ATLANTSAMMENSLUTNINGEN
– forum for sikkerhedspolitik

Atlant Brief

Russian Information Warfare - russisk informationskrigsførelse

Jeanette Serritzlev og Lars Bangert Struwe (ansvh.red.)

Maj 2020

Indledning og indholdsfortegenelse

For at kunne håndtere en trussel er det også væsentligt at forstå den. NATO's tilgang til informationsaktiviteter er typisk afgrænset geografisk og tidsligt, underlagt regulering og baseret på et demokratisk værdigrundlag. Det gælder sjældent for de aktiviteter, som NATO samlet og medlemslandene hver især møder i informationsmiljøet.

Udfordringerne er ikke altid er synlig eller erkendt. Påvirkninger kan antage mange former og har været brugt, langt før der var nogen, der tænkte på internettet. Det er derfor væsentligt at tænke ud over Twitter og Facebook - og ud over påvirkning af et enkelt valg.

Kampen i informationsmiljøet pågår kontinuerligt, og uanset om vi deltager aktivt eller ej, indgår vi passivt. Derfor er det også vigtigt at have kendskab til de udfordringer og muligheder, som det bringer.

Indhold

Introduktion til Information Warfare

Særligt siden den russiske annektering af Krim-halvøen i 2014 tegner der sig et billede af et Rusland, der agerer mere målrettet og offensivt i sine bestræbelser på opnåelse af sine strategiske målsætninger. En del af dette sker i konfrontationen med Vesten og bliver i stigende grad gennemført i informationsdomænet rettet mod forskellige målgrupper og med forskellige formål.

Disse aktiviteter kan samles under den engelske betegnelse "Information Warfare"; på dansk informationskrig. Kampen i informationsdomænet er naturligvis ikke afgrænset til Rusland; både andre stater og ikke-statslige aktører agerer ligeledes aktivt i informationsdomænet. Det er bare ikke emnet her.

Information Warfare som begreb opstod i 1980'erne* [1], men tankegangen er lige så gammel som krigen selv: Når Sun Tzu taler om, at den største krigskunst ligger i at undertvinge fjenden uden kamp, taler han således om at opnå en effekt i det kognitive domæne.

I dette Atlant Brief anvendes informationskrig som begreb for alt det, der foregår i informationsdomænet, og som sker med henblik på at præge modstanderens vilje, perception og adfærd. Information Warfare defineres her ifølge forfatterens egen definition på følgende måde:

Information Warfare er en samlebetegnelse for en tilgang til og anvendelse af indflydelsesmidler i informationsdomænet; indflydelsesmidlerne kan være fysiske eller elektroniske, der skal præge en målgruppes (stat; befolkningsgruppe; individ) perception, handling og adfærd med henblik på at påvirke dennes beslutningstagning. [2]

Note

* Ifølge Douglas H. Dearth vurderes Thomas P. Rona at være den første til at anvende termen Information Warfare allerede i 1976, jf. "Rethinking the Application of Power in the 21st Century", Military Intelligence Professional Bulletin, 1997-1.

Introduktion til Information Warfare

Information Warfare handler således om meget mere end falske Twitter-konti og memes. Aktiviteterne kan både foregå i den virtuelle og fysiske verden og handler ikke kun om information, som man distribuerer, men også om information, som man beskytter (informationssikkerhed; og information, som man besværliggør eller hindrer andre i at dele (f.eks. ved jamming eller cyberangreb).

Det er også vigtigt at forstå, at informationskrigsførelse foregår i alle dele af konfliktspektrummet og således ikke er afgrænset til konflikt eller krig. Information Warfare er hverken begrænset til en bestemt fase, et geografisk område eller et specifikt niveau: Information Warfare kan udføres som konkrete taktiske aktiviteter eller foregå på højeste politisk-strategiske niveau.

Russisk informationskrig

"In the 21st century, we have seen a tendency toward blurring the lines between the states of war and peace. Wars are no longer declared and, having begun, proceed according to an unfamiliar template."

General Valery Gerasimov
chef for den russiske generalstab (2013)

Ovenstående citat [3] er brugt så mange gange, at det synes klichépræget at medtage og mangelfuldt at undlade. Gerasimov er dog hverken den første eller eneste, der har skrevet om et opgør med den traditionelle skelnen mellem krig og fred. Lignende tanker findes eksempelvis også hos den militærteoretiker og tidligere oberst i zarens hær Evgeny Messner (1891-1974), der så fremtidens krige udmønte sig uden en egentlig frontlinje og med det psykologiske domæne som det vigtigste. [4] Hans begreb 'Myatezh Voina' er på engelsk både oversat som 'mutiny war' og 'rebellion war', og hans tanker om kombinationen af både militære og ikke-militære midler til krigslige handlinger betyder, at han også af flere beskrives som den egentlige ophavsmand til forståelsen af moderne hybridkrig.

64-årige general Valery Gerasimov, som præsident Vladimir Putin den 9. november 2012 udnævnte til chef for den russiske generalstab. General Valery Gerasimov, der tillige er 1. viceforsvarsminister, er bl.a. udmærket med medaljen Den russiske Føderations Helt - føderationens højeste udmærkelse.

Russisk informationskrig

Men der var selvfølgelig også nogen før ham. Længe før hybrid blev et modeord definerede den amerikanske diplomat George Kennan i 1948 'political warfare' som "the logical application of Clausewitz' doctrine in time of peace. In broadest definition, political warfare is the employment of all the means at a nation's command, short of war, to achieve its national objectives". [5]

Hybridkrigstermen er fravalgt i dette Atlant Brief, fordi det i sig selv er så omdiskuteret et begreb, og fordi dette Atlant Brief er afgrænset til informationskrigsførelse - selv om grænserne kan være flydende. Uanset hvad er information et væsentligt element i hybrid krigsførelse; Igor Panarin, en markant russisk teoretiker på området, kalder f.eks. informationskrigsførelse for kernen i hybrid krigsførelse. [6]

Russisk informationskrig bygger på gamle principper, som vi kender fra Den Kolde Krig, men som Vesten synes at skulle lære på ny. Information er et middel blandt flere til at opnå statens mål og til t bekæmpe interne som eksterne trusler. Information Warfare er ikke afgrænset til en væbnet konflikt, men indgår i et kontinuum over hele konfliktspektrummet. Ligeledes skal det ses som noget, der foregår på alle niveauer; fra politisk-strategisk niveau til militære enheders taktiske anvendelse af informationsaktiviteter.

Russisk informationskrig har ligeligt fokus på defensive og offensive aktiviteter samt interne og eksterne trusler mod statens sikkerhed. Tilgangen er tæt knyttet til russisk strategisk kultur, hvor der er tradition for en stram regulering af informationsmiljøet med statens sikkerhed for øje*.

Note

* For mere om strategisk kultur se f.eks. Jørgen Staun, "Ruslands strategiske kultur under Putin", Forsvarsakademiet, 2018.

Russisk informationskrig

Således lyder det da også i den russiske militærdoktrin fra 2014, at blandt de primære interne militære risici hører:

[S]ubversive information activities against the population, especially young citizens of the State, aimed at undermining historical, spiritual and patriotic traditions related to the defence of the Motherland. [7]

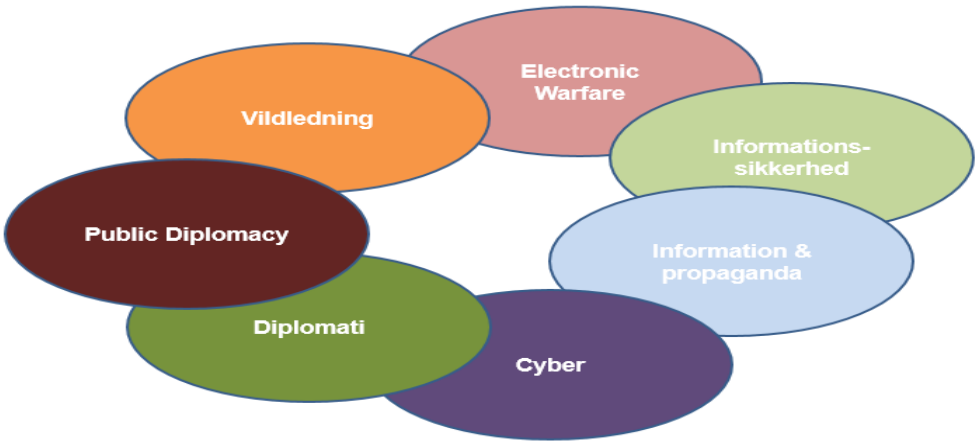
Militærdoктrinen fra 2014 er selvfølgelig skrevet til både et internt og et eksternt publikum, men der synes ingen tvivl om, at trusselsperceptionen af et Rusland, der er truet af [risikoen for] indre oprør og ydre aggression er til stede i visse miljøer. Den offensive anvendelse af påvirkningsaktiviteter, der i Vesten læses offensivt og aggressivt, kan derfor internt forsvares som defensivt i henhold til beskyttelsen af moderlandet.

Elementer og virkemidler

Russisk Information Warfare inddeles klassisk mellem informationspsykologisk og informationsteknologisk [8]:

- Informationspsykologisk krigsførelse er påvirkning af væbnede styrkers personel og civilbefolkningen. Dette er en proces, som gennemføres på permanent basis; altså også i fred.
- Informationsteknologisk krigsførelse er påvirkning af tekniske systemer, som modtager, samler og transmitterer information. Dette henhører under krige og væbnede konflikter.

Informationspsykologisk krigsførelse minder om det, der i NATO-doktrin er kendt som psykologiske operations og informationsoperationer, men adskiller sig blandt andet ved at være en kontinuerlig proces. Information Warfare er således paraplyen for alle discipliner i informationsdomænet og indeholder alle disse elementer:



Elementer og virkemidler

Virkemidlerne kan i princippet være alt, der understøtte opnåelse af målet. [9] Ovenstående virkemidler vil kunne anvendes simultant eller komplementerende - alt efter formål, tid til rådighed og prioritering af ressourcer.

Således vil en påvirkningskampagne rettet mod en bred målgruppe i forbindelse med en specifik sag eller aktivitet forventelig benytte flere medier og midler. Andre mindre aktiviteter rettet mod et begrænset publikum kan evt. være fokuseret om et bestemt medie eller virkemiddel. Dette kan både være, fordi den aktuelle sag ikke er prioriteret, eller fordi man vil teste et budskab af. Endelig kan en aktivitet også have til formål at agere informationsmæssigt røgslør, f.eks. ved at få målgruppens fokus til at flytte sig.

Reality Star eller Den russiske Føderations moderne zar? Præsident Vladimir Putin - der har en bachelor i jura og siden gjorde karriere i KGB med opnået rang af oberstløjtnant, og som blev chef for FSB - mestrer det meste. Det gælder også brugen af information til det publikum, han ønsker at ramme. Han lykkes med udtalelser, der fremstår som troværdige, selv om de i bund og grund ikke giver åbenbar mening, når man med kritiske øjne anskuer det russiske regime. Det gælder bl.a. udtalelsen om, at han ikke har lyst til at møde NATO-soldater i sin russiske baghave, medmindre de er inviteret som gæster - medmindre man er forbundet via en alliance. I alle tilfælde har præsident Vladimir Putin givet udtryk for, at han kan se Rusland som medlem af NATO. Sandt eller falsk? Ingen har indtil nu taget klar afstand fra, at han har ytret det - også, selv om det var RT, der den 3. juni 2017 bragte historien. [10]

Aktører

I princippet kan alle være aktører i informationsdomænet og dermed engagere sig i informationskampen. Men der er selvfølgelig forskel på, med hvilken effekt denne deltagelse sker, og hvilke kapaciteter forskellige aktører råder over.

I al væsentlighed er det værd at skelne mellem tre væsensforskellige aktørformer:

- Stater.
- Internationale organisationer.
- Ikke-statslige aktører.

Ikke-statslige aktører kan inddeles i to undergrupper:

1. Ikke-statslige aktører, der handler på vegne af en stat og/eller i en stats interesse; kan eksempelvis være (mere eller mindre) private virksomheder eller interesseorganisationer/tænketanke.
2. Ikke-statslige aktører, der handler uafhængigt, hvilket dækker over alt fra NGO'er, kommercielle organisationer og kriminelle netværk.

Informationsdomænet tilbyder således statslige som ikke-statslige aktører mulighed for at interagere med og influere på individers vilje og forståelse med en hidtidig uset hastighed og mængde af informationer, som går på tværs af landegrænser og platforme.

Målgrupper

I grove træk kan man i mange typer kommunikation tale om tre typer af målgrupper (modtagere):

1. Den gruppe, der allerede er enig med afsenderen.
2. Den gruppe, der aldrig bliver det.
3. Midtergruppen i form af tvivlerne, som kan tippe til begge sider.

Ofte er kampen om midtergruppen, som ikke behøver at være én homogen gruppe, men hvis eneste fællestræk af, at de ikke er overbevist til den eller anden side. Russiske informationsaktiviteter er ikke kun rettet mod målgrupper i Vesten og russere bosat uden for Rusland, men også rettet mod egne borgere i Rusland.

Fra push-strategi til pull-strategi

Inden for salg og marketing taler man om push- og pullstrategi. Pushstrategi er der, hvor man med reklamer og distributører aktivt forsøger at få promoveret sine varer over for målgruppen (kunden). Det er den strategi, man vil kunne tale om, når falske profiler eller bots videreformidler tweets eller opdateringer på sociale medier.

Pullstrategi handler derimod om at få målgruppen (kunden) til selv at opsøge varen. Det kan f.eks. være ved at stille professionelle medieprodukter til rådighed, som den relevante målgruppe selv opsøger og videreformidler, fordi det taler ind en bestemt holdning eller overordnet narrativ.

Når en dansk Facebook-bruger derfor deler et opslag fra RT (der tidligere var kendt som Russia Today) om integrationsproblemer i Sverige eller demonstrationer i Frankrig, er det jo - heldigvis - i vedkommendes gode ret at ytre et legitimt politisk synspunkt. Udfordringen kan være, at vedkommende ikke kender baggrunden for eller kilden til den delte information: Ud fra egne erfaringer er kendskabet til f.eks. RT forbavsende lavt blandt danskere. [11]

RT er som også interessant som 'informationsvåben', fordi det stiller kvalitetsprodukter gratis til rådighed for den borger, som måtte ønske et alternativt til det, som blandt andet præsident Donald Trump har gjort kendt som 'mainstream media'. Og dem er der mange af - også i Danmark.

På lignende vis kan man nævne memes. For fem år siden grinede mange måske af Putin-memes, hvor han red på bjørne eller var iscenesat i en heroisk rolle. Kendetegnende ved mange af disse memes er imidlertid, at de understøtter et narrativ om en potent, handlekraftig statsleder - som ofte står alene i rammen af naturens urkræfter eller sammenlignes med kastrerede ledere i Vesten, der fremstår handlingslammede.

Hvornår er der så tale om påvirkning, satire eller en demokratisk samtale på nettet? Svaret er ikke sort eller hvidt. Derfor er påvirkningsområdet også både vanskeligt og komplekst at håndtere - og så meget mere relevant at undersøge.

Interesse i en lavintensiv konflikt

Rusland vurderes bl.a. af Forsvarets Efterretningstjeneste ikke at være interesseret i en konventionel militær konflikt med NATO [12], men kan være overlegen i informationsdomænet, hvor den russiske tilgang tilbyder mere offensive midler, også i fredstid. NATO's medlemsstater har et svagt punkt, når det gælder effektive responsmuligheder i informationsdomænet, hvilket giver Rusland mulighed for at maksimere egen indflydelse.

Magtens mænd anno 2019/2020, som hver på deres vis påvirker udviklingen i verden baseret på deres definition af demokrati: Præsident Vladimir Putin (ved sin højre side ledsaget af general Valery Gerasimov), Rusland; præsident Hassan Rouhani, Iran; præsident Donald Trump, USA; og præsident Xi Jinping, Kina.

Interesse i en lavintensiv konflikt

Rusland har valgt en multifacetteret tilgang, der giver en høj grad af fleksibilitet i valg af midler og dermed opnå magtbalance eller i det mindste afbalancering i forholdet til Vesten. Russisk fokus på og anvendelse af informationsdomænet giver i denne henseende god logik, da aktiviteterne kan gennemføres under tærsklen for væbnet magt, men stadig føre til opnåelse af strategiske målsætninger, blandt andet ved anvendelse af strategisk maskirovka, hvor den statslige aktør kan gemme sig bag eller benægte relationer til ikke-statslige aktører, der handler i statens interesse.

Rusland kan indsætte statens samlede magtinstrumenter til at understøtte aktiviteter i informationsdomænet. Det gælder f.eks. anvendelsen af Russia Today og Sputnik, men også nationalt rettede medier, 'troldefabrikker' og mere subtile påvirkningsaktiviteter. Ruslands generelle mediekontrol gør informationsformidlingen lettere at styre og ensrette internt som eksternt.

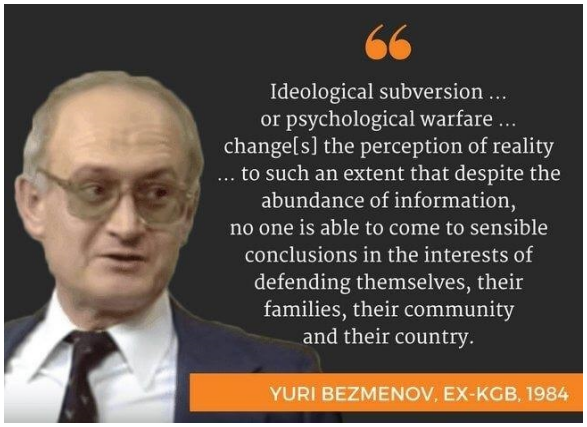
I informationsdomænet har Rusland fordelen og kan agere hele tiden og uden skelen til snitflader mellem information og propaganda. Rusland kan samtidig udnytte NATO's udfordringer med at skabe effektive modforanstaltninger.

Truslen i informationsdomænet

For at kunne håndtere en trussel er det også væsentligt at forstå den. NATO's tilgang til informationsaktiviteter er typisk afgrænset geografisk og tidsligt, underlagt regulering og baseret på et demokratisk værdigrundlag. Det gælder sjældent for de aktiviteter, som NATO samlet og medlemslandene hver især møder i informationsmiljøet.

En anden udfordring er, at truslen ikke altid er synlig eller erkendt. Når medierne skriver om risikoen for fremmede magters påvirkning, bliver det ofte et spørgsmål om troldehære, falske profiler på Twitter eller deep fake-videoer på YouTube. Men påvirkning kan dog antage mange former og har været brugt, langt før der var nogen, der tænkte på internettet. Det er derfor væsentligt at tænke ud over Twitter og Facebook - og ud over påvirkning af et enkelt valg. Det handler det ikke om, hvem der står som vinder af et diskursivt slag her og nu. Den inkrementelle metode kan vise sig stærkere end det hårde slag nu og her i form af prægning af perception over tid. Potentielt lang tid: Den sovjetiske afhopper Yuri Bezmenov taler i et kendt interview fra 1984 om plan på fire stadier for at ændre perceptionen hos en befolkning, hvor første stadie er en 'demoraliseringsfase' på 15-20 år.Det betyder selvsagt også, at det kan være vanskeligt at detektere undervejs. Yuri Bezmenov, der også var kendt under navnet Tomas David Schuman, var sovjetisk journalist arbejdende for RIA Novosti - forgængeren for RT - ligesom han også var informant for KGB. Under et ophold i Indien bliver han i 1970 afhopper, idet han flygter til Canada, hvor han tager fast ophold. I Canada bedrev han frem til sin død i 1993 journalistisk virksomhed med skarp kritik af Sovjetunionen.

Kampen i informationsmiljøet pågår kontinuerligt, og uanset om vi deltager aktivt eller ej, indgår vi passivt. Derfor er det også vigtigt at have kendskab til de udfordringer og muligheder, som det bringer.



Billedkreditering

Forsiden
dreamstime.com

Side 3
Mikhail Metzel, TASS.

Side 5
Matt Chase.

Side 6
Jeanette Serritzlev.

Side 9
globalsecurityreview.com.

Side 12
Screendump fra RT.

Side 13
glaringhypocrasy.com

Noter

[1]
Douglas H. Dearth, "Rethinking the Application of Power in the 21st Century, Military Intelligence Professional Bulletin, 1997-1": https://fas.org/irp/agency/army/mipb/1997-1/dearth.htm.

[2]
Jeanette Serritzlev, "Maskirovka.com: Ruslands tilgang vs. Natos til Information Warfare i et moderne informationsmiljø", 2018.

[3]
Valery Gerasimov, "The Value of Science Is in the Foresight", Military Insutrial Kurier, 2013.

[4]
Adam Klus, "Myatezh Voina: The Russian Grandfather of Wetern Hybrid Warfare": https://smallwarsjournal.com/jrnl/art/myatezh-voina-the-russian-grandfather-of-western-hybrid-warfare.

[5]
Rand, "Modern Political Warfare. Current Practices and Possible Responses, 2018: www.rand.org/t/RR1772.

[6]
Igor Panarin, "Strategic Communications and World Politics, in: Communications. Media. Design, Vol. 3, nr. 3", 2018.

[7]
Den russiske militærdoktrin 2014, punkt 13, stykke c.

[8]
Se bl.a. Keir Giles, "Handbook of Russian Information Warfare", 2016, side 9.

[9]
Se yderligere gennemgang i Keir Giles, "Handbook of Russian Information Warfare", 2016.

[10]
https://www.rt.com/news/390724-putin-clinton-russia-nato-stone/.

[11]
Egne erfaringer fra foredrag og undervisning samt en mindre onlineundersøgelse, hvor resultaterne kan læses her: https://www.linkedin.com/pulse/hvem-kender-russia-today-jeanette-serritzlev.

[12]
Forsvarets Efterretningstjeneste, "Efterretningsmæssig Risikovurdering 2019 - En aktuel vurdering af forhold i udlandet af betydning for Danmarks sikkerhed", 2019: https://fe-ddis.dk/Nyheder/nyhedsarkiv/2019/Pages/FEudgiverrisikovurderingfor2019.aspx.

Forfatterne

Jeanette Serritzlev
Jeanette Serritzlev er militæranalytiker på Institut for militære Operationer ved Forsvarsakademiet. Der arbejder hun med opgaver gældende hele påvirkningsområdet, hvilket vil sige informationsoperationer, psykologiske operationer m.fl. Jeanette Serritzlev er uddannet cand.mag. i dansk med speciale i politisk kommunikation fra Københavns Universitet. Derudover har hun en Master i Militære Studier fra Forsvarsakademiet med speciale i Information Warfare. Ud over ansættelsen ved Forsvarsakademiet har Jeanette Serritzlev gennem mange år beskæftiget sig med kommunikation og informationsoperationer i forsvaret - både som civilansat og som reserveofficer. Hun har i den forbindelse været udsendt til både Irak og Afghanistan som presseofficer.

Lars Bangert Struwe, ansvarshavende redaktør
Lars Bangert Struwe er ph.d. og generalsekretær i Atlantsammenslutningen. Lars Bangert Struwe har forud for sin ansættelse i Atlantsammenslutningen arbejdet med strategi og sikkerhedspolitik i bl.a. Forsvarsministeriet, Center for militære Studier og Forsvarskommandoen. Han har udgivet en større samling af faglitterært materiale, ligesom han er forfatter til Atlant Briefs.

Atlantsammenslutningen

Atlantsammenslutningen er en sikkerhedspolitisk tænketank, der med en forskningstilgang har til opgave at oplyse danskerne om sikkerheds-, forsvars- og udenrigspolitik.

Atlantsammenslutningen har i snart 70 år lagt stor vægt på det internationale samarbejde, det transatlantiske forhold og NATO.

Atlantsammenslutningen støttes af en årlig finanslovsbevilling via Udenrigsministeriet og Forsvarsministeriet.

Atlantsammenslutningen
Roskildevej 28A
2000 Frederiksberg C
Tlf. 3059 1944
Mail: atlant@atlant.dk

Læs mere på www.atlant.dk