hundrede år tilbage i tiden. Det er en konflikt, som er iværksat og vedligeholdt af Vesten. I forbindelse med dette er det oplagt for forskellige kilder at italesætte informationsoperationer fra Vesten som en næsten eksistentiel trussel mod den russiske stat (Astakhov, 2018). Mere konkret er denne italesættelse et mu-

ligt redskab til at legitimere dels en stadig mere omfattende kontrol med og begrænsning af adgangen til især information fra udlandet, dels en indsnævring af det politiske handlingsrum for især den russiske opposition, som ofte forbindes med Vestens hybridkrig mod Rusland.

Det må formodes, at de russiske myndigheder gennemfører en form for benchmarking, som muligvis endog indeholder f.eks. resultatkrav ifm. kontraktstyring. Denne formodning er baseret på en iagttagelse af praksis i den offentlige administration i Rusland, som er fokuseret på især kvantitative indikatorer. Som illustration kan nævnes Putins storstilede nationale projekter for årene 2018-2024 (Rådet for Strategisk Udvikling og Nationale Projekter under Ruslands Præsident, 2019), som f.eks. forudser fremstillingen af 900 klaverer til brug i børnehaver og opførelsen af 180 nye militære mindesmærker.

**➤➤ Den ubevidste og komplekse læring er ideelt set iværksat af afsenderen, så den imiterer en endogen præferenceformation hos modtageren. Sidstnævnte skal have fornemmelsen af selv at være kommet til den afgørende konklusion**

En benchmarking vil først og fremmest være baseret på kvantitative indikatorer, som når der f.eks. refereres til seertal for RT (f.eks. Panarin, 2018: 54). Denne type af måling kan tillige anvendes på f.eks. re-tweets og re-posts og lignende, og den er naturligvis lettere for de russiske afsendere at gennemføre end for andre. Og så forsøger de med stor sandsynlighed med kvalitative indikatorer også, dvs. en måling af effekten. Det er langt vanskeligere, og det er grundlæggende svært for såvel afsender som modtager at isolere operationen fra andre mulige påvirkninger. Den ubevidste og komplekse læring er ideelt set iværksat af afsenderen, så den imiterer en endogen præferenceformation hos modtageren. Sidstnævnte skal have fornemmelsen af selv at være kommet til den afgørende konklusion (Busjkova, 2018: 64). Ifølge Novikov og Gerasimov (2019: 47) opnår afsenderen dette ved at levere en ufuldstændig, men tilpas mængde information til modtageren. Skematisk kan det se således ud:

Afsender → information A og B → Modtager → Konklusion C. Ved denne proces er det vanskeligt at påvise effekt fra operationen.

Computational Propaganda Research Project ved Oxford Universitet (2018: 39) har analyseret data fra det amerikanske præsidentvalg i 2016 og har fundet, at IRA gennemførte en

”vedvarende indsats for at manipulere den amerikanske offentlighed og underminere demokratiet. På baggrund af års erfaring med at manipulere den offentlige mening i Rusland brugte IRA store sociale medier som Facebook, Instagram og Twitter til at ramme amerikanske vælgere og polarisere amerikanske brugere af sociale medier.”

Computational Propaganda Research Project (2018: 6-7) oplyser videre, at i årene 2015-2017 blev IRA's kommunikation på Facebook rettet mod amerikanske vælgere delt af knap 31 mio. brugere, givet likes 39 mio. gange, modtaget med emojis 5,4 mio. gange og med kommentarer 3,5 mio. gange. For Instagram er tallene 185 mio. likes og 4 mio. kommentarer. Denne trafik viser IRA's evne til at nå modtagerne via forskellige platforme, men den siger ikke noget om en eventuel effekt. Men det er naturligvis en forudsætning for en informationsoperation, at afsender finder en metode at overbringe sit budskab til modtager på. Her har IRA's strategi bekræftet den nuværende centrale placering for sociale medier og vist deres enorme potentiale. Trafikken blev i overvældende grad genereret af et meget lille antal sider og profiler, hvilket indikerer stor divergens i situationiteterne. Det har givetvis bragt værdifulde erfaringer til IRA og til andre russiske afsendere, som kan benytte denne viden til at forsøge at nå modtagerne mere præcist.

Den russiske litteratur indeholder af og til en forsigtigt indpakket kritik af den manglende effekt af den statskontrollerede russiske informationspolitik. Det sker typisk på baggrund af et ønske om at bidrage til at styrke Ruslands indsats i kampen mod Vestens informationskrig. Forskerne Buntovskij og Tonjan (2019: 20) konkluderer, at den russiske stat stort set kun kan påvirke udenlandske modtagergrupper via RT, og at den "praktisk taget ikke er i stand til at påvirke indholdet af sociale medier og deltage i den kamp om hjernerne, som bliver ført på internettet" (også Astakhov, 2018: 231).

Deres kollega Vitalij Korneev (2019, ingen sideangivelser) ser så nærmere på RT Tyskland, og han forklarer, at den tyske offentlighed forbinder platformen med "postfaktualitet", "russisk propaganda" og en "forvrængning af facts". Korneev forklarer endvidere, at RT Tyskland kun har "et lille publikum", og at kanalen er forblevet i "informationsundergrunden". Han foreslår i øvrigt, at RT Tyskland ændrer sin politik og bl.a. lægger en del af postfaktualiteten fra sig og desuden præsenterer en bredere vifte af holdninger.

Den russiske forsker Sergej Kara-Mursa (2018: 267), hvis forskellige arbejder om manipulation er anerkendt som nøglekilder blandt hans russiske fagfæller, forklarer, at forsøg på prægning er afhængige af, i hvor høj grad det lykkes at isolere modtageren fra "fremmed påvirkning". Det ideelle miljø, tilføjer han, er karakteriseret ved "et totalt fravær af alternative, ukontrollerbare kilder til information og holdninger". Som tidligere beskrevet er der en betydelig statskontrol med informationsrummet i Rusland, hvilket letter opgaven med at præge samfundet som helhed. Kara-Mursa diskuterer ikke russisk påvirkning af vestlige publikummer, men det er en implicit pointe i den netop nævnte kommentar, at påvirkning er vanskelig under forhold af pluralisme. Og så gør han det klart (2018: 235), at "middelklassen er en politisk aktiv klasse og et grundlag for demokratiet, og demokrati vanskeliggør manipulation af bevidstheden".

I den russiske litteratur findes tillige en lang række anbefalinger til forbedrede indsætter. Disse anbefalinger følger oftest af fortællingen om Rusland som offer for Vestens informationskrig. En af de mest vidtgående stemmer er Igor Panarin, en kendt russisk forsker med speciale i informationsoperationer og med stærke relationer til forsvaret og det politiske niveau. Panarin (2018: 58-9) anbefaler bl.a. en ”optimering af de statslige massemediers aktiviteter, gennemførelsen af en mere aktiv linje [for dem] i det globale informationsrum via dannelsen af et specielt integreret system af koordinerende og styrende organer til informationskamp”.

Jevgenij Astakhov fra MGIMO, udenrigsministeriets universitet, beklager, at ”på trods af visse fremskridt på informationsområdet er der fortsat en tendens til passivt forsvar, retfærdiggørelse og ikke til en initiativrig og offensiv politik” (Astakhov, 2018: 227). Han tager Panarins ide videre og foreslår ”dannelsen af en statslig institution til at koordinere alt informationsarbejdet; soft power (...), propaganda og kontrapropaganda”. Henset til vigtigheden af opgaven anbefaler han, at den nye koordinerende institution skal referere direkte til præsidenten (Astakhov, 2018: 226).

Fra en del af den militære forskning lyder tilsvarende kritik. Tisjin og Palunin (2018, ingen sideangivelser) har et omfattende katalog af forbedringspunkter. Det omfatter bl.a. bedre analyse, tættere koordination mellem institutioner, mere kvalificeret arbejdskraft og en højere grad af uafhængighed af vestlig teknologi. Popova og Fedorinov (2018: 19-20) gør det klart, at

”staten kan forsvare sig selv effektivt i informationskampen, men [det skal ske] under iagttagelse af et enkelt nødvendigt forhold – dette forsvar skal være aktivt, med anvendelse af alle midler til informationsaktiviteter, med eksponering af hele spektret af ydre og indre fjender, opbygningen af en kapacitet i informationssystemerne og eksponering og udnyttelse af modstanderens stærke og svage sider”.

Desuden er det en gennemgående klage i en del af litteraturen, at der mangler økonomiske ressourcer til at gennemføre operationer på et tilstrækkeligt højt niveau (f.eks. Astakhov, 2018).

## Interessen for informationskrig i Rusland er enorm

Computational Propaganda Research Project (2019: i) konkluderer i sin årsrapport fra 2019, at ”databaseret propaganda – brugen af algoritmer, automatiseringer og big data til at præge det offentlige liv – er blevet en gennemtrængende og allestedsnærværende del af hverdagslivet”. Det er meget sandsynligt, at den registrerede stigning i brugen af informationsoperationer på denne måde vil fortsætte sin dramatiske stigning i de kommende år. Forskerne bag projektet hæfter sig især ved autoritære regimers forsøg på at påvirke primært deres egne borgere, men i visse tilfælde tillige borgerne i andre lande (2019: i). Den overvældende kontrol med det nationale informationsrum gør det muligt for disse styre at nærme sig Kara-Mursas idealmiljø karakteriseret ved et

”totalt fravær af alternative, ukontrollerbare kilder til information og holdninger”. Samtidigt kan kontrollen bidrage til at muliggøre operationer rettet mod udenlandske modtagergrupper, da risikoen for at blive afsløret af hjemlige medier er minimal.

Interessen for informationskrig i Rusland er enorm, og der bliver tænkt og formuleret spændende nyt. Det er oplagt, at den russiske stat vil fortsætte med at udforske mulighederne for at opnå resultater i alle tre domæner. Ruslands konflikt med Vesten er så skarp og de tilgængelige ressourcer til brug i denne konflikt så forholdsvis få, at Rusland med stor sandsynlighed vil afsøge de videre potentialer i især de ikke-kinetiske redskaber. Fællesmængden mellem de digitale og kognitive domæner udvikler sig så hurtigt og er så perspektivrig for afsenderen af information, at alternativomkostningen ved et fravalg med stor sandsynlighed vil være uacceptabel.

Ruslands strategiske kultur tilsiger, at landet vil gå helt til stregen i sin anvendelse af informationsoperationerne. Russiske forskere pointerer ofte, at den moderne informationskrig føres ”uden nogen som helst form for moralske grænser” (f.eks. Butusova og Sobranskaja, 2018: 42), hvilket kan ses som en mulig legitimering af en robust politik. Den fremtidige udvikling vil primært foregå internt i Rusland, men det er meget sandsynligt, at Rusland tillige vil eftersøge samarbejde med ligesindede stater, f.eks. for at kunne afstemme og forstærke budskaber (Mainolov, 2018; Sakulin, 2018) og for at kunne retfærdiggøre operationer.

Samtidig skal det erindres, at der i den russiske debat er stemmer, som kritiserer Ruslands indsats for at være utilstrækkelig. Som nævnt er disse kilder vanskelige at håndtere, da de generelt er en del af fortællingen om Vestens informationskrig mod Rusland og om behovet for skrappere og flere midler for at forsvare landet mod indre og ydre fjender. Men der synes også i denne debat at være en reel kritik af, at Ruslands strategi er ukoordineret, underoplyst, underfinansieret og teknologisk underlegen. Den videre debat må vise, om disse kritikpunkter bliver adresseret.

Endelig er det vigtigt at pointere, at det vigtigste informationsrum for de russiske politikere er det hjemlige. Dette rum er blevet endnu mere væsentligt efter de omfattende demonstrationer, som fandt sted i Rusland, og især i Moskva, i august 2019 (Hansen, 2019c). Efter planen skal der afholdes valg til Dumaen i 2021 og til præsidentposten i 2024, og styret vil givetvis tilstræbe at styre informationsrummet og eliminere ”alternative og ukontrollerbare kilder”. Dette fokus vil muligvis tage en del af ressourcerne – tidsmæssige og økonomiske – fra operationer rettet mod Vesten i de kommende år.

## Noter

- 1 Vladislav Surkov er rådgiver for Ruslands præsident Vladimir Putin.
- 2 Våbenliggørelse er et nyttigt begreb, som minder os om tænkningen bag brugen af ikke-kinetiske redskaber til at opnå visse mål. Det er også problematisk, da vi fortsat mangler en klar forståelse af, hvornår og hvorledes handlinger løftes fra det ordinære til det våbenliggjorte.
- 3 De to processer, som er modsætninger, men også to ender af et spektrum, kan også beskrives som f.eks. hhv. adaptation og læring.
- 4 De tre domæner har forskellige ontologiske statusser.
- 5 Eksempler er gymnasten Alina Kabajeva, tennisspilleren Marat Safin og bryderen Aleksander Karelin.

## Referencer

- Akhatova, K. (2019), "Mesjkulturnaja kommunikatsija v sovremennikh realijakh informatsionnogo protivoborstva v mirovoj politike", *Nautjnie trudi KubGTU*, 4: 244-50.
- Antifake; på <https://theins.ru/category/antifake>.
- Argumenti i fakti (2019), "Stal isvesten 'spisok Lanovogo' na viborakh v MGD" (den 3. september).
- Astakhov, Jevgenij (2018), "K polemike ob informatsionnikh sadatjakh Rossii", *Mesjdunarodnie protsessi*, 16(2): 223-32.
- Bartosj, Aleksandr (2015), "Rasrusjitelnij tandem: tsvetnaja revolutsija – gibridnaja vojna", *Nesavisimoje voennoje obosrenie* (den 24. juli).
- Bartosj, Aleksandr (2018a), *Konflikti XXI-ogo veka – Gibridnaja vojna i tsvetnaja revolutsija*, Moskva: Gorjatjaja linija – Telekom.
- Bartosj, Aleksandr (2018b) "Strategija i kontstrategija gibridnoj vojni", *Voennaja misl*, 10: 5-20.
- Becker, Jonathan (2004), "Lessons from Russia", *European Journal of Communication*, 19(2): 139-63.
- Buntovskij, Sergej og Margarita Tonjan (2019), "Informatsionnie ugrosi novejshego vremeni i organi gosudarstvennogo upravlenija", *Aktualnie problemi ekonomii i obsjtjestva*, 3: 8-20.
- Busjkova, Assel (2018), "Tekhnologii informatsionnogo vosdejstvija na gosudarstvennost Rossijskoj Federatsii: Puti protivodejstvija", *Gramota*, 9: 63-7.
- Butusova, I. og I. Sobranskaja (2018), "Spetsifika informatsionnikh vojn v postindustrialnom obsjtjestve", i *Sotsialno-polititjeskie protsessi v menjajusjtjemsja mire: Mesjvusovskij sbornik nautjnikh trudov*, Tver: Tver Statsuniversitet: 39-43.
- Computational Propaganda Research Project (2018), *The IRA, Social Media and Political Polarization in the United States, 2012-2018*, Oxford: University of Oxford.
- Computational Propaganda Research Project (2019), *The Global Disinformation Order: 2019 Global Inventory of Organised Social Media Manipulation*, Oxford: University of Oxford.
- Dilevskij, I. et. al. (2014) "Mesjdunarodnij resjim nepasprostranenija informatsionnogo orusjija: utopija ili realnost?", *Voennaja misl*, 10: 3-12.
- Domke, David, David Perlmutter & Meg Spratt (2002), "The primes of our times?", *Journalism*, 3(2): 131-59.
- East Stratcom; på <https://euvsdisinfo.eu/>
- Ejdelman, Tamara (2018), *Kak raboet propaganda*, Moskva: individuum.
- Ekspert (2019), "Suverennij, sasjtjsjtjennij, svoj", 8: 12-7.
- Feldman, David (2000), "Public Confidence in Cyber-systems: Issues and Implications for Sustainability", *International Political Science Review*, 21(1): 23-42.
- Gamaeva, L. og D. Vojlova (2019), "Informatsionnie tekhnologii i informatsionnie vojni", *Nautjnie trudi KubGTU*, 3: 117-25.
- Garifullin, Ramil (2018), "Fenomen neopredeljonnosti v Vikipedii i jejo rol v obrasovatelnoj sisteme", i E. Baksjutovij, O. Jusupovoj og E. Dvojnukovoj, red., *Sbornik nautjnikh trudov*, Samara: Samara Statslige Tekniske Universitet, pp. 12-8.
- Gerasimov, N. og E. Sjakirova (2017), "Sotsialno-setetsentritjeskie vojni sovremennosti: realnost informatsionnoj epokhi", *Voennaja misl*, 10: 79-87.
- Gerasimov, Valerij (2013), "Tsennost nauki v predvideniii", *Voенno-promisjlennij kurer* (den 28. februar).
- Gerasimov, Valerij (2017), "Mir na granjakh vojni", *Voенno-promisjlennij kurer* (den 15. marts).
- Gnesdilova, Elena (2018), "Informatsionnaja vojna: Tekhnologija ili forma kommunikatsii?", *Strategitjeskie kommunikatsii v bisnese i politike*, 4: 107-12.
- Gontjarov, I. (2018), "Tekhnologii manipuljatsii massovim sosnaniem v internete (na primere sajta InoSMI)", i S. Akhmetov et. al., red., *Integririvannije kommunikatsii v sporte i turisme: Obrasovanie, tendensii, mesjdunarodnij opit*, Krasnodar: KGUFKST, pp. 170-5.
- Gratjev, S. og T. Baranova (2018), "Rol 'novikh media' v sovremmenikh konfliktakh", *Vestnik Moskovskogo gosudarstvennogo oblastnogo universiteta*, 4: 33-40.

- Hansen, Flemming Splidsboel (2016), "Russia's relations with the West: Ontological security through conflict", *Contemporary Politics*, 22(3): 1-17.
- Hansen, Flemming Splidsboel (2018a), "Russian influence operations", *DIIS Policy Brief*: 1-4.
- Hansen, Flemming Splidsboel (2018b) "Russisk disinformation på skærmen", *DIIS Policy Brief*: 1-4.
- Hansen, Flemming Splidsboel (2019a) "Inside the Russian digital domain", *DIIS Policy Brief*: 1-4.
- Hansen, Flemming Splidsboel (2019b) "Inde i det russiske digitale domæne", *DIIS Podcast*.
- Hansen, Flemming Splidsboel (2019c) "Putins Rusland", *DIIS Long-read*.
- Haselton, Martie, Daniel Nettle og Damian Murray (2016), "The Evolution of Cognitive Bias", i Davis Buss, red., *Handbook of Evolutionary Psychology*, Hoboken, NJ: John Wiley, pp. 968-87
- Ignatjuk, Natalja (2018), *Slukhi: Tekhnologii upravlenija*, Moskva: Justitsinform.
- Kahneman, Daniel (2011), *Thinking, fast and slow*, London: Penguin.
- Kaldor, Mary (1999), *New and old wars: organized violence in a global era*, Cambridge: Polity Press.
- Kapralov, V. og M. Tjernjakov (2018), "Vsaimosvjas ponjatij 'antigosudarstvennaja propaganda' i 'informatcionnaja vojna'", *Voennaja misl*, 1: 68-73.
- Kara-Mursa, Sergej (2018), *Manipuljatsija sosnaniem*, Moskva: Rodina.
- Kolnosjenko, V. og O. Kolnosjenko (2019), "Internet v kulture: snatjenie i posledstvija vlijanija", *Nautjnije trudi Moskovskogo gumanitarnogo universiteta*, 3: 71-81.
- Kommersant (2012), "Njet nikakoj objektivnosti" (den 7. april).
- Korneev, Vitalij (2019), "Problema vosprijatija telekanala Russia Today v FRG i ego perspektivi na nemetskom mediarinke", *Vek informatii*, 5; på [www.age-info.com/2019/5](http://www.age-info.com/2019/5).
- Krasovskaja, Natalija, et. al., (2019), "Tekhnologii informatcionnykh vojn protiv Rossii", *Vlast*, 3: 42-6.
- Kunakova, Ljudmila (2012), "Informatcionnaja vojna kak objekt nautjnogo analiza", *Almanakh sovremennoj nauki i obrasovanija*, 6: 93-6.
- Labusj, Nikolaj (2018), "Indeks aggressivnosti kak kriterij informatcionnij vojni", *Vek informatcii*, 1(2): 293-5.
- Lantis, Jeffrey og Darryl Howlett (2010), "Strategic Culture", i John Baylis, James Wirtz og Colin Gray, red., *Strategy in the contemporary world*, Oxford: Oxford University Press.
- Letunovskij, P. og G. Nikonorov (2018), "Sovremennij informatcionnij ekstremism kak ugrosa natsionalnoj besopastnosti Rossii", *Etnosotsium*, 4: 28-36.
- Linville, Darren og Patrick Warren (2018), "Troll Factories: The Internet Research Agency and State-Sponsored Agenda Building"; på [http://pwarren.people.clemson.edu/Linville\\_Warren\\_TrollFactory.pdf](http://pwarren.people.clemson.edu/Linville_Warren_TrollFactory.pdf).
- Ljagusjkin, Igor (2019), "Effekti primenenija strategitjeskikh kommunikatsii", *Sotsialno-gumanitarnoe obosrenie*, 1: 124-7.
- Manoilo, A. (2018), "Rossijskij podkhod k formirovaniju prostranstva kollektivnoj informatcionnoj besopastnosti stran BRIKS", *Sotsialnie i gumanitarnie snanija*, 4(3): 156-63.
- Manoilo, A., A. Petrenko og D. Frolov (2017), *Gosudarstvennaja informatcionnaja politika v uslovijakh informatcionno-psikhologitjeskoj vojni*, Moskva: Gorjatjaja linija – Telekom.
- Markov, Aleksandr (2018), "K istorii informatcionnykh vojn", i *Aktualnye problemy sotsiologii i upravlenija*, Sankt Petersburg: Sankt-Petersborgs Statslige Økonomiske Universitet, pp. 15-22.
- Meduza (2019a), "Troll factories? So 2016" (den 9. september).
- Meduza (2019b), "The information nation" (den 20. september).
- Morgan, Patrick (2019), "The Past and Future of Deterrence Theory", i Jon Lindsey og Erik Gartzke, red., *Cross-Domain Deterrence*, Oxford: Oxford University Press, pp. 50-65.
- Muratova, Ju. (2018), "Susjtjnost informatcionnoj vojni v regionalnom polititjeskom konflikte i osnovnie formi jejo projavljenija", *Kommunikologija*, 6(1): 34-45.
- Nemr, Christina og William Gangware (2019), *Weapons of Mass Distraction*, Washington, DC: Park Advisors.
- Nikulin, Je., A. Sidorin og O. Ivanov (2018), "Radioelektronnaja borba v sukhoputnikh vojskakh voorusjennikh sil SShA", *Voennaja misl*, 11: 100-9.
- NN (under udgivelse), "Conspiracy Theories in Russian Security Thinking", *Journal of Strategic Studies*.
- Novaja Gaseta (2013), "Gde sjivut trolli, i kto ikh kormit" (den 9. september).
- Novaja Gaseta (2015), "Kak stat trollkhanterom" (den 11. marts).
- Novikov, Vitalij og Konstantin Gerasimov (2019), *Tekhnologii propagandi*, Moskva: Flinta
- O'Regan, Valerie (2014), "The celebrity influence: do people really care what they think?", *Celebrity Studies*, 5(4): 469-83.
- Ofcom (2018), *Ofcom broadcast and on demand bulletin*, 369 (den 12. december)
- Panarin, Igor (2018), *Informatcionnaja vojna i kommunikatsii*, Moskva: Gorjatjaja linija – Telekom.
- Pease, Andrew og Paul Brewer (2008), "The Oprah Factor: The Effects of a Celebrity Endorsement in a Presidential primary Campaign", *Press/Politics*, 13(4): 386-400.
- Pesjkov, Dmitrij (2018), "Pesjkov rasskasal o sostojanii informatcionnoj vojni v mire", *Interfax* (den 20. december).
- Politiken (2017), "Seniorforsker: Russerne fucker med vores hjerner", (den 3. maj).
- Popova, S. og V. Fedorinov (2018), "Tseli i posledstvija informatcionnoj vojni", *Vosjdusjno-kosmitjeskie sili. Teorija i praktika*, 6: 15-21.

- Potjeptsov, Georgij (2000), *Informatsionnie vojni*, Moskva: Refl-buk.
- Ramsay, Gordon og Sam Robertshaw (2019), *Weaponising news – RT, Sputnik and targeted disinformation*, London: King's College.
- Reporters Without Borders (2019), *2019 World Press Freedom Index*; på <https://rsf.org/en/ranking>.
- Resnick, Brian (2018), "We're underestimating the mind-warping potential of fake video", *Vox* (den 24. juli).
- Roskomnadzor (2019), "Business FM: Roskomnadzor ugrojsjaet Google sanktsijami sa 'reklamu nesakonnikh massovikh meroprijatij'" (den 12. august); på <http://rkn.gov.ru/press/publications/news68986.htm>.
- Rådet for Strategisk Udvikling og Nationale Projekter under Ruslands Præsident (2019), *Natsionalnie projekti: Tselivie pokasateli i osnovnie rezultati*, Moskva: Rådet for Strategisk Udvikling og Nationale Projekter under Ruslands Præsident.
- Sakulin, Sergej (2018), "Kontent-analis informatsionnikh resursov rossijskoj diaspori", *Obosrevatel*, 8: 84-98.
- Savadskij, I. (1996), "Informatsionnaja vojna – sjto eto takoe?", *Konfident*, 4: 1-14.
- Soroka, Stuart et al. (2016), "The Impact of News Photos on Support for Military Action", *Political Communication* 33(4): 563-82.
- Speller, Ian og Christopher Tuck (2009), "Introduction", i David Jordan et al., red., *Understanding modern warfare*, Cambridge: Cambridge University Press, pp. 1-13.
- Straffeloven* (2019), LBK 376 (den 17. september).
- Surkov, Vladislav/under pseudonymet Natan Dubovitskij (2014), "Bes neba", *Pioner* (den 12. marts).
- Surkov, Vladislav/under pseudonymet Natan Dubovitskij (2019), "Dolgoe gosudarstvo Putina", *Nezavisimaja Gazeta* (den 11. februar).
- The Guardian* (2017), "Be ashamed, Alex': Salmond courts controversy with RT" (den 17. november).
- Tisjin, Maksim og Evgenij Polunin (2018), "Ugrosi informatsionnoj besopasnosti Rossijskoj Federatsii", *Filo Ariadne*, 4.
- Tjekinov, S. og S. Bogdanov (2016), "Voennaja strategija: Vsgljad v budusjee", *Voennaja misl*, 11: 3-15.
- Tjekinov, S. og S. Bogdanov (2017) "Evolutsija susjnosti i sodersjanija ponjatija 'vojna' v XXI stoletii", *Voennaja misl*, 1: 30-43.
- Tsimbal, E. (2018), "Informatsionnaja vojna i jejo manipulativnie atributi", *Trudi RGUPS*, 3: 68-72.
- Tversky, Amos og Daniel Kahneman (1974), "Judgment under uncertainty: Heuristics and biases", *Science*, 185: 1124-31.
- United States Senate, Committee on Foreign Relations (2018), *Putin's Asymmetric Assault On Democracy in Russia and Europe: Implications for US National Security*, Washington, DC: US Government Publishing Office.
- United States Senate, Select Committee on Intelligence (2019), *Russian Active Measures Campaigns and Interference in the 2016 U.S. Election*, Washington, DC: US Government Publishing Office.
- Vosoughi, Soroush, Deb Roy og Sinan Aral (2018), "The spread of true and false news online", *Science*, 359: 1146-51.
- Yablokov, Ilya (2015), "Conspiracy Theories as a Russian Diplomatic Tool: The case of *Russia Today (RT)*", *Politics*, 35(3-4): 301-15.