Vil vi som nation kunne erkende et dansk GRIZZLY STEPPE?

Masterprojekt
MASTER I MILITÆRE STUDIER
Af: KL Henrik Bøgh
Vejleder: Dorthe Nyemann
Aflevering: Tirsdag d. 6. juni kl. 08:00.

ABSTRACT

In this project, I examine the US termed GRIZZLY STEPPE programme in a Danish context, with the purpose of evaluating it, in a cyber enabled opinion shaping context, based on the Russian theory of Reflective Control. Through a model of connecting Reflective Control as a basic framework for opinion shaping activities with cyber centric perspectives on tools for information warfare, I study a number of reports released by the Danish governments Centre for Cyber Security, with the purpose of noting similarities and differences as well as two specific opinion shaping events, targeted at Denmark by Russian actors. Next I create four scenarios based on the activities found in the two theories, which I use for deducing possibilities for recognizing cyber enabled opinion shaping activities target at Denmark.

Following that I draw lines towards election related cyber enabled opinion shaping activities, with recent events in the Netherlands, Germany and France as the centre and the upcoming Danish municipal election as a future alignment marker.

Finally, I conclude that due to a solid understanding and open dialogue in Denmark we are as a nation relatively robust in our possibilities of recognizing cyber enabled opinion shaping activities targeted at Denmark.

RESUMÉ

Den teknologiske udvikling har ændret måden hvorpå en stat i det skjulte kan påvirke en anden stats beslutningstagere. Formål og motiver kan således være uændrede, men værktøjer og metoder er skiftet og derfor bliver måden vi skal erkende påvirkningen på det også. Cybermuliggjorte meningsdannende aktiviteter er nogle af de nye typer af aktiviteter. Disse aktiviteter er aktiviteter der sker i cyberlandskabet, men som har til formål at danne bestemte meninger hos subjekterne.

De amerikanske myndigheder *Department of Homeland Security: National Cybersecurity and Communications Integration Center* og *Federal Bureau of Investigation* udgav d. 7. oktober 2016 en pressemeddelelse i form af en *joint statement*, som de indleder med følgende tekst:

> *"The U.S. Intelligence Community (USIC) is confident that the Russian Government directed the recent compromises of e-mails from US persons and institutions […]."*

Dette skulle vise sig at blive starten på det der senere er blevet døbt program GRIZZLY STEPPE. GRIZZLY STEPPE er det navn som amerikanske myndigheder, har givet en række aktiviteter, som tillægges aktører med forbindelse til de russiske militære og civile efterretningstjenester. En så præcis og håndfast angivelse af en aktør, var hidtil nærmest uset og særligt fra store etablerede efterretningsorganisationer. GRIZZLY STEPPE blev senere det første af en mængde aktiviteter, hvor forskellige firmaer og nationer nu angav de russiske efterretningstjenester som aktøren bag specifikke (ondsindede) aktiviteter i cyberlandskabet. I Danmark er der tillige gjort erfaringer med denne form for aktiviteter og i lighed med (og efter) de amerikanske myndigheders udgivelse af GRIZZLY STEPPE dokumenterne, har det danske Center for Cybersikkerhed (CFCS) udgivet rapporter omkring indtrængen i statslige systemer, hvor russiske efterretningstjenester angives som værende aktøren.

I nærværende projekt arbejder jeg med eksisterende eksempler på aktiviteter – både cybermuliggjorte og meningsdannende – hvor Rusland ses at være aktør. Jeg udfolder begrebet 'erkende' som afhængigt af kompleksiteten af det område, man skal erkende noget i, kan have forskellige former. Jeg udvikler til dette formål hvad jeg kalder en forståelses- og koblingskæde, til at håndtere nogle af disse komplekse dele. Simplere kæder kunne f.eks. være erkendelse af smerte: Hvis man brænder sin hånd på en havegrill erkender man smerten med det samme. Dette fordi vi ved hvad smerte er og vi forstår – instinktivt – at koble smerten og kæde den til en handling. Denne slags erkendelser skal foregå hurtigt og instinktivt, således at vi hurtigt kan trække hånden væk og undgå at blive yderligere forbrændt.

På tilsvarende vis skal vi også kunne erkende aktiviteter i såvel cyberlandskabet, som i relation til meningsdannende aktiviteter. Og i nærværende projekt hvor der arbejdes med cybermuliggjorte meningsdannende aktiviteter, skal der kunne ske en erkendelse og kobling på tværs af cyberlandskabet og de meningsdannende aktiviteter.

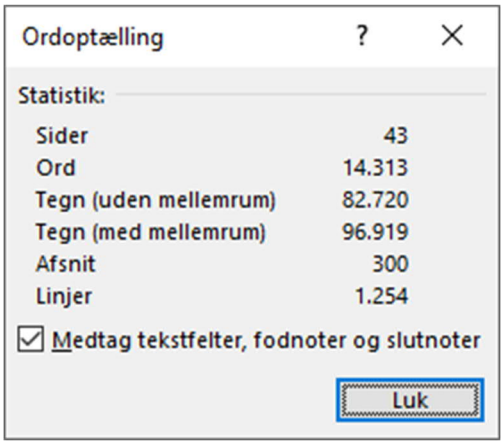
Jeg anvender to teorier der giver mig mulighed for, at undersøge cyberlandskabet som noget særligt og som giver mig mulighed for at undersøge et meningsdannende forhold.

Den første teori jeg har valgt er baseret på en tekst af assisterende generalsekretær i NATO Sorin Ducaru: *The Cyber Dimension of Modern Hybrid Warfare and its Relevance for NATO*. Ducarus tekst bringer tre anvendelser der ses at være særligt gældende for cyberlandskabet grundet den fordel som de knytter sig til: Det at informationer kan flyde frit, hurtigt og effektivt i cyberlandskabet. Den andel del af teoriapparatet er hentet fra Timothy L. Thomas' artikel *Russia's Reflexive Control Theory and the Military*. Thomas' tekst beskriver både den primære opgave, når der udføres refleksiv kontrol og relaterer det også til det underliggende begreb informationsressource. Gennem både opgavebeskrivelsen og informationsressourcebegrebet giver Thomas' tekst mulighed for, at knytte en særlig russisk doktrin til cybermuliggjorte meningsdannende aktiviteter.

På baggrund af de to teorier etablerer jeg en forståelse omkring begrebet *cybermuliggjorte meningsdannende aktiviteter*. Indeholdt i dette begreb skal der være elementer fra både cybermuliggørelse og meningsdannende i spil: Det er således ikke nok, kun at anvende ondsindet software eller have identificeret den effektive svaghed, men anvendes den ondsindede software på en sådan måde, at det er understøttet af identifikationen af den effektive svaghed, vil der være tale om cybermuliggjorte meningsdannende aktiviteter.

Endeligt gennemfører jeg en analyse hvorpå jeg konkluderer at det vurderes overvejende sandsynligt, at vi i Danmark er i stand til at erkende såfremt vi bliver udsat for cybermuliggjorte meningsdannende aktiviteter, der er tilsvarende til GRIZZLY STEPPE.

Antal anslag (med mellemrum) eksklusiv forside, abstract, resumé, indholdsforteg-nelse og referenceliste:



INDHOLD

INDLEDNING

Der er ikke noget nyt i at en stat i det skjulte forsøger at påvirke en anden stats beslutningstagere. Den teknologiske udvikling og globaliseringen har ikke ændret på det. Hvad den teknologiske udvikling har ændret på er måden, det kan gøres på. Formål og motiver kan således være uændrede, men værktøjer og metoder er skiftet. Dermed bliver måden vi skal erkende påvirkningen på det også. Cybermuliggjorte meningsdannende aktiviteter er nogle af de nye typer af aktiviteter. Disse aktiviteter er aktiviteter der sker i cyberlandskabet, men som har til formål at danne bestemte meninger hos subjekterne [1].

I gamle dage var internettet, der udgør en væsentlig del af cyberlandskabet, meget teknisk og forbeholdt de få, mens det særligt siden midt-00'erne har fået fæste som et bredt anvendeligt kommunikationsmiddel. Internettet er således i dag et væsentligt – og måske endda det væsentligste – kommunikationsmiddel, hvilket også åbner op for nye anvendelser.

Da det amerikanske Department of Homeland Security og Federal Bureau of Investigation i slutningen af december 2016 udgav den fælles rapport *GRIZZLY STEPPE – Russian Malicious Cyber Activity* [2], gjorde et forhold sig særligt gældende: En statslig, vestlig aktør[3] pegede på en anden statslig aktør som den udførende part af cybermuliggjorte meningsdannende aktiviteter. *Cybermuliggjorte meningsdannende aktiviteter* er aktiviteter der er en konvergens mellem aktiviteter for cybermuliggørelse og meningsdannende aktiviteter. Der er ikke vandtætte skotter mellem aktiviteterne [4], hvilket også ses i såvel GRIZZLY STEPPE rapporten [5], den udvidede analyserapport [6] og projektets efterfølgende behandling.

I Danmark er der tillige gjort erfaringer med aktiviteter for cybermuliggørelse, og i lighed med (og efter) de amerikanske myndigheders udgivelse af GRIZZLY STEPPE dokumenterne, har det danske Center for Cybersikkerhed (CFCS) udgivet rapporter omkring indtrængen i

[1] Et *subjekt* forstås i det efterfølgende som en eller flere personer eller grupper, der er målpersoner eller -grupper for aktørernes aktiviteter. Disse kan være enkeltindivider, grupper af personer eller organisationer. Se afsnittet *Aktører, subjekter og brugere*.

[2] U.S. Department of Homeland Security: National Cybersecurity and Communications Integration Center og U.S. Federal Bureau of Investigation, "GRIZZLY STEPPE – Russian Malicious Cyber Activity".

[3] En *aktør* forstås i det efterfølgende som en person eller gruppe der udfører handlinger, der har til formål at kompromittere, skade eller chikanerer en målperson eller en målgruppe. Dette kan være gennem de metoder og ved anvendelse af de værktøjer, der beskrives senere i projektet, men også gennem et antal andre aktiviteter. Se afsnittet *Aktører, subjekter og brugere*.

[4] De pågældende aktiviteter bliver i den fælles rapport karakteriseret som tre typer af aktiviteter: Spearphishing campaigns, cyber attacks og masquerading.

[5] U.S. Department of Homeland Security: National Cybersecurity and Communications Integration Center og U.S. Federal Bureau of Investigation, "GRIZZLY STEPPE – Russian Malicious Cyber Activity".

[6] U.S. Department of Homeland Security: National Cybersecurity and Communications Integration Center, "Enhanced Analysis of GRIZZLY STEPPE Activity".

statslige systemer. Således udgav CFCS i 2016 [7] undersøgelsesrapporten *Phishing uden fangst* om et langvarigt phishing-angreb mod det danske udenrigsministerium og i 2017 undersøgelsesrapporten *Én aktør, mange angreb* [8] om en mængde aktiviteter, der formodes at stamme fra den aktør, som i GRIZZLY STEPPE dokumenterne angives til at være støtte af eller en del af de russiske sikkerhedstjenester.

Vi er alle sammen potentielle ofre for ondsindede aktiviteter i cyberlandskabet og i mange tilfælde kan vi også håndtere disse – både som enkelte borgere såvel som større organisationer. Men der er en større og overlæggende udfordring når statslige aktører, med store mængder af ressourcer (teknologiske, vidensbaserede, menneskelige, økonomiske og infrastrukturmæssige) bringer (hvad subjekterne vil opfatte som) ondsindede aktiviteter i spil med henblik på at understøtte en særlig meningsdannelse.

Problemformulering

GRIZZLY STEPPE er et konkret produkt baseret på nogle konkrete hændelser. Skønt der er en del udfordringer omkring det at nå til bunds i hvem aktøren bag de specifikke aktiviteter er, sættes der med relativ fast hånd navn på: Rusland. Jeg vil med nærværende projekt gennem anvendelse af to teorier, lave en kobling mellem aktiviteter der bliver særligt muliggjorte i cyberlandskabet, grundet cyberlandskabets unikke karakteristika hvor informationer kan flyde frit, hurtigt og effektivt og meningsdannende aktiviteter. Jeg vil betragte de meningsdannende aktiviteter i et særligt russisk perspektiv for til sidst at fokusere en konvergens mellem cyberlandskabet og meningsdannende aktiviteter mod danske perspektiver.

Min problemformulering bliver som følger:

> *Med udgangspunkt i de aktiviteter Rusland påstås at have gennemført under "program GRIZZLY STEPPE", ses Danmark så at have mulighed for at erkende tilsvarende cybermuliggjorte meningsdannende aktiviteter?*

Motivering

Den 21. november 2017 bliver der afholdt kommunalvalg i Danmark. Både efter det engelske valg omkring fortsat medlemskab af den europæiske union ("brexit") i sommeren 2016 og efter det amerikanske præsidentvalg i efteråret 2016, har der været (til tider ganske heftig) debat om mulig russiske påvirkning af selve valget. Særligt i forbindelse med det amerikanske præsidentvalg har der været stærke påstande og voldsomme debatter, mens Rusland naturligt nok selv benægter alt.

[7] Center for Cybersikkerhed, "Phishing uden fangst - Udenrigsministeriet under angreb".

[8] Center for Cybersikkerhed, "Én aktør, mange angreb".

Idet der er parlamentsvalg i England d. 8. juni og forbundsvalg i Tyskland d. 24. september i år, er det nok ikke sandsynligt at det danske kommunalvalg i november er det, der vil have det største potentiale i forhold til russisk påvirkning, men omvendt kan der stadigvæk nogle aktører, der har en interesse i at udføre meningsdannende aktiviteter ved såvel kommunal- som parlaments- og forbundsvalg.

Med det som affarende punkt ser jeg det således som værende interessant at se på hvilke muligheder der er for at udføre aktiviteter i stil med dem, der er gennemgået i GRIZZLY STEPPE i Danmark og hvilken indflydelse det kan have og i forlængelse heraf: Hvordan de tekniske aktiviteter, aktiviteter for cybermuliggørelse og meningsdannende aktiviteter konvergerer. Dette leder i sig selv frem til en kontekst af valg, hvorfor det vil være naturligt at bringe det kommende danske kommunalvalg ind.

Dette forudsætter at der bliver foretaget en undersøgelse på hvilken form for meningsdannelse Rusland vil kunne være interesseret i udøve overfor såvel Danmark som specifikt i relation til valget. I sagens natur er det ikke muligt at vide præcist hvilke ideer og ønsker man kunne have i Rusland, men man kan sagtens forestille sig det følgende:
Rusland vil næppe være interesseret i at udføre aktiviteter der styrker det Konservative folkeparti, der som bekendt ønsker er meget forsvarsvenlige.

En undersøgelse over kommunalvalg i 2009, har påvist at kun 27% ville stemme på et andet parti til kommunalvalget, såfremt der var et samtidigt folketingsvalg [9]. Der ses således - desuagtet at kommunalvalgspolitikeres begrænsede indflydelse på den nationale sikkerhedspolitik [10] –, at gøres det konservative folkeparti svagere i kommunal sammenhæng, hvor måske også det danske dobbeltmandatprincip medfører indflydelse, vil dette også kunne have en effekt på den landspolitiske politiske udøvelse i partiet.
Et andet bud kunne derfor at skabe en offentlig mening, der sår tvivl om valgets legitimitet og dermed enten fordrer et nyt valg relativt hurtigt eller medfører at valget skal afholdes på et andet tidspunkt.
Partier der har udviser en generel form for ukonventionel adfærd og i noget omfang baserer sig på brud med den traditionelle politiske opfattelse kunne ligeledes få fremdrift simpelthen fordi de bryder med de traditionelle politiske normer. Og der vil også kunne være lokale partier, der læner sig op ad ”fredsteserne”, som det vil kunne være relevante for aktøren at støtte gennem sine aktiviteter.

[9] Børsmose, “Landspolitik og lokalpolitik splitter vælgerne”.

[10] Der kan dog være nogle anden- eller tredjeordenseffekter, hvorigennem kommunalpolitik påvirker national sikkerhedspolitik. Et eksempel på dette er diskussionerne om lukningen af militære installationer kontra lokale forhold omkring bibeholdelse af arbejdspladser.

Valget er dog kun en specifik kontekst, hvor der kan drages paralleller til GRIZZLY STEPPE dokumenterne, mens det i praksis må konstateres, at der finder en løbende og mere bred anvendelse af meningsdannende aktiviteter, hvor Rusland ses enten at være aktøren eller i hvert tilfælde yde indflydelse på aktøren. Som oftest vil vi som eksterne aktører se den del af den samlede kommunikationsmaskine der eksisterer officielt: RT.com, Sputnik News, Russia Insider og politiske bemærkninger gengivet i vestlige medier. I forlængelse heraf vil dokumenter frigivet fra aktører støttet af den russiske stat via WikiLeaks [11], også kunne støttes af såvel trolls [12] på blogs, Facebook og andre sociale medier, mens bolden løftes videre op af RT.com, Sputnik News, Russia Insider og politiske bemærkninger som gengives i vestlige medier på aktuel og relevant vis.

[11] Reuters, "CIA Identifies Russians Who Gave DNC Emails to WikiLeaks".

[12] Walker, "Salutin' Putin".

METODE OG DEFINITIONER

I det følgende vil jeg kort præsentere de kapitler som følger dette kapitel og projektets struktur. En udfordring der gør sig særligt gældende for det valgte område er begrebsanvendelse. Cyberområdet er på mange måder stadigvæk nyt og derfor er der en del begreber, hvor der ikke er etableret en fast standard for betydningen. En tværministeriel arbejdsgruppe har tidligere konkluderet at "[b]egreberne bliver anvendt forskelligt i den offentlige debat og af forskellige myndigheder. Dette kan bidrage til uklarhed på et i forvejen teknologisk komplekst område." [13] Det er derfor nødvendigt, for at kunne arbejde effektivt i nærværende projekt, at behandle udvalgte begreber særligt således at der findes en ens og gennemgående forståelse specifikt for dette projekt. Disse begreber beskrives i de efterfølgende underafsnit til dette afsnit. Afsnittet her afsluttes med afgrænsningerne for projektet.

Kapitlet *Teori* beskriver de to teorier, der er anvendt i nærværende projekt, herunder hvilke dele af de teorier jeg har valgt at fokusere på. Desuden gennemgås nøglebegreberne der vil være relevante for den videre analyse i projektet.

Det næste kapitel er *Sammenhængen mellem cybermuliggørelse og meningsdannende aktiviteter* og heri operationaliseres de to teorier, gennem en beskrivelse af hvordan cybermuliggørelsen sker for meningsdannende aktiviteter og hvad det er der er særligt for cyberlandskabet i forhold til meningsdannende aktiviteter i øvrigt.

Kapitlet *Hvad er GRIZZLY STEPPE og hvilke aktiviteter er der i det*, gennemgår de tekniske aktiviteter, der er beskrevet i de tre officielle GRIZZLY STEPPE dokumenter samt et baggrundsdokument udgivet af udgivet af det amerikanske *Office of the Director of National Intelligence*.

Efterfølgende er der i kapitlet *Hvilke danske aktiviteter har vi haft, der minder om GRIZZLY STEPPE?* en gennemgang af to undersøgelsesdokumenter fra Center for Cybersikkerhed (CfCS) om aktiviteter rettet mod det danske Udenrigsministerium [14] udgivet i 2016 og aktiviteter rettet mod især det danske forsvar [15] udgivet i 2017. Herigennem undersøges frem mod den særlige danske kontekst i forhold til GRIZZLY STEPPE dokumenterne. Efterfølgende gennemgås to meningsdannende aktiviteter, hvor det i det ene tilfælde formelt er Rusland der står som aktør, mens det i det andet antages at kunne være Rusland som stat (direkte eller indirekte).

[13] Forsvarsministeriet, "Redegørelse fra den tværministerielle arbejdsgruppe om Folketingets inddragelse ved anvendelse af den militære Computer Network Attack (CNA)-kapacitet", 5.

[14] Center for Cybersikkerhed, "Phishing uden fangst - Udenrigsministeriet under angreb".

[15] Center for Cybersikkerhed, "Én aktør, mange angreb".

Dette efterfølges af kapitlet *Hvilke aktiviteter kan vi se, der hvor meningsdannende og cybermuliggjorte aktiviteter konvergerer?* hvor der foretages en analyse af hvilke former for aktiviteter vi kan se. Forståelsen for hvilke former vi kan se, er nødvendig for, at kunne etablere mulighederne for at erkende de pågældende aktiviteter.

Kapitlet *Hvilke valgrelaterede cybermuliggjorte aktiviteter er der set?* analyserer et antal nutidige aktiviteter, der er såvel valgrelaterede og hvor der ses cybermuliggørelse.

Endeligt afsluttes projektet med en *Konklusion.*

Cyberlandskabet

Begrebet *cyberlandskabet* indgår ikke i selve problemformuleringen, men er et implicit begreb for hele projektet og derfor er det i denne sammenhæng nødvendigt at begrebsafklare. Begrebet ses at dække over alt, der foregår på eller transmitteres via elektroniske netværk, der er koblet på internettet. Der er normalt ikke tale om en klar og entydig definition, og f.eks. vil et Apple Watch falde udenfor definitionen, da det ikke selvstændigt transmitterer data på internettet, men anvender en iPhone til at gøre det. I dette projekt er definitionen dog nød til at omfatte alle enheder, der på den ene eller anden måde har forbindelse til internettet og kan derfor omfatte alt fra toastere til banksystemer og Apple Watches. Disse enheder kan kommunikere via særlige teknikker, der gør at indholdet er ”pakket ind” og i nogle tilfælde i flere eller mange lag eller gennem andre enheder. I de senere år er enheder, der bliver en del af cyberlandskabet dels blevet mindre og billigere, mens dels også at de finder ny udbredelse (som i f.eks. nogle fly, hvor man nu har internetadgang via WiFi mens flyet er i luften), hvorved cyberlandskabet og dets muligheder udvides.

Tilsvarende cybermuliggjorte meningsdannende aktiviteter

Tilsvarende cybermuliggjorte meningsdannende aktiviteter kan groft sagt udfoldes som de tekniske aktiviteter som beskrevet i GRIZZLY STEPPE dokumenterne og de danske undersøgelsesrapporter og dertil de cybermuliggørelsesaktiviteterne når disse konvergerer med de meningsdannende aktiviteter.

Overordnet set, ses GRIZZLY STEPPE dog at have understøttet meningsdannende aktiviteter gennem to cybermuliggørelsesaktiviteter: Dels gennem tyveriet af mails fra den demokratiske nationale kongres og efterfølgende frigivelse af interne mails. Herved opnåede man at påvirke det demokratiske partis kandidat og dels at så tvivl om det amerikanske valgs legitimitet ved at opnå adgang til de systemer der bliver anvendt i valgprocessen [16].

[16] U.S. Department of Homeland Security: National Cybersecurity and Communications Integration Center og U.S. Federal Bureau of Investigation, “Joint Statement from the Department Of Homeland Security and Office of the Director of National Intelligence on Election Security | Homeland Security”.

De tekniske aktiviteter kunne for eksempel også have været et Distributed Denial of Service (DDoS) angreb. Det er værd at bemærke at det faktisk ikke nævnes at der har fundet DDoS angreb sted i GRIZZLY STEPPE dokumenterne, men det medtages her til forklaringsbrug, da det er et begreb, som de fleste kender, da det har været anvendt hyppigt i den offentlige debat og af offentlige myndigheder og i øvrigt er et begreb, som der er en fælles forståelse af. Tilsvarende aktiviteter til et DDoS angreb ville således være, en aktivitet der medfører at en given service (det kunne være et partis hjemmeside) ikke længere er tilgængelig.

I relation til de konkrete aktiviteter, vil tilsvarende aktiviteter i en dansk kontekst kunne forløbe på den samme vis. Man vil således kunne forestille et phishingangreb mod en kandidat eller meningsdanner, med henblik på at dels at udstille personen og dels at foretage data extraction. Såfremt aktøren har succes med data extraction (der i princippet også kan baseres på mere ”klassiske” dyder, så som at klone en USB-stick der tilhører vedkommende), får man noget viden og indsigt, der giver mulighed for planlægge og gennemføre en mere effektiv phishing-kampagne mod såvel den pågældende, som andre personer i den relevante kreds. Dette kunne til eksempel være ved adgang til simple oplysninger som bankens navn og bankkonto eller telefonnummer på en relevant og nær samarbejdspartner.

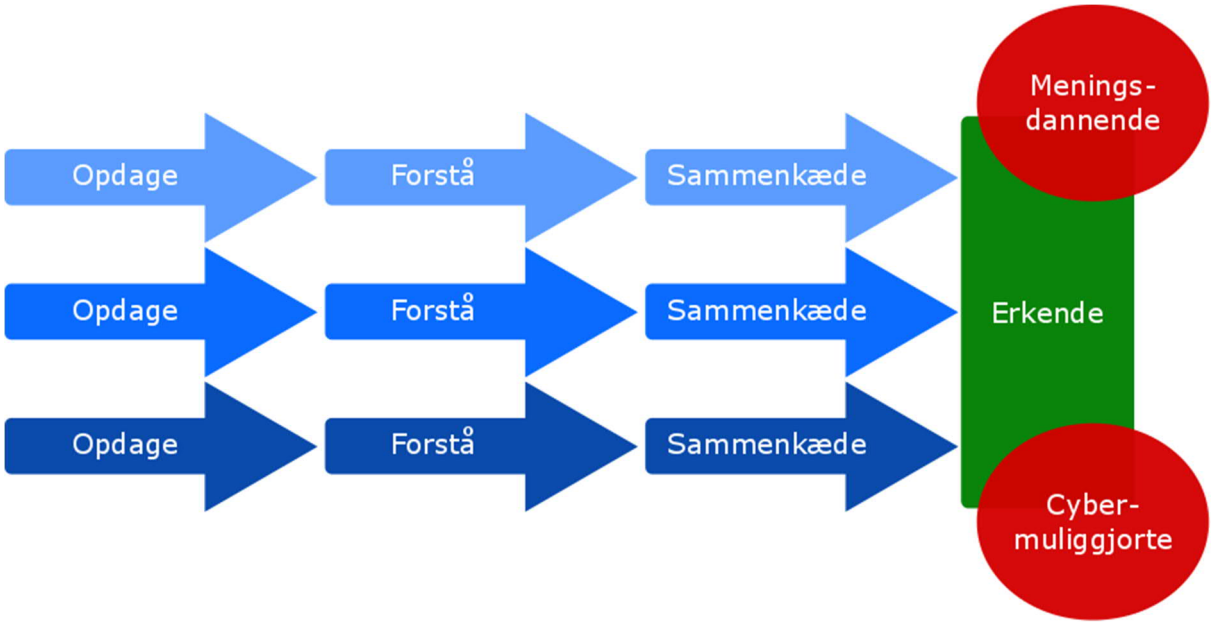
Resultatet af det første kan være at det bliver svært for nogle parter at få udbredt deres budskaber og de derfor bliver sat i en sværere position end andre parter, fordi de ikke har samme muligheder. Resultatet af det sidste kan være at informationer der ikke var tiltænkt for en bred kreds, pludseligt finder vej til offentligheden. Dette kan være f.eks. informationer om lovbrud, økonomiske forhold, medlemslister o.s.v.

Dertil kommer cybermuliggjorte meningsdannende aktiviteter, hvor der kan fødes data ind fra de to øvrige aktiviteter. Det oplagte mål her, vil være at miskreditere en aktør, men man kunne også forestille sig det modsatte, nemlig at en aktør vil kunne stilles i et mere favorabelt lys.

Erkende

At erkende kan være mange ting og afhængigt af kompleksiteten af det område, man skal erkende noget i, kan der være flere eller færre ting der bliver aktuelle. Jeg har valgt at kalde dette for en forståelses- og koblingskæde og i det aktuelle tilfælde er den designet således, at den passer til nærværende projekts emne. Simplere kæder kunne f.eks. være erkendelse af smerte: Hvis man brænder sin hånd på en havegrill erkender man smerten med det samme. Dette fordi vi ved hvad smerte er og vi forstår – instinktivt – at koble smerten og kæde den til en handling. Denne slags erkendelser skal foregå hurtigt og instinktivt, således at vi hurtigt kan trække hånden væk og undgå at blive yderligere forbrændt.

På tilsvarende vis skal vi også kunne erkende aktiviteter i såvel cyberlandskabet, som i relation til meningsdannende aktiviteter. Og i nærværende projekt hvor der arbejdes med cybermuliggjorte meningsdannende aktiviteter, skal der kunne ske en erkendelse og kobling på tværs af cyberlandskabet og de meningsdannende aktiviteter:



Figur 1 - Forståelses- og koblingskæde

Forudsætningen for at kunne *opdage* er at man som minimum forstår, det miljø som man kan udsættes for aktiviteter i. Dertil kommer at man på baggrund af opdagelsen også skal kunne forstå hvad det er for en form for aktivitet der sker. Man skal således ikke blot forstå miljøet, men også de muligheder og aktører der findes i – og påvirker – miljøet. I det efterfølgende trin skal man så – på baggrunden af forståelsen for muligheder, aktører, miljøet og den opdagelse man har gjort, kunne sammenkæde det til de opdagelser og forståelser man i øvrigt har gjort. Her er der ikke blot tale om i det pågældende miljø, men i alle de relevante miljøer. Først derefter vil det være muligt at nå frem til en egentlig erkendelse af, hvilken form for aktiviteter man bliver udsat for.

I ovenstående skitse illustrerer hver sekvens af 'opdage', 'forstå', og 'sammenkæde' et antal aktiviteter, der kan tage forskellige former og ske i forskellige miljøer. Der kan således være tale om, at man både skal opdage og sammenkæde en phishing-kampagne, en data extraction kampagne og en rekrutterings kampagne, før man rent faktisk er i stand til at erkende aktiviteten i sin helhed.

Alene det at opdage at man bliver udsat for disse aktiviteter kan være enormt udfordrende. Det forudsætter at man er i besiddelse af den tekniske kompetence og det nødvendige materiel (herunder hardware og software), der gør en i stand til at forstå de bevægelser der sker i ens systemer. Dette kan være gældende på flere lag – startende med det meget

tekniske (firewalls, sikre tunneller, 2 faktor godkendelse osv.) over til mere bløde værdier som f.eks. konkrete awareness kampagner, der har til hensigt at sikre eller ændre en given adfærd hos brugere og borgere i almindelighed og til de endnu blødere værdier i form af et oplyst samfund, frie medier og reflekteret dialog.

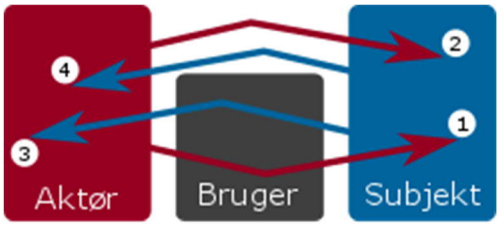
Aktører, subjekter og brugere

Generelt anvendes begreberne aktører, mål, ofre, afsendere, ondsindede personer m.m. på forskellige måder til at beskrive deltagerne i cyberaktiviteter og i refleksiv kontrol.

For cyberområdet skyldes det at der ikke findes en ensartet begrebskonvention og hvilket begreb man anvender afhænger ofte af hvem man kommunikerer til og hvilket område man beskæftiger sig med. I dette projekt har jeg valgt at anvende følgende tre begreber om de tre typer af deltagere, der behandles. Begreberne anvendes både i relation til refleksiv kontrol og til aktiviteter i cyberlandskabet og jeg har valgt at sammenkoble de to begreber, således at koblingen mellem cybermuliggørelse og meningsdannende aktiviteter tydeliggøres.

- Aktører i cyberlandskabet er dem der udfører handlinger, der har til formål at kompromittere, skade eller chikanere en målperson eller en målgruppe. Dette kan være gennem de metoder og ved anvendelse af de værktøjer, der beskrives senere i projektet, men også gennem et antal andre aktiviteter.
- Aktører for refleksiv kontrol er dem der udfører den refleksive kontrol. De leder subjektet i en bestemt beslutningsmæssig retning gennem kommunikation af og om bestemte motiver og årsager.
- Subjekter i cyberlandskabet er den eller dem, der er målpersoner eller -grupper for aktørernes aktiviteter. Disse kan være enkeltindivider, grupper af personer eller organisationer.
- Subjekter for refleksiv kontrol kan være grupper (herunder organisationer og stater) eller individer (typisk med stor indflydelse eller høj beslutningskompetence). Det er den eller dem der udføres refleksiv kontrol imod.
- Brugere i cyberlandskabet er neutrale tredjeparts personer, grupper og organisationer, der ikke er forbundet med hverken aktører eller subjekter og som i nogle tilfælde ingen rolle spiler i forhold til de specifikke aktiviteter, men som i nogle tilfælde kan være brugt til at levere springbrætsfunktionalitet for aktøren (f.eks. ved at dele falske nyheder på sociale medier eller ved at være i besiddelse af en server eller en computer, der kan misbruges af aktøren).

Jeg har i figuren til højre præsenteret de tre typer af deltageres indbyrdes forhold i cyberlandskabet, hvor farverne er valgt samstemmigt med figuren på side 33 fra GRIZZLY STEPPE dokumenterne, da det er de samme funktioner som optræder. Relation nummer et er et cyberangreb fra aktøren mod subjektet, men hvor der anvendes funktionaliteter hos en intetanende bruger (det kan være en kompromitteret computer, server eller e-mail-postkasse). Relation nummer to er et cyberangreb, men hvor aktøren angriber subjektet direkte. Relation nummer tre er data extraction fra subjektet til aktøren, men hvor der igen anvendes en bruger (som også kan være pastebin.com eller hushfile.it). Den fjerde relation er hvor data extraction sker direkte fra subjektet til aktøren. Som oftest vil det være relationerne et og tre der bringes i anvendelse, hvilket også ses på figuren på side 33.



Figur 2 - relationer mellem de tre typer af deltagere

Empiri

Det empiriske materiale er udvalgt fra hensyn til tilgængelighed, validitet og nutidighed. Af hensyn til håndteringen af såvel kilder som selve udarbejdelsen og den efterfølgende håndtering af projektet, er der alene arbejdet med uklassificerede – og i langt de fleste tilfælde også offentligt tilgængelige – kilder. Af hensyn til nutidighed er der primært valgt empirisk materiale, der er under fem år gammelt, dog med enkelte udvalgte kilder der er af ældre dato. Sidstnævnte for at kunne drage det i anvendelse i en historisk kontekst.

Selve kilderne baserer sig primært på to typer: Den ene type er officielt udgivne rapporter, der lægges til grund for og står centralt i etableringen af en forståelsesmæssig ramme, i relation til anvendelse af de valgte teorier samt en gennemgang af konkrete aktiviteter, der bliver arbejdet videre med.

Den anden type er artikler fra dagspressen, tidsskrifter og i enkelte tilfælde blogindlæg. Disse bruges primært som eksempler på – især meningsdannende – aktiviteter og forståelsen af disse aktiviteter.

De officielle kilder ses at have en høj grad af validitet i forhold til anvendelsen, mens kilderne fra dagspressen, tidsskrifter og blogindlæg i højere grad suppleres af flere kilder, for at understøtte validitet.

Afgrænsning og begrænsninger

Jeg vil i projektet alene behandle de tekniske aktiviteter der bliver beskrevet i GRIZZLY STEPPE dokumenterne. Der findes, som også kort nævnt tidligere, en række andre typer af angreb, der dels kan støtte op om de samme formål, men som dels også åbner op for nogle andre muligheder. Alligevel vælger jeg at holde fast i de samme typer af angreb, da det er

dem der findes empiri for anvendelsen af og de derfor giver det bedste sammenligningsgrundlag.

I valg af empiri til eksempler, har det vist sig umuligt at finde eksempler, der ikke har en vis grad af berøring af cyberlandskabet. Der kan her være tale om eksempler, der er baseret på blog-indlæg eller eksempler, der har fået en væsentlig eksponering gennem sociale medier på nettet. Dette medfører, at det ikke har været muligt at arbejde med meningsdannende aktiviteter uden påvirkning fra cyberlandskabet. Givet cyberlandskabets udbredelse vurderes dette dog at have begrænset betydning.

Som skrevet under empiri er der truffet et valg om anvendelse af uklassificerede materialer, hvilket kan have konsekvens for konklusionen. Henset til projektets omfang og formål vurderes dette dog at være uden betydning.

TEORI

Jeg har valgt et teoriapparat der ses at understøtte to formål: Dels at kunne undersøge koblinger og adskillelser mellem cybermuliggjorte meningsdannende aktiviteter og de teknologifokuserede aktiviteter og dels for at kunne håndtere et russisk perspektiv. Det russiske perspektiv ses at være vigtigt, da der peges specifik på Rusland som udøver af aktiviteterne beskrevet i GRIZZLY STEPPE dokumenterne.

Begge teorierne har et væsentligt militært fokus, men jeg ser dog at de også ville kunne anvendes i ikke-militære sammenhænge. Dette af to grunde: Den første er at det er svært at holde militært og civilt fokus adskilt i cyberlandskabet. I modsætning til en traditionel konflikt, hvor der i stort udstrækning var en klar grænse mellem den militære indsats og det civile samfund, er disse to i cyberlandskabet vævet ind i hinanden. En bruger kan i løbet af få minutter skifte sine aktiviteter mellem civile og militære og det samme hardware kan på samme tid understøtte såvel civile som militære funktioner. Den anden er intensiteten i aktiviteter i cyberlandskabet kan ændres enormt hurtigt. Således kan eskaleringen fra overvældende fred til behov for kollektivt forsvar i cyberlandskabet i princippet ske i løbet af få sekunder. Specifikt i forhold til Rusland understøttes dette af, at Danmark og EU har implementeret et antal sanktioner mod Rusland [17] [18], hvorfor vi ikke længere kan siges at være i en tilstand af overvældende fred i forhold til Rusland.
Dertil kommer at der – set fra Ruslands side – ikke tale om rene militære eller civile funktioner og at forberedelse af forsvar og angreb i cyberlandskabet, er noget der sker løbende både i forhold til ekstern praksis og intern praksis. Det handler om at forstå og kontrollere eget samfunds og forstå partnere og subjekters brug af cyberlandskabet, således at der også kan ydes beskyttelse af eget cyberlandskab og udføres aktiviteter i subjekternes.

Jeg har ønsket at bruge teorier der giver mig mulighed for, at undersøge cyberlandskabet som noget særligt og som giver mig mulighed for at undersøge et meningsdannende forhold.

Den første teori jeg har valgt er baseret på en tekst af assisterende generalsekretær i NATO Sorin Ducaru: *The Cyber Dimension of Modern Hybrid Warfare and its Relevance for NATO* [19]. Ducarus tekst bringer tre anvendelser der ses at være særligt gældende for cyberlandskabet grundet den fordel som de knytter sig til: Det at informationer kan flyde frit, hurtigt og effektivt i cyberlandskabet.

[17] Udenrigsministeriet, "Gældende sanktioner".

[18] European External Action Service, "EU sanctions against Russia - EEAS - European External Action Service - European Commission".

[19] Ducaru, "Cyber Dimension of Modern Hybrid Warfare and Its Relevance for NATO, The".

Den andel del af teoriapparatet er hentet fra Timothy L. Thomas' artikel *Russia's Reflexive Control Theory and the Military* [20]. Thomas' tekst beskriver både den primære opgave, når der udføres refleksiv kontrol og relaterer det også til det underliggende begreb informationsressource. Gennem både opgavebeskrivelsen og informationsressourcebegrebet giver Thomas' tekst mulighed for, at knytte en særlig russisk doktrin til cybermuliggjorte meningsdannende aktiviteter.

Cybermuliggørelse

Anvendelsen af cyberlandskabet ses ifølge Ducaru at bibringe to overordnede fordele [21], der hver igen er opdelt i et antal mere konkrete anvendelser [22].

Som Ducaru også selv påpeger er der her tale om en ren analytisk adskillelse og i virkeligheden må de to fordele ses at være samhørende og begreber, metoder, virkemidler m.m. vil i praksis flyde i mellem de to fordele, ligesom de indbyrdes ses at kunne understøtte hinanden.

1) Fordelene ved at informationer kan flyde frit, hurtigt og effektivt, og
2) Fordele ved at anvende cyberlandskabet som et tillæg til øvrig (konventionel) krigsførelse.

Fokus for dette projekt vil være baseret på de tre anvendelser som falder ind under den første fordel:

1) Propaganda/manipulation/"distortion" af information,
2) Rekruttering og udnyttelse af ekstremister, samt
3) Anvendelse af ondsindet software[23]

Grunden til at den anden fordel (ved at anvende cyberlandskabet som et tillæg til øvrig (konventionel) krigsførelse) er udeladt, er ønsket om at se på den aktuelle situation, hvor der ikke er tale om konventionel krigsførelse, men at vi selv om vi ikke længere er i en tilstand af overvældende fred med Rusland, stadigvæk er i den lave ende intensitetsskalaen hvor den formelle ageren i særdeleshed baserer sig på udtalt kritik og sanktioner.

Anvendelsen om *propaganda/manipulation/"distortion"* af information' ses relevant i tesen om at fjerne valgets legitimitet. Det kunne også være et spørgsmål om at udføre refleksiv kontrol overfor danske politikeres syn på Rusland og Ruslands ageren. Et eksempel på førstnævnte kunne være Donald Trump, der "købte" ind på visse russiske forståelser under

[20] Thomas, "Russia's Reflexive Control Theory and the Military".

[21] Ducaru selv anvender udtrykket 'perspectives', men givet konteksten har jeg valgt at oversætte det til fordele.

[22] Ducaru, "Cyber Dimension of Modern Hybrid Warfare and Its Relevance for NATO, The", 16.

[23] Ducaru anvender selv begrebet 'etablering af kommando og kontrol (C2)', men som en del af den bredere kobling til det civile miljø og væk fra det militære, åbner jeg begrebet op en smule. Se næste side.

valgkampen [24]. Forbindelsen til refleksiv kontrol står mindre skarp, da en af forudsætningerne for refleksiv kontrol, er at subjektet ikke kan få kendskab til den beslutning, som aktøren ønsker at subjektet tager.

Anvendelsen *rekruttering og udnyttelse af ekstremister* er relevant i kontekst af støtte til politiske organisationer, der bryder med den traditionelle politiske orden. Ducau anvender udtrykket bredere (og inkluderer også kriminelle, medlemmer af undergrundsbevægelser, hacktivister[25] og lejesoldater) end blot ekstremister og ordet skal i denne kontekst opfattes, som værende personer, der er villige til at give udtryk for en art af ekstreme holdninger. Det kunne f.eks. være subjekter eller brugere der understøtter det russiske forståelse om stærke og traditionelle dyder kontra det Rusland, der nu beskriver [26] "vestens moralske forfald", "tabet af de traditionelle dyder i vesten", "vestens dekadence", "den vestlige intolerance" og "Danmark som amerikanernes skødehund". Da Danmark i 2006 sendte et af søværnets skibe til Skt. Petersborg for at aflevere Kejserinde Dagmars kiste og det danske kongehus i øvrigt deltog i begravelsen [27], var vi langt fra det moralske forfald og den dekadente tilværelse. Perspektivet i dag er blevet væsentligt ændret.

Ducaru anvender selv begrebet *kommando og kontrol*, men som en del af den bredere kobling til det civile miljø og væk fra det militære, åbner jeg begrebet op og vælger at fortolke det som *anvendelse af ondsindet software*. Ducaru ser at der er tale om et "*communication tool [...] and control instrument of choice for insurgents or terrorists*" med henvisning til et indlæg fra den daværende chef for det britiske *Government Communications Headquarters*, Robert Hannigan [28]. Hannigan omtaler alment tilgængelige services (Twitter, WhatsApp), som værktøjer som ISIL anvender til kommando og kontrol, mens Al-Qaeda anvendte de mørkere dele af internettet til kommando og kontrol. Betragter man rent anvendelsen af disse er det nærliggende også at inkludere servere og computere, der har fået installeret ondsindet software som en del af kommando og kontrol-tankegangen. Derfor kommer Ducarus kommando og kontrol også til at omhandle egentlig hacking, denial of service el. lign. af den infrastruktur der anvendes af eller i relation til subjektet. I konteksten af et valg kunne det være defacement af partiers hjemmesider, twitter-konti o.s.v. Medie-outlets kunne også være en mulighed, hvor DR/TV2/YouSee hackes på selve valgdagen (eller dagen før). Et subjekt vil på denne vis kunne stilles dårligere ved f.eks. hyppige denial of service eller

[24] Naylor, "Trump Apparently Quotes Russian Propaganda To Slam Clinton On Benghazi".

[25] Hacktivister er en sammentrækning af hackere og aktivister, hvor hackere skal forstås som personer med dyb indsigt i cyberlandskabet, snarere end de kriminelle som ordet hackere også bliver anvendt om.

[26] Fidler, "Putin Depicts Russia as a Bulwark Against European Decadence"; Higgins, "In Expanding Russian Influence, Faith Combines With Firepower"; Matthews, "Revealed"; Grønkjær, "Sådan fører Kreml informationskrig mod Vesten".

[27] Ritzau, "Kronprinsparret til kejserinde Dagmars genbegravelse".

[28] Hannigan, "The web is a terrorist's command-and-control network of choice".

defacement angreb, hvorfor subjektet vil have ulige vilkår for at kommunikere ud til (igen i kontekst af valget) potentielle vælgere og medier, i modsætning til partier som ikke bliver ramt på samme vis.

Refleksiv kontrol

En af de russiske doktriner der findes på området – og den jeg vil beskræftige mig med i nærværende projekt – er *рефлексивное управление* (*refleksivnoye upravleniye*), der som oftest oversættes til refleksiv kontrol (på engelsk *reflexive control*).

Refleksiv kontrol kan betragtes som værende en særlig form for manipulation på et højt og strategisk niveau, der gennem koordination og kommunikation anvender et antal forskellige værktøjer. Refleksiv kontrol baserer sig på en tanke om, at der er en udøver af refleksiv kontrol (aktør) og en modtager af refleksiv kontrol (subjekt). Subjektet kan være grupper (herunder organisationer og stater) eller individer (typisk med stor indflydelse eller høj beslutningskompetence). Refleksiv kontrol sker når aktøren leder subjektet i en bestemt beslutningsmæssig retning, gennem kommunikation af og om bestemte motiver og årsager [29], således at subjektet frivilligt træffer den beslutning som aktøren ønsker at subjektet skal træffe.

Fælles for denne anvendelse er, at der stilles krav om en høj grad af forståelse af subjektet og dennes informationsressourcer, således at iboende svagheder hos modtageren kan identificeres og udnyttes. Uden dyb forståelse af subjektet er der ikke tale om refleksiv kontrol og heri kan en skelnen mellem information warfare generelt og refleksiv kontrol ses [30]: Der kan godt gennemføres information warfare uden en dybere forståelse af modtageren, men refleksiv kontrol stiller ikke alene krav om forståelse af modtageren, men også at forståelsen er så dyb, at der er identificeret svagheder, der kan udnyttes.

Refleksiv kontrol kan ses som et værktøj til at opnå geopolitisk overlegenhed og i den russiske kontekst er det derfor også et værktøj, der kan bringes i anvendelse i relation til f.eks. forhandlinger med andre nationer [31]. I den valgte tekst af Thomas defineres det konkret *som et middel til levere særligt tilrettelagt information til et subjekt, således at denne frivilligt træffer den beslutning udøveren af refleksiv kontrol måtte ønske* [32] [33] [34].

[29] Thomas, "Russia's Reflexive Control Theory and the Military", 237, 241.

[30] Ibid., 248.

[31] Ibid., 240.

[32] Min oversættelse af følgende originaltekst: "Reflexive control is defined as a means of conveying to a partner or an opponent specially prepared information to incline him to voluntarily make the predetermined decision desired by the initiator of the action."

[33] Thomas, "Russia's Reflexive Control Theory and the Military", 237.

[34] Andre engelsksprogede tekster tilbyder tilsvarende definitioner, hvor ordvalget kan afvige en smule. En dybere forståelse kræver adgang til russisksprogede tekster.

Det er her vigtigt at bemærke, at der ikke findes en entydig og globalt gældende definition for refleksiv kontrol og at den desuden også har varieret en smule over årene. Den definition som jeg gengiver fra Thomas' tekst ovenfor, ses at udgøre en kontemporær oversættelse af begrebet.

Begrebet informationsressource ses at være essentielt i forståelsen af refleksiv, der igen er nødvendigt for at forstå kontrol. En informationsressource er en af de følgende [35]:

- Selve informationen og aktørerne bag informationen, inklusive metoder og/eller teknologi til at opnå, formidle, indsamle, akkumulere, behandle, lagre og udnytte af disse informationer,
- infrastruktur, inklusive informationscentre, midler til at automatisere informationsprocesser, omstillingsborde og netværk til overførsel af data,
- programmering og matematik, der bringes i anvendelse i styringen af information, samt
- administrative og organisatoriske enheder der håndterer informationsprocesser, videnskabeligt personale, skabere af datamasser og viden samt personer der beskæftiger sig med informationens væsen.

Gennem forståelsen af subjektets informationsressourcer, lægges grundlaget for at kunne arbejde med refleksiv kontrol, hvilket bringer os til kernen i arbejdet med det refleksiv-begrebet: At opnået en forståelse for subjektet, gennem indsigt i dennes koncepter, viden, ideer, erfaring[36] og om muligt også psyke og moralske standpunkter[37] og derigennem finde den effektive svaghed hos subjektet (f.eks. den frie presse, korruption hos en central meningsdanner eller en hårdt presset mindretalsregering). Når denne forståelse er opnået, er man i stand til at udnytte den gennem kendte metoder (se efterfølgende), som kan være både information og desinformation. Herigennem søges kontrol af subjektet og der er tale om egentlig refleksiv kontrol [38].

Effektiv anvendelse af refleksiv kontrol baserer sig på et multiplum af metoder, der er tilpasset den aktuelle situation og subjekt. For at kunne anvende metoderne bedst muligt, er det nødvendigt dels at have identificeret subjektets informationsressourcer og have opbygget forståelsen for subjektet.
Det er således først når disse to trin er foretaget, at der er mulighed for at finde den effektive

[35] Thomas, "Russia's Reflexive Control Theory and the Military", 240.

[36] Ibid., 241.

[37] Ibid., 242.

[38] Ibid., 241.

svaghed, der kan udnyttes og de fire metoder i det efterfølgende kan bringes i spil [39]:

1) Magtpres
2) Midler til at levere falske informationer om situationen
3) Påvirkning af subjektets tankevej til beslutningen
4) Påvirkning af den tid subjektet har til rådighed for sin beslutning

Magtpresset kan leveres fra mange forskellige sider og kan være såvel et geopolitisk pres (øget militær tilstedeværelse, sanktioner), men også være mere lokaliserede i form af støtte til interne aktører hos subjektet, der kan påvirke i en ønsket retning. I en dansk kontekst kunne det f.eks. være støtte til et parti, der er venligsindet overfor Rusland eller hyppigere gennemsejlinger af Storebælt med militære fartøjer.

Midlerne til at levere falske informationer om situationen dækker over både skjulte og åbne metoder, hvor vi på den ene side kan kigge i den traditionelle spionkasse og på den anden side har de etablerede medie-outlets som RT.com, Sputnik News og Russia Insider og endeligt velvalgte politiske bemærkninger der finder frem til vestlige medier.

Påvirkning af subjektets vej til beslutningen handler om at bringe f.eks. spilteori og simulationer i spil, således at der opnås en forståelse for subjektets tankevej frem mod en given beslutning. Herigennem afklares hvilke (baggrunds-) data subjektet ligger til grund for sin beslutning, hvorved der opnås indblik hvordan disse træffes. Gennem afklaringen af data, er det muligt at påvirke disse. I dansk kontekst kunne dette være gennem påvirkning af meningsmålinger og manipulation af visse statistiske data, der indgår i politiske diskussioner.

Endeligt er der påvirkningen af den tid subjektet har til rådighed for sin beslutning, der handler om enten at tvinge subjektet til at træffe sin beslutning tidligere, eller skabe en ”død” periode omkring det valgte beslutningstidspunkt, således at subjektet udsætter beslutningen til et senere tidspunkt. Dette kunne i forhold til Danmark, f.eks. være i relation til EU-debatten, hvor der skabes ”stemninger” (*nu skal vi have det valg* eller *det giver ikke mening at have valg om dette nu*).

En væsentlig betragtning hertil er at Rusland siden starten af 90’erne har gjort sig nogle erfaringer fra Tjetjenien-konflikten [40] omkring anvendelse af former for propaganda. Under konflikten med Tjetjenien havde Rusland førstehånds oplevet effekten af velgennemført information warfare (som refleksiv kontrol er en del af). Tjetjenien har traditionelt ikke været

[39] Ibid., 244–45.

[40] Fayutkin, “Russian-Chechen Information Warfare 1994–2006”.

begejstret for tanken om kommunisme og den sovjetiske internationalisme og derigennem etableret stærke nationalistiske kræfter. Disse kræfter forstod til fulde hvordan den russiske tankegang (ligeledes baseret på nationalisme) var, og vidste derfor hvor de svage punkter var: Legitimiteten i den russiske kampagne i Tjetjenien. Gennem en spejling (refleksiv) af de russiske nationalistiske bevægelser og det fundament de bygger på, stillede Tjetjenerne spørgsmålstegn ved om det "gav mening af ofre russiske mænds liv" og om Rusland havde en berettigelse i et andet land. Rusland på den anden side var nød til at fastholde, at Tjetjenien-konflikten var et internt russiske anlæggende. Baseret på disse konkrete erfaringer har Rusland været i stand til at udvikle taktikker og værktøjer, der også kan drages til anvendelse i cyberlandskabet. Et eksempel herpå er de meget omtalte "troldefabrikker" [41], mens også mere "hårde" virkemidler så som de aktiviteter der er beskrevet i GRIZZLY STEPPE dokumenterne [42].

Refleksiv kontrol er – set fra Ruslands side – ikke alene et udtryk for en militær funktion, men også noget der anvendes i ikke-militære sammenhænge. Dette udgør et modstykke til informationsoperationer, som Vesten som oftest ser i kontekst af krise, konflikt eller krig [43]. Det russiske perspektiv derimod er at håndtering af informationsressourcer, er noget der sker løbende og ikke alene handler om en ekstern praksis men også en intern praksis. Det handler om at forstå og kontrollere samfundets informationsressourcer, således at der også kan ydes beskyttelse af dem.

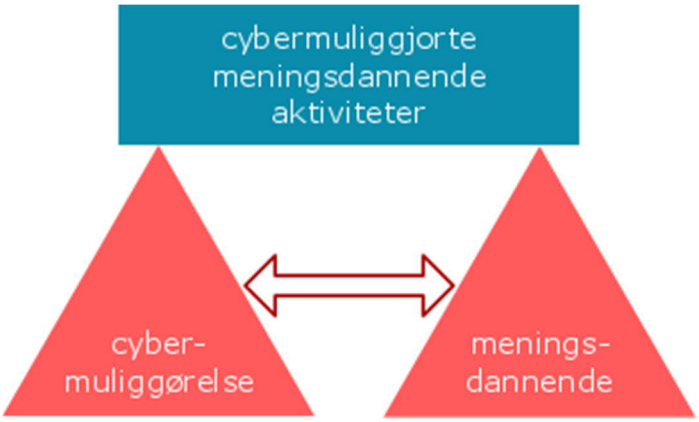
[41] Walker, "Salutin' Putin".

[42] Rebala, "Here's The Evidence Russia Hacked The Democratic National Committee".

[43] Thomas, "The Russian Understanding of Information Operations and Information Warfare [chapter 23]", 787.

SAMMENHÆNGEN MELLEM CYBERMULIGGØRELSE OG MENINGSDANNENDE AKTIVITETER

Som illustreret på side 14 omkring det at erkende, er det ikke nok blot at kunne opdage og forstå de enkelte aktiviteter. Der skal også kunne ske en meningsfyldt sammenkobling mellem de enkelte aktiviteter og de to former for aktiviteter. Effektivt gennemførte cybermuliggjorte meningsdannende aktiviteter består af en kobling af både cybermuliggørelse og meningsdannelse:



Figur 3 - sammenhæng mellem cybermuliggjorte meningsdannende aktiviteter, cybermuliggørelse og meningsdannende aktiviteter

Cybermuliggørelse og meningsdannelse – og de aktiviteter der ligger inden for de to teorier - er repræsenteret ved de to røde trekanter, som begge leder frem til cybermuliggjorte meningsdannende aktiviteter (den blå kasse). I cybermuliggørelses-trekanten, ses de aktiviteter der særligt drager nytte af fordelen ved at informationer kan flyde frit, hurtigt og effektivt. Det er de aktiviteter som Ducaru har udlagt som propaganda/manipulation/"distortion", rekruttering og udnyttelse af ekstremister og anvendelse af ondsindet software [44]. I meningsdannelses-trekanten ses den refleksive kontrol: Det er forståelse af subjektet og dettes informationsressourcer, det er det at finde frem til den effektive svaghed og det er anvendelse af de fire metoder. Når aktiviteterne sættes sammen lægges grundlaget for at gennemføre cybermuliggjorte meningsdannende aktiviteter. En egentlig refleksiv kontrol forudsætter at alle aktiviteterne i meningsdannelses-trekanten gennemføres, mens alene det at gennemføre dele af aktiviteterne blot er meningsdannende aktiviteter.

Aktiviteterne i de enkelte teorier sker (principielt) uafhængigt af hinanden. I praksis medfører disse aktiviteter til tider at der, inden for hver teori, sker erkendelser eller bliver opsamlet

[44] Foruden den egentlige etablering af en C2-struktur, sker der også en kobling til de aktiviteter der er beskrevet i GRIZZLY STEPPE dokumenterne. Det kunne også have været andre typer af aktiviteter, som f.eks. Denial of Service aktiviteter (herunder Distributed Denial of Service (DDoS), som kort berøres på næste side) eller Defacement, hvor indholdet på en modtagers hjemmeside ændres (nogle gange på meget diskret vis, således at modtageren ikke nødvendigvis opdager det, før der er gået et stykke tid) uden modtagerens vidende.

viden, der kan medføre at den anden aktivitet, kan drage nytte af den nye erkendelse eller viden. Således sker der imellem de to teorier en løbende udveksling af relevante informationer, der kan være med til at forbedre effektiviteten af "den anden teori". De to teorier føder derudover viden, som er omsat til cybermuliggjorte meningsdannende aktiviteter.

I det følgende vil jeg eksemplificere hvordan cybermuliggørelse og meningsdannelse interagerer med hinanden. Det er vigtigt at pointere, at der alene er tale om et eksempel og at der kan være en mængde forskellige kombinationer af interageren mellem cybermuliggørelse og meningsdannelse.

Således kan en forståelse af subjektet og dettes informationsressourcer bruges til at etablere en mere effektiv propaganda/manipulation/"distortion" i cyberlandskabet. Den frie, hurtige og effektive kommunikation gør så, at en given informationsressource kan angribes gennem propaganda/manipulation/"distortion" på en måde, der ikke ses i det konventionelle landskab. Angrebet kan sættes ind som en kombination af hård propaganda, hvor man anvender egne medie outlets (RT.com, Sputnik News, Russia Insider og politiske bemærkninger i vestlige medier), men også føder ønskede budskaber ind i troldefabrikkerne, som derigennem kan udføre "distortion" i f.eks. kommentarsport på danske mediers hjemmesider eller politikeres sociale medier.

Dette kan ligeledes lede til en effektiv og hurtig rekruttering af "ekstremister". Det kunne f.eks. være subjekter eller brugere der abonnerer på budskaberne om "vestens moralske forfald", "vestens dekadence", "den vestlige intolerance" eller "Danmark som amerikanernes skødehund". Disse "ekstremister" vil så kunne bringes i anvendelse for at finde frem til den effektive svaghed, således at denne kan udnyttes gennem de fire metoder (magtpres, midler til at levere falske informationer om situationen, påvirkning af subjektets tankevej til beslutningen og påvirkning af den tid subjektet har til rådighed for sin beslutning). Er det f.eks. den frie presse der er den effektive svaghed, handler det om at bruge pressen som vej til:

- at udøve magtpres (som f.eks. da den russiske ambassadør i Danmark i marts 2015, advarede om at "danskerne [ikke] helt forstår konsekvenserne af, hvad der sker, hvis Danmark tilslutter sig det amerikansk-styrede missilforsvar. Sker det, bliver danske krigsskibe mål for russiske atommissiler" [45]),
- at drage de midler man har til rådighed til at levere falske informationer i spil (RT.com, Sputnik News og Russia Insider og i ønsket omfang, hvis man kan få danske medier til at gengive indslag og artikler uden anden vinkling),

[45] From, "Ruslands ambassadør".

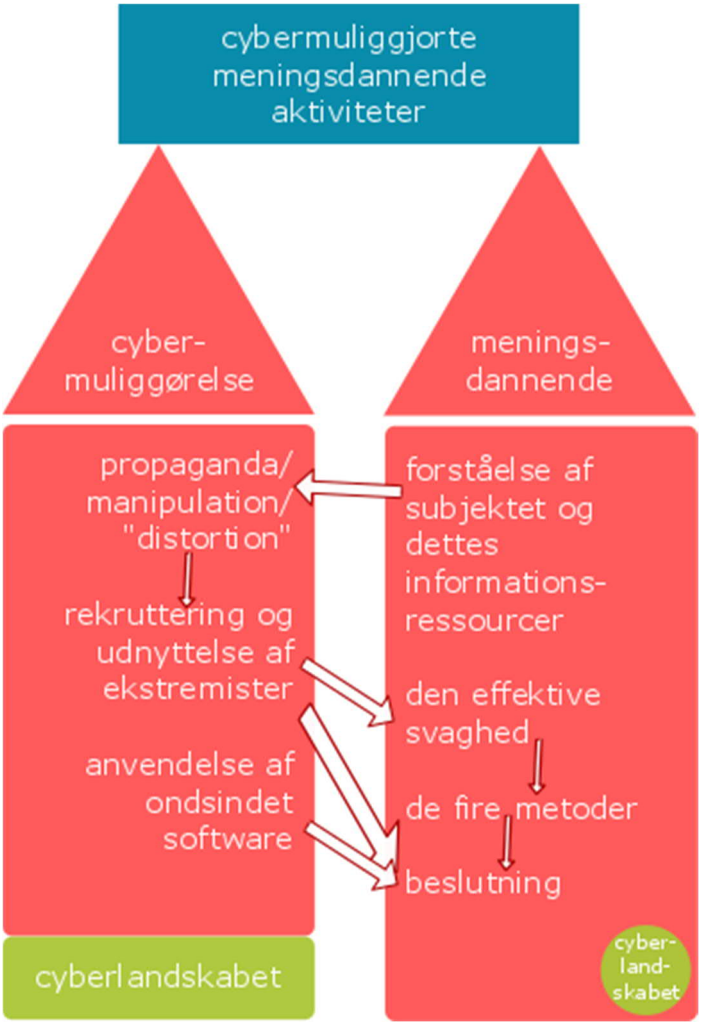
- at påvirke subjektets tankevej ved at forsøge at påvirke meningsmålinger eller manipulation af statistiske data, herunder ved at præsentere korrekte statistiske data på en bestemt måde, ved at udelade visse dele eller lave skæve koblinger mellem to uafhængige kilder, og
- at påvirke den tid subjektet har til rådighed for sin beslutning, ved at skabe en stemning i den ene eller anden retning. Et eksempel på tid der er til rådighed er valg om EU retsforbeholdet, som Socialdemokraterne i opposition i 2009 ville have den daværende VK-regering til at gennemføre, som Venstre i opposition ville have den daværende S-R-SF-regering til at gennemføre [46] og som først blev gennemført i 2015. Oppositionen agerer her som aktør mod en regering der er subjekt og anvender den frie presse til at forsøge at påvirke den tid subjektet har til rådighed (ved at forsøge at få valg tidligere).

Parallelt med dette kan der ske en etablering af en platform med ondsindet software, der enten kan være hos en neutral bruger eller hos subjektet (eller begge steder) afhængigt af formålet. Aktøren vil forsøge at få adgang til subjektets informationsressourcer med henblik på enten at udtrække konkrete data (f.eks. mails, medlemslister eller regnskaber), for at opnå en dybere forståelse af subjektets administrative og organisatoriske enheder, der håndterer informationsprocesser eller kunne anvende subjektets infrastruktur til videre udbredelse af ondsindet software.

For at der kan være tale om cybermuliggjorte meningsdannende aktiviteter, skal der være elementer fra både cybermuliggørelse og meningsdannende i spil: Det er således ikke nok, kun at anvende ondsindet software eller have identificeret den effektive svaghed, men anvendes den ondsindede software på en sådan måde, at det er understøttet af identifikationen af den effektive svaghed, vil der være tale om cybermuliggjorte meningsdannende aktiviteter. Cybermuliggjorte meningsdannende aktiviteter kan være simple aktiviteter der anvender enkelte elementer fra både meningsdannende og cybermuliggørelse, men det også være anvendelsen af hele paletten af aktiviteter, hvorved der ikke blot er tale om cybermuliggjorte meningsdannende aktiviteter, men cybermuliggjort refleksiv kontrol.

[46] Malicinski, “Afstemning om EU-forbehold”.

Grafisk kan forbindelserne illustreres som følger:



Figur 4 - forbindelser mellem cybermuliggørelse og meningsdannende

På figuren kan det fremstå som om at udgangspunktet er forståelse af modstanderen og dennes informationsressourcer er starten på en proces. Dette kan godt være tilfældet i relation til eksemplet, men i det bredere virke, er der ikke tale om en lineær proces med et klart defineret startpunkt. Slutningen er til gengæld klart defineret i form af den frivillige beslutning truffet som konsekvens af de cybermuliggjorte meningsdannende aktiviteter. Såfremt subjektet træffer den ønskede beslutning frivilligt, er der ikke blot tale om cybermuliggjorte meningsdannende aktiviteter men cybermuliggjort refleksiv kontrol.

Cyberlandskabet er tegnet ind for at vise, forskellene imellem dets rolle i forhold til de to kategorier for aktiviteter. I cybermuliggørelses-søjlen er cyberlandskabet en nødvendig forudsætning; aktiviteterne baserer sig på eksistensen og muligheden for at kunne anvende cyberlandskabet. I meningsdannelses-søjlen er cyberlandskabet blot en komponent, der indgår. Aktiviteterne kan godt eksistere uden cyberlandskabet, men vil – grundet den teknologiske og samfundsmæssige udvikling – i mange tilfælde vælge at gøre brug af

cyberlandskabet. Selv om cyberlandskabet optræder to forskellige steder i illustrationen er der tale om det samme cyberlandskab.

HVAD ER GRIZZLY STEPPE OG HVILKE AKTIVITETER ER DER I DET?

GRIZZLY STEPPE er det navn som amerikanske myndigheder, har givet et "program" [47] bestående af en række aktiviteter, som tillægges aktører med forbindelse til de russiske militære og civile efterretningstjenester. Disse aktører er benævnt henholdsvis Advanced Persistent Threat (APT) 28 og 29 (forkortet APT28 og APT29), men optræder også med en række andre navne [48] som f.eks. *Fancy Bear*, *COZYBEAR*, *Dragonfly*, *OnionDuke* and *Operation Pawn Storm*. Disse navne kan være både selvvalgte af aktørerne eller tildelt af private eller offentlige entiteter.

Joint Statement

Det første dokument, der blev udgivet var en Joint Statement [49] (herefter pressemeddelelsen), der blev udgivet 7. oktober 2016 [50]. Denne pressemeddelelse indledes som følger:

> *The U.S. Intelligence Community (USIC) is confident that the Russian Government directed the recent compromises of e-mails from US persons and institutions, including from US political organizations. The recent disclosures of alleged hacked e-mails […] are consistent with the methods and motivations of Russian-directed efforts.*

Pressemeddelelsen omtaler to typer af aktiviteter og et motiv (om end motivet ikke præciserer nærmere i hverken den citerede tekst eller pressemeddelelsen i øvrigt). Den første aktivitet der nævnes er "*theft*" (tyveri), og behandler mails der er stjålet og frigivet via "whistleblower"-sites som f.eks. DCLeaks.com og WikiLeaks, men også andre sites, hvor aktører (og brugere i øvrigt) kan gøre store mængder data frit tilgængeligt, som f.eks. pastebin.com eller hushfile.it. Der nævnes ingen konkrete mails eller hvor mails er stjålet fra, men omtales alene "*recent disclosures*" af mails fra "*US persons and institutions, including from US political organizations*". Pressemeddelelsen omtaler desuden "*scanning and probing*" aktiviteter mod nogle delstaters valg-relaterede systemer ("*election-related systems*"). Scanning og probing er gængse teknologier, der bedst kan sammenlignes med at

[47] De amerikanske myndigheder beskriver ikke det selv som et program, men som 'this malicious cyber activity by [Russian civilian and military intelligence Services" (U.S. Department of Homeland Security: National Cybersecurity and Communications Integration Center og U.S. Federal Bureau of Investigation, "GRIZZLY STEPPE – Russian Malicious Cyber Activity", 1.). Ordet program anvendes her som en samlende entitet for de tre anvendte dokumenter og de aktiviteter der er beskrevet heri.

[48] Ibid., 4.

[49] U.S. Department of Homeland Security: National Cybersecurity and Communications Integration Center og U.S. Federal Bureau of Investigation, "Joint Statement from the Department Of Homeland Security and Office of the Director of National Intelligence on Election Security | Homeland Security".

[50] Den amerikanske valgkamp fandt I særligt stor udstrækning sted i perioden fra juni 2016, hvor de sidste primærvalg og caucuser blev afholdt, og frem til valgdagen d. 8. november 2016.

banke på døre og kigge ind af vinduer. I praksis kan en hvilken som helst computer gøre det mod andre computere og det sker i stor udstrækning på internettet fra et væld af aktører.

I det aktuelle tilfælde bemærker pressemedelelsen dog, at de aktuelle scanninger og probinger "*in most cases originated from servers operated by a Russian company*", men at de to agenturer "*are not now in a position to attribute this activity to the Russian Government*".

Joint Analysis Report on GRIZZLY STEPPE – Russian Malicious Cyber Activity

Pressemeddelelsen blev efterfølgende fulgt op med en Joint Analysis Report[51] (29. december 2016), der igen blev udgivet i samarbejde mellem de to førnævnte agenturer. De to agenturer beskriver i dokumentet nærmere de konkrete metoder, som de tillægger *Russian civilian and military intellligence Services*. Dokumentet indeholder allerede i første afsnit koblingen til de russiske efterretningstjenester og bemærker i 2. afsnit, at tidligere Joint Analysis Reports "*have not attributed malicious cyber activity to specific countries or threat actors*", men at koblingen sker gennem "*technical indicators from the U.S. Intelligence Community, DHS, FBI, the private sector, and other entities*". Dokumentet opstiller tre metoder, der ses at have været i anvendelse:

1) Spearphishing campaigns
2) Cyber-attacks
3) Masquerading

Disse tre metoder er ikke uafhængige af de to der er nævnt i pressemeddelelsen, men kobler sig til dem. Phishing campaigns (også omtalt som *Spearphihing)* [52] omhandler mails, hvor aktørerne forsøger at "fange" subjekter, gennem mails, der er noget andet end det de udgiver sig for at være. Dette typisk med formål at lokke kreditkortinformationer eller login-oplysninger (*harvesting*) ud af brugerne eller få brugeren til at installerede ondsindet software.

Eksempler på dette er mails, der beder subjektet eller subjekterne om at følge et link, for at verificere sit kodeord eller indtaste sine kreditkortoplysninger for at få frigivet en pakke. Mailsne og den hjemmeside vil så være forklædt som værende fra f.eks. en bank eller en post-service. I denne kontekst er det særligt login-oplysnignerne der er interessante, da de

[51] U.S. Department of Homeland Security: National Cybersecurity and Communications Integration Center og U.S. Federal Bureau of Investigation, "GRIZZLY STEPPE – Russian Malicious Cyber Activity".

[52] *Spearphishing* er en sammentrækning af ordene 'spearfishing' (spyd- eller harpun-fiskeri) og phishing er en nydannelse af det engelske ord 'fishing', der i denne kontekst leder hen til, at man forsøger at "fange" en bruger.

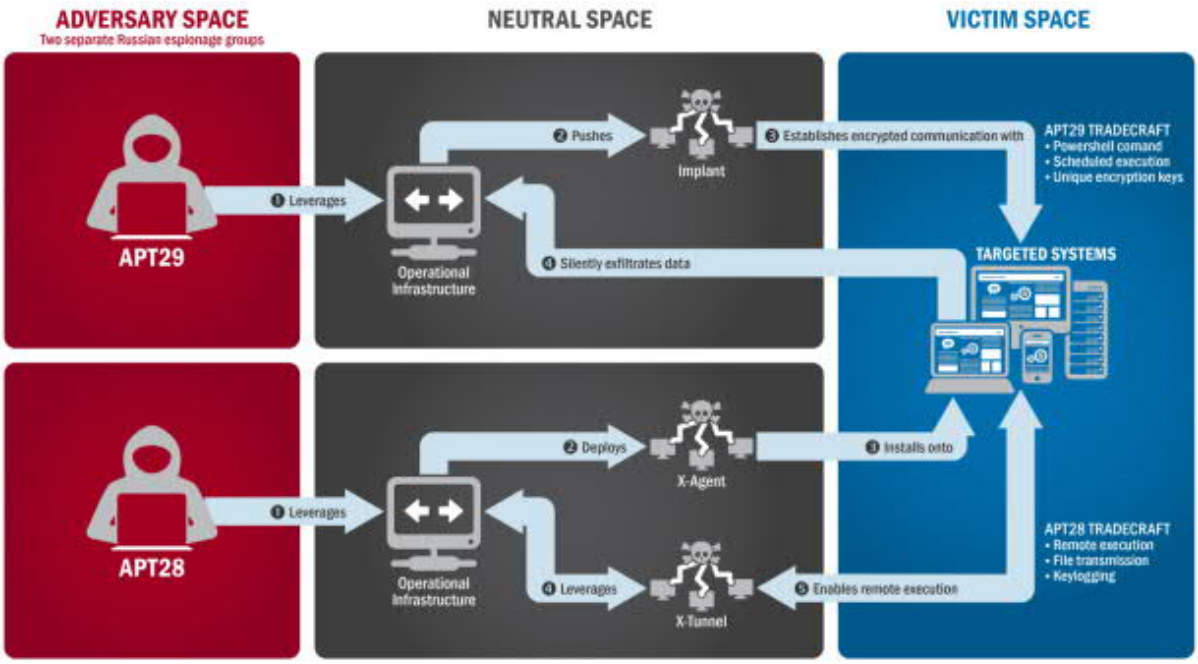
ville kunne bruges af aktørerne til at tilgå f.eks. mailkonti hos subjekterne, med henblik på tyveri af mails.

Ved installation af ondsindet software på subjekternes computere vil der være tale om software, der enten tillader aktøren at fjernstyre computeren, bruge den som en slags ”springbræt” for videre aktiviteter eller software der udfører specifikke kommandoer (så som at sende alle Word-dokumenter på computeren til aktøren). Inden for de senere år er der set en variant, hvor softwaren krypterer indholdet på computeren og afpresser brugeren for penge, såfremt brugeren vil have adgang til sine filer igen (såkaldt ransomware – senest set med WannaCry i april/maj måned).

Der nævnes tre typer af aktiviteter i GRIZZLY STEPPE dokumenterne. Disse baserer sig på svagheder i software eller i opsætningen af software. Selve svagheden er typisk bare en trin på vejen til enten at tilgå informationer på serverne eller til at lægge ondsindet software på serverne. Den ondsindede software til servere er meget lig den der lægges på computere og tjener samme formål, idet typisk servere er kendetegnede ved at være tændte og tilgængelige 24/7, mens brugernes computere vil have en mere begrænset tilgængelighed.

Den ondsindede software kan også bruges til masquerading, som er disciplinen at skjule sig overfor subjektet. Jo flere computere/servere aktøren anvender til at skule sin identitet, jo sværere bliver det at finde frem til hvem aktøren er. Ved gennemførsel af aktiviteterne beskrevet i GRIZZLY STEPPE dokumenterne er det i aktørens interesse, at holde sin sande identitet skjult da det derved i langt højere udstrækning bliver muligt at benægtet aktiviteterne.

Joint Analysis Reporten sætter de tre typer af aktiviteter sammen på følgende måde:



Figur 5 - koblingen mellem adversary, neutral og victim space

I figuren ses aktørerne til venstre (med rød baggrund) udføre aktiviteter gennem det neutrale område (med grøn baggrund) overfor subjekterne (til højre, blå baggrund). Det neutrale område, er der hvor masquerading, men også andre aktiviteter, med henblik på masquerading foregår samt gennemførsel af phishing-kampagner. Det blå subjektets område omhandler så de systemer som subjektet råder over (computere, servere, mailsystemer etc.), som aktøren af den ene eller anden grund ønsker at tilgå. Selve tyveriet foregår så fra subjektets område via det neutrale område til aktørens område. Efterfølgende er de stjålne dokumenter så blevet frigivet gennem et andet neutralt område (ikke vist på illustrationen) som i dette tilfælde har været DCLeaks.com eller WikiLeaks.

Enhanced Analysis of GRIZZLY STEPPE Activity

Det sidste dokument er en *Enhanced Analysis* rapport, der blev udgivet d. 10. februar 2017. I dokumentet bliver de anvendte aktiviteter foldet yderligere ud i mere specifikke teknikker og værktøjer, ligesom de beskrives i en ramme [53] som typisk anvendes til at beskrive de berørte aktiviteter (spearphishing, cyber-attack og masquerading). Der nævnes i Enhanced Analysis Report 13 teknikker og værktøjer, der understøtter de tre metoder gengivet i Joint Analysis

[53] Denne ramme heder 'Cyber Kill Chain' og består af syv aktiviteter som aktører må gennemføre overfor subjektet, for at have succes med deres aktiviteter som helhed. Cyber Kill Chain bliver ikke behandlet i dette projekt i øvrigt.

Report (spearphishing, cyber-attacks og masquerading). Særligt tre teknikker skal fremhæves, da disse ikke er dækket af de foregående beskrivelser.

Den første er en teknik kaldet *typo-squatting*, hvor en aktør anskaffer og idriftsætter et domæne, der minder om et kendt domæne. Dette kunne f.eks. være forvsaret.dk i stedet for forsvaret.dk. Hjemmesiden på forvsaret.dk designes så, således at den ligner forsvaret.dk, men med formål enten at udbrede falske nyheder, indsamle login-informationer eller narre subjektet til at downloade ondsindet programmel.

Den næste teknik kaldes for *watering hole attack*, hvor aktøren i stedet for at angribe forsvaret.dk, angriber en side, som forventes brugt meget af forsvarets ansatte, men som i udgangspunktet kan have et lavere sikkerhedsniveau. Det kunne være f.eks. diis.dk eller olfi.dk. Når så den pågældende side er kompromitteret, forsøges subjekterne narret til at downloade ondsindet software til deres computere derfra gemt i f.eks. en PDF-fil eller et Word-dokument.

Den sidste teknik minder om *watering hole attack*, men anvender i stedet kendte sider, som bruges bredt (og er dermed ikke så målrettet som *watering hole attack*). Det kunne være en hjemmeside, hvor mange folk henter PDF-værktøjet CutePDF fra. I stedet for at anvende PDF-filer eller Word-dokumenter gemmer aktøren så sin ondsindede software i CutePDF-programmet. Derigennem omgås nogle af de sikkerhedsmekanismer, der vil fange PDF-filerne eller Word-dokumenterne fra *watering hole attack*et. Til gengæld er det et sværere angreb at gennemføre og sandsynligheden, for at netop subjektet bliver ramt er mindre.

Baggrundsdokument omkring den analytiske proces og konstateringen af aktøren i forbindelse med GRIZZLY STEPPE dokumenterne

De tre undersøgelsesdokumenter om GRIZZLY STEPPE kan ikke stå alene. Dels er dokumenterne af ret teknisk karakter og dels siger de ikke noget om det russiske perspektiv. Desuden efterlader de stadigvæk læseren med en grad af tvivl om fuldstændigheden af Rusland som aktør.

Dette håndteres i forlængelse af GRIZZLY STEPPE dokumenterne, i et baggrundsdokument omkring den analytiske proces og konstateringen af aktøren i forbindelse med GRIZZLY STEPPE dokumenterne. Baggrundsdokumentet er udgivet af det amerikanske *Office of the Director of National Intelligence*, angives følgende under *key judgements* [54]:

> "*Russian efforts to influence the 2016 US presidential election represent the most recent expression of Moscow's longstanding desire to undermine the US-led liberal*

[54] Office of the Director of National Intelligence, "Background to 'Assessing Russian Activities and Intentions in Recent US Elections': The Analytic Process and Cyber Incident Attribution", ii–iii.

democratic order, but these activities demonstrated a significant escalation in directness, level of activity, and scope of effort compared to previous operations.

We assess Russian President Vladimir Putin ordered an influence campaign in 2016 aimed at the US presidential election. Russia's goals were to undermine public faith in the US democratic process, denigrate Secretary Clinton, and harm her electability and potential presidency. We further assess Putin and the Russian Government developed a clear preference for President-elect Trump. We have high confidence in these judgments.

Moscow's influence campaign followed a Russian messaging strategy that blends covert intelligence operations—such as cyber activity—with overt efforts by Russian Government agencies, state-funded media, third-party intermediaries, and paid social media users or "trolls."

We assess Moscow will apply lessons learned from its Putin-ordered campaign aimed at the US presidential election to future influence efforts worldwide, including against US allies and their election processes."

De understregede passager ses værende særligt relevante i kontekst af de meningsdannende aktiviteter, da de ikke alene giver bud på Ruslands motivation og mål, men også hvilken strategi Rusland har og hvordan de vil bruge den fremadrettet.

Der er tale om en ret direkte form for cybermuliggjorte meningsdannende aktiviteter, hvor alle tre elementer fra cybermuliggørelse og i hvert tilfælde tre elementer fra meningsdannende er tilstede: Forståelse af subjektet og dettes informationsressourcer, den effektive svaghed og de fire metoder. Med den amerikanske befolkning som subjekt har aktøren udnyttet den effektive svaghed, der ses i stigende politikerlede, som særligt Hillary Clinton var eksponent for. Aktøren har tillige forstået både den informationsressource som man har kunnet stjæle mails fra, men også den informationsressource, hvorigennem man har gjort mails offentligt tilgængelige. Dertil kommer forsøg på at tilgå det valg-softwaren og med disse to aktiviteter har aktøren kunnet både levere falske informationer om situationen og påvirke subjektets tankevej til beslutningen (hvilken af de to kandidater man stemmer på).

Det er nødvendigt kort at betragte den russiske opfattelse af GRIZZLY STEPPE. RT.com, Sputnik News, Russia Insider og politiske bemærkninger i vestlige medier bidrager i noget omfang hermed, men det er væsentligt at bemærke, at såfremt disse er underkastet refleksiv kontrol, så ved vi faktisk ikke hvilket mål, de støtter op om. Som skrevet tidligere er en væsentlig udfordring ved de teknikker der er anvendt i GRIZZLY STEPPE, at det er svært eller helt umuligt at konkludere hvem der er aktøren alene på baggrund af de tekniske aktiviteter. Anvendelse af efterretningsinformationer vil muligvis kunne bistå tekniske

undersøgelser og baggrundsdokumentet og understøtte de indikatorer, der trækkes frem her. Det er dog ikke sikkert at disse vil kunne beskrives offentligt og baggrundsdokumentet nævner eksplicit, at det er en nedklassificeret udgave af et højere klassificeret dokument. Det er derfor for Rusland vedvarende muligt, dels at benægte at være aktør, men også at stille spørgsmålstegn ved om påstandene er ægte og finde postulater og andet, der understøtter at det var nogle andre der gjorde det – f.eks. Ukraine.

HVILKE DANSKE AKTIVITETER HAR VI HAFT, DER MINDER OM GRIZZLY STEPPE?

Der er ikke fra Danmark udgivet et antal sammenhængende rapporter, der beskriver en specifik begivenhed svarende til den der er behandlet i foregående afsnit om GRIZZLY STEPPE. Der er dog et antal både tekniske aktiviteter og et antal meningsdannende aktiviteter (som ikke ses værende cybermuliggjorte), det er relevante at behandle for at få etableret den særlige danske kontekst.

Hvilke aktiviteter i dansk kontekst har vi set, der minder om GRIZZLY STEPPE?

I Danmark er særligt to dokumenter relevante at trække frem, ved brug for en gennemgang af aktiviteter rettet mod Danmark, der minder om dem der er beskrevet i GRIZZLY STEPPE dokumenterne. Begge dokumenterne er udgivet af Center for Cybersikkerhed (CFCS), og omhandler indtrængen i statslige systemer. Det første blev udgivet i 2016 [55] og var undersøgelsesrapporten *Phishing uden fangst*, mens det næste var *Én aktør, mange angreb* [56] der blev udgivet i 2017. Sidstnævnte sætter – i modsætning til det første – navn på den formodede aktør: APT28. I store træk minder de aktiviteter der er beskrevet i de to undersøgelsesrapporter om de aktiviteter der er beskrevet i GRIZZLY STEPPE dokumenterne, hvorfor fokuseringen i det efterfølgende vil være på den særlige danske vinkel.

Phishing uden fangst-rapporten omhandler alene at langt og vedvarende phishingangreb mod Udenrigsministeriet. I rapporten bemærkes det at aktørernes "*vedholdenhed og gentagne forsøg mod postkasse #1 resulterer i en kompromittering af denne enkelte maskine*" [57] og at modtagerne i Udenrigsministeriet "*i visse tilfælde [har] haft mail-korrespondance med personen bag den kompromitterede afsenderadresse, som de har modtaget en phishing-mail fra*" [58]. Bortset fra den særlige danske vinkel på adresserne og en tilsyneladende ihærdighed mod særligt en mail-konto beskrives der ikke nogle træk, der adskiller det der er sket mod Udenrigsministeriet væsentligt fra det, der er beskrevet i GRIZZLY STEPPE dokumenterne.

En aktør, mange angreb-rapporten beskriver en større mængde aktiviteter af forskellig karakter og beskriver bl.a. at der er tale om "*en enkelt aktør [der] udfører spionage mod Danmark*" [59] og at denne har anvendt forskellige former for manipulation, med henblik på at få subjekterne til at klikke på indlejrede links i phishing-mails. Disse mails leder så til sider,

[55] Center for Cybersikkerhed, "Phishing uden fangst - Udenrigsministeriet under angreb".

[56] Center for Cybersikkerhed, "Én aktør, mange angreb".

[57] Center for Cybersikkerhed, "Phishing uden fangst - Udenrigsministeriet under angreb", 6.

[58] Ibid., 7.

[59] Center for Cybersikkerhed, "Én aktør, mange angreb", 4.

der ligner Forsvarets webmail-løsning, således at subjektet narres til at indtaste login og kodeord, hvorefter aktøren har adgang til subjektets mailkonto.

Foruden udlevering af login og kodeord er også beskrevet en anden phising-kampagne, der havde til formål at inficere subjektets maskiner med ondsindet software. Der bliver ikke i undersøgelsesrapporten beskrevet hvilken form for ondsindet software der har været anvendt og hvad formålet med den kan have været, men som med GRIZZLY STEPPE dokumenterne har der givetvis været tale om software, der enten tillader aktøren at fjernstyre computeren, bruge den som en slags "springbræt" for videre aktiviteter eller software der udfører specifikke kommandoer (så som at sende alle Word-dokumenter på computeren til aktøren) eller til masquerading (som er disciplinen at skjule sig overfor subjektet).

En af de store udfordringer omkring aktiviteter, er naturligvis alle de aktiviteter som vi ikke ser. Som beskrevet tidligere, er vejen til at erkende at opdage. Men der kan også være en mængde aktiviteter (både tekniske og meningsdannende, men her fokuseret på tekniske) som vi aldrig opdager, og som derfor aldrig bliver erkendt, eller bliver erkendt på et uhensigtsmæssigt tidspunkt, hvor f.eks. interne mails bliver lækket via "whistleblower"-sites eller andre sites, hvor aktører og brugere kan gøre store mængder data frit tilgængeligt [60].

Meningsdannende aktiviteter og Danmark

Jeg vil i dette kapitel gennemgå de meningsdannende aktiviteter, der er fundet i forhold til en dansk/russisk kontekst. De meningsdannende aktiviteter kan være både fragmenterede eller indgå i en større kontekst, som vi – såfremt der er tale om refleksiv kontrol fra Rusland – ikke kender det fulde billede af: Således kan vi godt have en fornemmelse af konteksten, men vi er ikke klar over hvilken beslutning Rusland ønsker at vi frivilligt træffer.

De to eksempler der er udvalgt, er valgt ud for en hensigt om, at finde eksempler hvor cyberlandskabet spiller mindre ind og som er nutidige i sin form.

Den første aktivitet kan nærmest karakteriseres som værende rå propaganda, i form af et eksempel fra efteråret 2016. I en af de mest populære russiske aviser, Gazeta.ru, leveres et blogindlæg skrevet af en russer, der har boet i Danmark i fem år [61]. I avisen fremstilles danskere som værende urene, have dårlig omgang med fødevarer og lade sine børn gøre alt. Isoleret set er der blot tale om et blogindlæg, der ikke nødvendigvis skal tillægges nogen større betydning. Men det at det er blevet publiceret via Gazeta.ru og i øvrigt er "*er blevet delt flittigt*

[60] Se side 18, nederst.

[61] Larsen, "Kreml og medier vil lokke russerne til at blive hjemme".

på det russiske svar på Facebook, vk.com" [62], ses alligevel at gøre det relevant at tage med, idet det viser at der også kan ske propaganda-lignende aktiviteter internt i Rusland.

Under antagelse af at eksemplet er rettet mod såvel danske som russiske subjekter, vil den danske subjektsforståelse være baseret på en informationsressource i form af en form af den frie danske presse. Indlægget er gengivet i et større antal danske medier som f.eks. TV2 [63], Jyllands-Posten [64] og Politiken [65], med en tydelig kritisk opfattelse af den oprindelige russiske skribent. Den effektive svaghed her kan være den frie danske presse eller en dansk selvforståelse, som der fra skribents side kan søges et opgør med. TV2 korrespondent i Rusland, Uffe Dreesen bemærker følgende: "*De fleste russere ville blive meget overraskede over at opdage, hvor beskedne køretøjer, vi bevæger os rundt i. Alle russere, der kommer til fadet, investerer i en stor SUV. Så at København er præget af cyklister, vil de tolke som et udtryk for tilbagestående, fattigdom*" [66]. Ligeledes bemærker bloggeren selv at "*[k]vinderne [i Danmark] gør intet ud sig selv [og] at den typiske danske kvinde har uredt hår samlet i en sjusket hårknude og går i sort tøj og spraglede gummisko*" [67]. I den danske selvforståelse er cyklisme sjældent – hvis overhovedet – opfattet med tilbagestående eller fattigdom. Ligeledes er opfattelsen af en kvinde i sort tøj og spraglede gummisko, som værende noget særligt tilbagestående eller uciviliseret næppe særligt udbredt. Den meningsdannende aktivitet rettet mod Danmark kan derfor være, at skabe en opfattelse i Danmark om at Rusland opfatter danskere som tilbagestående, fordi vi cykler meget og kvinderne går i spraglede gummisko. Såfremt det antages at der er en forståelse af subjektet (blog-forfatteren har boet i Danmark i fem år), kan metoden eksempelvis være et middel til at levere falske informationer om situationen (russiske kvinder er mere civiliserede og knap så tilbagestående), i en kontekst hvor vi som danskere måske mere ser cykling og spraglede gummisko som udtryk for ligestilling og frigørelse, hvilket vil være i tråd med Vesten som havende tabt de traditionelle dyder.

Et andet eksempel var da den russiske ambassadør i Danmark i marts 2015, advarede om at "danskerne [ikke] helt forstår konsekvenserne af, hvad der sker, hvis Danmark tilslutter sig det amerikansk-styrede missilforsvar. Sker det, bliver danske krigsskibe mål for russiske atommissiler" [68]. Indlægget fik stor udbredelse på de sociale medier i Danmark og reaktionerne på det var mange og forskellige.

[62] Møller, "Russisk avis sviner Danmark".

[63] Ibid.

[64] Larsen, "Kreml og medier vil lokke russerne til at blive hjemme".

[65] Heine, "Vi er uhumske, har uredt hår og børnene får brugt legetøj".

[66] Møller, "Russisk avis sviner Danmark".

[67] Heine, "Vi er uhumske, har uredt hår og børnene får brugt legetøj".

[68] From, "Ruslands ambassadør".

I dette tilfælde kan der næppe drages tvivl om at aktiviteten er rettet mod danske subjekter: Advarslen var en del af et indlæg i Jyllands-Posten. Igen ses den frie presse anvendt som platform for den russiske kommunikation, om end det i dette eksempel er langt mere direkte end i det forrige tilfælde. Den frie presse kan således ses som værende den effektive svaghed (i modsætning til den russiske udlægning, hvor selve påstanden om trusler om anvendelse af russiske atommissiler beskrives som "*bizarre*" [69]), idet det tillades at budskaber af denne type (trusler) får lov til at blive publiceret. Den meningsdannende aktivitet rettet mod Danmark kan derfor være, at vise danskerne at Rusland skal tages seriøst og at man ønsker at være ret præcis i sin kommunikation om, at Danmark ikke skal deltage i det amerikansk-styrede missilforsvar. Gennem udøvelse af et magtpres overfor Danmark, ønsker Rusland at få Danmark til at ændre holdning til missilforsvaret. Ambassadøren har givetvis selv – eller medarbejdere han kan trække på – med god forståelse af Danmark som subjekt, hvorfor kommunikationen også kan formodes tilrettelagt derefter. Dette vil være i tråd med, at Rusland ser sig selv som værende en stærk stat.

[69] RT.com, "Russia threatened to use nukes?"

HVILKE AKTIVITETER KAN VI SE, DER HVOR MENINGSDANNENDE OG CYBERMULIGGJORTE AKTIVITETER KONVERGERER?

Det er der hvor cybermuliggørelse og meningsdannende aktiviteter konvergerer at cybermuliggjorte meningsdannende aktiviteter opstår. Som skrevet i kapitlet *Sammenhængen mellem cybermuliggørelse og meningsdannende aktiviteter* (side 25) er det aktiviteter, der både drager særlig nytte af fordelen ved at informationer kan flyde frit, hurtigt og effektivt og som har til formål, at lede frem til en specifik frivillig beslutning hos subjektet. De tekniske aktiviteter som er beskrevet i både GRIZZLY STEPPE dokumenterne og i de danske undersøgelsesrapporter, understøtter særligt de aktiviteter der er beskrevet under cybermuliggørelse, men som vist i illustrationen på side 28 kan aktiviteterne sagtens smelte sammen med meningsdannende aktiviteter. Det amerikanske baggrundsdokument påpeger to meninger (der kan lægges til grund for meningsdannende aktiviteter) [70], som når oversat til en mere generel kontekst end blot USA kan fremlægges som følger:

- Ruslands ønske om at underminere [...] liberale, demokratiske systemer
- Ruslands ønske om at underminere den offentlige tillid til [...] demokratiske processer

Disse to meninger ses umiddelbart også at kunne anvendes i en dansk kontekst, da vi i Danmark både er baseret på et (fungerende) liberalt, demokratisk system og indeholdt heri et antal demokratiske processer; herunder ikke mindst folketings-, regions- og kommunalvalg.

Dertil kommer Danmarks geografiske nærhed til Rusland (set i forhold til USA, der står bag førnævnte baggrundsdokument) og måske en kraftigere eksponering til den russiske forståelse om stærke og traditionelle dyder kontra det Rusland for nuværende beskriver som [71] "vestens moralske forfald", "tabet af de traditionelle dyder i vesten", "vestens dekadence", "den vestlige intolerance" eller "Danmark som amerikanernes skødehund".

Der ses således et større antal meninger, der vil kunne danne grundlag for cybermuliggjorte meningsdannende aktiviteter, hvor Danmark er subjektet.

For at der kan være tale om cybermuliggjorte meningsdannende aktiviteter, skal der være elementer fra både cybermuliggørelse og meningsdannende i spil: Det er således ikke nok, kun at anvende ondsindet software eller have identificeret den effektive svaghed.

De egentlige cybermuliggjorte meningsdannende aktiviteter, må nødvendigvis have et klart defineret subjekt. Rusland næppe være interesseret i at udføre aktiviteter der styrker det Konservative folkeparti, der som bekendt er meget forsvarsvenlige og i øvrigt på

[70] Se side 34-35.

[71] Fidler, "Putin Depicts Russia as a Bulwark Against European Decadence"; Higgins, "In Expanding Russian Influence, Faith Combines With Firepower"; Matthews, "Revealed"; Grønkjær, "Sådan fører Kreml informationskrig mod Vesten".

landspolitisk plan ønsker at øge Danmarks forsvarsbudget ganske markant. I stedet kan støtte til partier som udviser en ukonventionel adfærd og i noget omfang baserer sig på brud med den traditionelle politiske opfattelse kunne være mulige områder for russisk støtte, ligesom lokale partier, der læner sig op ad fredsteserne kunne være relevante. Dette vil understøtte det russiske ønske om at underminere liberale, demokratiske systemer og der ses et antal forskellige variationer af cybermuliggjorte meningsdannende aktiviteter, der vil kunne bringes i spil:

1. Rekruttering og udnyttelse af ekstremister som kampagnefolk for en bestemt agenda, vil kunne være et affarende punkt for den russiske indsats. Derigennem kan der opbygges en forståelse af subjektets og dettes informationsressourcer og muligvis også den effektive svaghed. Såfremt subjektet er de traditionelle danske partier (Socialdemokratiet, Konservative folkeparti, Radikale venstre og Venstre), kan den effektive svaghed være sammenhængskraften i partierne. Er dette tilfældet vil den valgte metode kunne være en kombination af anvendelse af ondsindet software og midler til at levere falske informationer om situationen: Den ondsindede software bruges til at få adgang til udvalgte interne informationer, der efterfølgende gøres tilgængelige, omgivet af informationer der dels understreger sandhedsværdien af informationerne og samtidigt tydeliggør partiernes interne konflikter. En erkendelse heraf baserer sig dels på en teknisk erkendelse af datatyveriet (før informationerne er gjort tilgængelige), men også den mere åbenlyse, når først informationerne er gjort offentligt tilgængelig.
2. Anvendelse af ondsindet software i kombination med propaganda/manipulation/"distortion" og midler til at levere falske informationer om situationen, vil kunne bruges til at skabe tvivl om det IT-baserede valg-software (og afledt deraf måske valgets legitimitet). Igennem disse tre muligheder vil en aktør kunne udsætte subjektets valg-software. Det er muligvis ikke engang nødvendigt at opnå adgang til valg-softwaren. Såfremt det bliver erkendt at denne er under massive angreb og aktøren udgiver informationer, der indeholder både elementer af sandhed om det faktiske angreb og elementer af "distortion", hvori det påstås at aktøren har fået adgang til systemerne, vil dette i sig selv kunne så tvivl om valg-softwaren. I dette tilfælde er selve erkendelsen med til at understøtte aktørens agenda og der skal således kunne foretages en form for "meta-erkendelse", af hvilke dele af aktørens budskaber der er sande og hvilke der ikke er.
3. En mere ekstrem variant af cybermuliggjorte meningsdannende aktiviteter er en kombination af anvendelse af ondsindet software, magtpres og den effektive svaghed. Såfremt aktøren opnår kendskab til en effektiv svaghed hos et subjekt, vil dette kunne udnyttes. Tidligere – i større skala – er den frie presse nævnt som et bud

på en effektiv svaghed hos Danmark som aktør, men når aktøren er nede på enkeltpersoner, er det muligt at anvende en anden form for effektive svagheder, som er rettet mod individerne. Dette er ikke ulig afpresning, men hvor formålet er at få subjektet til at gøre eller beslutte en specifik ting (som ikke nødvendigvis er den ting som aktøren har ultimativt, men som blot leder frem til at subjektet frivilligt træffer den beslutning som aktøren ønsker). Den umiddelbare erkendelse aktiviteten synes ret åbenlys, mens den dybere erkendelse kan være svær, og kræver en dyb analyse af anden og tredjeordens effekter fra subjektets beslutning.

4. Endeligt er der en kombination af de tre foregående aktiviteter, hvor der både udstilles manglende sammenhængskraft hos de etablerede partier og hvor der sås tvivl om valg-softwaren (og dermed valgets legitimitet). Gennem denne kombination kan de mindre etablerede partier komme frem, der kan sås tvivl om valgets legitimitet og enkelte – og muligvis centrale spillere – ender med at træffe en bestemt beslutning. I yderste konsekvens vil dette kunne medføre en markant ændring af nogle af de nationale præmisser for forsvaret: Hvis det kommunale fokus ændrer sig fra at være på at beholde arbejdspladser i forbindelse med kasserne, til at ønske dem ud af kommunerne, vil dette kunne have konsekvenser for dansk forsvar. Hvis kommunerne i mindre grad får valgt personer ind fra de etablerede partier, vil sammenhængskraften mellem regeringen til regioner og kommuner kunne svækkes. Dette vil senere kunne være en brugbar faktor ved næste folketingsvalg. Det er vigtigt at pointere her, at der ikke ses at være tale om russiske ”marionetdukker” i kommunerne, men folkevalgte der selvstændigt og af egen fri vilje træffer beslutninger, der tilgodeser russiske interesser på en anden vis. Erkendelse heraf bygger på en effektiv sammenkædning af alle de erkendelser, der er opstillet i de forrige tre aktiviteter: Teknisk erkendelse af datatyveriet (før informationerne er gjort tilgængelige), en ”meta-erkendelse” hvor der skal ske en udredning af, hvilke af aktørens budskaber der er sande og hvilke der ikke er og endeligt en dybere erkendelse af anden- og tredjeordens effekter af beslutninger der bliver truffet under magtpres.

HVILKE VALGRELATEREDE CYBERMULIGGJORTE AKTIVITETER ER DER SET?

Der er parallelt med og særligt efter både GRIZZLY STEPPE udgivelserne og det seneste af de to danske undersøgelsesdokumenter kommunikeret en øget bevågenhed ud. Flere lande er nu begyndt at sætte særligt Rusland på, som værende enten aktøren eller knytte til aktører, der gennemfører aktiviteter, hvor subjekterne er valgrelaterede personer, grupper eller organisationer i Vesten. Et antal af disse nyder særligt fokus og vil i det efterfølgende blive gennemgået kronologisk efter offentliggørelsestidspunktet.

Ved det kommende britiske parlamentsvalg har der på nuværende tidspunkt ikke været nogle rapporter om valg-relaterede cybermuliggjorte aktiviteter, idet det skal bemærkes at der har været enkelte røster fremme i starten af 2017, omkring cybermuliggjorte aktiviteter mod det britiske parlamentsvalg i 2015 [72] [73] og i den forbindelse et ønske om, at få støtte fra det britiske *Government Communications Headquarters* til sikring i cyberlandskabet.

Februar 2017: Ministerier i Holland

I februar måned offentliggjorde den hollandske sikkerhedstjeneste Algemene inlichtingen- en Veiligheidsdienst,(AIVD) informationer om, at der gennem de sidste seks måneder, havde været observeret en stor mængde cyberangreb, som blev tillagt at have særligt Rusland, men også Kina og Irland som aktører [74]. Metoden der har været anvendt beskrives umiddelbart ikke særligt detaljeret, men det nævnes at der har været hundreder af forsøg på at nå specifikke personer via e-mail og at formålet har været at få adgang til fortrolige oplysninger.

Formålet om at få adgang til fortrolige oplysninger understøtter anvendelsen af ondsindet software. Da det ikke lykkedes for aktøren at få adgang til oplysningerne, ved vi ikke hvilken form for meningsdannelse aktøren ønskede at opnå: Det kan være at aktøren blot ønsker at få bedre indsigt i subjektets informationsressourcer eller finde kilder, der kan hjælpe aktøren med at identificere den effektive svaghed. Men der kan også være tale om en mere direkte form for anvendelse gennem f.eks. magtpres eller påvirkning af subjektets tankevej til beslutningen. Dermed kan det at gennemføre valget på papir være resultatet af cybermuliggjorte meningsdannende aktiviteter, idet Holland nu har valgt en mere omkostningsfuld metode, Holland er blevet bragt i en mere tilbagestående situation og der bliver sat en præcedens for at en stat vender tilbage til papirvalg.

Umiddelbart ses dette at kunne være traditionelle spionage-aktiviteter, men to ting gør dem relevante i denne sammenhæng. Dels det, at Holland efterfølgende besluttede at der ved

[72] Forster, "Clear evidence Russia interfered in 2015 UK election, says former Labour minister".

[73] MacAskill, "British Political Parties Ask GCHQ for Advice on Preventing Cyber-Attacks".

[74] Vaessen, "AIVD: 'Honderden cyberaanvallen door Rusland en China'".

valget der blev afholdt i marts, skulle være manuel optælling og opregning, idet man på grund af frygt for svagheder i softwaren der ellers anvendes, så muligheder for at manipulere med optælling og i forlængelse heraf, vigtigheden af at have sikret at der ikke hænger en "skygge af tvivl" over valgresultatet. Specifikt udtalte den hollandske indenrigsminister[7576]:

> *"Jeg kan ikke udelukke, at der kan være statslige aktører, der vil forsøge at opnå fordele gennem påvirkning af politiske beslutninger og befolkningens holdninger i Holland. [...] Der er nu indikationer på, at Rusland kunne være interesseret [i valget] og derfor er vi nød til at falde tilbage til det gode gamle pen og papir ved de kommende valg."*

Dette underbyggedes ved chefen for AIVD, der så det som muligt at Rusland ville forsøge at påvirke valgprocessen og "skubbe" vælgerne i "en forkert retning" [77] gennem anvendelse af cyberdomænet og falske nyheder [78].

April 2017: Konrad-Adenauer-Stiftung & Friedrich-Ebert-Stiftung

Konrad-Adenaur-Stiftung og *Friedrich-Ebert-Stiftung* er to fonde i Tyskland, der er tæt knyttet til de to tyske partier Kristendemokraterne (CDU, kansler Angela Merkels parti) og Socialdemokraterne (SPD). Ved udgangen af april udgav sikkerhedsvirksomheden Trend-Micro en analyse [79], hvori en organisation benævnt *Pawn Storm* forsøgte at franarre login-informationer fra ansatte ved Konrad-Adenaur-Stiftung gennem anvendelse af målrettede mails til de ansatte. Desuden er det konstateret at en computer placeret i Ukraine har været anvendt til at udøve spionage mod ansatte i Friedrich-Ebert-Stiftung, herunder adgang til informationer om de ansatte og forsøg på at sprede ondsindet software videre [80].

Trend-Micro angiver oplyser i den forbindelse, at det ikke med sikkerhed kan konstateres om de to fonde har været subjekter for aktiviteterne, eller om de alene har været tænkt som springbrætter for videre aktiviteter, hvor det så sandsynligvis har været CDU og SPD der har været subjekter.

Da vi ikke engang er klar over om de to fonde har været subjekterne eller blot har været brugere, der skulle bruges til at opnå adgang til subjekterne, er det også svært at vurdere den meningsdannende effekt her. En væsentlig pointe er den ukrainske computer, som kan være med til at afklare den meningsdannende effekt. Dette ville i så tilfælde være som et middel til at levere falske informationer om situationen, hvorfor Rusland kan positionere

[75] France-Presse, "Dutch Will Count All Election Ballots by Hand to Thwart Hacking".

[76] Min oversættelse fra The Guardian artikel (engelsk) til dansk

[77] "AIVD: Rusland probeerde met nepnieuws onze verkiezingen te beïnvloeden - RTL Nieuws".

[78] Ibid.

[79] "Pawn Storm Abuses Open Authentication in Advanced Social Engineering Attacks".

[80] Reuters, "Hacker greifen politische Stiftungen von SPD und CDU an".

Ukraine i en mindre favorabel situation overfor Tyskland. Dette ses dog ikke at have nogen nævneværdig indflydelse på valget.

Hverken den tyske informationssikkerhedstjeneste, *Bundesamt für Sicherheit in der Informationstechnik*, eller de berørte fonde har dog uddybet hvilke metoder eller teknikker der har været brugt, men der bemærkes fra flere sider ligheder med aktivisterne som er beskrevet i GRIZZLY STEPPE dokumenterne [81] [82].

Maj 2017: Emmanuel Macron

Ved det franske valg i maj 2017, offentliggjorde den ene af kandidaterne, Emmanuel Macron, 1½ dag før anden valgrunde, at vedkommende havde været målet for et "massivt hacker-angreb", der gjort 9 gigabyte data herunder e-mails tilgængelige på sitet pastebin.com. Dataene kom fra bevægelsen bag Macron, En Marche!, og indeholdt bl.a. interne informationer af forskellig karakter. En undersøgelse gennemført af sikkerhedsfirmaet *Flashpoint*, konkluderer at der er indikationer på at APT28 har stået bag lækagen og at der er ligheder med aktiviteterne beskrevet i GRIZZLY STEPPE dokumenterne, bl.a. nævnes typo squatting hvor domænerne onedrive-en-marche.fr and mail-en-marche.fr (der skal forsøge at snyde subjektet i forhold til onedrive.en-marche.fr og det eksisterende mail.en-marche.fr) [83].

Det er nærliggende at antage at det er lignende aktiviteter som dem der er beskrevet i GRIZZLY STEPPE dokumenterne der har været anvendt her [84]. En væsentlig forskel er dog at resultatet af de cybermuliggjorte meningsdannende aktiviteter ikke nødvendigvis har været det ønskede. Dette givetvis fordi den franske lovgivning forbyder medier og kandidater i at føre valgkamp og begrænser dækningen af valget ganske voldsomt 44 timer før og frem til det sidste valgsted lukker og da dokumenterne blev gjort tilgængelige kun få timer før, fik de ikke meget fodfæste i medierne og hos kandidaterne frem til valget. På de sociale medier – bl.a. under hashtagget #MacronLeaks – fik de derimod en del opmærksomhed, bl.a. med støtte fra amerikanske, højreorienterede grupper [85] og den franskprogede udgave af RT.com [86].

[81] Ibid.

[82] Handelsblatt Global Staff, "Russia-linked Hackers Target German Political Foundations".

[83] "French candidate Macron claims massive hack as emails leaked".

[84] Se 33-34.

[85] Scott, "U.S. Far-Right Activists Promote Hacking Attack Against Macron".

[86] Donadio, "Why the Macron Hacking Attack Landed With a Thud in France".

KONKLUSION

Effektivt gennemførte cybermuliggjorte meningsdannende aktiviteter, består af en kobling af både cybermuliggørelse og meningsdannelse og der er en mængde forskellige aktiviteter, hvorigennem cybermuliggørelse og meningsdannelse kan kobles. I figuren på side 28 hvordan disse koblinger kan ske. Jeg har gennem et antal scenarier (siderne 42-43) eksemplificeret hvordan aktiviteterne kan bringes i anvendelse, med henblik på at opnå forskellige mål. For de forskellige scenarier opstilles et antal erkendelsesmåder:

1. En teknisk erkendelse af datatyveri (ved anvendelse af ondsindet software)
2. En forberedelse af den åbenlyse erkendelse, såfremt informationerne (stjålet i punkt 1) er gjort offentligt tilgængelige.
3. En ”meta-erkendelse” af en aktørs handlinger mod valgsystemer, der er så dækkende at subjektet hurtigt kan vurdere og kommunikere mod aktørens budskaber, om at aktøren har gennemført aktiviteter overfor valgsystemet.
4. En dybere analyse af anden- og tredjeordenseffekter når subjektet tager beslutninger, der bliver truffet under magtpres fra aktøren.

Nogle af disse erkendelsesmåder er lettere at implementere end andre og kombineres disse, ses der en meget høj grad af kompleksitet og et højt abstraktionsniveau.

Den frie presse og Center for Cybersikkerhed er to elementer, der bidrager til at håndtere og sortere i den høje grad af kompleksitet og det høje abstraktionsniveau. Center for Cybersikkerhed har med sine undersøgelsesrapporter vist, at de er i stand til at lave tekniske erkendelser (1) og at de kan agere med disse erkendelser i lang tid, uden at erkendelserne bliver gjort offentligt tilgængelige (2). Meta-erkendelsen i (3) er til gengæld sværere at vurdere, men da danske valg stadigvæk er baseret på papir og blyant, er den kritiske komponent herfor af mindre betydning. De dybere analyser af anden- og tredjeordenseffekter på beslutninger taget under pres (4) kan ikke behandles her. Det kræver i praksis adgang til informationer om beslutninger der er taget under et sådant pres.

Foruden koblingerne og erkendelserne er også de meninger som aktøren ønsker at kommunikere væsentlige. I baggrundsdokumentet til GRIZZLY STEPPE dokumenterne præsenteres to generelle russiske meninger:

- Ruslands ønske om at underminere [...] liberale, demokratiske systemer
- Ruslands ønske om at underminere den offentlige tillid til [...] demokratiske processer

De to meninger suppleres endvidere af andre meninger om særligt ”vestens moralske forfald” og ”tabet af de traditionelle dyder i vesten”.

Da vi i Danmark har en god forståelse og en fri dialog omkring disse meninger og vi i øvrigt i stor udstrækning er enige om de danske forståelser, ses der at være en høj grad af

robusthed i relation til disse. Dette kombineret med den frie presse og Center for Cybersikkerhedsvirke, gør at det vurderes overvejende sandsynligt, at vi i Danmark er i stand til at erkende såfremt vi bliver udsat for cybermuliggjorte meningsdannende aktiviteter, der er tilsvarende til GRIZZLY STEPPE.

Da såvel både det franske og det tyske valg på tidspunktet for det danske kommunalvalg er veloverstået, vil der kunne være rig lejlighed for dels at udnytte erfaringer fra de to øvrige valg og dels at anvende Danmark som en slags ”sandkasse”. En sandkasse er er et sted, hvor nye ideer kan afprøves under stærkt kontrollerede rammer. Typisk vil man i en sandkasse forsøge at gøre tingene mindre komplekse end i virkeligheden (begrebet sandkasse, afspejler f.eks. børns leg i en sandkasse, hvor der kan etableres et simplificeret regelkompleks inden for de fysiske kanter af sandkassen). Dette kunne være dels at afprøve nye, konkrete teknologier til hacking eller nye metoder for phishing, men også at afprøve tanker om hvordan man kan påvirke udfaldet af et valg.

På baggrund af erfaringerne høstet fra sandkassen vil der kunne gennemføres mere effektive kampagner frem mod f.eks. det finske præsidentvalg (januar 2018), det tjekkiske præsidentvalg (januar/februar 2018) eller det montenegrinske præsidentvalg (marts/april 2018).

På tilsvarende vis vil Danmark og vores partnernationer kunne ruste sig bedre mod cybermuliggjorte meningsdannende aktiviteter, ved at udveksle informationer med de nationer der har været ramt og de nationer der har valg i fremtiden.

REFERENCELISTE

"AIVD: Rusland probeerde met nepnieuws onze verkiezingen te beïnvloeden - RTL Nieuws". Set 5. juni 2017. https://www.rtlnieuws.nl/nederland/politiek/aivd-rusland-probeerde-met-nepnieuws-onze-verkiezingen-te-beinvloeden.

Børsmose, Anders. "Landspolitik og lokalpolitik splitter vælgerne". *Politiken*. Set 5. juni 2017. http://politiken.dk/indland/politik/Kommunalvalg/art5470054/Landspolitik-og-lokalpolitik-splitter-v%C3%A6lgerne.

Center for Cybersikkerhed. "Én aktør, mange angreb", april 2017. https://fe-ddis.dk/cfcs/CFCSDocuments/Unders%C3%B8gelsesrapport%20-%20En%20akt%C3%B8r%20mange%20angreb.pdf.

———. "Phishing uden fangst - Udenrigsministeriet under angreb", januar 2016. https://fe-ddis.dk/cfcs/cfcsdocuments/phishing%20uden%20fangst.pdf.

Donadio, Rachel. "Why the Macron Hacking Attack Landed With a Thud in France". *The New York Times*, 8. maj 2017. https://www.nytimes.com/2017/05/08/world/europe/macron-hacking-attack-france.html.

Ducaru, Sorin Dumitru. "Cyber Dimension of Modern Hybrid Warfare and Its Relevance for NATO, The". *Europolity: Continuity & Change Eur. Governance* 10 (2016): 7.

European External Action Service. "EU sanctions against Russia - EEAS - European External Action Service - European Commission". *EEAS - European External Action Service*, 2017. https://eeas.europa.eu/headquarters/headquarters-homepage_en/3762/EU sanctions against Russia.

Fayutkin, Dan. "Russian-Chechen Information Warfare 1994–2006". *The RUSI Journal* 151, nr. 5 (oktober 2006): 52–55. doi:10.1080/03071840608522874.

Fidler, Stephen. "Putin Depicts Russia as a Bulwark Against European Decadence". *WSJ*, 20. september 2013. https://blogs.wsj.com/brussels/2013/09/20/putin-depicts-russia-as-a-bulwark-against-european-decadence/.

Forster, Katie. "Clear evidence Russia interfered in 2015 UK election, says former Labour minister". *The Independent*, 21. februar 2017. http://www.independent.co.uk/news/uk/home-news/chris-bryant-russia-interfered-uk-election-former-labour-minister-2015-vladimir-putin-cyber-attack-a7592226.html.

Forsvarsministeriet. "Redegørelse fra den tværministerielle arbejdsgruppe om Folketingets inddragelse ved anvendelse af den militære Computer Network Attack (CNA)-kapacitet", september 2016. http://www.ft.dk/samling/20151/almdel/fou/bilag/170/1663433.pdf.

France-Presse, Agence. "Dutch Will Count All Election Ballots by Hand to Thwart Hacking". *The Guardian*, 2. februar 2017, par. World news. https://www.theguardian.com/world/2017/feb/02/dutch-will-count-all-election-ballots-by-hand-to-thwart-cyber-hacking.

"French candidate Macron claims massive hack as emails leaked". *Reuters*, 6. maj 2017. http://www.reuters.com/article/us-france-election-macron-leaks-idUSKBN1812AZ.

From, Lars. "Ruslands ambassadør: Danske skibe kan blive mål for russisk atomangreb", 20. marts 2015. http://jyllands-posten.dk/indland/ECE7573125/Ruslands-ambassad%C3%B8r-Danske-skibe-kan-blive-m%C3%A5l-for-russisk-atomangreb/.

Grønkjær, Louise. "Sådan fører Kreml informationskrig mod Vesten". *Information*, 1. juni 2015. https://www.information.dk/udland/2015/05/saadan-foerer-kreml-informationskrig-vesten.

Handelsblatt Global Staff. "Russia-linked Hackers Target German Political Foundations". *Handelsblatt Global Edition*, 26. april 2017. https://global.handelsblatt.com/politics/russia-linked-hackers-target-german-political-foundations-755236.

Hannigan, Robert. "The web is a terrorist's command-and-control network of choice". *Financial Times*, 3. november 2014. https://www.ft.com/content/c89b6c58-6342-11e4-8a63-00144feabdc0#axzz3O7qCcpPj.

Heine, Thomas. "Vi er uhumske, har uredt hår og børnene får brugt legetøj". *Politiken*, 27. oktober 2016. http://politiken.dk/udland/article5648421.ece.

Higgins, Andrew. “In Expanding Russian Influence, Faith Combines With Firepower”. *The New York Times*, 13. september 2016, par. Europe. https://www.nytimes.com/2016/09/14/world/europe/russia-orthodox-church.html.
Larsen, Poul Funder. “Kreml og medier vil lokke russerne til at blive hjemme, men flere og flere rejser mod vest”. *Jyllands-Posten*, 22. oktober 2016. http://finans.dk/protected/finans/politik/ECE9095476/kreml-og-medier-vil-lokke-russerne-til-at-blive-hjemme-men-flere-og-flere-rejser-mod-vest/.
MacAskill, Ewen. “British Political Parties Ask GCHQ for Advice on Preventing Cyber-Attacks”. *The Guardian*, 14. februar 2017, par. UK news. https://www.theguardian.com/uk-news/2017/feb/14/british-political-parties-ask-gchq-advice-prevent-cyber-attacks.
Malicinski, Leny. “Afstemning om EU-forbehold: Nu er aldrig det rigtige tidspunkt”. *RÆSON*, 21. august 2013. http://raeson.dk/2013/afstemning-om-eu-forbehold-nu-er-aldrig-det-rigtige-tidspunkt/.
Matthews, Owen. “Revealed: Putin’s covert war on western decadence”. *The Spectator*, 1. oktober 2016. https://www.spectator.co.uk/2016/10/revealed-putins-covert-war-on-western-decadence/.
Møller, Peter. “Russisk avis sviner Danmark: Børn drikker af vandpytter og folk har lus - TV 2”. *nyheder.tv2.dk*, 24. oktober 2016. http://nyheder.tv2.dk/udland/2016-10-24-russisk-avis-sviner-danmark-boern-drikker-af-vandpytter-og-folk-har-lus.
Naylor, Brian. “Trump Apparently Quotes Russian Propaganda To Slam Clinton On Benghazi”. *NPR.org*, 11. oktober 2016. http://www.npr.org/2016/10/11/497520017/trump-apparently-quotes-russian-propaganda-to-slam-clinton-on-benghazi.
Office of the Director of National Intelligence. “Background to ‘Assessing Russian Activities and Intentions in Recent US Elections’: The Analytic Process and Cyber Incident Attribution”, 6. januar 2017. http://www.sciencedirect.com/science/article/pii/S1361372317300301.
“Pawn Storm Abuses Open Authentication in Advanced Social Engineering Attacks”. *TrendLabs Security Intelligence Blog*, 25. april 2017. http://blog.trendmicro.com/trendlabs-security-intelligence/pawn-storm-abuses-open-authentication-advanced-social-engineering-attacks/.
Rebala, Massimo Calabresi, Pratheek. “Here’s The Evidence Russia Hacked The Democratic National Committee”. *Time*. Set 5. juni 2017. http://time.com/4600177/election-hack-russia-hillary-clinton-donald-trump/.
Reuters. “CIA Identifies Russians Who Gave DNC Emails to WikiLeaks”. *Time*. Set 5. juni 2017. http://time.com/4625301/cia-russia-wikileaks-dnc-hacking/.
———. “Hacker greifen politische Stiftungen von SPD und CDU an”, 25. april 2017. http://de.reuters.com/article/deutschland-cdu-spd-hackerangriff-idDEKBN17R1V5.
Ritzau. “Kronprinsparret til kejserinde Dagmars genbegravelse”. *Berlingske*, 9. maj 2006. https://www.b.dk/danmark/kronprinsparret-til-kejserinde-dagmars-genbegravelse.
RT.com. “Russia threatened to use nukes? US commission produces wildest claims in push for military buildup”. *RT International*, 18. maj 2017. https://www.rt.com/news/388769-us-commission-russia-nuclear-threat/.
Scott, Mark. “U.S. Far-Right Activists Promote Hacking Attack Against Macron”. *The New York Times*, 6. maj 2017. https://www.nytimes.com/2017/05/06/world/europe/emmanuel-macron-hack-french-election-marine-le-pen.html.
Thomas, Timothy. “Russia’s Reflexive Control Theory and the Military”. *The Journal of Slavic Military Studies* 17, nr. 2 (juni 2004): 237–56. doi:10.1080/13518040490450529.
Thomas, Timothy L. “The Russian Understanding of Information Operations and Information Warfare [chapter 23]”. I *Information Age Anthology, vol. III: The Information Age Military*, redigeret af David S. Alberts og Daniel S. Papp, 777–814. Washington, D.C.: United States Department of Defence C4ISR Cooperative Research Program, 2001. http://www.dodccrp.org/files/Alberts_Anthology_III.pdf.

Udenrigsministeriet. “Gældende sanktioner”, 2017. http://um.dk/da/udenrigspolitik/folkeretten/sanktioner/gaeldende-sanktioner.
U.S. Department of Homeland Security: National Cybersecurity and Communications Integration Center. “Enhanced Analysis of GRIZZLY STEPPE Activity”. U.S. Department of Homeland Security, 10. februar 2017. https://www.us-cert.gov/sites/default/files/publications/AR-17-20045_Enhanced_Analysis_of_GRIZZLY_STEPPE_Activity.pdf.
U.S. Department of Homeland Security: National Cybersecurity and Communications Integration Center, og U.S. Federal Bureau of Investigation. “GRIZZLY STEPPE – Russian Malicious Cyber Activity”, 29. december 2016. https://www.us-cert.gov/sites/default/files/publications/JAR_16-20296A_GRIZZLY%20STEPPE-2016-1229.pdf.
———. “Joint Statement from the Department Of Homeland Security and Office of the Director of National Intelligence on Election Security | Homeland Security”, 7. oktober 2016. https://www.dhs.gov/news/2016/10/07/joint-statement-department-homeland-security-and-office-director-national.
Vaessen, Emilie, red. “AIVD: ‘Honderden cyberaanvallen door Rusland en China’”. EenVandaag, 3. februar 2017. http://justitie.eenvandaag.nl/tv-items/71885/aivd_honderden_cyberaanvallen_door_rusland_en_china_.
Walker, Shaun. “Salutin’ Putin: Inside a Russian Troll House”. *The Guardian*, 2. april 2015, par. World news. http://www.theguardian.com/world/2015/apr/02/putin-kremlin-inside-russian-troll-house.