KØBENHAVNS UNIVERSITET
CENTER FOR MILITÆRE STUDIER

Når Hydra angriber

Hybrid afskrækkelse i gråzonen mellem krig og fred

André Ken Jakobsson

Oktober 2019

Kolofon

Når Hydra angriber

Denne rapport er en del af Center for Militære Studiers forskningsbaserede myndighedsbetjening for Forsvarsministeriet og de politiske partier bag forsvarsforliget. Formålet med rapporten er at give et indblik i gråzonekonfliktens logik og de hybride metoder samt at afsøge, hvordan andre vestlige stater arbejder med at opbygge hybrid afskrækkelse gennem nægtelse (hybrid modstandsdygtighed). På den baggrund kommer rapporten med en række anbefalinger til mulige danske initiativer på området, rettet mod såvel statslige aktører som civilsamfundsaktører.

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

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

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

Forfatter:
Postdoc, ph.d. André Ken Jakobsson

Masthead

When Hydra attacks

This report is a part of Centre for Military Studies' policy research services for the Ministry of Defence and the political parties to the Defence Agreement. The purpose of the report is to provide an insight into the logic of gray zone conflict and hybrid methods as well as to explore, how other Western states are working to build hybrid deterrence through denial (hybrid resilience). Building on this, the report formulates a number of recommendations to future Danish initiatives in this area, directed at both state actors and civil society actors.

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

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

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

Author:
Postdoc, Dr. André Ken Jakobsson

ISBN: 978-87-7393-843-0

Indholdsfortegnelse

Dansk resumé og anbefalinger

Danmark skal forholde sig til en ny sikkerhedspolitisk rolle som hybrid frontlinjestat i stormagtskonkurrencen mellem USA, Kina og Rusland. Det danske medlemskab af NATO og EU samt tilhørsforholdet til kredsen af vestlige liberale stater gør, at Danmark udsættes for en diversitet af hybride trusler og angreb i gråzonen mellem krig og fred, der alle finder sted under tærsklen for konventionel krig. Det sker blandt andet gennem desinformationskampagner, cyberangreb og kompromittering af infrastruktur og udgør en ny normaltilstand, som Danmark skal kunne imødegå. Rapporten giver et indblik i gråzonekonfliktens logik og de hybride metoder og afsøger, hvordan andre vestlige stater arbejder med at opbygge hybrid afskrækkelse gennem nægtelse (hybrid modstandsdygtighed). Hovedformålet er at informere og inspirere både statslige aktører og civilsamfundsaktører til at iværksætte danske initiativer baseret på udenlandske erfaringer.

Rapporten identificerer tre overordnede indsatsområder, der kræver handling: holdningsdannelse, infrastruktur og koordination. Karakteren af de hybride trusler udfoldes inden for hvert af disse områder, og derefter præsenteres en systematiseret palet af nationale tiltag og særligt udvalgte eksempler til inspiration. 1) Hybrid modstandsdygtighed på holdningsdannelsesområdet angår påvirkningskampagner og valgkampe, hvor regulering af sociale medier, politiske reklamer og græsrodsinitiativer til bekæmpelse af desinformation bliver undersøgt. 2) På infrastrukturområdet angår hybrid modstandsdygtighed især cyberinfrastruktur og kritisk fysisk og sikkerhedsrelevant infrastruktur. Rapporten peger på nødvendigheden af et bredt sikkerhedsbegreb og præsenterer blandt andet, hvordan andre stater beskytter viden og teknologi og screener udenlandske investeringer for at imødegå gråzonens stormagtskonkurrence, der også strækker sig ind i eksempelvis handelspolitik. Den brede forståelse af cyberinfrastruktur angår også dybe, tværgående samarbejder mellem staten, forskningsinstitutioner og private virksomheder om udviklingen af cybersikkerhed. 3) Sidste indsatsområde handler om den koordination, der står centralt i hybrid afskrækkelse gennem nægtelse. Hybride angreb er ofte designet til at undgå detektering og foretages derfor ved hjælp af forskellige instrumenter på samme tid. Når Danmark skal kunne opdage, afværge og reagere på disse, er det nødvendigt med en tæt koordination mellem myndigheder og private aktører, både nationalt og internationalt. Her undersøges et omfattende sikkerhedskoncept for nationale processer, en hybrid doktrin, og interorganisatoriske samarbejder mellem blandt andre EU og NATO samt hybridt diplomati. Rapporten konkluderer med anbefalinger for hvert indsatsområde samt mere generelle retningsanvisninger.

Overordnede anbefalinger: Prioritering af strategisk beredskabsplanlægning, der bygger på forståelsen af, at i gråzonekonflikten bliver almindelig drift til en del af dansk sikkerhedspolitik.

- Strategisk beredskabsplanlægning gennem *whole-of-government*- og *whole-of-society-tilgang*, der kombinerer sektoransvarsprincippet med en høj dansk organisationsgrad for at skabe tværsektoriel koordination lig Finland og et styringsdokument lig den britiske hybride *Fusion*-doktrin. Det inkluderer harmonisering af indsatser på rigsfællesskabsniveau.
- Strategisk beredskabsplanlægning via et styrket nationalt sikkerhedsbillede gennem overvågning af kerneindikatorer, hvilket inkluderer rutinemæssige hybride sårbarhedsanalyser, der udvider og fusionerer Beredskabsstyrelsens *Nationalt Risikobillede* med situations-, trussels- og risikovurderinger fra PET og FE.

Anbefalinger til holdningsdannelse, påvirkningskampagner og valgkamp

- Håndbog om psykologisk forsvar til offentligt ansatte på forskellige niveauer, fra centraladministrationen til kommuner, der giver værktøjer til at opdage og håndtere påvirknings- og hvervningskampagner, i stil med den svensk udviklede *Countering information influence activities: A handbook for communicators.*
- Gennemsigtighed i politiske kampagner kræver større åbenhed om partistøtte, indskrænkning af udenlandske aktørers adgang til partipolitiske aktiviteter i Danmark med inspiration fra Canada og yderligere regulering af sociale medier, herunder af brugen af bot-netværk.

Anbefalinger til kritisk cyberinfrastruktur samt fysisk og sikkerhedsrelevant infrastruktur

- Hurtig udbedring af sårbare IT-systemer ved at identificere og udbedre systemer i utilstrækkelig systemtilstand gennem et tilbundsgående eftersyn af den offentlige sektors IT-sikkerhed med inspiration fra den franske cybersikkerhedsmyndighed, ANSSI, der opstiller sikkerhedskrav også til private aktører. Opprioritering af cybersikkerhed inkluderer også øget samarbejde mellem staten, forskningsinstitutioner og industrien.
- Investeringsscreening gennem bred definition af kritisk infrastruktur med inspiration fra det kontinuerlige tyske arbejde på området, der bør dække potentielt kritiske og ikketraditionelle sikkerhedsrelevante emner som specialiseret viden og teknologi med konsekvenser for handels- og forskningssamarbejder.

Anbefalinger til national og international koordination

- Oprettelse af et hybridt situationscenter til at overvåge og koordinere de nationale tiltag samt imødekomme det øgede behov for et nationalt kontaktpunkt for udenlandske aktører (NATO, EU, efterretningstjenester) med inspiration fra Finlands situationscenter under statsministerens kontor. Dette inkluderer oprettelse af en dansk hybrid ambassadørstilling.
- Styring efter hybrid sikkerhed, så risikostyring i den offentlige sektor i forbindelse med mål- og resultatstyring (*New Public Management*) på udvalgte forvaltningsområder formelt tilpasser sig gråzonens øgede sikkerhedsbehov, hvilket i praksis eksempelvis kræver bredere involvering af aktører i KRISØV.

Abstract and recommendations

Denmark must accustom itself to its new role as a hybrid front-line state in the great power competition between the US, China and Russia. The Danish membership of NATO, the EU and the circle of Western liberal states, means that Denmark is exposed to a variety of hybrid threats and attacks in the gray zone between war and peace under the threshold of conventional war. These take place through – amongst other methods – disinformation campaigns, cyber-attacks and compromise of infrastructure, and constitutes a new normal that Denmark must be able to counter. This report provides a view into the logic of gray zone conflict and hybrid methods and explores how other Western states are working to build hybrid deterrence through denial (hybrid resilience). The main purpose is to inform and inspire both state actors and civil society actors to launch Danish initiatives based on foreign experiences.

The report identifies three focus areas that require action: opinion formation, infrastructure and coordination. The nature of hybrid threats is unfolded within each of these areas after which a systematic palette of national initiatives and selected examples is presented as inspiration. 1) Hybrid resilience in the field of opinion formation relates to influence campaigns and elections in which regulation of social media, political advertising and grassroots initiatives to deter disinformation are investigated. 2) In the field of infrastructure, hybrid resilience is particularly related to cyber infrastructure and critical physical and security-related infrastructure. The report points to the necessity of a broad concept of security and presents, among other initiatives, how states protect knowledge and technology and screen foreign direct investment to counter the gray zone competition, which also extends into trade policy. The broad understanding of cyber infrastructure also concerns deep, cross-sector collaborations between the state, research institutions and private companies on development of cyber security. 3) Last focus area concerns the coordination that is central to hybrid deterrence through denial. Hybrid attacks are often designed to avoid detection and are therefore conducted using different instruments at the same time. Therefore, as Denmark must be able to detect, resist and respond to these, close coordination between authorities and private actors, both nationally and internationally, is necessary. Thus the report examines a comprehensive security concept for national processes, a hybrid doctrine, and interorganizational cooperation between, for example, the EU and NATO, as well as hybrid diplomacy. The report concludes with recommendations for each focus area as well as more general instructions.

General recommendations: Prioritize strategic contingency planning, based on the understanding that in the gray zone conflict, ordinary and everyday operations become part of Danish security policy.

- Strategic contingency planning through a whole-of-government and whole-of-society approach, which combines the Danish public sector principle of sector responsibility with the high membership levels of Danish civil society organizations to create cross-sectoral coordination as in Finland and a strategic management document like the British Fusion doctrine. This includes harmonization of efforts at the level of the Danish realm (Greenland and Faroe Islands).
- Strategic contingency planning through strengthened situational awareness by monitoring core indicators, which includes routine hybrid vulnerability analyses that expand on and merge the Danish Emergency Management Agency's *National Risk Picture* with situational, threat and risk assessments from the Police Intelligence Service and the Danish Defence Intelligence Service.

Recommendations on opinion formation, influence campaigns and election campaigns

- Handbook on psychological defense for civil servants at various levels, from the central administration to municipalities providing tools for detecting and managing influence and recruitment campaigns, in line with the Swedish developed *Countering information influence activities: A handbook for communicators.*
- Transparency in political campaigns requires greater openness about party donors, restricting foreign actors' access to party political activities in Denmark with inspiration from Canada and further regulation of social media, including on the use of bot networks.

Recommendations on critical cyber, physical and security-relevant infrastructure

- Speedy upgrades of vulnerable IT systems by identifying and improving on legacy systems and systems with insufficient security through an in-depth analysis of public sector IT with inspiration from the French cybersecurity authority, ANSSI, who also sets IT security requirements for private actors. Prioritization of cyber security includes increased cyber-cooperation between the state, research institutions and industry.
- Investment screening through a broad definition of critical infrastructure, inspired by the ongoing German work in this area, which should cover potentially critical and non-traditional security-relevant areas such as specialized knowledge and technology with implications for trade and research collaborations.

Recommendations on national and international coordination

- Establish a hybrid situation center to monitor and coordinate national initiatives as well as to answer the increased need for a national contact point for foreign actors (NATO, EU, intelligence services) with inspiration from Finland's Situation Center under the Prime Minister's Office. This includes establishing a Danish hybrid ambassador position.
- Adopt hybrid security management, so that risk management in specific areas of the public sector formally adjusts to the increased security needs of the gray zone, which in practice requires, for example, wider involvement of actors in KRISØV emergency exercises.

1 Gråzonen: I et udvidet kamprum er Danmark en hybrid frontlinjestat

Danmark står over for en bred vifte af nye trusler, der spænder lige fra desinformation og påvirkningskampagner i forbindelse med valgkampe over cyberangreb på kritisk infrastruktur såsom trafik-, forsynings- og kommunikationssystemer til risici for, at udenlandske investeringer eller lån skaber afhængigheder og udnyttes politisk. Rapportens formål er at gøre det muligt at øge Danmarks modstandsdygtighed over for disse trusler og inspirere til afskrækkende tiltag ved at undersøge andre vestlige staters initiativer.

De nye udfordringer er resultatet af en ændret sikkerhedspolitisk situation, hvor den liberale verdensorden ikke længere tages for givet, og hvor det amerikanske lederskab er udfordret af især Rusland og Kina i en konfrontation, der bevidst udkæmpes under tærsklen for konventionel krig. Rapporten beskriver, hvordan denne nye type konflikt udspiller sig i gråzonen mellem tilstandene krig og fred, samt hvordan den strategiske konkurrence bliver langstrakt. Derfor er Vesten i færd med at ruste sig til denne gråzonekonflikt, som i stedet for at anvende krudt og kugler på kampplads en rykker ind i hverdagens politiske, sociale og økonomiske rum. Konfliktens metoder udnytter svagheder ved modstanderens stat og samfund, og i Vesten er det særligt i de åbne samfunds frie rammer, at angrebsmulighederne byder sig til. Ytringsfrihed, forsamlingsfrihed og det frie marked gør det nemmere for modstanderen at udøve undergravende eller direkte skadelig virksomhed. Danmark er som en del af Vesten klart defineret som en aktør i denne gråzonekonflikt og er derfor af interesse for gråzoneaktørers hybride angreb og destabilisering af allianceforhold. Andre stater er løbet i forvejen og kan derfor inspirere til den videre danske tænkning.

Rapporten identificerer på den baggrund tre overordnede udfordringer, som nye danske initiativer skal forholde sig til. Den første er udfordringen fra udenlandsk påvirkning af den danske holdningsdannelse generelt samt mere specifikt påvirkning af valg. Den anden udfordring handler om at beskytte dansk kritisk infrastruktur, hvilket angår både cybermodstandsdygtighed og fysisk og intellektuel modstandsdygtighed. Den tredje udfordring kommer fra truslernes meget brede karakter, der nødvendiggør koordination gennem både nationalt og internationalt samarbejde. Det danske svar på disse udfordringer må gå på to ben. For det første en erkendelse af, at Danmark i lighed med andre vestlige stater er en frontlinjestat i stormagternes konfrontation, og at det er en ny sikkerhedspolitisk kontekst, som en række politiske, administrative og civile aktører skal forholde sig til. Det betyder, for det andet, at den nye konflikts karakter forpligter disse aktører til at gentænke deres roller og ansvar med hensyn til at beskytte og opretholde et velfungerende samfund. Hverdagens drift og beredskab er pludselig blevet en del af dansk sikkerhedspolitik.

1.1 Formål, metode og struktur

Rapportens formål er at afdække bredden og dybden af det mulighedsunivers af initiativer, som andre stater har fundet anvendelige, og vurdere disse i forhold til danske forhold og behov. Rapporten er et deskstudy og bygger på et bredt udvalg af videnskabelige kilder, officielle dokumenter og pressemateriale, der samlet set tegner et situationsbillede med hensyn til hybride trusler og imødegåelsen af disse – et såkaldt *horizon scan*. Rapportens referencer henviser, hvor det er muligt, direkte til love eller regeringsdokumenter, da ønsket er at levere det mest konkrete grundlag for læring. Derudover har forfatteren deltaget i en række aktiviteter, der kvalificerer rapporten, deriblandt det tredages nationale Counter Hybrid Threat Seminar, afholdt af NATO's specialoperationshovedkvarter og det danske Forsvar på Forsvarsakademiet i 2017, det opfølgende regionale firedages Northern Regional Countering Hybrid Threats Seminar, afholdt på European Centre of Excellence for Countering Hybrid Threats i Finland i 2018, samt konferencen #Misinformation #Propaganda #Fake News – A Danish Perspective, afholdt i 2018 i et samarbejde mellem Mandag Morgen, Udenrigsministeriet og den amerikanske ambassade i København. Rapporten omhandler vestlige staters tiltag, men udgør ikke en udtømmende analyse eller et udtømmende overblik. Derimod præsenteres udvalgte eksempler af interesse for Danmark, som kan inspirere til nye initiativer eller udbygge allerede eksisterende.

Rapporten er opbygget efter følgende struktur:

- **Kapitel 2. Gråzonekonflikt er den nye normaltilstand: Brug alle midler under tærsklen for krig**: Kapitlet udfolder gråzonens logik om konflikt under tærsklen for konventionel krig, præsenterer dynamikkerne i hybride angreb og redegør for, hvordan hybrid afskrækkelse gennem øget modstandsdygtighed fungerer.

- **Kapitel 3. Indsatsområder: hybrid modstandsdygtighed gennem afskrækkelse:** Kapitlet præsenterer hybrid afskrækkelse og konkrete initiativer, som andre stater har taget for at opbygge modstandsdygtighed. Initiativerne bliver præsenteret inden for tre overordnede indsatsområder: holdningsdannelse, infrastruktur og koordination.

- **Kapitel 4. Konklusion og anbefalinger**: Kapitlet formulerer anbefalinger i en dansk kontekst set i lyset af andre landes imødegåelse af hybride trusler.

I præsentationen af hvert indsatsområde bliver der i tekstbokse givet særlige eksempler, som rapporten udfolder med en lidt højere detaljeringsgrad. Formålet er at fremhæve, hvordan hybrid afskrækkelse kan fungere på det specifikke indsatsområde og give inspiration til en bred skare af aktører. Dermed åbner rapporten for, at både private organisationer, virksomheder, civilsamfundet og statens forskellige lag kan finde inspiration til at tage initiativer og tilpasse disse på egen hånd. Hybrid afskrækkelse kan og skal ikke alene løftes af den danske stat. En vigtig distinktion at have med sig i resten af rapporten er derfor, at statens og samfundets sikkerhed og modstandsdygtighed på samme tid er integreret og adskilt. Mens staten har en tydelig selvopfattelse med en medfødt forpligtelse til at yde sikkerhed for sig selv og samfundet, så er samfundets mange forskellige byggeklodser modsat ikke orienteret mod at producere sikkerhed, men derimod andre individuelle eller samfundsmæssige

goder. Mange af de hybride virkemidler udnytter dette i formelt set lovlige angreb mod samfundet. Civilsamfundet og virksomhederne spiller derfor en afgørende rolle, og rapportens tekstbokse understøtter disse i at samskabe Danmarks hybride modstandsdygtighed.

1.2 Når Hydra angriber: dansk hybrid modstandsdygtighed

Rapporten kategoriserer de ovennævnte nye udfordringer som hybride trusler, der består af en diversitet af både åbenlyse og skjulte eller svært identificerbare virkemidler. Formålet med hybride angreb under tærsklen for konventionel krig er at opnå politiske effekter, der fremmer angriberens sag.

Den mytologiske fortælling om Herkules' 12 arbejder fremmaler en passende metafor for hybride angreb i form af det mangehovedede monster Hydra. Skærer Herkules ét af Hydras mange hoveder af, så vokser to nye frem, mens helten Herkules samtidig må kæmpe mod Hydras giftige ånde og blod. Hydra er en i særklasse hybrid modstander, der formår at koordinere forskellige virkemidler for at opnå en synergieffekt. Ikke engang halvguden Herkules kan overvinde Hydra alene og får derfor hjælp af allierede både på jorden og i gudernes rige. En illustration af, at imødegåelse af hybride trusler og angreb kræver mindst den samme spændvidde og det samme samarbejde (og oftest større), som angriberen anvender. I Vesten har anerkendelsen af sådanne hybride trusler været langsomt stigende, men Ruslands selvhævdende og aggressive adfærd siden den ulovlige annektering af Krim i 2014 har accelereret debatten, og det samme har det nye amerikanske fokus på Kina som en strategisk konkurrent.

Derfor har Danmark søsat en række initiativer for at imødegå hybride trusler, der overordnet består af tre tiltag. Det første handler om at undgå udenlandsk påvirkning af danske valg, og derfor blev en valghandlingsplan iværksat i september 2018. Planens 11 initiativer har blandt andet fokus på intern regeringskoordination gennem en tværministeriel taskforce, overvågning af desinformation, styrket efterretningsfokus på påvirkningsforsøg samt dialog og samarbejde med medier og partier om imødegåelse af disse trusler.[1] I tillæg hertil er straffelovens milde spionparagraf, § 108, blevet strammet, så det klart fremgår som strafbart gennem et samarbejde at hjælpe fremmede efterretningstjenester til at udføre påvirkningsvirksomhed.[2]

Det andet tiltag består i at give staten mulighed for ultimativt at tvinge danske organisationer til at tilslutte sig Center for Cybersikkerheds (CFCS') Netsikkerhedstjeneste, der skal overvåge og beskytte Forsvaret, virksomheder og statslige myndigheder mod cyberangreb. Det sker gennem det nationale Cybersituationscenter hos CFCS[3], og ordningen er grundlæggende tænkt som frivillig, mens den nye lovgivning giver mulighed for, at staten kan vurdere en organisations samfundsmæssige vigtighed som så stor, at organisationen kan påbydes tilslutning.[4]

Det tredje tiltag angår screening af udenlandske direkte investeringer i Danmark samt andre økonomiske aktiviteter, som kan have betydning for national sikkerhed og offentlig orden. Lovforslaget, som en tværministeriel arbejdsgruppe udarbejder, har som opdrag, at det i yderste konsekvens bliver muligt for den danske stat at forbyde en sådan risikofyldt aktivitet. Lovens dækningsområde er indtil videre bredt defineret og koncentrerer sig især om kritisk infrastruktur og udvalgte sektorer såsom energi, IT- og tele, transport, fødevarer og sundhed, men har også fokus på virksomheder, der udvikler eller bruger avancerede teknologier.[5] Bekymringen består i, at udenlandske firmaer

eller stater kan få adgang til følsom information eller aktiver, der kan bruges til at presse Danmark politisk.[6]

Disse tre overordnede tiltag udgør kun en første etape i imødegåelsen af den langstrakte gråzonekonflikts hybride trusler. De er på ingen måde endestationen. Det vidner den kritiske debat også om, for tiltagene har skabt bekymring for indskrænkning af det frie samfunds fundamentale søjler, og dermed er selve den danske selvforståelse bragt i spil. Derfor er det vigtigt, at danske initiativer til imødegåelse af hybride trusler kan spejle sig i andre staters overvejelser og initiativer, hvilket denne rapport bidrager til.

Den optimale situation for Danmark vil være at undgå hybride angreb gennem etablering af afskrækkelse, hvilket kan ske ved enten at true med – samt have evnen til – at *straffe* angriberen eller at *nægte* modstanderen mulighed for at opnå en effekt af hybride angreb. Rapporten fokuserer på den anden mulighed, nemlig *afskrækkelse gennem nægtelse*, hvilket betyder, at Danmark skal opbygge modstandsdygtighed på en række centrale områder, hvor hybride angreb kan sættes ind.

Rapportens overordnede tilgang til modstandsdygtighed bygger på den eksisterende praksis for beredskabsplanlægning, men analysen understreger nødvendigheden af at gøre denne beredskabstænkning strategisk bevidst om gråzonens udvidede kamprum, hvor civilsamfundet og den private sektor angribes i langt højere grad. Afskrækkelse gennem modstandsdygtighed handler om at etablere en strategisk beredskabsplanlægning, som kan indoptages hos en diversitet af samfundsaktører, og hvor fjendtlige, menneskeskabte hændelser er det centrale fokus. Et sådant skifte fra natur (uforudsete ulykker og naturkatastrofer) til aktør (bevidste angreb) bringer også nye snitflader med sig, hvor koordination både internt i staten og mellem staten og den private sektor bliver afgørende. Det betyder nye opgaver og et tættere samarbejde mellem eksempelvis Beredskabsstyrelsen, Politiets Efterretningstjeneste (PET) og Forsvarets Efterretningstjeneste (FE) og dermed også overvejelser om organisering, ansvar og kontrol – både politisk og administrativt.

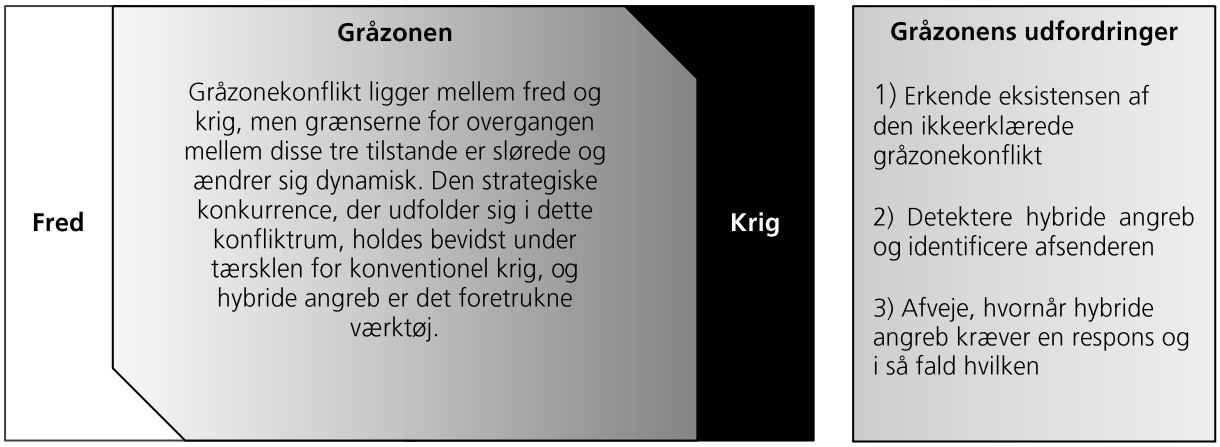
2 Gråzonekonflikt er den nye normaltilstand: Brug alle midler under tærsklen for krig

En ny normaltilstand af langstrakt konflikt har indfundet sig i international politik. Den udfolder sig i gråzonen mellem krig og fred og pågår især mellem det liberale, demokratiske og markedskapitalistiske Vesten og illiberale, autoritære stater som Rusland og Kina. Konflikt i gråzonen handler om staters fjendtligtsindede og egennyttige aktiviteter, der befinder sig mellem hvid (fredelig sameksistens) og sort (konventionel væbnet kamp). Mens det kan være en udfordring at konkretisere gråzoneaktiviteter samt klart at definere gråzonens afgrænsning mellem hvid og sort, så står fred og krig langt skarpere frem ikke kun i sig selv, men også fordi de er tilstande, som Vesten hidtil har analyseret konflikter ved hjælp af. De skandinaviske landes politiske relationer vil klart være i den hvide zone med fredeligt samarbejde, gennemsigtig samhandel og diplomati, mens de væbnede konflikter i 90'erne mellem stater på Balkan klart er i den sorte zone, altså krig.

Gråzonens overordnede konfliktrelation domineres af den stigende strategiske rivalisering mellem USA, Rusland og Kina, hvilket den seneste amerikanske forsvarsstrategi understreger som en mere permanent tilstand.[7] Gråzonen er kendetegnet ved en bevidst tilbageholdenhed for at undgå direkte konfrontation, konstant udfordring af vedtagne normer og regler samt opretholdelse af en plausibel benægtelse af de handlinger, man foretager sig. Tvetydigheden er en kunstart i rummet mellem krig og fred.

Danmark er placeret midt i gråzonekonflikten via medlemskabet af NATO og EU og som en dedikeret og loyal forsvarer af den liberale og regelbundne verdensorden, der tjener en småstat godt, men som står i vejen for stormagter, der ønsker at undergrave og omgøre de nuværende spilleregler og alliancer. Gråzonen fungerer som et konfliktrum i en fredstid, hvor den nuværende orden bliver udfordret, uden at en direkte konventionel konfrontation med USA og Vesten finder sted. Alternativet til at operere i gråzonen vil være den sorte zone og dermed krig, da hverken Rusland eller Kina, som de største gråzoneaktører ud over USA, kan opnå deres ønskede målsætninger via den hvide zones fredelige diplomati.

Figur 1: Gråzonens logik og udfordringer



Den strategiske stormagtskonkurrence indebærer stærke modsatrettede interesser og handler om enten at bevare den globale magtbalance eller ændre den, så Vesten får mindre politisk, økonomisk og kulturel indflydelse. Gråzonens lavere konfliktintensitet fungerer derfor som et rum, hvor stormagtsrivaliseringen har mulighed for at udspille sig uden den traditionelle krigs ødelæggende dynamik. Evnen til at konkurrere i gråzonen bliver dermed afgørende for fremtidens konfliktniveau. Hvis en stat oplever sig som voldsomt udfordret i gråzonen ved eksempelvis ikke at kunne imødegå udenlandsk undergravende virksomhed af statens politiske eller økonomiske system, så stiger risikoen for enten et konventionelt svar (hvilket er utænkeligt i forhold til de konventionelle stormagter Rusland og Kina) eller en grad af politisk kollaps og eftergivenhed for det eksterne pres.

Verdensordenen kan således ændres bid for bid, når de illiberale stormagters ide om berettigede interessesfærer udfordrer mindre nationalstaters suverænitet til at udøve selvstændig indenrigs- og udenrigspolitik. Kina ønsker ligesom Rusland at indtage en ny global og respekteret rolle med større frihedsgrader til at forfølge nationale interesser, som anerkendes af USA, EU og regionale stater. På trods af at Rusland og Kina har væsensforskellige udgangspunkter, ressourcer og ambitioner, så deler de analysen af Vesten, og der er også tegn på et gryende antivestligt partnerskab, der blandt andet for første gang placerede tre kinesiske flådefartøjer i Østersøen som led i den russiske flådeøvelse Joint Sea 2017.[8] På samme vis ses tendenser til, at Rusland og Kina også nærmer sig hinanden i brugen af gråzoneaktiviteter ved at lære af hinandens erfaringer.[9] Forskellene i mulighederne for at benytte gråzonens værktøjer vil dog bestå, i kraft af at Rusland har et økonomisk set pauvert udgangspunkt[10], mens Kinas imponerende opstigning meget muligt er begyndelsen på et nyt imperialistisk projekt.[11] Rusland har modsat Kina ikke økonomiske ressourcer til at opkøbe eksempelvis vestlig kritisk infrastruktur[12] og forsøger derfor i højere grad at nedbryde end at opbygge ved at agere som en *spoiler,* der smider grus ind i det globale maskinrum i stedet for at tilføre olie.[13] Men uanset motivation og ambition er det bydende nødvendigt, at begge staters gråzoneaktiviteter imødegås.

Gråzonekonfliktens essens fanges af den amerikanske diplomat George F. Kennans beskrivelse af politisk krigsførelse under denne kolde krig:

> "I bredeste forstand er politisk krigsførelse anvendelsen af alle midler, som en nation har til rådighed, der befinder sig under tærsklen for krig,

> for at opnå nationale målsætninger. Sådanne operationer er både åbne og skjulte."[14]

Denne rapport adresserer alene tilstanden af konflikt i rummet mellem krig og fred, og selvom gråzonekonflikt har potentialet til at eskalere til traditionel krig[15], så er konventionel krig en ganske særskilt tilstand, hvor andre logikker gør sig gældende. Logikken, der driver konflikt i gråzonen, handler derimod om at benytte alle statens til rådighed stående midler til at opnå politiske mål, men samtidig bevidst søge at holde aktiviteterne under tærsklen for væbnet konflikt.

Den grundlæggende dynamik i gråzonen fanges i dag stadig af Kennans beskrivelse fra 1948, men den teknologiske udvikling siden da har tilladt en væsentlig afkobling af geografiens betydning for en stats udsathed. Tidligere var en frontlinjestat defineret ved sin geografiske placering tæt på en modstander, men den placering har i dag langt fra samme betydning for, i hvor høj grad en stat er udsat for gråzoneaktiviteter. Nye teknologier både øger intensiteten og udvider skalaen med hensyn til at benytte velkendte og gamle gråzoneværktøjer, og på samme vis er geografien også til dels afkoblet evnen til at gennemføre disse angreb. Sammenlagt giver det grund til at genevaluere en række staters status – deriblandt den danske.

Danmarks status må erkendes som værende en frontlinjestat i gråzonekonflikten eller mere præcist en hybrid frontlinjestat. Værktøjerne såsom spionage, rekruttering af centralt placerede personer, oprettelse af femte kolonne, sabotage af infrastruktur eller undergravende propaganda er velkendte, men samtidig er mulighederne for en fjendtlig aktør for at producere en effekt øget voldsomt som følge af Danmarks høje grad af digitalisering, der både handler om borgernes kommunikation med det offentlige og om private aktører som eksempelvis banker samt den store danske tilstedeværelse på sociale medier. Døren står i overført betydning mere end blot på klem for fjendtlige aktører, der ønsker at udnytte de risici, der åbner sig ved omstilling til og afhængighed af digitale teknologier – deriblandt især internettet.

2.1 Fra gråzonens strategiske konflikt til hybride trusler og angreb

Stormagtsrivaliseringen i gråzonen handler, jævnfør ovenstående analyse, om at forfølge store strategiske målsætninger gennem brugen af alle statens til rådighed stående midler, der forbliver under tærsklen for krig. Karakteren og indholdet af disse gråzoneaktiviteter på det konkrete niveau forstås bedst ved at se disse som hybride trusler. Rapporten ønsker at rette fokus mod det udvidede kamprum, hvor områder (sociale rum), der i Vesten hidtidigt har været relativt undtaget fra at være en del af international rivalisering og konflikt, nu bliver inddraget heri. Inden rapporten går i dybden med hybride trusler, så skal den fundamentale forudsætning for hybride angreb erindres: det politiske formål. Ifølge Carl von Clausewitz er krig politikkens fortsættelse med anvendelse af andre midler[16], og det samme gør sig gældende i gråzonen, hvor det ligeledes handler om 'at påtvinge modstanderen vor vilje'.[17] Viljen og formålet varierer dog for de enkelte hybride aktører, når de handler på baggrund af forskellige motivationer og målsætninger og angriber forskellige mål, og derfor vil eksempelvis Rusland og Kina handle på forskellig vis, men ud fra den samme logik.

Den første udfordring med hensyn til at imødegå hybride trusler og angreb handler om at identificere disse, men deres omskiftelige og til dels

uhåndgribelige karakter gør det svært at formulere en fast og dækkende definition. Den kendsgerning udgør netop grundideen i at benytte hybride angreb: De er svære at få en klar forståelse af og dermed vanskelige at opdage og beskytte sig mod. Den abstrakte forståelse konkretiseres af NATO's "Multinational Capability Development Campaign project: Countering Hybrid Warfare Project" (MCDC-projektet)[18], der beskriver hybride angreb som 'den synkroniserede brug af flere magtinstrumenter [instruments of power] der er skræddersyet til specifikke sårbarheder på tværs af hele spektret af samfundsfunktioner for at opnå synergieffekter'.[19] Statens magtinstrumenter[20], som synkroniseres for at opnå en synergieffekt, er det politiske, økonomiske, civile og informationsmæssige, og hver især har de særlige egenskaber, der fleksibelt kan tilpasses omstændighederne.

Det økonomiske instrument kan med fordel benyttes mod en lille, skrøbelig økonomi, hvor angriberen eksempelvis har betydelige investeringer eller aftager store mængder eksport fra, eller hvor angriberen finder favorable forhold til at udføre økonomisk kriminalitet, mens informationsinstrumentet eksempelvis kan have stor effekt over for en stat med stærk politisk polarisering og lav tillid til medierne, så desinformationskampagner har lettere gang på jorden. Den tilpasningsparate tilgang kommer til udtryk i angriberens indsats for at skabe synkroniserede angrebspakker (*Synchronized Attack Packages*), hvor de tilgængelige magtinstrumenter doseres og kombineres for at udnytte de svagheder, som det angrebne mål antages at have, og hvis svækkelse vil fremme angriberens politiske dagsorden.[21] Det hybride angreb handler dermed om at udnytte svagheder, kløfter og potentielle spaltninger (på engelsk *cleavages* og *seams*) i de strukturer, systemer og organisationer, som er målet for angrebet. MCDC-projektet udpeger svagheder i det politiske, økonomiske, sociale, informationsmæssige og infrastrukturelle spektrum, og hybride angreb på disse svagheder gennem brugen af en hybrid aktørs magtinstrumenter kan kombineres på utallige måder. Angrebene er svære at opdage og udpege som led i et hybrid angreb og endnu sværere at koble sammen med andre dele af et synkroniseret angreb, som derfor kan risikere at pågå uset og opnå effekt uden den rette imødegåelse og afværgelse.

Den hybride angriber har mange muligheder for at anvende magtinstrumenterne til at eskalere angrebet. Det kan foregå gennem både *vertikal eskalering*, hvor angriberen intensiverer brugen af det enkelte instrument, og *horisontal eskalering,* hvor angriberen synkroniserer brugen af flere forskellige instrumenter.[22] Fleksibiliteten tillader angriberen at udføre det særligt skræddersyede angreb mod en specifik modstanders svagheder, og muligheden for at skrue ned for intensiteten af det enkelte magtinstrument, men op for synkroniseringen, gør, at tvetydigheden, der karakteriserer hybride angreb, kan sløre angrebet og hæmme dets opdagelse og den angrebnes mulighed for at udpege afsenderen.

3 Indsatsområder: hybrid modstandsdygtighed gennem afskrækkelse

Rapportens hovedformål er at skabe et overblik over samt inspiration til, hvordan Danmark kan opbygge hybrid modstandsdygtighed, og derfor præsenteres nu en systematisering af, hvordan vestlige stater har reageret på deres egen udsathed med hensyn til de magtinstrumenter, som et hybridt angreb vil kunne benytte. Indsatsområderne er identificeret gennem analyser af en lang række initiativer for hybrid modstandsdygtighed, iværksat af stater, der, i forhold til både geografisk placering og trusselsmæssig udsathed, er forskellige. Disse initiativer er kategoriseret og konkretiseret i en række overordnede indsatsområder baseret på relevans for en dansk kontekst. Processen danner grundlaget for kapitel 3, der præsenterer de tre indsatsområder holdningsdannelse, infrastruktur og koordination med tilhørende underkategorier af initiativer.

Tabel 1: Indsatsområder for hybrid modstandsdygtighed

Holdningsdannelse	Infrastruktur	Koordination
- Påvirkningskampagner - Valgkamp	- Cyberinfrastruktur - Kritisk fysisk og sikkerhedsrelevant infrastruktur	- National koordination - International koordination

Inden de tre indsatsområder bliver udfoldet, skal de placeres i den hybride afskrækkelses forståelsesramme. Formålet med afskrækkelse er at ændre modstanderens adfærd, så et angreb optimalt set slet ikke finder sted. Afskrækkelse handler således om at kommunikere klart til modstanderen, at man har både viljen og evnen til at imødegå og svare på et angreb, og derigennem minimere risikoen for, at modstanderen overhovedet forsøger sig.

Hybrid afskrækkelse udgøres derfor af to sammenhængende logikker: en beredskabslogik, hvor hybrid modstandsdygtighed har en funktionel karakter (opbygning af processer, ressourcer, regulering og oplysning) og en sikkerhedspolitisk logik, hvor hybrid modstandsdygtighed som nægtelse er signalgivning til angriberen. Dermed lægger hybrid afskrækkelse sig i kølvandet på nuklear og konventionel afskrækkelse[23], men er grundet sin foranderlige og netop hybride karakter vanskeligere at sætte på formel. Nuklear afskrækkelse kendes fra udviklingen af atomvåben og de nukleare strategier, som USA og Sovjetunionen udarbejdede under den kolde krig, mens den konventionelle afskrækkelse handler om niveauet under brugen af atomvåben, hvor staters konventionelle militære styrker måles mod hinanden for at afgøre afskrækkelsespotentialet. NATO's definition forklarer logikken:

> "Afskrækkelse er truslen om magtanvendelse for at modvirke en modstander fra at foretage en uvelkommen handling. Dette kan opnås gennem en trussel om gengældelse (afskrækkelse ved straf) eller ved at nægte modstanderen sine krigsmål (afskrækkelse ved nægtelse)."[24]

Hvor straf handler om at kunne reagere, *efter at* en uvelkommen hændelse har fundet sted, så handler nægtelse om at forhindre den uvelkomne hændelse i overhovedet at *kunne* finde sted.

Udfordringen ved at opbygge hybrid afskrækkelse er, at aktøren bag hybride angreb gennem overvejelser om risici, omkostninger og udbytte, altså ultimativt nytten af angrebet, sigter nøje mod at undgå at aktivere logikkerne i nuklear og konventionel afskrækkelse ved at holde de hybride angreb under tærsklen for konventionel krig. Hvor straf i nuklear afskrækkelse normalt vil betyde, at et angreb med atomvåben mod en anden atommagt vil resultere i et nukleart svar, så er straf langt vanskeligere at praktisere i hybrid afskrækkelse.

Hvordan skal Danmark eksempelvis straffe påvirkningskampagner under en folketingsvalgkamp, som ikke har nogen tydelig afsender, og hvor effekten er svær at vurdere? Eller hacking af politikere og partier med læk af følsomme informationer, når ingen stat tager ansvaret? Gråzonens eskalationsstiger for offensiv og defensiv anvendelse af hybride aktiviteter er stadig uprøvede, og selv de øgede vestlige konventionelle afskrækkelsesinitiativer samt sanktioner efter Krimkrisen har ikke fået Rusland til at standse hybride angreb.[25] Hybrid afskrækkelse som straf er et underudviklet felt,[26] og rapporten fokuserer derfor på afskrækkelse som nægtelse. Oparbejdelsen af hybrid modstandsdygtighed er også den form for nægtelse, som både EU og NATO tilskynder,[27] og som de fleste stater har udviklet som svar. Nægtelse gennem modstandsdygtighed handler om at minimere eller helt nægte en angribers mulighed for at udnytte svagheder og kløfter i de systemer og organisationer, som udgør den mulige flade for hybride angreb. Essensen af nægtelse er, at hybride angreb undgås ved at signalere til den angribende aktør, at den hybride modstandsdygtighed gør det uforholdsmæssigt svært eller umuligt at opnå de ønskede politiske målsætninger.

Den konkrete organisatoriske tænkning om afskrækkelse som nægtelse gennem modstandsdygtighed kan med fordel basere sig på Beredskabsstyrelsens veletablerede praksis, der 'arbejder for et robust samfund ved at udvikle og styrke beredskabet, så ulykker og katastrofer forebygges og afhjælpes'.[28] Beredskabsstyrelsens tilgang er en helhedsbaseret beredskabsplanlægning, der kan inspirere og anvendes af et bredt spektrum af offentlige og private organisationer med kritiske samfundsmæssige funktioner. Denne tænkning skal hjælpe organisationer til blandt andet at forbedre varsling og forebyggelse af særlige hændelser samt genoprettelse efter et hændelsesforløb.[29] Den form for organisatorisk selvindsigt kræver kortlægning af kritiske funktioner, identificering og overvågning af trusler samt risiko- og sårbarhedsanalyser,[30] som det blandt andet demonstreres for en række hændelsestyper i Beredskabsstyrelsens udgivelse *Nationalt Risikobillede*.[31] Denne tænkning og praksis i form af beredskabsplanlægning skal genfortolkes i lyset af gråzonekonflikten for at sikre et klart sikkerhedspolitisk fokus drevet af hybride trusler. Hybrid afskrækkelse skal gennem denne praksis og tænkning udøve en samlet strategisk effekt ved at tvinge den hybride modstander til at ændre adfærd.

Hvordan dette kan praktiseres inden for de tre overordnede områder, er fokusset for resten af kapitlet og starter med initiativer til at afskrække hybride angreb i informationsrummet.

3.1 Hybrid modstandsdygtighed: holdningsdannelse

Debatten om påvirkningskampagner og *fake news* har haft global opmærksomhed siden det amerikanske præsidentvalg i 2016, hvor blandt andre makedonske teenagere på jagt efter hurtige penge[32] og det russiske Internet Research Agency markerede sig med falske historier. Desinformation, hvor forkert eller manipuleret information spredes for at skade en modstander, udgør den mest åbenlyse trussel fra hybride angreb på national og international holdningsdannelse, og værktøjerne til at skabe og sprede disse udvikles og forfines konstant, eksempelvis via kunstig intelligens og brugen af *deepfake*-teknologi.[33]

Ruslands nuværende omstilling til at håndtere nye typer af konflikter handler især om at kunne operere i gråzonen via hybride angreb og med et særligt fokus på at udkæmpe konflikter i informationsrummet, der bruges til at understøtte alle typer gråzoneaktiviteter i det udvidede kamprum. Muligheden for at opnå synergieffekter i relation til brug af andre magtinstrumenter er meget stor, og det er derfor i informationsrummet, at påvirkningskampagner, psykologiske operationer som led i fortolkning og forvrængning af virkeligheden samt ansporing til kulturel og politisk polarisering finder sted og skal lede til modstanderens indre forfald.[34] Informationsrummet er også rammen for den gamle sovjetiske disciplin refleksiv kontrol, der handler om at bibringe enten en partner eller en modstander særligt tilrettelagt information, der skal påvirke disse til ganske frivilligt at træffe beslutninger, der flugter med den russiske politiske dagsorden.[35] Refleksiv kontrol har dermed til formål at forme konkrete beslutningsprocesser og deres udkomme.

Holdningsdannelse og psykologiske operationer udgør også officielt to ud af de tre typer af operationer i doktrinen "De Tre Krigsførelser" (den tredje er juridisk krigsførelse), som den kinesiske hær har haft til opgave at udføre siden 2003,[36] og dermed arbejder de to største udfordrere af den vestlige verdensorden specifikt med denne hybride trussel. Ifølge FE og PET udgøres den hybride trussel mod Danmark på dette område især af russiske påvirkningskampagner i og rettet mod Danmark generelt[37] og specifikt gennem valgpåvirkning.[38]

Påvirkningskampagner

Overordnet set finder påvirkningskampagner sted gennem to slags handlinger: offentlige mediekampagner målrettet civilbefolkningen (eksempelvis statspropaganda eller direkte desinformation) og skabelse samt udnyttelse af relationer af politisk eller forretningsmæssig karakter.[39] Gråzonens tvetydighed betyder også her, at grænserne for legitime og ikke mindst lovlige handlinger er slørede, og forsøg på at regulere området risikerer især at indskrænke ytringsfriheden. Regulering fører ligeledes spørgsmål med sig om, hvem der skal varetage opgaven med overvågning og efterforskning, samt hvem der skal kontrollere denne indsats. Den ressourcemæssigt mest effektive måde at føre påvirkningskampagner på ser for nuværende ud til at være via sociale medier, hvor især Facebook udmærker sig som en attraktiv arena grundet det store antal informationer, som mediet genererer om den enkelte bruger, og som tillader målrettede budskaber til enkeltindivider og grupper.[40] En problemstilling, der i en dansk kontekst understreges af, at 70 % af de 16-89-

årige har en Facebook-konto, og at over halvdelen logger på hver dag.[41] Formålet med påvirkningskampagner er grundlæggende at underminere modstanderens vilje og evne til at modarbejde afsenderens politiske mål. Det bliver forsøgt opnået gennem propaganda, falske nyheder, forstærkning af uenigheder ved at støtte flere sider i polariserende debatter samt skabelse af tvetydighed om fakta ved at så tvivl om autoriteter såsom myndigheder, eksperter og medier.[42] Det sker gennem anonyme brugere, falske identiteter eller bots, der kan styre tusindvis af brugerkonti og sprede budskaber på mange platforme med én enkelt handling.[43] En sådan hybrid trussel kræver modstandsdygtighed på flere samfundsmæssige niveauer.

Tekstboks 1:
Eksempel - Irland

Irske modtræk i debatten om retten til abort

Den stærkt polariserende irske debat om adgang til abort blev i 2018 forsøgt påvirket af udenlandske aktører, der blandt andet brugte automatiserede bot-netværk på sociale medier til spredning af deres budskaber.[44] Påvirkningskampagnen fandt sted under optakten til en folkeafstemning om at lovliggøre abort og blev opdaget blandt andet via et projekt drevet af frivillige, der indsamlede målrettede Facebook-reklamer gennem Transparent Referendum Initiative og advokerede for større gennemsigtighed i digitale politiske reklamer.[45] Civilsamfundets indsats fik konsekvenser for det private marked, da Facebook cirka 2½ uge inden afstemningen forbød udenlandsk finansierede reklamer i relation til afstemningen,[46] og Google dagen efter forbød alle folkeafstemningsreklamer på deres platforme, inklusive YouTube.[47] I forlængelse heraf har der på politisk niveau rejst sig en debat om lovgivning mod brugen af bot-netværk på sociale medier,[48] og den irske tilsynsmyndighed for offentlige anliggender presser blandt andet på for hjemmel til at overvåge indholdet og finansieringen af online politiske reklamer.[49] De irske modtræk understreger relevansen af initiativer på alle samfundsmæssige niveauer, men fremhæver samtidig den svære balancegang mellem modstandsdygtighed og censur, eftersom politiske reklamer fuldstændigt forsvandt fra Googles platforme og dermed ikke kunne informere debatten om afstemningen.

Et fundamentalt initiativ for at opbygge modstandsdygtighed mod påvirkningskampagner handler om at opdage og håndtere disse, når de forekommer. Det gælder særligt for det nationale embedsværk, der har fingeren på den samfundsmæssige puls fra kommune til centraladministration og samtidig ønsker at levere et faktabaseret svar på undergravende virksomhed. En sådan evne vil have en afskrækkende virkning på brugen af påvirkningskampagner, da effekten i så fald vil mindskes betragteligt. Det har Sveriges pendant til Beredskabsstyrelsen, Myndigheten för samhällsskydd och beredskap (MSB), arbejdet med siden 2016 i kraft af sit opdrag om at udvide egen kapacitet i forhold hertil samt at bidrage til andre myndigheders og relevante stakeholders kapacitet, hvilket blandt andet har resulteret i to publikationer målrettet embedsværket, der kortlægger konkrete trin for, hvordan påvirkningskampagner virker og effektivt kan imødegås.[50] [51]

En mere koncentreret indsats findes i den britiske regerings oprettelse af en ni medarbejdere stor enhed (fem fuldtids, fire deltids) dedikeret til overvågning af og hurtig respons på påvirkningskampagner samt koordinering af

svar fra regeringen på tværs.[52] Udfordringen fra desinformation og konkurrerende versioner af eksempelvis det russiske mordforsøg på den tidligere dobbeltagent Sergei Skripal i Salisbury og nedskydningen af passagerflyet MH17[53] gjorde, at beslutningen om at oprette enheden blev truffet i det nationale sikkerhedsråd, og motivationen blev direkte formuleret som afskrækkelse rettet mod desinformationskampagner.[54]

På et bredere samfundsmæssigt plan har den svenske regering besluttet at oprette en ny myndighed for psykologisk forsvar, hvis forgænger eksisterede fra 1950'erne og helt frem til, at Styrelsen för psykologiskt försvar blev lukket i 2009. Denne var under den kolde krig en central del af det svenske totalforsvar, men som følge af den nye strategiske kontekst skal enheden fokusere på at fungere i fredstid frem for at forberede til krig. Det psykologiske forsvar handler om at identificere, analysere og imødegå påvirkningskampagner, at øge befolkningens modstandsdygtighed og forsvarsvilje samt at sikre opretholdelse af information og kommunikation i krisesituationer.[55] Disse opgaver er i Sverige, ligesom i Danmark, en del af mange forskellige myndigheders ansvarsområde, men i Sverige anser kun en tredjedel af disse sig selv som en del af et psykologisk forsvar, og den manglende forventningsafstemning er en udfordring.[56] Derfor er en udredning om den kommende enheds omfang og virkemåde under udarbejdelse.[57]

Befolkningens psykologiske modstandsdygtighed handler især om kritiske mediefærdigheder, hvilket Storbritannien har taget så alvorligt, at en kommission har undersøgt børn og unges evner udi at navigere i mediebilledets mange historier og kilder. Kun 2 % af de undersøgte evnede at adskille en falsk og sand nyhedshistorie,[58] og sammenholdt med, at ældre amerikanere over 65 år i gennemsnit delte næsten syv gange så mange fake news-historier som 18-29-årige under 2016-præsidentvalget[59], så tegnes et billede af en udfordring, der er aktuel på tværs af generationer. Derfor har man i Sverige siden 2017 haft et forøget fokus på at sikre en bred digital dannelse i folkeskolen og gymnasiet, hvilket specifikt inkluderer styrkelse af elevernes kildekritiske evner, der skal indskrives i lærervejledninger,[60] mens italienske elever gennemgår lignende undervisning i samarbejde med blandt andet Facebook.[61]

Civilsamfundets rolle står således som en af de centrale søjler i afskrækkelse af påvirkningskampagner, og i Litauen har selvorganiserede såkaldte elvere formået at oprette et korps af mange hundrede frivillige, der aktivt bekæmper russiske trolde online ved at tage til genmæle og endda samarbejde med det litauiske forsvar.[62] Et sådan samarbejde er dog et skridt længere, end de fleste vestlige stater vil finde sig trygge ved, og det samme er den litauiske mulighed for at lukke eksempelvis servere ned i op til 48 timer uden dommerkendelse, hvis de benyttes som led i en desinformationskampagne eller en anden skadelig cyberhændelse.[63]

Denne top-down-metode via lovgivning står i kontrast til de foregående bottom-up-initiativer, men konkret regulering risikerer nemt at komme i konflikt med ytrings- og pressefriheden. Tyskland indførte i 2018 lovgivning[64] rettet mod det brede og svært definerbare begreb hadtale, som også dækker klart ulovlige udsagn, og pålagde derigennem sociale medier at fjerne den type opslag i løbet af 24 timer, eller i svært håndterbare tilfælde op til en uge, under trusler om store bøder. Tiltaget vil kunne adressere påvirkningskampagner, der netop sigter mod samfundsmæssigt betændte emner, der kan polarisere grupper, som eksempelvis den russiske desinformation, der fandt sted omkring den tyske Lisa-sag med en indvandringsvinkel.[65] Lovgivningen kritiseres dog for at være alt for bred samt give private firmaer censuropgaver og

-rettigheder, og den har direkte inspireret lignende lovgivning i langt mindre liberale stater som Rusland, Singapore og Filippinerne.[66]

Valgkamp

Ulovlig eller illegitim påvirkning af holdningsdannelse antager en særligt kritisk karakter omkring afholdelse af nationale valg. I denne proces har hybride angreb favorable vilkår for at udnytte medier og politikere til at fremme angriberens politiske dagsorden. Hvis valgafholdelsen anses for at være kompromitteret af udenlandsk påvirkning, vil det politiske lederskab også risikere at stå svagt, og påvirkningskampagner vil efterfølgende have endnu lettere spil.

Canada har på baggrund af den russiske indblanding i den amerikanske præsidentvalgkamp i 2016 strammet voldsomt op på sin valglov for at afskrække en lignende situation. Det er sket gennem tiltag, der især søger at undgå involvering fra udenlandske aktører og finansiering af partipolitiske aktiviteter, politiske reklamer og vælgerundersøgelser. Det skal blandt andet sikres gennem øget gennemsigtighed, der kræver, at tredjepartsinvolvering i de førnævnte aktiviteter klart rapporteres, et krav om at åbne en separat bankkonto for disse aktiviteter, og at politiske partier samt tredjeparter skal identificere sig selv i politiske reklamer, i en periode før valget finder sted. [67] Desuden forbydes det for interessegrupper at bruge udenlandsk finansiering til at føre partipolitiske kampagner, og onlineplatforme som eksempelvis Facebook skal registrere alle politiske reklamer samt gøre denne information offentligt tilgængelig i to år.[68] Derudover forbydes det udbydere at tillade internetreklamer fra udenlandske aktører, der indeholder valgkampsmateriale, men trods disse tiltag ønsker senatskomiteen yderligere initiativer.[69] Den canadiske debat om valgpåvirkning har også handlet om afskrækkelse som straf (som USA har udøvet[70]) ved at overveje muligheden for at bruge sanktioner, straffeloven og Magnitsky-loven[71], der gør det muligt at indefryse bestemte individers aktiver og forbyde dem indrejse i landet.[72]

Tekstboks 2:
Eksempel - Frankrig

Hybrid afskrækkelse i fransk valgkamp

I optakten til præsidentvalget i 2017 gjorde den franske forsvarsminister det klart, at et angreb mod et andet lands valgproces er en underminering af landets suverænitet, og at Frankrig var villig til at straffe udenlandsk valgpåvirkning med både cybermidler og konventionelle midler om nødvendigt.[73] I god tid før valget blev hybrid modstandsdygtighed gennem nægtelse prioriteret højt med uddannelse af og dialog med blandt andet de politiske partier, så de var forberedte på mulige angreb. Det resulterede blandt andet i, at præsidentkandidat Emmanuel Macrons kampagne skiftede kommunikationsplatform fra den russiske Telegram-app til Facebooks WhatsApp.[74] Trusselsbevidstheden betød også, at Macron-kampagnen fabrikerede falske mails og dokumenter for at forvirre i tilfælde af et hack-og-læk-angreb, som rigtignok fandt sted kort før valgdagen. Bevidstheden hos vælgerne blev også øget, ved at Macron-kampagnen offentliggjorde alle hackingforsøg, de blev udsat for. Desuden var Macrons stab meget aktiv på sociale medier for at gendrive desinformation fra lækket.[75] En professionel og bevidst håndtering af den hybride trussel fik således nægtet påvirkningsforsøgets effekter, og Macron vandt valget som forudsagt af meningsmålingerne.

Frankrig har ligeledes strammet sin lovgivning i forbindelse med valgafholdelse og har vedtaget, at kandidater på valg under valgkampe kan søge en hurtig afgørelse fra en dommer om at få fjernet potentielt manipulerende information.[76] Den svenske beredskabsstyrelse MSB forberedte det seneste svenske Riksdagsvalg ved at uddanne 8.400 medarbejdere i staten, regionerne og kommunerne til at opdage påvirkningskampagner[77] og finansierede også forskning, der undersøgte omfanget af påvirkningsforsøg i valgkampen.[78] Et supplement til menneskelig opmærksomhed er brugen af kunstig intelligens til at identificere disse forsøg, og det er netop, hvad en række projekter i øjeblikket forsøger,[79] men der er stadig et stykke vej endnu.[80]

3.2 Hybrid modstandsdygtighed: infrastruktur

Den løbende danske debat om kritisk infrastruktur har blandt andet kredset om, hvorvidt kinesiske Huawei måtte levere udstyr til opbygning af næste generation af trådløse netværk, 5G[81], hvilken udenlandsk køber der måtte erhverve sig elforsyningsvirksomheden Radius,[82] samt hvilken entreprenør der måtte udvide den grønlandske lufthavnskapacitet.[83] Kritisk infrastruktur dækker således over en bred vifte af systemer og aktiver, som er nødvendige for at opretholde regeringsførelsen og centrale funktioner i samfundet, men i Danmark findes der i modsætning til eksempelvis USA og Storbritannien[84] ingen vedtaget definition at forholde sig til.[85] *National Strategi for Cyber- og Informationssikkerhed – 2018-2021* udpeger dog seks samfundskritiske sektorer, nemlig energi-, sundheds-, transport-, tele-, finans- og søfartssektoren,[86] hvilket indkredser karakteren af, hvad der henholdsvis udgør infrastruktur og er kritisk.

Tekstboks 3:
Eksempel - USA

Definition af kritisk infrastruktur i USA

Kritisk infrastruktur kan være næsten alt eller intet, hvis ikke der findes en afgrænsende definition. Bevidsthed om den kritiske værdi af specifikke enheder og relation til større helheder faciliterer en fokuseret og modstandsdygtig indsats, der også kan informere om afhængigheder, der allerede findes eller kan opstå. Den amerikanske Patriot Act 2001 definerer kritisk infrastruktur som:

'Systemer og aktiver, hvad enten de er fysiske eller virtuelle, der er så afgørende for USA, at uarbejdsdygtighed eller ødelæggelse af sådanne systemer og aktiver vil have en svækkende indvirkning på sikkerhed, national økonomisk sikkerhed, folkesundhed eller en kombination af disse forhold'.[87]

Et centralt næste led efter definitionen handler om at analysere den kritiske infrastruktur, og til det formål har USA etableret *National Infrastructure Simulation and Analysis Center*[88], der fungerer som et nationalt kompetencecenter, der kan rådgive på baggrund af modelleringer og simuleringer. Disse øvelser hjælpes på vej af en specificering af 16 sektorer og deres ansvarsområder[89] samt en lovbestemt national plan[90] for beskyttelse af kritisk infrastruktur og nøgleressourcer i samarbejde med private aktører.[91] Samtænkning øger den hybride modstandsdygtighed.

Udpegningen sender et vigtigt budskab til stakeholdere, der varetager en diversitet af funktioner i disse sektorer, om, at de er centrale for opretholdelsen af stat og samfund. Det er ifølge Atlantpagtens artikel 3 også en konkret forpligtelse for Danmark at udvikle og sikre evnen til at modstå angreb, hvilket i det udvidede kamprum især handler om en bred forståelse af infrastruktur.[92] Den forståelse står også centralt i formuleringen af NATO's syv grundlæggende krav til modstandsdygtighed (*baseline requirements*)[93], som omhandler evnen til at sikre videreførelse af regeringen, offentlige serviceydelser, energiforsyning, evnen til at håndtere ukontrollerede menneskevandringer, fødevare- og vandressourcer, evnen til at håndtere mange omkomne samt civile kommunikations- og transportsystemer.

Den kritiske infrastruktur udsættes overordnet set for hybride trusler gennem to processer: For det første gennem ulovlige cyberangreb eller fysiske angreb og for det andet gennem lovlig erhvervelse af adgang eller ejerskab, der så kan udnyttes på både lovlig og ulovlig vis. Og gråzonen lægger også her sit slørende lys på aktiviteter mellem fred og krig, når handelspolitik bliver til sikkerhedspolitik af frygt for at skabe økonomiske, teknologiske og politiske afhængigheder, der kan udgøre hybride trusler. Det har også været centralt i debatten om linjeføring af Nord Stream 2-gasledningen gennem dansk territorialfarvand, hvor afhængighed af russisk gas i Europa kan give Rusland yderligere et hybridt håndtag at dreje på.[94]

Opbygningen af hybrid modstandsdygtighed i kritisk infrastruktur handler derfor om at kunne beskytte bestående systemer og aktiver, men også om at forstå og forme fremtiden under hensyn til hybride trusler. Herigennem opstår der imidlertid en risiko for at knægte markedsmekanismerne, når den frie bevægelighed af kapital, arbejdskraft og investeringer bliver forstået gennem gråzonens sikkerhedspolitiske logik, og det kan betyde, at både det offentlige og erhvervslivet må bevidstgøres om at indregne ekstra sikkerhedsudgifter i forretningsførelsen, når indgåelse af kontrakter kræver flere hensyn end udgifter og profit alene. Rapporten skelner mellem kritisk cyberinfrastruktur og kritisk fysisk infrastruktur, men det er en skillelinje, som den accelererende digitalisering af hverdagsenheder (*Internet of Things*)[95] og især brugen af internetforbundne industrielle kontrolsystemer i forsyningskæder[96] gør det tiltagende svært at opretholde.

Kritisk cyberinfrastruktur

Cyberinfrastruktur handler grundlæggende om udstyrs og programmers håndtering af information, der kan være af både følsom og ikkefølsom karakter, og som kan resultere i fysiske hændelser, hvad enten disse relaterer sig til eksempelvis forsyningssikkerhed, holdningsdannelse eller industrispionage. Informationssikkerhed er dermed et centralt element i hybrid modstandsdygtighed i kritisk cyberinfrastruktur.

Den seneste måling af danske statslige myndigheders overholdelse af ISO 27001-standarden for informationssikkerhed viser dog, at kun 15 % af 109 deltagende myndigheder har opnået fuld implementering, hvilket ifølge målingen kræver et modenhedsniveau på minimum 4 på en skala fra 1-5 på syv områder – hvoraf ét handler om beredskabsplaner, hvilket kun lidt over 20 % har udviklet.[97] Den viden skal kombineres med, at 86 ud af landets 98 kommuner har været udsat for cyberangreb mellem 2015 og maj 2018,[98] samt at 68 % af de danske virksomheder i 2018 havde oplevet cyberangreb det seneste år, og selvom hovedparten blev standset, var det under en tredje-

del, som blev anmeldt til myndighederne, og de fleste fløj dermed under radaren.[99] Den skrøbelige tilstand af både forretningskritiske og samfundskritiske offentlige IT-systemer fremhæves af, at eksempelvis hverken SKAT[100] eller Rigspolitiet[101] i en årrække har kunnet lave lovpligtige udbud, da de sammenfiltrede og gamle IT-systemer er umulige at dokumentere og dermed ugennemskuelige at udbyde driften af.

Tekstboks 4:
Eksempel - Norge

Tværgående samarbejde i Norge

En centralisering af ekspertise på et så specialiseret og samtidig vidtforgrenet område som cyberinfrastruktur har indbyggede stordriftsfordele, da især indkøb og implementering for en del organisationer vil være en forholdsvis sjælden foreteelse. Denne stordriftslogik kan udnyttes ved at styrke vidensopbygning og -deling hos staten, private aktører og akademiske institutioner og mellem disse. Norge tog i 2014 udfordringen fra kritisk cyberinfrastruktur op ved at etablere et tæt samarbejde mellem myndigheder, industri og forskning gennem oprettelsen af en central enhed, Center for Cyber and Information Security (CCIS) ved Norges teknisk-naturvitenskabelige universitet. Centerets talrige partnere[102] tæller de private virksomheder IBM, Telenor og PwC, det statslige energiselskab Statkraft, Politiets Sikkerhedstjeneste samt ØKOKRIM, der er politiets specialiserede enhed for økonomisk kriminalitet. Centeret udfører rådgivning samt forskning og uddannelse sammen med partnerinstitutioner[103] og udbyder som led i kompetenceudvikling eksempelvis en kandidatgrad i informationssikkerhed sammen med Politihøgskolen, Cyberforsvaret og Norsk Center for Informationssikkerhed.[104]

Alvoren bliver understreget af, at det danske Forsvarsministeriums myndighedsområde og Udenrigsministeriet over en toårig periode i 2015 til 2016 blev angrebet og hacket af den russiske gruppe APT28/Fancy Bear[105], der knyttes til Ruslands militære efterretningstjeneste GRU, at den danske energisektor i 2017 var udsat for forsøg på spionage fra en udenlandsk efterretningstjeneste,[106] og at den private virksomhed Mærsk gennem det russiske NotPetya-cyberangreb i 2017[107] tabte op mod 1,9 milliarder kroner.[108] De ovenstående udfordringer omhandler de hybride truslers ulovlige processer, men hybride modstandere arbejder også bevidst i gråzonen med at udnytte lovgivningen, og det kan eksempelvis være gennem at vinde offentlige udbud ved at underbyde på prisen for at opnå langsigtet strategisk indflydelse. USA har på baggrund af spionagefrygt forbudt brugen af kinesisk Huawei-udstyr hos statslige myndigheder, mens en række danske ministerier – inklusive Statsministeriet og Forsvarsministeriet – benytter Huawei, eftersom myndighederne ganske rigtigt forklarer, at 'de følger retningslinjerne for brug af statslige leverandører'.[109] Udfordringen for kritisk cyberinfrastruktur er dermed tostrenget, men overlappende, da både de klart ulovlige, men også de lovlige hybride trusler, skal håndteres.

Storbritannien oprettede i 2016 National Cyber Security Centre (NCSC)[110], der underlagt indenrigsefterretningstjenesten MI5 har ansvar for at overvåge, beskytte og rådgive om kritisk cyberinfrastruktur og blandt andet publicerer offentligt tilgængelige vejledninger samt kampagnemateriale for

bedre informationssikkerhed til internt brug for virksomheder og organisationer.[111] Og ligesom i Norge prioriteres samarbejdet med industri og forskning, som skal sikre vidensdeling gennem to programmer: Industry 100, der besætter 100 nøglestillinger i NCSC med eksperter fra den private sektor, der senere kan vende tilbage til det private med fornyet indsigt, og CyberInvest-programmet, der har fået blandt andre AIRBUS, BAE Systems og Hewlett Packard til at finansiere forskning i cybersikkerhed.[112]

Centeret har som led i en holistisk tilgang et tæt samarbejde med Centre for the Protection of National Infrastructure (CPNI),[113] der er den overordnede myndighed for beskyttelse af fysisk infrastruktur, hvilket gør, at man i Storbritannien kan sikre og løse problemstillinger på tværs af det hastigt svindende skel mellem cyberinfrastruktur og fysisk infrastruktur. Med denne holistiske tilgang og især på grund af ekspertisen i fysisk infrastruktur i CPNI undgår man eksempelvis det danske problem fra 2017, hvor Bygherreforeningen efterspurgte en offentlig vejledning om terrorsikring, men ikke kunne få en sådan rådgivning fra PET.[114]

Tekstboks 5:
Klassificering af cyberangreb

Klassificering af cyberangreb øger evnen til at gennemskue gråzonens tåge

Gråzonens hybride angreb baserer sig i høj grad på, at motivationen og intentionen bag ofte er tvetydige, og at den angrebne part derfor risikerer at reagere disproportionalt. En overreaktion på et cyberangreb kan være selve formålet med angrebet, da effekten således mangedobles. En mangelfuld reaktion kan på den anden side være langt farligere. Derfor anbefalede den franske evaluering af statens cyberforsvar i 2018[115], at Frankrig implementerer en klassificeringsmodel lig det amerikanske *Cyber Incident Scoring System* (CISS).[116] Etableringen og offentliggørelsen af disse kriterier hjælper til både at informere national beslutningstagning og at signalere afskrækkelse til en hybrid modstander om, at visse hændelsestyper tages meget alvorligt. Klassifikationssystemet hjælper til at forstå cyberangrebets karakter og tyngde ved blandt andet at vurdere funktionel indvirkning, observeret aktivitet, placering af observeret aktivitet, aktørkarakteristika, afbødningsmuligheder og tværsektoriel afhængighed. Gennemsigtighed og koordineringsevne mellem aktører via CISS er i sig selv et betragteligt bidrag til hybrid modstandsdygtighed. EU's NIS-samarbejdsgruppe udarbejder en lignende klassificering.[117]

Tættere integration mellem det offentlige og private kan styrkes yderligere gennem aktiv inddragelse af civilsamfundets ressourcer, og mens USA forgæves har kæmpet med dette siden 11. september-angrebene i 2001[118], så har Estland med succes siden 2011 haft en cyberenhed af frivillige IT-specialister som en del af det estiske hjemmeværn.[119] Udviklingen af Estonian Defence League's Cyber Unit (EDL CU) blev intensiveret på grund af de voldsomme synkroniserede hybride angreb mod det gennemdigitaliserede Estland i 2007 efter russisk utilfredshed med flytningen af en bronzestatue.[120] Enhedens lovgrundlag, organisering og formål er veludviklet[121] og muliggør derigennem udnyttelse af civile talenter og ressourcer, der ellers er utilgængelige, i bestræbelserne på at øge den hybride modstandsdygtighed i cyberinfrastrukturen.

Det kan eksempelvis hjælpe til at afbøde manglen på kvalificerede IT-specialister i den danske offentlige sektor, der ikke kan konkurrere med ansættelsesvilkårene i det private.[122] EDL CU har en løbende rolle i forbindelse med både uddannelse og øvelser og udvikling og test af kritiske IT-systemer og fungerer samtidig som en vigtig ressource i krisesituationer.

Modsat den ovenstående bottom-up-tilgang, hvor staten aktivt støtter frivillige samarbejder, så vil en top-down-tilgang handle om at indføre adgangsgivende regulering og overvågning af cyberinfrastruktur for at kontrollere samt forhindre uvelkomne cyberhændelser. Tilgangen risikerer at komme i konflikt med borgernes ret til privatliv og virksomhedernes evne til at beskytte sig selv og deres kunders følsomme oplysninger. Derfor har et australsk lovforslag om ophævelse af kryptering skabt stor modstand, da det netop pålægger virksomheder som Facebook, Apple og Google at sikre australske myndigheder adgang til krypterede beskeder og dermed altså bevidst skabe sikkerhedshuller, som andre aktører risikerer at udnytte.[123]

Det britiske NCSC har i kraft af den britiske *National Cyber Security Strategy 2016-2021* en hovedrolle i at facilitere, vurdere og i yderste tilfælde gribe ind, hvis centralt placerede organisationer ikke i tilstrækkelig grad lever op til cybersikkerhedskravene.[124] Den tilgang har Frankrig praktiseret siden 2013[125], hvor en 'operatør, hvis utilgængelighed i høj grad kan true det økonomiske eller militære potentiale, nationens sikkerhed eller modstandsdygtighed'[126] er underlagt den franske cybersikkerhedsmyndighed ANSSI og de sikkerhedsstandarder, som myndigheden opstiller, inklusive stærke detektionsmekanismer, som enten ANSSI eller en godkendt udbyder leverer, og desuden skal der føres tilsyn, der kan resultere i påbud.[127] Norges arbejde med at sikre sin militære udenrigsefterretningstjeneste øgede beføjelser med hensyn til cyberinfrastruktur og informationen, der flyder derigennem, har også mødt modstand i form af kritik fra indenrigsefterretningstjenesten Politiets Sikkerhedstjeneste[128], der blandt andet frygter for tilliden i samfundet.[129] Rusland er af frygt for selv at blive ramt at hybride angreb i informationsrummet (cyber- og påvirkningskampagner) også i færd med at regulere cyberinfrastrukturen. Med kinesisk inspiration[130] arbejder Rusland på at skabe et såkaldt suverænt internet, der kan fungere uafhængigt af det globale internet – en vision, hvor al russisk internettrafik allerede i 2020 skal håndteres internt i Rusland, og hvor det russiske tilsyns- og censuragentur, Roskomnadzor, får fuld kontrol over alle ind- og udkommende data. [131]

Mens de ovenstående initiativer handler om afskrækkelse gennem nægtelse, så har USA[132] og Storbritannien valgt også at signalere afskrækkelse gennem straf. Briterne har åbent omtalt deres offensive cyberoperationer mod Islamisk Stats økonomi, logistik og propaganda og har planer om etablering af en 2.000 personer stor offensiv cyberenhed rettet mod at afskrække Rusland. [133] I 2018 meddelte Danmark NATO, at man nu også kan bidrage med offensive cyberkapaciteter[134], hvilket naturligvis bærer en ny form for logik med sig, der kan ændre interessen og motivationen for at rette fokus på Danmark.[135]

Kritisk fysisk og sikkerhedsrelevant infrastruktur

Når stater lægger stor vægt på at beskytte kritisk fysisk infrastruktur, så er det, fordi en stats autoritet i høj grad baserer sig på en grundlæggende evne til at levere samt have kontrol over samfundets centrale forsyningslinjer, hvad enten disse er veje, tunneller, vandværker, elnet eller havne. Derfor er der grænser for, i hvor høj grad en stat kan overlade til udenlandske aktører at eje

kritisk fysisk infrastruktur, da kontrollen med denne kan glide regeringsapparatet af hænde, og man risikerer at blive udsat for politisk afpresning.

Det er således en bunden opgave, som staten skal løse, men gråzonens dynamik har også lagt et ikketraditionelt sikkerhedsrelevant kriterium ind i denne opgave, som de ovenstående cyberudfordringer er én dimension af, og intellektuel ejendomsret og komparative fordele en anden. Her handler det om at have fremtidens strategiske overhånd i afgørende sektorer, og på et mere abstrakt niveau udgør sektorerne fundamentet i statens magtinstrumenter (*instruments of power*, som omtalt i kapitel 2), som kan anvendes både defensivt og offensivt i gråzonen.

Kina opruster stort i denne dimension med den ambitiøse *Made in China 2025*-plan om at blive verdensførende inden for en række nøgleindustrier (såsom kommunikationsteknologi, kunstig intelligens og nye materialer).[136] Planen har vakt skepsis mod kinesiske opkøb af specialiserede virksomheder og den medfølgende forskning og viden, ligesom den kinesiske målsætning om øget udvikling af *dual-use*-teknologier,[137] der både kan bruges til militære og civile formål, også møder bekymring hos vestlige aktører og handelspartnere. I 2018 blokerede den amerikanske præsident Trump eksempelvis for historiens største teknologihandel, da han forbød Broadcom fra Singapore at købe amerikanske Qualcomm, baseret på vurderingen fra Committee on Foreign Investment in the United States, der mente, at handlen kunne resultere i, at Qualcomm mindskede sin udviklingsindsats i trådløs 5G-teknologi, hvilket ville have 'substantielle negative konsekvenser for den nationale sikkerhed',[138] da kinesiske Huawei i så fald vil dominere 5G-patenter og -standarder.

Beskyttelse af sikkerhedsrelevant infrastruktur handler således også om at undgå udenlandsk erhvervelse af statens komparative fordele enten gennem opkøb inden for statens grænser, eller ved at den udenlandske aktør importerer denne teknologi. USA er derfor i færd[139] med at øge begrænsningerne med hensyn til begge typer af tab af komparative fordele gennem intellektuel ejendomsret, når det gælder 'spirende og fundamentale teknologier'.[140] Da det statsejede kinesiske selskab China Communications Construction Company (CCCC), der var at finde blandt seks prækvalificerede firmaer til at udbygge Grønlands lufthavnskapacitet,[141] forsøgte at overtage det canadiske entreprenørfirma Aecon, fandt et lovhjemlet gennemsyn, at handlen ville udgøre en risiko for Canadas nationale sikkerhed.[142] Det mere end 100 år gamle canadiske firma er involveret i en bred vifte af brancher lige fra atomkraftværker, olie- og gaslinjer, kunstige vandveje og hoteller til el- og vandforsyninger samt landingsbaner og vejnet,[143] og canadisk lovgivning gør det blandt andet muligt at tage hensyn til potentielle indvirkninger på canadiske forsvarskapaciteter og -interesser samt overførsel af følsom teknologi.[144]

Tekstboks 6:
Eksempel – Tyskland

Tysk beskyttelse af sikkerhedsrelevant viden og teknologi

Kritisk ikketraditionel sikkerhedsrelevant infrastruktur kan eksempelvis være det tyske firma Leifeld Metal Spinning AG, der producerer maskiner til fremstilling af højstyrkestål til brug i bil-, rumfarts- og atomindustrien. Derfor benyttede den tyske regering i 2018 for første gang et lovkompleks introduceret i 2004 til at blokere salget af Leifeld til en kinesisk køber på grund af bekymringer for den nationale sikkerhed.[145] Tyskland opdaterede i 2017 lovgivning om udenlandske investeringer og køb[146] og strammede allerede kriterierne igen i 2018, så der er obligatorisk underretningspligt ved salg til købere uden for EU/EFTA i en række specifikke sektorer, og regeringen kan på eget initiativ iværksætte en sikkerhedsvurdering, hvis en udenlandsk aktør køber mere end 10 % af en tysk virksomhed inden for blandt andet forsvar, teknologi og medier.[147] Generelt er offentlig-privat samarbejde om beskyttelse af kritisk infrastruktur i Tyskland i stigende grad institutionaliseret i UP KRITIS-initiativet.[148] Den forsvindende afstand mellem de forskellige typer af kritisk infrastruktur og private og offentlige aktører kan også ses i et udkast til ny tysk regulering af cyberinfrastruktur, der samler op på de her nævnte udfordringer.[149]

Danmark har ikke en lignende lovgivning,[150] og den danske tilgang til kritisk fysisk infrastruktur har i overvejende grad også været fokuseret på terrorsikring, hvilket betyder, at PET's rådgivning om sikring af kritisk national infrastruktur tager eksplicit udgangspunkt i den seneste vurdering af terrortruslen mod Danmark.[151] Den ovenstående gennemgang af både fysisk og ikketraditionel sikkerhedsrelevant kritisk infrastruktur fortæller dog, at andre stater har indført lovhjemmel til at tage bredere hensyn og dermed har effektive værktøjer til at håndtere gråzonens nye hybride udfordringer. Et sådant bredere hybridt hensyn vil eksempelvis tage EU og NATO's krav om, at europæisk infrastruktur skal sikre smidig militær mobilitet over hele Europa,[152] i betragtning, når et statsejet kinesisk firma viser interesse i at bygge en tunnel mellem Danmark og Sverige – med de mulige risici, en sådan privilegeret adgang og viden kan udgøre i en krisesituation.[153]

3.3 Hybrid modstandsdygtighed: koordination

De hybride trusler, som rapporten i det ovenstående har identificeret, har deres største effekt, når flere eller alle magtinstrumenter aktiveres i en synkroniseret hybrid operation, så flest mulige af målets svagheder udnyttes på samme tid. Derfor er de enkelte sektorers, organisationers, enheders og individers modstandsdygtighed ikke fyldestgørende i sig selv. Uden øget koordination mellem disse vil en hybrid operation potentielt lykkes ved at samordne flere lavintensive operationer, der enten ikke opdages i tide eller ikke kan imødegås med en koordineret indsats. Den fundamentale hybride afskrækkelse gennem nægtelse består derfor i at kunne opdage og modstå en synkroniseret hybrid operation, hvilket forudsætter både horisontalt og vertikalt integrerede strukturer, der understøtter, at informationer kan bevæges, beriges og benyttes i alle hierarkiske retninger.

Koordinationens formål, uanset om den er national eller international, handler om tre grundlæggende processer, der finder sted før, under og efter

en hybrid operation. For det første etablering af et koordineret situationsbillede, der i overført betydning tager temperaturen i hele det hybride spektrum, så staten har et opdateret og velinformeret grundlag at handle ud fra – altså en kontinuerlig overvågning af nøgleområder, uanset trusselsniveauet. Koordination for at etablere og vedligeholde et hybridt situationsbillede har den særlige udfordring, at både den hybride operations vertikale eskalering i intensitet af ét enkelt anvendt magtinstrument og den horisontale eskalering, der synkroniserer to eller flere magtinstrumenter, skal kunne dækkes. Det er eksempelvis muligt at opdage en intensiveret påvirkningskampagne, men det skal samtidig være muligt at sammenholde denne information med udviklingen i den horisontale eskalering med cyberangreb på den finansielle sektor, bandeuroligheder og fysiske anslag mod elnettet, der kan have internationale konsekvenser.[154]

For det andet imødegåelse af en konkret hybrid operation, som er under udførelse. Her lægges der koordination af operationel planlægning og udførelse oven i det hybride situationsbillede. Processen handler både om en koordineret reaktion og imødegåelse og om udadvendt kommunikation til borgere, allierede, modstandere samt aktøren bag den hybride operation. Her skal det operationelle og politiske niveau koordineres, så regeringen under pres kan skabe en sammenhængende strategisk analyse og respons.

Tredje og sidste koordinationsproces handler om vidensdeling, læring og opbygning af ny hybrid modstandsdygtighed baseret på de høstede erfaringer, der så danner grundlag for nye initiativer. Et eksempel på national og international koordination i forhold til hybride trusler er oprettelsen af Cybersituationscenteret hos CFCS.[155] Centeret skaber et nationalt cybersituationsbillede via overvågning af datatrafik gennem det omdiskuterede[156] sensornetværk Nettjenesten og er samtidig en del af Den Europæiske Unions tiltag for europæisk cyberkoordination i net- og informationssikkerhedsdirektivet (NIS-loven).[157]

National koordination

Krisehåndtering finder i Danmark normalt sted på ét af tre overordnede niveauer, baseret på hændelsestype og omfang: skadesstedet, den lokale beredskabsstab og den nationale krisestyringsorganisation.[158] Når en særligt kompleks hændelse finder sted, som en større hybrid operation mod Danmark per definition vil være, så aktiveres National Operativ Stab (NOST) for at sikre koordinationen mellem myndigheder og opretholdelse af et retvisende situationsbillede.[159]

NOST og det nationale beredskabs evne til at koordinere under pres er hvert andet år siden 2003 blevet afprøvet gennem en større krisestyringsøvelse, KRISØV, der tryktester planer, procedurer, ansvarsfordeling og samarbejde. KRISØV 2013 simulerede i kølvandet på oprettelsen af CFCS et stort, koordineret cyberangreb mod centrale myndigheder og kritisk infrastruktur, og trods en generelt optimistisk evaluering[160] var der udfordringer med at etablere et samlet overblik, klar ansvarsfordeling og kommunikation til befolkningen.[161] Disse udfordringer var vokset under KRISØV 2017, der simulerede et terrorangreb i Nordjylland, hvor der ikke kunne skabes det nødvendige nationale overblik, og IT-systemet til at understøtte dette var mangelfuldt, og ligeså var kommunikationen til offentligheden, institutionel udholdenhed, kendskab til egne planer og procedurer samt afgrænsning af roller og ansvar.[162] En rigtig hybrid operation vil med stor sandsynlighed ramme scenarier

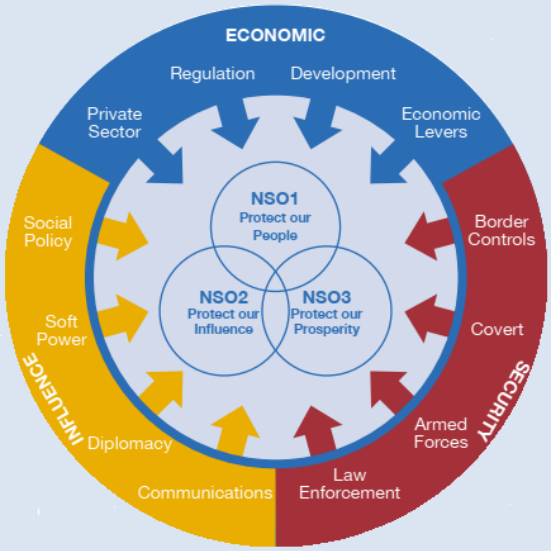
fra begge disse to øvelser, ligesom under KRISØV 2011 med fem spor, inklusive energi-, terror- og IT-hændelser.[163]

Disse udfordringer kan kædes sammen med sektoransvarsprincippet, hvor den 'myndighed, der har ansvaret for en opgave til daglig, bevarer ansvaret for opgaven under en større ulykke eller katastrofe',[164] og dermed risikeres silotænkning inden for sektoren frem for tværgående koordination. Til gengæld sikrer sektoransvarsprincippet, at den relevante ekspertise og faglighed og det relevante organisationskendskab er til stede, hvilket kan sættes over styr ved et alternativt krisestyringsprincip.

Tekstboks 7:
Eksempel – Storbritannien

Storbritanniens moderne afskrækkelse samler kræfterne i *Fusion*-doktrinen

Det voksende hybride trusselsbillede fik i 2018 Storbritannien til at formulere *Fusion*-doktrinen, der binder *whole-of-government*- og *whole-of-society*-tilgangene sammen i et strategisk sigte. Fusionsprincippet benytter de tre store kapabiliteter sikkerhed, økonomi og indflydelse til at beskytte det britiske folk, britisk indflydelse og britisk velstand (se diagram).[165] Formålet er 'moderne afskrækkelse', hvor angriberens omkostninger ved at foretage hybride angreb under tærkslen for en konventionel respons skal øges, og samtidig skal evnen til nægtelse styrkes ved at benytte alle tilrådighed stående midler.[166] Doktrinen skal sikre dette gennem styrkelse af offentlig-private partnerskaber samt fælles målbevidsthed blandt statens aktører, der bidrager til, at det nationale sikkerhedsråd kan træffe informerede strategiske beslutninger. Vedtagelsen af *Fusion*-doktrinen er afskrækkelse gennem nægtelse både som funktion og signalering til den hybride modstander. En risiko ved denne tilgang viser sig dog eksempelvis i ønsket om benytte det uafhængige BBC World Service som led i en global blød magt-strategi, der skal forme billedet af Storbritannien.[167]



Spørgsmålet er så, hvordan disse koordinationsudfordringer kan imødegås for at skabe national hybrid modstandsdygtighed. Et fundamentalt udgangspunkt bliver fremført i Taksøe-udredningen om dansk udenrigs- og sikkerhedspolitik, da den ligesom rapportens hybride trusler arbejder 'på tværs af

traditionelle skel mellem udenrigs-, sikkerheds-, forsvars-, handels-, og udviklingspolitik' og derfor opfordrer til større samtænkning 'på tværs mellem ministerier og myndigheder (*whole-of-government*) og i højere grad involvere relevante aktører fra hele samfundet (*whole-of-society*)'.[168] En så bred sikkerhedstænkning har været byggestenen for kontinuerlig udvikling af finsk national koordination fra totalforsvarskonceptet til den nuværende og hidtil bredeste forståelse i form af et såkaldt omfattende sikkerhedskoncept (*comprehensive security*).[169]

Dette omfattende finske sikkerhedskoncept bliver udfoldet i den seneste *Sikkerhedsstrategi for samfundet fra 2017*, der bliver udarbejdet, og hvis implementering kontrolleres, af det særlige sikkerhedsudvalg under Forsvarsministeriet, bestående af topembedsfolk fra departementer, politi og forsvar samt en håndfuld eksperter, der mødes en gang om måneden.[170] Sikkerhedsstrategien for samfundet præciserer gennem detaljerede forskrifter, hvordan syv vitale samfundsfunktioner skal beskyttes: lederskab, internationale aktiviteter og EU-aktiviteter, forsvarskapabiliteter, intern sikkerhed, økonomi og infrastruktur samt forsyningssikkerhed, funktionel befolknings- og servicekapacitet samt psykologisk modstandsdygtighed.[171]

Beredskabstænkningen bag en så bredspektret samfundsbeskyttelse kræver veltilrettelagte processer for informationsopbygning og -deling samt beslutningstagning i en diversitet af enheder og niveauer – kort sagt en klar koordinationsinfrastruktur. Derfor bygger det omfattende sikkerhedskoncept på en veldefineret organisationsstruktur og ansvarsfordeling,[172] der udlægges i hvert af sikkerhedsstrategiens omfangsrige emner lige fra sikring af offentlig orden, sikre grænser, immigration og økonomiske ressourcer til kommunikationsinfrastruktur, brændstofforsyning, arbejdskraft samt religiøse aktiviteter.[173]

Strategien er den fjerde siden 2003, men i den seneste udgave er beredskabsevnen på alle operationelle samfundsniveauer blevet opprioriteret i lyset af det nye, hybride trusselsbillede.[174] Den særlige samarbejdsmodel inddrager derfor aktivt offentlige autoriteter, civilsamfundsorganisationer, virksomheder, sågar kirker og naturligvis helt ned til borgerniveau, der alle indgår i en fødekæde af deling og analyse af sikkerhedsrelevant information, forberedelse af fælles planer samt træning og arbejdsrelaterede samarbejder på statsligt, regionalt og kommunalt niveau.[175]

Beredskabsplanlægning antager dermed ganske rigtigt en omfattende karakter, der bliver samlet på det politiske niveau under den finske statsministers kontor. Her findes regeringens situationscenter[176], der har til opgave at opretholde et opdateret situationsbillede og derfor opererer i døgndrift på at behandle alle indrapporterede sikkerhedshændelser for at underbygge beslutninger, opdage angreb og følge udviklingstendenser – en særlig dansk udfordring med henblik på rigsfællesskabets store territorium. En situationsbillede-*baseline* etablerer en normaltilstand at måle ud fra og gør det muligt at registrere afvigelser.

Denne kapacitet er en helt grundlæggende forudsætning for at kunne opdage og imødegå synkroniserede hybride angreb, der forsøger at udnytte svagheder i hele det offentlige og private spektrum. Den hybride modstandsdygtighed risikerer dog at få størst opmærksomhed på det statslige niveau, men Finland har i lighed med Danmark en udpræget grad af kommunalt selvstyre, der bidrager til at gøre hovedstadskommunen Helsinki til en hybrid sårbarhed. Mange forsyningslinjer og servicer leveres på dette niveau, og derfor har det NATO- og EU-støttede Centre of Excellence for Countering Hybrid

Threats med hovedsæde i Helsinki i samarbejde med bystyret udarbejdet en undersøgelse af Helsinki som en by, der kan være et mål for hybrid påvirkning,[177] og bidrager dermed til en vigtig niveaudelt hybrid bevidsthed.

National koordination som hybrid modstandsdygtighed gennem nægtelse handler også om kommunikation via og til offentligheden, der kan have interne og eksterne afskrækkelseseffekter. Her spiller tre forskellige niveauer af attribution – tilskrivning af ansvar for et hybridt angreb – en central rolle: teknisk, politisk og offentlig. Teknisk attribution identificerer gennem kriminalteknisk efterforskning metoder og aktører bag et hybridt angreb, altså eksempelvis en hackergruppe. Politisk attribution er at træffe beslutninger om, hvem afsenderen er, selv på trods af eventuelt utilstrækkelige beviser, hvilket eksempelvis vil være at holde en udenlandsk regering ansvarlig for hackergruppen. Offentlig attribution er det mest delikate niveau, for her går den angrebne stat ud i offentligheden og attribuerer det hybride angreb til den udenlandske regering. Alle tre niveauer er til en vis grad at finde i Estlands hjemlige efterretningstjeneste KAPO's årlige rapporter,[178] der er meget eksplicitte i forhold til hybride hændelser.

Den åbenhed bidrager til at vække den brede offentligheds hybride bevidsthed og signalerer samtidig til hybride angribere, at deres metoder bliver opdaget, og at der er omkostninger ved at udføre disse angreb. KAPO's rapport fra 2014 gjorde eksempelvis det undersøgende medie Re:Baltica i stand til at forbinde tre russisksprogede nyhedshjemmesider til den russisks stats propagandanetværk.[179] Offentlig attribution kan således fungere som smøremiddel for vanskelige processer i koordinationsinfrastrukturen.

International koordination

En væsentlig forudsætning for international koordination er en fælles forståelse af hybride trusler og hybrid modstandsdygtighed – altså et fælles formål. Men i kontrast til den nationale kontekst, hvor regeringen fra centralt hold kan styre en koordinationsproces (som eksempelvis via det finske situationscenter[180]), så kræver international koordination mellemstatslig og institutionel politisk enighed.

Danmark er som en småstat i høj grad afhængig af interstatslig koordination, og i særdeleshed når det kommer til deling af efterretninger til at skabe både et nationalt og internationalt hybridt situationsbillede. Dette gælder også i forhold til at respondere på potentielle eller konkrete hybride trusler, hvor dansk enegang vil være umuligt. NATO og EU er de to dominerende vestlige institutioner, der kan løfte den hybride udfordring, og trods det vanskeligt definerbare område har de en overordnet fællesmængde i deres hybride forståelse,[181] men de har også væsensforskellige opgaver og indre logikker. Overordnet tilgår NATO som et militært forsvarssamarbejde hybride trusler med udgangspunkt i hård sikkerhed (konventionelle våben og afskrækkelse) og tilnærmer sig derfra de problemstillinger, som rapportens fokus på hybrid modstandsdygtighed vedrører, mens EU tilnærmer sig fra den modsatte flanke, nemlig med udgangspunkt i blød sikkerhed (indsatser mod ikke konventionelle trusler som kriminelle netværk, menneske- og våbensmugling osv.).[182] Afskrækkelse gennem nægtelse er også i højsædet for de internationale koordinationsindsatser og bygger på samme logik om modstandsdygtighed som de nationalt funderede tiltag. Men hvor især småstater kan være tilbageholdende med at investere ressourcer i indsatser for at øge hybrid modstandsdygtighed, så bør stordriftsfordelene i forbindelse med eksempelvis NATO- og EU-tiltag have en motiverende effekt.

NATO-EU-samarbejdet om at imødegå hybride trusler blev knæsat på NATO's topmøde i Warszawa i 2016[183] og senere konkretiseret gennem 42 tiltag,[184] der blandt andet har betydet en tættere kontakt og vidensudveksling mellem EU's Hybrid Fusion Cell, NATO's Hybrid Analysis Branch og det finske Centre of Excellence for Countering Hybrid Threats (Hybrid CoE).[185] NATO vedtog i 2015 en overordnet strategi på det hybride område[186] og har fastslået, at et cyberangreb mod et NATO-medlem kan aktivere den fælles forsvarspagt i artikel 5. Et kerneeksempel på koordination mellem NATO og EU inden for en central delmængde af den hybride dagsorden er det såkaldte *Technical Arrangement* indgået i 2016, der udgør en ramme for deling af information og *best practices* mellem de to organisationers cyberkrisestyringsteams.[187] En ordning, som med fordel kan anvendes på andre hybride delmængder.

Tekstboks 8:
Eksempel – den hybride ambassadør

Den hybride ambassadør

Indsatsen for international koordination bliver i voksende omfang opprioriteret af nationale regeringer gennem nyoprettede hybride ambassadørstillinger. Sverige, Finland, Litauen og Spanien har eksempelvis alle en hybrid ambassadør, der skal skabe tættere integration mellem koordinationsinfrastrukturer både mellem stater og i internationale organisationer. Bredden i det hybride trusselbillede gør, at den hybride ambassadør har berøringsflader til hele det udenrigsministerielle område inklusive sikkerheds- og handelspolitik samt strategisk kommunikation og cyber.[188] Tematisk diplomati er allerede knæsat indenfor det hybride område, hvor eksempelvis Finland fik sin første cyberambassadør i 2014 og Australien i 2016, mens Danmarks første ambassadør for teknologi og digitalisering fra 2017 og frem har beskæftiget sig med centrale dele af den hybride dagsorden. Den hybride ambassadør samler og løfter nationale interesser, der normalt ikke bliver tilgodeset, da de ofte forstås gennem selvstændige kategorier uden nogen særlig sikkerhedspolitisk dimension. I forhold til hybride imødegåelsesinitiativer, der opstår gennem international koordination (NATO og EU), er den hybride ambassadør et nationalt kontaktpunkt, der ellers ville mangle.

NATO oparbejder også international koordination gennem NATO-akkrediterede centre som Strategic Communications Centre of Excellence i Letland, Energy Security Centre of Excellence i Litauen og Cooperative Cyber Defence Centre of Excellence i Estland, der alle bidrager til policy- og doktrinudvikling, uddannelse og forskning samt understøttelse af effektive NATO-operationer.[189] Danmark blev i 2018 medlem af det finske Hybrid CoE,[190] og dermed har danske forskere og praktikere en direkte indgang til centerets netværk og vidensproduktion. De NATO-akkrediterede centres fokus på ikkekonventionelle sikkerhedstrusler åbner mulighed for en både politisk og praktisk/teknisk hybrid dagsordensfastsættelse i NATO's officielle kommandostruktur og er dermed en komplementær måde at højne bevidstheden om disse trusler og varetage nationale interesser på.

EU's arbejde med hybride trusler har taget som udgangspunkt, at de forgrenede indsatser til imødegåelse skal samles, og EU vedtog derfor i 2016 'Fælles ramme for imødegåelse af hybride trusler – Den Europæiske Unions indsats', der indeholder 22 foranstaltninger.[191] Den fælles ramme samler særligt[192] udfordringer og indsatser fra blandt andet *Den europæiske dagsorden*

om sikkerhed[193] fra 2015, *EU's strategi for cybersikkerhed*[194] fra 2013 og *Europæisk energisikkerhedsstrategi* fra 2014.[195] Foranstaltningerne og strategierne er alle tværsektorielle og dermed tværministerielle i national kontekst, hvilket øger nødvendigheden af en *whole-of-government*- og *whole-of-society*-tilgang til oparbejdelse af hybrid modstandsdygtighed. Organisatorisk leverer en del af disse indsatser informationer til EU's Intelligence and Situation Centre's Hybrid Fusion Cell. Fusionscellen har siden 2016 produceret mere end 100 vurderinger og briefinger til brug for beslutningstagning både på EU-niveau og i nationalstaterne.[196]

Tænkningen bag en sådan hybrid fusionscelle spejler dermed det finske situationscenter, omend med et langt større dækningsområde og langt mindre autoritet, og lider desuden under mangel på både efterretninger, ekspertise og ressourcer.[197] Den internationale koordination står således centralt i den fælles ramme og konkretiseres gennem EU's *Hybrid Playbook*,[198] der bygger på eksisterende EU-krisestyringsmekanismer og integrerer den hybride fusionscelle. *Hybrid Playbook* hjælper til at klarlægge protokollen for hierarki, ansvar og anvendelsesmuligheder for EU's eksisterende koordinationsinfrastruktur og udgør også et centralt element i relation til EU's – og NATO's – hybride øvelser såsom EU's første hybride øvelse, PACE17, og NATO's CMX17.[199]

Inden for EU's virke finder der ligesom i NATO også oprustning sted i forhold til rapportens kategorier holdningsdannelse og infrastruktur. EU's East StratCom står centralt placeret i forhold til imødegåelse af undergravende påvirkning af holdningsdannelse i EU og partnerlande. Enheden blev oprettet i 2015 og driver blandt andet *EUvsDisinfo,* der udarbejder offentligt tilgængelige analyser af hovedsageligt russiske påvirkningskampagner og har identificeret tusindvis af individuelle desinformationssager.[200] I tillæg hertil har EU adresseret de store sociale mediers platforme i et forsøg på at dæmme op for desinformation, hvilket har fået blandt andre Google, Facebook og Twitter til at underskrive EU-kodekset om desinformation, der opstiller et adfærdskodeks for politiske reklamer og gennemsigtighed om afsendere, faktatjek og fjernelse af falske profiler.[201]

Imødegåelse af hybride trusler mod kritisk infrastruktur sker gennem EU's regelsæt for screening af udenlandske direkte investeringer.[202] Regelsættet sætter rammerne for at undersøge risikoen for hybrid udnyttelse af europæisk kritisk infrastruktur, når en sådan investering kan 'påvirke sikkerheden eller den offentlige orden'.[203] Den enkelte medlemsstat træffer den endelige beslutning, men både EU-Kommissionen og andre medlemsstater vil ifølge regelsættet kunne afgive kommentarer om konkrete investeringer. Regelsættet forstår investeringsområdet bredt, så både traditionel kritisk infrastruktur og teknologier og støtteteknologier er dækket af processerne, og alle medlemsstater opfordres til at etablere en sådan screeningsmekanisme og udarbejde årlige rapporter om udenlandske direkte investeringer.[204]

Interstatslige afhængigheder af forsyningslinjer og teknologier hæves gennem regelsættet således op fra det nationale eller bilaterale niveau til at være en legitim overvejelse for hele EU's medlemskreds og stiller således højere krav til den nationale hybride bevidsthed og modstandsdygtighed. Graden og modenheden af disse vil være af afgørende betydning for, hvilke udenlandske direkte investeringer en stat kan håndtere.

4 Konklusion og anbefalinger

Rapportens *horizon scan* har udlagt en bred palet af tiltag rettet mod at opbygge hybrid afskrækkelse gennem nægtelse. Tiltagene omhandler alle samfundsmæssige niveauer og er tværsektorielle af natur – grundet den hybride trussels natur – og understreger derigennem den fundamentale forudsætning for hybrid modstandsdygtighed: tiltag og koordination baseret på en *whole-of-government*- og *whole-of-society*-tilgang.

Overblikket understreger således rapportens fokus på at gøre strategisk beredskabsplanlægning til den overordnede logik at forstå og håndtere Danmarks hybride udfordringer gennem, og forståelsen af Danmark som en hybrid frontlinjestat placerer rapportens anbefalinger i gråzonens sikkerhedspolitiske kontekst. Under den kolde krig gjorde Danmarks geografiske placering som både stopklods og operationshub i Østersøområdet ved en eventuel konflikt med Sovjetunionen Danmark til en frontlinjestat. Det er Danmark igen blevet i gråzonekonflikten mellem Kina, Rusland og Amerika, men grundet gråzonens markant anderledes karakter, så er det ikke længere geografien, der er afgørende for, hvilke stater der står i forreste linje for hybride angreb.

Afkoblingen af geografi som begrænsende for angrebsmulighederne er i overvejende grad faciliteret af udnyttelse af digital teknologi, der eksempelvis gør det muligt at bryde ind i kritisk infrastruktur uden fysisk at krydse en eneste landegrænse. Den danske offentlige og private sektors imponerende grad af digitalisering og befolkningens udbredte brug af sociale medier er åbenbare hybride angrebspunkter, og selvforståelsen af Danmark som en hybrid frontlinjestat vil understøtte analyse og handling hos både offentlige og private aktører. Det stiller nye og øgede krav om at kunne identificere og imødegå en diversitet af trusler, som Danmark ikke tidligere har mødt eller prioriteret. Derfor har rapporten forsøgt at skabe en forståelse for den hybride konflikts udvidede kamprum, der bevidst indtager det nationale politiske og civile rum.

4.1 Overordnede anbefalinger: prioritering af strategisk beredskabsplanlægning

Truslen fra hybride angreb gør, at beredskabsplanlægning fremadrettet må bygge på en fundamentalt ny strategisk bevidsthed om gråzonens stormagtskonkurrence og et fokusskifte fra naturskabte hændelser til fjendtlige aktørers overlagte handlinger. En sådan prioritering af strategisk beredskabsplanlægning bør ske gennem tre overordnede initiativer:

- **Strategisk beredskabsplanlægning gennem en *whole-of-government*- og *whole-of-society*-tilgang**
  Den danske samfundsmodel har et robust udgangspunkt med en velsmurt offentlig sektor, der i vidt omfang inddrager civilsamfundets organisationer. Tiltaget vil derfor bygge på to centrale søjler, der udgøres af sektoransvarsprincippet, hvor myndigheders ansvarsområder forbliver de samme i krisesituationer, og den høje danske organisationsgrad. Det åbner for en opprioritering af tværsektoriel koordination på både horisontalt og vertikalt niveau, der vil øge den hybride modstandsdygtighed.

Den finske tilgang til national koordination gennem et omfattende sikkerhedskoncept kan med fordel fungere som et organisatorisk forbillede, og det er værd at bemærke, at den danske helhedsorienterede antiradikaliseringsindsats allerede benytter lignende principper.[205] Et overordnet dansk styringsdokument kan finde inspiration i den britiske tilgang med at formulere en hybrid *Fusion*-doktrin, som alle aktører kan orientere sig efter.

- **Strategisk beredskabsplanlægning på rigsfællesskabsniveau**
  Hybride angreb vil udnytte samfundsmæssige svagheder både internt i de tre dele af rigsfællesskabet og mellem disse. Den strategiske beredskabsplanlægning bør grundet disse interne afhængigheder derfor opprioriteres både i Grønland, på Færøerne og i Danmark. Bekymringer for udenlandske direkte investeringer i Grønland bør eksempelvis også ses i lyset af, at den grønlandske cyberinfrastruktur ikke er underlagt NIS-loven, og at CFCS ikke umiddelbart kan operere i Grønland.[206] En større harmonisering af indsatser for at øge den hybride modstandsdygtighed bør derfor forfølges, så rigsfællesskabet som helhed kan drage fordel af og få beskyttelse fra hybride tiltag, både lovgivningsmæssigt, efterretningsmæssigt og ressourcemæssigt.

- **Strategisk beredskabsplanlægning via et styrket nationalt sikkerhedsbillede**
  Tredje overordnede tiltag samler de to foregående og anbefaler en udvikling og intensivering af overvågning af kerneindikatorer til at afdække hybride trusler og angreb for at skabe et nationalt sikkerhedsbillede. Rutinemæssige hybride sårbarhedsanalyser bør gennemføres på baggrund af den aktørfokuserede strategiske beredskabsplanlægning, der eksempelvis udvider og fusionerer Beredskabsstyrelsens *Nationalt Risikobillede* med situations-, trussels- og risikovurderinger fra PET og FE. Størst mulig offentlig åbenhed om forsøg på eller gennemførte hybride operationer vil øge den generelle trusselsbevidsthed og kan finde inspiration i eksempelvis den estiske efterretningstjeneste KAPO's rapporter.

4.2 Anbefalinger til rapportens tre indsatsområder

De overordnede anbefalinger sætter rammen for de konkrete anbefalinger, som bliver præsenteret i det følgende. Disse anbefalinger vokser direkte ud af rapportens tre indsatsområder, og derfor er det muligt at vende tilbage til rapportens behandling af området for yderligere inspiration og henvisninger.

<u>Anbefalinger til holdningsdannelse, påvirkningskampagner og valgkamp</u>

- **Håndbog om psykologisk forsvar**
  Danske offentligt ansatte fra centraladministrationen til kommunerne bør have adgang til konkrete værktøjer til at opdage og håndtere påvirknings- og hvervningskampagner, hvilket også højner bevidstheden hos disse aktører om at være en del af det psykologiske forsvar i hybrid afskrækkelse. Det bør ske gennem udvikling af en håndbog specifikt målrettet danske udfordringer eller alternativt en oversættelse og tilpasning af den svenske håndbog *Countering information influence activities: A handbook for communicators*[207] udgivet af MSB.

- **Gennemsigtighed i politiske kampagner**
  Der er to dimensioner i denne anbefaling: partier og platforme. Politiske partiers åbenhed om partistøtte bør lovgivningsmæssigt strammes, hvilket der allerede foreligger en ekspertrapport om.[208] På samme vis bør udenlandske aktørers adgang til partipolitiske aktiviteter i Danmark (finansiering, reklamer og vælgerundersøgelser) indskrænkes med inspiration fra Canada. De digitale platforme som Facebook, Twitter og Google bør reguleres yderligere (under hensyn til ytringsfriheden) som forudsætning for, at de kan operere i Danmark, hvilket inkluderer, at brugen af bot-netværk indskrænkes til udvalgte formål, der ikke undergraver den demokratiske samtale.

Anbefalinger til kritisk cyberinfrastruktur samt fysisk og sikkerhedsrelevant infrastruktur

- **Hurtig udbedring af sårbare IT-systemer**
  De største og mest umiddelbare hybride trusler mod Danmark relaterer sig på alle fronter til cyberinfrastruktur, og derfor bør en helt fundamental indsats være at identificere og udbedre systemer i utilstrækkelig systemtilstand. For statens vedkommende gjaldt det 117 ud af statens 377 kritiske IT-systemer i 2018.[209] Rapportens andre anbefalinger blegner ved siden af den alvorlige hybride sårbarhed, som dette udgør. Derfor bør der gennemføres et tilbundsgående eftersyn af den offentlige sektors IT-sikkerhed med hurtigst mulig opfølgning. Et højt cybersikkerhedsniveau bør hente inspiration hos den franske cybersikkerhedsmyndighed, ANSSI, der har opstillet sikkerhedskrav, der skal overholdes også af private aktører.

- **Opprioritering af cybersamarbejde mellem staten, forskningsinstitutioner og industri**
  Udvikling og udveksling af viden på cybersikkerhedsområdet bør understøttes gennem et statsstøttet initiativ, der samler forskningen og industrien sammen med efterretningstjenesternes behov og indsigter. Tiltaget bør finde inspiration i Norges og Storbritanniens tilgange, hvor formaliserede programmer opnår stor privat tilslutning og finansiering og leverer uddannelsestilbud som eksempelvis en kandidatgrad i informationssikkerhed. Der ligger også et klart kommercielt sigte i denne anbefaling, der vil mindske presset grundet manglende IT-professionelle på det danske arbejdsmarked, og samtidig vil Danmark kunne fremme sin position i et voksende og profitabelt cybersikkerhedsmarked.

- **Investeringsscreening gennem bred definition af kritisk infrastruktur**
  En fleksibel og bred forståelse bør være udgangspunktet for Danmarks definition af kritisk infrastruktur. Den bør kunne dække potentielt kritiske og ikketraditionelt sikkerhedsrelevante områder såsom viden og teknologi. Tilgangen bør få konsekvenser for eksempelvis fremtidige handels- og forskningssamarbejder, der skal tilpasses i lyset af hybride trusler. Inspiration bør findes i det fortsatte tyske arbejde med at udvikle lovgivning, der kan screene og ultimativt forhindre udenlandske opkøb

eller investeringer inden for særligt kritiske sektorer som forsvar, teknologi og medier.

Anbefalinger til national og international koordination

- **Oprettelse af et hybridt situationscenter**
  De etablerede danske tiltag, såsom CFCS' eget Cybersituationscenter, valghandlingsplanen, den tværministerielle Task Force for Tværgående Beredskabsinitiativer, mediescreening i Udenrigsministeriet og kommende tværministeriel investeringsscreening samt øgede behov for et nationalt kontaktpunkt for hybride anliggender for udenlandske aktører (NATO, EU, efterretningstjenester) bør koordinere informationsstrømmene i et hybridt situationscenter. Her bør Finlands situationscenter under statsministerens kontor tjene som inspiration, og da den danske statsminister også er minister for rigsfællesskabet og pressen, vil placeringen af centeret i Statsministeriet være en oplagt mulighed for at gøre det hybride situationscenter til en konkret implementering af den anbefalede *whole-of-government*- og *whole-of-society*-tilgang.

- **Styring efter hybrid sikkerhed**
  Risikostyring handler i den offentlige sektor i dag om projektstyring og overholdelse af budgetter, men ikke om gråzonens sikkerhedspolitik og de afledte hybride risici. Dansk offentlig forvaltning bør bevidst og formelt tilpasse sig denne nye normaltilstand. For at understøtte både national og international hybrid koordination bør det nuværende sigte i mål- og resultatstyringen inden for udvalgte forvaltningsområder nyorienteres. Den almindelige drift er blevet sikkerhedspolitik, og derfor bør strategisk beredskabsplanlægning opprioriteres som en bøje at styre den offentlige sektor efter. Det bør eksempelvis resultere i en bredere involvering af aktører i KRISØV, der bør have klare hybride elementer indbygget hvert år og dermed teste den nye sikkerhedspolitiske styringslogik.

- **Oprettelse af en dansk hybrid ambassadørstilling**
  Den internationale dimension af hybrid koordination handler i høj grad om at løfte den hybride dagsorden gennem både formelle og uformelle koalitioner. Det gælder eksempelvis i EU, hvor EU's Hybrid Fusion Cell behøver flere ressourcer og bedre samarbejde med de enkelte medlemsstater. Danmark bør oprette en stilling som hybrid ambassadør, der vil kunne indgå i et styrket samarbejde med især andre nordiske hybride ambassadører om netværksdannelse i regionalt sikkerhedspolitisk regi (NORDEFCO, NB8 og Northern Group).[210] En hybrid ambassadør vil ligeledes understøtte imødegåelse af hybride trusler på rigsfællesskabsniveau. Denne anbefaling inkluderer også en øget dansk tilstedeværelse i NATO-akkrediterede Centres of Excellence med fokus på hybride trusler.

Noter

1 Justitsministeriet, "Styrket værn mod udenlandsk påvirkning af danske valg og demokratiet", 7. september 2018: http://www.justitsministeriet.dk/nyt-og-presse/pressemeddelelser/2018/styrket-vaern-mod-udenlandsk-paavirkning-af-danske-valg-og

2 Justitsministeriet, *Forslag til Lov om ændring af straffeloven (Ulovlig påvirkningsvirksomhed)*, 14. november 2018: https://www.retsinformation.dk/eli/ft/201812L00095

3 Center for Cybersikkerhed, "Situationscenterets opgaver", (tilgået 18. juni 2019): https://fe-ddis.dk/cfcs/sitcen/Pages/opgaver.aspx

4 Forsvarsministeriet, *Forslag til Lov om ændring af lov om Center for Cybersikkerhed,* Lovforslag nr. L 215, 2. maj 2019: https://www.ft.dk/ripdf/samling/20181/lovforslag/l215/20181_l215_som_vedtaget.pdf

5 Folketinget, "Åbent samråd om regeringens overvejelser om at iværksætte de såkaldte 'investeringsscreeninger'", 28. februar 2019: https://www.ft.dk/udvalg/udvalgene/URU/kalender/42308/samraad.htm

6 Kristian Klarskov, Anders Bæksgaard, "Ny lov skal forhindre farlige opkøb i Danmark og pression fra lande som Kina", *Politiken* (tilgået 18. juni 2019): https://politiken.dk/indland/art6850533/Ny-lov-skal-forhindre-farlige-opkøb-i-Danmark-og-pression-fra-lande-som-Kina

7 U.S. Department of Defense, *Summary of the 2018 National Defense Strategy of The United States of America*, (2018): https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf

8 David Rebouh, Benjamin Gregersen, "Forsker om kinesiske krigsskibe: Kina vil vise militære muskler i Danmark", *DR Nyheder,* (19. juli 2017): https://www.dr.dk/nyheder/indland/forsker-om-kinesiske-krigsskibe-kina-vil-vise-militaere-muskler-i-danmark

9 Lora Saalman, "Little Grey Men: China and the Ukraine Crisis", *Survival,* vol. 58 no. 6, December 2016–January 2017 (2017), 135–156, DOI 10.1080/00396338.2016.1257201: http://cs.brown.edu/courses/csci1800/sources/Little_Grey_Men.pdf

10 Holly Ellyatt, "Russia kicks off economic forum, but its wealth is on shaky ground", *CNBC,* (6. juni 2016): https://www.cnbc.com/2019/06/06/russia-kicks-off-spief-as-the-economy-is-on-shaky-ground.html; Ben Aris, "The Russian Economy is Stagnating", *The Moscow Times*, (27. maj 2019): https://www.themoscowtimes.com/2019/05/27/the-russian-economy-is-stagnating-a65760

11 Adam Taylor, "Mattis compared Xi's China to the Ming Dynasty. Xi might be happy to hear it.", *The Washington Post*, (20. juni 2018): https://www.washingtonpost.com/news/worldviews/wp/2018/06/20/mattis-compared-xis-china-to-the-ming-dynasty-xi-might-be-happy-to-hear-it/?utm_term=.b9d8319be299

12 John Lee, "China's Trojan Ports", *The American Interest*, (29. november 2018): https://www.the-american-interest.com/2018/11/29/chinas-trojan-ports/

13 André Ken Jakobsson, "Den hybride krig", *Weekendavisen*, (15. juni 2018): https://www.weekendavisen.dk/2018-24/samfund/den-hybride-krig

14 George Kennan, "269. Policy Planning Staff Memorandum", (4. maj 1948): https://history.state.gov/historicaldocuments/frus1945-50Intel/d269

15 Jens Stoltenberg, "Stoltenberg Provides Details of NATO's Cyber Policy", *Atlantic Council,* (16. maj 2018): https://www.atlanticcouncil.org/blogs/natosource/stoltenberg-provides-details-of-nato-s-cyber-policy

16 Carl von Clausewitz, *On War,* (1832)

17 Ibid.

18 Patrick J. Cullen, Erik Reichborn-Kjennerud, "MCDC Countering Hybrid Warfare Project: Understanding Hybrid Warfare". *Multinational Capability Development Campaign*, 2017: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/647776/dar_mcdc_hybrid_warfare.pdf

19 Ibid., 8

20 MCDC-projektet beskriver også det militære magtinstrument, men denne rapport vælger alene at fokusere på ikkemilitære aspekter af gråzonens hybride angreb, og derfor medtages dette instrument ikke her.

21 Ibid., 9

22 Ibid.

23 Henrik Ø. Breitenbauch, Niels Byrjalsen, Mark Winther, Mikkel Broen Jakobsen, *Orden og afskrækkelse – Vestens håndtering af Rusland efter annekteringen af Krim*, Center for Militære Studier, 2017, 17-18: https://cms.polsci.ku.dk/publikationer/orden-og-afskraekkelse/CMS_Rapport_2017_Orden_og_afskr_kkelse_opdateret_version_31-08-17.pdf

24 Michael Rühle, "Deterrence: what it can (and cannot) do", *NATO Review Magazine,* (2015): https://www.nato.int/docu/review/2015/also-in-2015/deterrence-russia-military/en/index.htm

25 Breitenbauch et al., *Orden og afskrækkelse – Vestens håndtering af Rusland efter annekteringen af Krim*, 17-18.

26 Heine Sørensen, Dorthe Bach Nyemann, *Going Beyond Resilience: A revitalized approach to countering hybrid threats.* The European Centre of Excellence for Countering Hybrid Threats, 2018: https://www.hybridcoe.fi/wp-content/uploads/2019/01/Strategic-analysis-Sorensen-Nyeman-11-2018.pdf

27 Ibid., 2

28 Beredskabsstyrelsen, "Opgaver og organisation", (12. november 2018): https://brs.dk/omstyrelsen/opgaver/Pages/Forside.aspx

29 Beredskabsstyrelsen, *Helhedsorienteret beredskabsplanlægning*, 5: https://brs.dk/viden/publikationer/documents/hob-vejledning.pdf

30 Ibid., 12-14

31 Beredskabsstyrelsen, *Nationalt Risikobillede,* (2017): https://brs.dk/viden/publikationer/Documents/Nationalt-Risikobillede-2017-LowRes.pdf

32 Saska Cvetkovska, Aubrey Belford, Craig Silverman, J. Lester Feder, "The Secret Players Behind Macedonia's Fake News Sites*", The Organized Crime and Corruption Reporting Project,* (18. juli 2018): https://www.occrp.org/en/spooksandspin/the-secret-players-behind-macedonias-fake-news-sites

33 Robert Chesney, Danielle Citron, "Deepfakes and the New Disinformation War – The Coming Age of Post-Truth Geopolitics*", Foreign Affairs*, (2019): https://www.foreignaffairs.com/articles/world/2018-12-11/deepfakes-and-new-disinformation-war

34 Janis Berzins*, Russia's New Generation Warfare in Ukraine: Implications for Latvian Defense Policy*, Center for Security and Strategic Research, National Defence Academy of Latvia, Policy Paper no 02 April (2014), 5: https://sldinfo.com/wp-content/uploads/2014/05/New-Generation-Warfare.pdf

35 Timothy L. Thomas, "Russia's Reflexive Control Theory and the Military*", Journal of Slavic Military Studies* 17: 237–256 (2004), DOI:10.1080/13518040490450529: https://www.rit.edu/~w-cmmc/literature/Thomas_2004.pdf

36 Elsa B. Kania, "The PLA's Latest Strategic Thinking on the Three Warfares", *China Brief,* Volume 16 Issue 12, August 22, The Jamestown Foundation (2016): https://jamestown.org/wp-content/uploads/2016/08/CB_16_13_2.pdf?x25462

37 Politiets Efterretningstjeneste, *Årlig redegørelse 2017*, (2018), 9: https://www.pet.dk/~/media/Aarsberetninger/rligredegrelsefor-PET2017WEBpdf.ashx

38 Andreas Krog, "Efterretningstjenesten forbereder sig på russisk påvirkning af folketingsvalget", *Altinget*, (28. juni 2018): https://www.altinget.dk/artikel/efterretningstjenesten-forbereder-sig-paa-russisk-paavirkning-af-folketingsvalget

39 Olga Oliker, "Russian Influence and Unconventional Warfare Operations in the 'Grey Zone': Lessons from Ukraine", Statement before the Senate Armed Services Committee Subcommittee on Emerging Threats and Capabilities, (29 marts 2017), 3: https://www.armed-services.senate.gov/imo/media/doc/Oliker_03-29-17.pdf

40 Alex Hern, "Cambridge Analytica: how did it turn clicks into votes?", *The Guardian,* (6. maj 2018):

https://www.theguardian.com/news/2018/may/06/cambridge-analytica-how-turn-clicks-into-votes-christopher-wylie

41 Agnes Tassy, Monika Bille Nielsen, Ditte Trier Jakobsen, *It-anvendelse i befolkningen 2018*. Danmarks Statistik, 2018, 21: https://www.dst.dk/Site/Dst/Udgivelser/GetPubFile.aspx?id=29448&sid=it-bef2018

42 Christopher Paul, Miriam Matthews, "The Russian 'Firehose of Falsehood' Propaganda Model – Why It Might Work and Options to Counter It". RAND Corporation, 2016: https://www.rand.org/pubs/perspectives/PE198.html

43 Soroush Vosoughi, Deb Roy, Sinan Aral, "The spread of true and false news online", *Science*, Vol. 359, Issue 6380, pp. 1146-1151, DOI: 10.1126/science.aap9559: https://science.sciencemag.org/content/359/6380/1146

44 Rachel Lavin, Roland Adorjani, "How Ireland Beat Dark Ads", *Foreign Policy*, (1. juni 2018): https://foreignpolicy.com/2018/06/01/abortion-referendum-how-ireland-resisted-bad-behaviour-online/

45 Transparent Referendum Initiative (tilgået 18. juni 2019): http://tref.ie/

46 Ciara O'Brien, "Facebook bans foreign ads for Eighth Amendment referendum", *The Irish Times* (8. maj 2018): https://www.irishtimes.com/business/technology/facebook-bans-foreign-ads-for-eighth-amendment-referendum-1.3487895

47 Jim Waterson, "Google bans Irish abortion referendum adverts", *The Guardian,* (9. maj 2018): https://www.theguardian.com/world/2018/may/09/google-bans-irish-abortion-referendum-adverts

48 Laura Larkin, "Twitter backs new Bill on online political ads", *Independent.ie* (27. november 2018): https://www.independent.ie/business/technology/twitter-backs-new-bill-on-online-political-ads-37569217.html

49 Fiachra Ó Cionnaith, "Watchdog wants powers to probe funding of fake news", *Irish Examiner,* (27. november 2018): https://www.irishexaminer.com/breakingnews/ireland/watchdog-wants-powers-to-probe-funding-of-fake-news-888066.html

50 James Pamment, Howard Nothhaft, Henrik Agardh-Twetman, Alicia Fjällhed, *Countering Information Influence Activities: The State of the Art*, Swedish Civil Contingencies Agency (2018): https://www.msb.se/RibData/Filer/pdf/28697.pdf

51 Swedish Civil Contingencies Agency, *Countering information influence activities: A handbook for communicators,* (2019): https://www.msb.se/RibData/Filer/pdf/28698.pdf

52 Sam Trendall, "What next for the government's anti-fake news unit?", *PublicTechnology,* (21. december 2018): https://publictechnology.net/articles/features/what-next-government's-anti-fake-news-unit

53 EUvsDisinfo, "Defensive disinformation as decoy flare: Skripal and Flight MH17", (24. marts 2018): https://euvsdisinfo.eu/defensive-disinformation-as-decoy-flare-skripal-and-flight-mh17/

54 William James, Elizabeth Piper, Catherine Evans, "Britain to set up unit to tackle 'fake news': May's spokesman", *Reuters,* (23. januar 2018): https://www.reuters.com/article/us-britain-politics-fakenews/britain-to-set-up-unit-to-tackle-fake-news-mays-spokesman-idUSKBN1FC2AL

55 Statskontoret, *Myndigheternas arbete med psykologiskt försvar,* (2017), 7: http://www.statskontoret.se/globalassets/publikationer/2017/201705.pdf

56 Ibid., 31

57 Justitiedepartementet, *Kommittédirektiv – En ny myndighet för psykologiskt försvar,* (2018): https://www.regeringen.se/4a566c/contentassets/b4b90c231b4144e683d5b4a594fe27b1/en-ny-myndighet-for-psykologiskt-forsvar-dir.-201880

58 Commission on Fake News and the Teaching of Critical Literacy Skills, *Fake news and critical literacy – The final report of the Commission on Fake News and the Teaching of Critical Literacy in Schools.* National Literacy Trust, 2018, 4: https://literacytrust.org.uk/documents/1722/Fake_news_and_critical_literacy_-_final_report.pdf

59 Andrew Guess, Jonathan Nagler, Joshua Tucker, "Less than you think: Prevalence and predictors of fake news dissemination on Facebook", *Science Advances,* Vol. 5, no. 1, DOI: 10.1126/sciadv.aau4586 (2019): http://advances.sciencemag.org/content/5/1/eaau4586

60 Regeringskansliet, "Stärkt digital kompetens i skolans styrdokument", (2017), 1: https://www.regeringen.se/contentassets/acd9a3987a8e4619bd6ed95c26ada236/informationsmaterial-starkt-digital-kompetens-i-skolans-styrdokument.pdf

61 Jason Horowitz, "In Italian Schools, Reading, Writing and Recognizing Fake News", *The New York Times* (18. oktober 2017): https://www.nytimes.com/2017/10/18/world/europe/italy-fake-news.html?_r=0

62 Michael Peel, "Fake news: How Lithuania's 'elves' take on Russian trolls", *Financial Times,* (4. februar 2019): https://www.ft.com/content/b3701b12-2544-11e9-b329-c7e6ceb5ffdf

63 Ibid.

64 Bundesministerium der Justiz und für Verbraucherschutz, *Act to Improve Enforcement of the Law in Social Networks (Network Enforcement Act),* 12. juli 2017: https://www.bmjv.de/SharedDocs/Gesetzgebungsverfahren/Dokumente/NetzDG_engl.pdf?__blob=publicationFile&v=2

65 Jakub Janda, "The Lisa Case – STRATCOM Lessons for European states", *Security Policy Working Paper*, No. 11/2016 (2016): https://www.baks.bund.de/sites/baks010/files/working_paper_2016_11.pdf

66 Human Rights Watch, "Germany: Flawed Social Media Law – NetzDG is Wrong Response to Online Abuse", (14. februar 2018): https://www.hrw.org/news/2018/02/14/germany-flawed-social-media-law

67 Parliament of Canada: *An Act to amend the Canada Elections Act and other Acts and to make certain consequential amendments,* Bill

C-76, (13. december 2018): http://www.parl.ca/DocumentViewer/en/42-1/bill/C-76/royal-assent

68 Joan Bryden, "Election reform bill passed in time for implementation in 2019 federal vote", *The Canadian Press,* (10. december 2018): https://www.ctvnews.ca/politics/election-reform-bill-passed-in-time-for-implementation-in-2019-federal-vote-1.4212822

69 Standing Senate Committee on Legal and Constitutional Affairs*, Observations to the Twenty-ninth Report of the Standing Senate Committee on Legal and Constitutional Affairs (Bill C-76).* Canadian Senate: https://sencanada.ca/content/sen/committee/421/LCJC/Reports/LCJCC-762018-12-06v7_e.pdf

70 BBC, "US punishes 19 Russians over vote meddling and cyber-attacks", *BBC News* (15. marts 2018): https://www.bbc.com/news/world-us-canada-43419809

71 Udenrigsudvalget, "Høring om Magnitsky-listen", Folketinget (6. juni 2018):https://www.ft.dk/udvalg/udvalgene/uru/kalender/35571/hoering.htm

72 Joan Bryden, "Bill C-76 just one tool to deter foreign election interference: Gould", *National Post,* (21. november 2018): https://nationalpost.com/pmn/news-pmn/canada-news-pmn/bill-just-one-tool-to-deter-foreign-interference-in-canadian-elections-gould

73 Heather A. Conley, Jean-Baptiste Jeangène Vilmer, "Successfully Countering Russian Electoral Interference", *CSIS Brief* (21. juni 2018): https://www.csis.org/analysis/successfully-countering-russian-electoral-interference

74 Ibid.

75 Ibid.

76 Zachary Young, "French Parliament passes law against 'fake news'", *Politico* (4. juli 2018): https://www.politico.eu/article/french-parliament-passes-law-against-fake-news/; Marine Guillaume, "Combating the manipulation of information – a French case*", Strategic Analysis 2/2019*, Hybrid Centre of Excellence (2019): https://www.hybridcoe.fi/wp-content/uploads/2019/05/Hybrid-CoE_SA_Combating-the-manipulation-of-information.pdf

77 Simon Kruse, "8.000 embedsmænd skal beskytte det svenske valg mod fremmede magter", *Berlingske,* (9. juni 2018): https://www.berlingske.dk/internationalt/8.000-embedsmaend-skal-beskytte-det-svenske-valg-mod-fremmede-magter

78 Chloe Colliver, Peter Pomerantsev, Anne Applebaum, Jonathan Birdwel*, Smearing Sweden: International Influence Campaigns in the 2018 Swedish Election*, Institute for Strategic Dialogue, (2018): http://www.lse.ac.uk/iga/assets/documents/arena/2018/Sweden-Report-October-2018.pdf

79 BBC, "Election interference to be sniffed out by early-alert system", *BBC News*, (17. juli 2018): https://www.bbc.com/news/technology-44820416; Radio Free Europe, "Group Says It Detected Campaign To Suppress Voter Turnout In Macedonia", (27. september 2018): https://www.rferl.org/a/pro-democracy-group-detects-online-campaign-suppress-voter-turnout-macedo-

nian-referendum-name-change-greece/29512150.html; Iryna Somer, "Lithuanians create artificial intelligence with ability to identify fake news in 2 minutes", *Kyiv Post*, (21. september 2018): https://www.kyivpost.com/technology/lithuanian-creates-artificial-intelligence-with-ability-to-identify-fake-news-within-2-minutes.html

80 Karen Hao, "Even the best AI for spotting fake news is still terrible", *MIT Technology Review,* (3. oktober 2018): https://www.technologyreview.com/s/612236/even-the-best-ai-for-spotting-fake-news-is-still-terrible/

81 Keld Vrå Andersen, "TDC dropper Huawei og lover 5G-net til hele Danmark i 2020", *TV 2 NYHEDER,* (18. marts 2019): http://nyheder.tv2.dk/samfund/2019-03-18-tdc-dropper-huawei-og-lover-5g-net-til-hele-danmark-i-2020

82 Finansudvalget, "Samrådsspørgsmål A", Folketinget, (9. oktober 2018):https://www.ft.dk/samling/20181/almdel/fiu/samspm/a/index.htm

83 Ritzau, "Overblik: Balladen om Grønlands nye lufthavne", (10. september 2018): https://www.avisen.dk/overblik-balladen-om-groenlands-nye-lufthavne_515199.aspx

84 Den britiske definition af kritisk infrastruktur lyder: "Those critical elements of infrastructure (namely assets, facilities, systems, networks or processes and the essential workers that operate and facilitate them), the loss or compromise of which could result in: a) Major detrimental impact on the availability, integrity or delivery of essential services – including those services whose integrity, if compromised, could result in significant loss of life or casualties – taking into account significant economic or social impacts; and/or b) Significant impact on national security, national defence, or the functioning of the state." Centre for the Protection of National Infrastructure, "Critical National Infrastructure", (tilgået 2. juli 2019): https://www.cpni.gov.uk/critical-national-infrastructure-0.

85 Thomas Foght, "Kinesisk firma vil bygge tunnel mellem Danmark og Sverige", *Radio24syv,* (28. november 2018): https://www.24syv.dk/udvalgte-nyhedshistorier/kinesisk-firma-vil-bygge-tunnel-mellem-danmark-og-sverige; Jakob Schjoldager, "Manglende definition af kritisk infrastruktur i Danmark møder massiv kritik: 'Ser man på FN's liste over lande med den bedste it-sikkerhed, så ligger vi ikke engang i top 10'", *Computerworld,* (26. juli 2018): https://www.computerworld.dk/art/244156/manglende-definition-af-kritisk-infrastruktur-i-danmark-moeder-massiv-kritik-ser-man-paa-fn-s-liste-over-lande-med-den-bedste-it-sikkerhed-saa-ligger-vi-ikke-engang-i-top-10

86 Finansministeriet, *National strategi for cyber- og informationssikkerhed – 2018-2021*, Regeringen, (2018): https://www.fmn.dk/nyheder/Documents/National-strategi-for-cyber-og-informationssikkerhed-2018.pdf p. 38-40

87 United States Congress, *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA Patriot Act) Act Of 2001, Public law 107–56—Oct. 26, 2001* (2001), 401: https://www.sec.gov/about/offices/ocie/aml/patriotact2001.pdf

88 Sandia National Laboratories, "National Infrastructure Simulation and Analysis Center", (tilgået 2. juli 2019): https://www.sandia.gov/nisac-ssl/

89 Department of Homeland Security, *Homeland Security Presidential Directive 7: Critical Infrastructure Identification, Prioritization, and Protection*, (17. december 2003): https://www.dhs.gov/homeland-security-presidential-directive-7

90 Department of Homeland Security, *NIPP 2013 Partnering for Critical Infrastructure Security and Resilience*, (2013): https://www.dhs.gov/sites/default/files/publications/national-infrastructure-protection-plan-2013-508.pdf

91 Department of Homeland Security, "National Infrastructure Protection Plan", (tilgået 2. juli 2019): https://www.dhs.gov/cisa/national-infrastructure-protection-plan

92 NATO, "Resilience and Article 3", (25. juni 2018): https://www.nato.int/cps/en/natohq/topics_132722.htm

93 Wolf-Diether Roepke, Hasit Thankey, "Resilience: the first line of defence", (27. februar 2019): https://www.nato.int/docu/review/2019/Also-in-2019/resilience-the-first-line-of-defence/EN/index.htm

94 Rem Korteweg, *Energy as a tool of foreign policy of authoritarian states, in particular Russia*, Policy Department, Directorate-General for External Policies, European Parliament's Committee on Foreign Affairs, doi:10.2861/951739, 2018: http://www.europarl.europa.eu/RegData/etudes/STUD/2018/603868/EXPO_STU(2018)603868_EN.pdf

95 Deloitte, "Cyber risk in an Internet of Things world", (tilgået 2. juli 2019): https://www2.deloitte.com/us/en/pages/technology-media-and-telecommunications/articles/cyber-risk-in-an-internet-of-things-world-emerging-trends.html

96 Jakob Schjoldager, "Kritisk infrastruktur er plaget af usikre systemer: 'De er afgjort ikke sikre og vil ikke være det de næste mange år'", *Computerworld,* (21. november 2018): https://www.computerworld.dk/art/245477/kritisk-infrastruktur-er-plaget-af-usikre-systemer-de-er-afgjort-ikke-sikre-og-vil-ikke-vaere-det-de-naeste-mange-aar

97 Digitaliseringsstyrelsen, *Hovedresultater: ISO 27001-modenhed i staten*, (2018), 3-6: https://digst.dk/media/18741/hovedresultater-af-iso-maalingen-for-2018.pdf

98 Thomas Riber-Sellebjerg, Mads Møller Okholm, "Afsløring: 86 kommuner hacket", *Ekstra Bladet,* (18. september 2018): https://ekstrabladet.dk/nyheder/samfund/article7221664.ece

99 Rambøll, *Analyse af data- og cybersikkerhed. Delrapport 2: Cybersikkerhed,* IDA og FSR – Danske Revisorer, (19. marts 2018) 9; 1: https://ida.dk/media/2389/delrapport_2_-_cybersikkerhed.pdf

100 John Hansen, Jakob Sorgenfri Kjær, "Politikere har kendt Skats ulovlige it-aftaler i 15 år", *Politiken*, (28. januar 2016): https://politiken.dk/oekonomi/art5609183/Politikere-har-kendt-Skats-ulovlige-it-aftaler-i-15-år; Rigs-

revisionen, *Rigsrevisionens beretning om statens udbud af it-drift og -vedligeholdelse afgivet til Folketinget med Statsrevisorernes bemærkninger,* (2016): http://www.rigsrevisionen.dk/media/2104443/sr0816.pdf

101 Joachim Kühlmann Selliken, "Rigspolitiet har ikke sendt CSC-opgaver i udbud i årevis: System-dokumentation mangler på 19. år", *Computerworld,* (1. december 2015): https://www.computerworld.dk/art/235067/rigspolitiet-har-ikke-sendt-csc-opgaver-i-udbud-i-aar-evis-system-dokumentation-mangler-paa-19-aar

102 Center for Cyber and Information Security, *Årsrapport 2017*, NTNU, (1. marts 2018), 1: https://www.ntnu.edu/documents/1269858715/1278988725/NTNU+CCIS+2017.pdf/aec1871d-9806-4a49-b9bc-c05c046d90d2

103 Centerets fem faggrupper dækker biometri, kritisk infrastrukturs sikkerhed og modstandsdygtighed, cyberforsvar, digital efterforskning, e-helbred og velfærdssikkerhed samt informationssikkerhedsmanagement og har til formål at "bidrage til at styrke samfundets, virksomhedernes og de enkelte borgeres evne til at beskytte deres informationsaktiver, opdage relevante trusler, behandle aktuelle hændelser og om nødvendigt undersøge kriminelle handlinger i cyberdomænet". Center for Cyber and Information Security, *Årsrapport 2017*,
NTNU, 1. marts 2018, 1: https://www.ntnu.edu/documents/1269858715/1278988725/NTNU+CCIS+2017.pdf/aec1871d-9806-4a49-b9bc-c05c046d90d2

104 NTNU, "Experienced based master´s degree, 3 years, Gjøvik, Information Security", (tilgået 2. juli 2019): https://www.ntnu.edu/studies/miseb

105 Center for Cybersikkerhed, "Udenlandsk aktør spionerer mod danske myndigheder", Forsvarets Efterretningstjeneste, 23. april 2017: https://fe-ddis.dk/cfcs/nyheder/arkiv/2017/Pages/Udenlandskaktoerspionerermod-danskemyndigheder.aspx

106 Center for Cybersikkerhed, *Undersøgelsesrapport – Målrettede forsøg på hacking af den danske energisektor*. Forsvarets Efterretningstjeneste, 2018: https://fe-ddis.dk/cfcs/publikationer/Documents/Undersøgelsesrapport%20%20energisektor.pdf

107 Sarah Marsh, "US joins UK in blaming Russia for NotPetya cyber-attack", *The Guardian,* (15. februar 2018): https://www.theguardian.com/technology/2018/feb/15/uk-blames-russia-notpetya-cyber-attack-ukraine

108 Lisbeth Quass og Kasper Duncan Gram, "Hackerangreb koster Mærsk milliardbeløb", *DR Nyheder,* (16. august 2017): https://www.dr.dk/nyheder/penge/hackerangreb-koster-maersk-milliardbeloeb

109 Jakob Sorgenfri Kjær, Sebastian Stryhn Kjeldtoft, "Spionagemistænkte Huawei leverer it-udstyr til dansk politi og forsvaret", *Politiken,* (19. februar 2019): https://politiken.dk/indland/art7042686/Spionagemist%C3%A6nkte-Huawei-leverer-it-udstyr-til-dansk-politi-og-forsvaret

110 National Cyber Security Center, "About the NCSC", (tilgået 2. juli 2019): https://www.ncsc.gov.uk/information/about-ncsc

111 Centre for Protection of National Infrastructure, "Security Awareness Campaigns", (tilgået 2. juli 2019): https://www.cpni.gov.uk/security-awareness-campaigns

112 National Cyber Security Center, "CyberInvest", (tilgået 2. juli 2019): https://www.ncsc.gov.uk/articles/cyber-invest

113 Centre for Protection of National Infrastructure, "About CPNI", (tilgået 2. juli 2019): https://www.cpni.gov.uk/about-cpni

114 Michael Thykier, "PET vil ikke hjælpe – bygherrer må gætte sig til god terrorsikring", *Jyllands-Posten,* (5. november 2017): https://jyllands-posten.dk/indland/ECE10004235/pet-vil-ikke-hjaelpe-bygherrer-maa-gaette-sig-til-god-terrorsikring/

115 Alex Grigsby, "Three Takeaways from the French Cyber Defense Review", *Council on Foreign Relations,* (26. februar 2018): https://www.cfr.org/blog/three-takeaways-french-cyber-defense-review

116 Department of Homeland Security, "NCCIC Cyber Incident Scoring System", (tilgået 2. juli 2019): https://www.us-cert.gov/NCCIC-Cyber-Incident-Scoring-System

117 NIS Cooperation Group, *Cybersecurity Incident Taxonomy*, Europa-Kommissionen, 2018: http://ec.europa.eu/information_society/newsroom/image/document/2018-30/cybersecurity_incident_taxonomy_00CD828C-F851-AFC4-0B1B416696B5F710_53646.pdf

118 Monica M. Ruiz, "Is Estonia's Approach to Cyber Defense Feasible in the United States?", *War on the Rocks,* (9 januar 2018): https://warontherocks.com/2018/01/estonias-approach-cyber-defense-feasible-united-states/

119 Kaitseliit, "Estonian Defence League's Cyber Unit", (tilgået 2. juli 2019): http://www.kaitseliit.ee/en/cyber-unit

120 Damien McGuinness, "How a cyber attack transformed Estonia", *BBC News*, (27. april 2017): https://www.bbc.com/news/39655415

121 Kadri Kaska, Anna-Maria Osula, Jan Stinissen, *The Cyber Defence Unit of the Estonian Defence League,* NATO Cooperative Cyber Defence Centre of Excellence (2013): https://ccdcoe.org/uploads/2018/10/CDU_Analysis.pdf

122 Kristian Villesen, Sebastian Stryhn Kjeldtoft, "Offentlige it-projekter går ofte galt. Måske fordi vi privatiserede området i 90'erne og ikke længere har ekspertisen i staten", *Information,* (15. juli 2017): https://www.information.dk/moti/2017/07/offentlige-it-projekter-gaar-ofte-galt-maaske-fordi-privatiserede-omraadet-90erne-laengere-ekspertisen-staten

123 Jon Porter, "Australia's encryption-busting law is 'deeply flawed,' says tech industry", *The Verge,* (7. december 2018): https://www.theverge.com/2018/12/7/18130806/australia-access-and-assistance-encryption-bill-2018-facebook-google-apple-respond

124 United Kingdom Government, *National Cyber Security Strategy 2016-2021,* (2016), 41: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf

125 French Government, *Livre Blanc Défense Et Sécurité Nationale* – 2013, (2013): http://www.livreblancdefenseetsecurite.gouv.fr/pdf/le_livre_blanc_de_la_defense_2013.pdf

126 ANSSI, *Cybersecurity in France,* (tilgået 2. juli 2019): https://www.ssi.gouv.fr/en/cybersecurity-in-france/

127 Ibid.

128 Politiets Sikkerhetstjeneste, "Høringssvar fra PST – Forslag til ny lov om Etterretningstjenesten", Forsvarsdepartementet, (12. februar 2019): https://www.regjeringen.no/contentassets/287d2d52ddb847849cddb49796456129/horingssvar-med-merknader---pst.pdf?uid=PST

129 Simon Kruse, Mikkel Fyhn Christensen, "Norges svar på PET siger stop for mere cyberovervågning – i Danmark henligger høringssvar i mørke", *Berlingske,* (14. februar 2019): https://www.berlingske.dk/internationalt/norges-svar-paa-pet-siger-stop-for-mere-cyberovervaagning-i-danmark

130 Elizabeth C. Economy, "The great firewall of China: Xi Jinping's internet shutdown", *The Guardian*, (29. juni 2018): https://www.theguardian.com/news/2018/jun/29/the-great-firewall-of-china-xi-jinpings-internet-shutdown

131 André Ken Jakobsson, "Putins suveræne internet er grænsekontrol i cyberdomænet", *Berlingske,* (10. marts 2019): https://www.berlingske.dk/kommentarer/putins-suveraene-internet-er-graensekontrol-i-cyberdomaenet

132 Dell Cameron, "White House: We're Going to Cyber Harder", *Gizmodo, (*20. september 2018): https://gizmodo.com/white-house-were-going-to-cyber-harder-1829209779

133 Deborah Haynes, "Britain to create 2,000-strong cyber force to tackle Russia threat", *Sky News,* (21. september 2018): https://news.sky.com/story/britain-to-create-2000-strong-cyber-force-to-tackle-russia-threat-11503653

134 Forsvarsministeriet, "Offensive cybereffekter", (2019): https://www.fmn.dk/temaer/nato/Documents/2018/Faktaark-cyber-effekter.pdf

135 Joe Devanny, "Why it's unwise for the UK to boast about its cyber attack capability", *The Conversation*, (13. september 2018): https://theconversation.com/why-its-unwise-for-the-uk-to-boast-about-its-cyber-attack-capability-102870

136 Lorand Laskai, "Why Does Everyone Hate Made in China 2025?", *Council on Foreign Relations,* (2018): https://www.cfr.org/blog/why-does-everyone-hate-made-china-2025

137 Meia Nouwens, "China's pursuit of advanced dual-use technologies", *IISS,* (18. december 2018): https://www.iiss.org/blogs/analysis/2018/12/emerging-technology-dominance

138 Department of the treasury, *Re: CFIUS Case 18-036: Broadcom Limited (Singapore)/Quallcomm Incorporated*, (5. marts 2018): http://online.wsj.com/public/resources/documents/cfiusletter.pdf

139 Federal Register, "Review of Controls for Certain Emerging Technologies", *Bureau of Industry and Security*, Commerce (19. november 2018):https://www.federalregister.gov/documents/2018/11/19/2018-25221/review-of-controls-for-certain-emerging-technologies

140 Steve Dickinson, "New Restrictions on High Tech Technology Transfers to China", *China Law Blog,* (27. november 2018): https://www.chinalawblog.com/2018/11/new-restrictions-on-high-tech-technology-transfers-to-china.html

141 Jørgen Schultz-Nielsen, "Kalaallit Airports: 6 entreprenører får lov at byde på lufthavnsbyggerierne", *Sermisiaq AG* (26. marts 2018): https://sermitsiaq.ag/node/204638

142 Taenaz Shakir, Rama Venkat Raman, Leah Schnurr, Brenda Goh, Michael Martina, "Canada blocks Chinese takeover of Aecon on national security grounds", *Reuters,* (24. maj 2018): https://www.reuters.com/article/us-aecon-group-m-a-canada/canada-blocks-chinese-takeover-of-aecon-on-security-grounds-idUSKCN1IO3F2

143 Aecon, "Aecon Industrial", (tilgået 2. juli 2019): https://www.aecon.com/What_We_Do/Aecon_Industrial

144 Government of Canada, "Guidelines on the National Security Review of Investments", (2016): https://www.ic.gc.ca/eic/site/ica-lic.nsf/eng/lk81190.html

145 Arne Delfs, "Germany Toughens Stance and Blocks China Deal", *Bloomberg,* (1. august 2018): https://www.bloomberg.com/news/articles/2018-08-01/germany-said-to-block-company-purchase-by-chinese-for-first-time

146 Anahita Thoms, "Germany Tightens Rules on Foreign Investments. What are the implications?", *Baker McKenzie,* (2. oktober 2017): https://www.bakermckenzie.com/en/insight/publications/2017/10/germany-tightens-rules

147 Bundesregierung, *Zwölfte Verordnung zur Änderung der Außenwirtschaftsverordnung,* (2018): https://www.bmwi.de/Redaktion/DE/Downloads/XYZ/zwoelfte-verordnung-zur-aenderung-der-aussenwirtschaftsverordnung.pdf?__blob=publicationFile&v=4

148 UP KRITIS, *Öffentlich-Private Partnershaft zum Schutz Kritischer Infrastrukturen*, (Frankfurt: Druck- und Verlagshaus Zarbock GmbH & Co. KG 2014): https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Kritis/Fortschreibungsdokument.pdf;jsessionid=63AFC8733588446F3B3053D5BEEBFE3E.1_cid341?__blob=publicationFile&v=2

149 Taylor Wessing, "German IT security law 2.0 – draft bill of March 2019", *Lexology, (*11. april 2019): https://www.lexology.com/library/detail.aspx?g=8a3936e9-1c10-446d-8179-5e15521a5d3a

150 Thomas Klose Jensen, "Claus Hjort: Vi kan ikke forbyde Huawei*", DR Nyheder*, (22. januar 2019): https://www.dr.dk/nyheder/politik/claus-hjort-vi-kan-ikke-forbyde-huawei

151 Politiets Efterretningstjeneste, "Kritisk national infrastruktur", (tilgået 2. juli 2019): https://www.pet.dk/Forebyggende%20Afdeling/Kritisk%20national%20infrastruktur.aspx

152 Chase Winter, "EU outlines plans for 'military Schengen zone'", *Deutsche Welle,* (28. marts 2018): https://www.dw.com/en/eu-outlines-plans-for-military-schengen-zone/a-43171043

153 Thomas Foght, "Kinesisk firma vil bygge tunnel mellem Danmark og Sverige", *Radio24syv,* (28. november 2018): https://www.24syv.dk/udvalgte-nyhedshistorier/kinesisk-firma-vil-bygge-tunnel-mellem-danmark-og-sverige

154 European Regulators' Group for Electricity and Gas, *The lessons to be learned from the large disturbance in the European power system on the 4th of November 2006,* (2007): https://www.ceer.eu/documents/104400/-/-/b4f16360-b355-5d50-bf33-01f8a76fc95a

155 Center for Cybersikkerhed, "Situationscenterets opgaver", Forsvarets Efterretningstjeneste, (tilgået 2. juli 2019): https://fe-ddis.dk/cfcs/sitcen/Pages/opgaver.aspx

156 Jakob Schjoldager, "It-eksperter: Drop Center for Cybersikkerhed til at overvåge Danmark mod hackere: Opret en ny myndighed", *Computerworld,* (26. februar 2019): https://www.computerworld.dk/art/246576/it-eksperter-drop-center-for-cybersikkerhed-til-at-overvaage-danmark-mod-hackere-opret-en-ny-myndighed

157 European Union, "Directive (EU) 2016/1148 of The European Parliament and of the Council of 6 July 2016, L 194/1*", Official Journal of the European Union,* (19. juli 2016): https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC

158 Beredskabsstyrelsen, *Krisestyring i Danmark,* (2015), 3: https://brs.dk/viden/publikationer/Documents/Krisestyring%20i%20Danmark.pdf

159 De faste medlemmer af NOST, som træder sammen, er Rigspolitiet (formand), Beredskabsstyrelsen, Forsvarskommandoen, Politiets Efterretningstjeneste, Forsvarets Efterretningstjeneste, Sundhedsstyrelsen og, afhængigt af omstændighederne, Udenrigsministeriet samt andre relevante aktører; Ritzau, "Statens kriseberedskab aktiveret efter togulykke", *DR Nyheder,* (2. januar 2019): https://www.dr.dk/nyheder/indland/statens-kriseberedskab-aktiveret-efter-togulykke

160 Beredskabsstyrelsen, *Evaluering af KRISØV 2013,* (2014): https://brs.dk/viden/publikationer/Documents/KRISØV%202013%20%20Evalueringsrapport.pdf

161 Mads Elkær, "Kæmpe cyber-krigsøvelse afslører seriøse problemer", *Computerworld*, (8. november 2013): https://www.computerworld.dk/art/228936/kaempe-cyber-krigsoevelse-afsloerer-serioese-problemer#eodZvMz03G87JFHZ.99

162 Beredskabsstyrelsen, *Evaluering af KRISØV 2017,* (2018), 3-5: https://brs.dk/viden/publikationer/Documents/Evaluering-af-KRISOEV-2017.pdf

163 Beredskabsstyrelsen, *Evaluering af KRISØV 2011,* (2012): https://brs.dk/beredskab/idk/Documents/EvalueringsrapportKRISOV2011.pdf

164 Beredskabsstryelsen, *Krisestyring i Danmark,* (2015), 5: https://brs.dk/viden/publikationer/Documents/Krisestyring%20i%20Danmark.pdf

165 United Kingdom Government, *National Security Capability Review,* (2018), 10: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/705347/6.4391_CO_National-Security-Review_web.pdf

166 Ibid., 11

167 Ibid., 32

168 Peter Taksøe-Jensen, *Dansk diplomati og forsvar i en brydningstid: Vejen frem for Danmarks interesser og værdier mod 2030,* Udenrigsministeriet (2016), X; bilag 2, 6: http://um.dk/~/media/UM/Danish-site/Documents/Udenrigspolitik/Aktuelle%20emner/148396_udredning_indhold_FINAL_PRINTVENLIG.pdf?la=da

169 The Security Committee, "The Finnish Concept for Comprehensive Security", (2017): https://www.defmin.fi/files/3827/Valtonen_2017_06_14_FI_Concept_for_Comprehensive_Security_Valtonen.pdf

170 The Security Committee, "Security Committee", (tilgået 2. juli 2019): https://turvallisuuskomitea.fi/en/security-committee/

171 The Security Committee, *The Security Strategy for Society,* 2017, 14: https://turvallisuuskomitea.fi/wp-content/uploads/2018/04/YTS_2017_english.pdf

172 Finnish Government, "Government resolution clarifies organisation and responsibilities with respect to comprehensive security", (5. december 2012): https://valtioneuvosto.fi/en/article/-/asset_publisher/periaatepaatos-selkiyttaa-kokonaisturvallisuuden-jarjestelyja-ja-vastuita

173 The Security Committee, *The Security Strategy for Society*

174 Ibid., 5-6

175 Ibid., 5

176 Prime Minister's Office Finland, "Situation Centre", (tilgået 2. juli 2019): https://vnk.fi/en/situation-centre

177 City of Helsinki, *Helsinki in the era of hybrid threats – Hybrid influencing and the city.* The European Centre of Excellence for Countering Hybrid Threats,

2018: https://www.hel.fi/static/kanslia/Julkaisut/2018/hybridi-raportti_eng_020818_netti.pdf

178 Kaitsepolitseiamet, "Annual reviews", (tilgået 2. juli 2019): https://www.kapo.ee/en/content/annual-reviews.html

179 Committee On Foreign Relations United States Senate, *Putin's Asymmetric Assault On Democracy In Russia And Europe: Implications For U.S. National Security,* 2018, 106: https://www.foreign.senate.gov/imo/media/doc/FinalRR.pdf

180 Prime Minister's Office Finland, "Situation Centre", (tilgået 2. juli 2019): https://vnk.fi/en/situation-centre

181 NATO holder sig for nuværende til definitionen fra 2010, der lyder: "Hybride trusler udgøres af modstandere med evnen til samtidigt at anvende konventionelle og ikkekonventionelle midler på en tilpasningsparat måde i forfølgelsen af deres mål." Hybride trusler vil ifølge NATO være karakteriseret ved tæt forbundne individer og grupper, der understøttes af fire karakteristika: 1) større muligheder for uventede samarbejder mellem potentielle modstandere på alle niveauer, 2) stigende brug af misinformation i medier for at skabe strategisk effekt, 3) anvendelse af en diversitet af metoder inkluderende både dødbringende og ikke dødbringende brug af kemiske og op til nukleare materialer, spionage, påvirkningskampagner samt misbrug af legitime forretningsorganisationer og 4) udnyttelse af NATO's samt internationale love og reglers dækningsområder, især i forhold til hvornår et konventionelt militært svar aktiveres. NATO, "Bi-SC Input to a New NATO Capstone Concept for the Military Contribution to Countering Hybrid Threats", (2010), 2: http://www.act.nato.int/images/stories/events/2010/20100826_bi-sc_cht.pdf; Europa-Parlamentets forskningsservice peger på en tredelt distinktion ved at skelne mellem hybride trusler, hybrid konflikt og hybrid krig. Her er en hybrid trussel, ligesom hos NATO, resultatet af forskellige konvergerende og forbundne elementer, der tilsammen udgør en kompleks og flerdimensional trussel. Hybrid konflikt handler om at kombinere militær intimidering, der forbliver under tærsklen for et konventionelt angreb, sammen med udnyttelse af økonomiske og politiske svagheder hos den angrebne part samt benytte diplomatiske og teknologiske midler til at opnå de ønskede politiske mål. Mens den hybride konflikt kendetegnes ved, at deltagerne afholder sig fra åbenlys brug af væbnede styrker, så er hybrid krig her defineret som netop den utilslørede brug af væbnede styrker kombineret med andre midler, såsom økonomiske, politiske og diplomatiske; European Parliamentary Research Service, "Understanding hybrid threats", (2015), 1: http://www.europarl.europa.eu/RegData/etudes/ATAG/2015/564355/EPRS_ATA(2015)564355_EN.pdf

182 Julian Lindley-French, "The Revolution in Security Affairs: Hard and Soft Security Dynamics in the 21st Century", *European Security*, 13:1-2, 1-15, DOI: 10.1080/09662830490484773, (2004), 12:

183 NATO, *Warsaw Summit Communiqué,* (9. juli 2016): https://www.nato.int/cps/en/natohq/official_texts_133169.htm#hybrid

184 Council of the European Union, "Council Conclusions on the Implementation of the Joint Declaration by the President of the European Council, the President of the European Commission and the Secretary General of the North

Atlantic Treaty Organization", (2016): http://data.consilium.europa.eu/doc/document/ST-15283-2016-INIT/en/pdf

185 Council of the European Union, "Third progress report on the implementation of the common set of proposals endorsed by EU and NATO Councils on 6 December 2016 and 5 December 2017", (2018), 1: https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2018_06/20180608_180608-3rd-Joint-progress-report-EU-NATO-eng.pdf

186 NATO, "Press statements by the NATO Secretary General Jens Stoltenberg and the EU High Representative for Foreign Affairs and Security Policy, Federica Mogherini", (3. december 2015): https://www.nato.int/cps/en/natohq/opinions_125361.htm; NATO, "NATO's response to hybrid threats", (17 juli 2018): https://www.nato.int/cps/en/natohq/topics_156338.htm?selectedLocale=en

187 NATO, "NATO and the European Union enhance cyber defence cooperation", (10. februar 2016): https://www.nato.int/cps/en/natohq/news_127836.htm

188 Ministry for Foreign Affairs of Finland, "Mikko Kinnunen appointed Finland's first Ambassador for Hybrid Affairs", (30. marts 2018): https://um.fi/press-releases/-/asset_publisher/ued5t2wDmr1C/content/suomen-ensimmaiseksi-hybridisuurlahettilaaksi-mikko-kinnunen

189 NATO, NATO Strategic Communications Centre of Excellence, *Report for the period from 1 January 2017 to 31 December 2017*, (2017), 3: https://www.stratcomcoe.org/download/file/fid/79624

190 The European Centre of Excellence for Countering Hybrid Threats, "Denmark becomes the 14th member of Hybrid CoE", (10. april 2018): https://www.hybridcoe.fi/news/denmark-becomes-14th-member-hybrid-coe/

191 Europa-Kommissionen, "Fælles ramme for imødegåelse af hybride trusler – Den Europæiske Unions indsats". 6. april 2016: https://eur-lex.europa.eu/legal-content/DA/TXT/PDF/?uri=CELEX:52016JC0018

192 Europa-Kommissionen, "Sikkerhed: EU styrker indsatsen mod hybride trusler", (6. april 2016), 1: https://europa.eu/rapid/press-release_IP-16-1227_da.pdf

193 Europa-Kommissionen, "Why a new European Agenda on Security", (tilgået 3. juli 2019): https://ec.europa.eu/home-affairs/what-we-do/policies/european-agenda-security_en

194 Europa-Parlamentet, "Europa-Parlamentets beslutning af 12. september 2013: EU's strategi for cybersikkerhed: Et åbent, sikkert og beskyttet cyberspace (2013/2606(RSP))", (2013): http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+TA+P7-TA-2013-0376+0+DOC+PDF+V0//DA

195 Europa-Kommissionen, "Meddelelse fra Kommissionen til Europa-Parlamentet og Rådet: Europæisk energisikkerhedsstrategi /* COM/2014/0330 final */", (2014): https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52014DC0330

196 Europa-Kommissionen, *Increasing resilience and bolstering capabilities to address hybrid threats,* (13. juni 2018), 2: https://eeas.europa.eu/sites/eeas/files/joint_communication_increasing_resilience_and_bolstering_capabilities_to_address_hybrid_threats.pdf

197 Ibid., 5; 10

198 Council of the European Union, "Joint Staff Working Document: EU operational protocol for countering hybrid threats 'EU Playbook'", (7. juli 2016): http://statewatch.org/news/2016/jul/eu-com-countering-hybrid-threats-playbook-swd-227-16.pdf

199 European Union External Action, "EU launches exercise to test crisis management mechanisms in response to cyber and hybrid threats", (28. september 2017): https://eeas.europa.eu/headquarters/headquarters-homepage/32969/eu-launches-exercise-test-crisis-management-mechanisms-response-cyber-and-hybrid-threats_en

200 EUvsDisinfo, "Disinformation Cases", (tilgået 2. juli 2019): https://euvsdisinfo.eu/disinformation-cases/

201 Europa-Kommissionen, "EU Code of Practice on Disinformation", (2018): https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=54454

202 Europa-Parlamentet, *Europa-Parlamentets og Rådets forordning om et regelsæt for screening af udenlandske direkte investeringer i Unionen,* 20. februar 2019: https://data.consilium.europa.eu/doc/document/PE-72-2018-INIT/da/pdf

203 Ibid., 7

204 Ibid., 6; 10

205 Regeringen, *Forebyggelse og bekæmpelse af ekstremisme og radikalisering: National handlingsplan,* (2016), 13: http://uim.dk/publikationer/forebyggelse-og-bekaempelse-af-ekstremisme-og-radikalisering/@@download/publication

206 Forsvarsudvalget, "Medlem af Folketinget Aaja Chemnitz Larsen (IA) har den 12. februar 2019 stillet følgende spørgsmål nr. 49, som hermed besvares. Sagsnr.: 2019/001068 Dok.nr.: 878959", (12. marts 2019): https://www.ft.dk/samling/20181/almdel/gru/spm/49/svar/1564685/2028492.pdf; Steffen McGhie, "Trods stigende russisk trussel: Grønland er ubeskyttet mod cyberangreb", *Berlingske*, (21 maj 2019): https://www.berlingske.dk/samfund/trods-stigende-russisk-trussel-groenland-er-ubeskyttet-mod-cyberangreb

207 Swedish Civil Contingencies Agency, *Countering information influence activities: A handbook for communicators*, (2019): https://www.msb.se/RibData/Filer/pdf/28698.pdf

208 Justitsministeriet, *Betænkning om åbenhed om økonomisk støtte til politiske partier – Betænkning nr. 1550,* (2015): http://www.justitsministeriet.dk/sites/default/files/media/Pressemeddelelser/pdf/2015/Betaenkning%20Partistoetteudvalg.pdf

209 Finansministeriet, *Regeringens kasseeftersyn på it-området*, (2018), 12: https://www.fm.dk/~/media/files/nyheder/pressemeddelelser/2018/06/kasseeftersyn/regeringens-kasseeftersyn-paa-it_omraadet-2018-_-publikation.ashx?la=da

210 Henrik Ø. Breitenbauch, Kristian Søby Kristensen, Gary John Schaub Jr, André Ken Jakobsson, Mark Winther. *Options for Enhancing Nordic–Baltic Defence and Security Cooperation: An Explorative Survey.* Copenhagen: Center for Militære Studier, Københavns Universitet, 2017. 43 s. https://cms.polsci.ku.dk/publikationer/options-for-enhancing-nordicbaltic-defence/CMS_Rapport_2017_Options_for_enhancing_Nordic-Baltic_Defence_and_Security_Cooperation.pdf

Litteraturliste

Aecon. "Aecon Industrial". Tilgået 2. juli 2019. https://www.aecon.com/What_We_Do/Aecon_Industrial

Andersen, Keld Vrå. "TDC dropper Huawei og lover 5G-net til hele Danmark i 2020". *TV2 NYHEDER*, 18. marts 2019. http://nyheder.tv2.dk/samfund/2019-03-18-tdc-dropper-huawei-og-lover-5g-net-til-hele-danmark-i-2020

ANSSI. "Cybersecurity in France". Tilgået 2. juli 2019. https://www.ssi.gouv.fr/en/cybersecurity-in-france/

Aris, Ben. "The Russian Economy is Stagnating". *The Moscow Times*, 27. maj 2019. https://www.themoscowtimes.com/2019/05/27/the-russian-economy-is-stagnating-a65760

BBC. "Election interference to be sniffed out by early-alert system". *BBC News,* 17. juli 2018. https://www.bbc.com/news/technology-44820416

BBC. "US punishes 19 Russians over vote meddling and cyber-attacks". *BBC News, 15.* marts 2018. https://www.bbc.com/news/world-us-canada-43419809

Beredskabsstyrelsen. *Krisestyring i Danmark*. 2015. https://brs.dk/viden/publikationer/Documents/Krisestyring%20i%20Danmark.pdf

Beredskabsstyrelsen. *Helhedsorienteret beredskabsplanlægning*. https://brs.dk/viden/publikationer/documents/hob-vejledning.pdf

Beredskabsstyrelsen. *Nationalt Risikobillede.* 2017. https://brs.dk/viden/publikationer/Documents/Nationalt-Risikobillede-2017-LowRes.pdf

Beredskabsstyrelsen. "Opgaver og organisation". 12 november 2018. https://brs.dk/omstyrelsen/opgaver/Pages/Forside.aspx

Beredskabsstyrelsen. *Evaluering af KRISØV 2011.* 2012. https://brs.dk/beredskab/idk/Documents/EvalueringsrapportKRISOV2011.pdf

Beredskabsstyrelsen. *Evaluering af KRISØV 2013.* 2014. https://brs.dk/viden/publikationer/Documents/KRISØV%202013%20%20Evalueringsrapport.pdf

Beredskabsstyrelsen. *Evaluering af KRISØV 2017.* 2018.
https://brs.dk/viden/publikationer/Documents/Evaluering-af-KRISOEV-2017.pdf

Berzins, Janis. *Russia's New Generation Warfare in Ukraine: Implications for Latvian Defense Policy*. Center for Security and Strategic Research, National Defence Academy of Latvia, Policy Paper no 02
April, 2014.
https://sldinfo.com/wp-content/uploads/2014/05/New-Generation-Warfare.pdf

Breitenbauch, Henrik Ø.; Kristensen, Kristian Søby; Schaub Jr, Gary John; Jakobsson, André Ken; Winther, Mark. *Options for Enhancing Nordic–Baltic Defence and Security Cooperation: An Explorative Survey*. Copenhagen: Center for Militære Studier, Københavns Universitet, 2017. 43 s.
https://cms.polsci.ku.dk/publikationer/options-for-enhancing-nordicbaltic-defence/CMS_Rapport_2017_Options_for_enhancing_Nordic-Baltic_Defence_and_Security_Cooperation.pdf

Breitenbauch. Henrik Ø.; Byrjalsen, Niels; Winther, Mark; Jakobsen, Mikkel Broen. *Orden og afskrækkelse – Vestens håndtering af Rusland efter annekteringen af Krim*. Center for Militære Studier, 2017.
https://cms.polsci.ku.dk/publikationer/orden-og-afskraekkelse/CMS_Rapport_2017_Orden_og_afskr_kkelse_opdateret_version_31-08-17.pdf

Bryden, Joan. "Bill C-76 just one tool to deter foreign election inter ference: Gould". *National Post,* 21. november 2018.
https://nationalpost.com/pmn/news-pmn/canada-news-pmn/bill-just-one-tool-to-deter-foreign-interference-in-canadian-elections-gould

Bryden, Joan. "Election reform bill passed in time for implementation in 2019 federal vote." *The Canadian Press*, 10. december 2018.
https://www.ctvnews.ca/politics/election-reform-bill-passed-in-time-for-implementation-in-2019-federal-vote-1.4212822

Bundesministerium der Justiz und für Verbraucherschutz. *Act to Improve Enforcement of the Law in Social Networks (Network Enforce ment Act).* 12. juli 2017.
https://www.bmjv.de/SharedDocs/Gesetzgebungsverfahren/Dokumente/NetzDG_engl.pdf?__blob=publicationFile&v=2

Bundesregierung. *Zwölfte Verordnung zur Änderung der Außenwi rtschaftsverordnung.* 2018.
https://www.bmwi.de/Redaktion/DE/Downloads/XYZ/zwoelfte-verordnung-zur-aenderung-der-aussenwirtschaftsverordnung.pdf?__blob=publicationFile&v=4

Cameron, Dell. "White House: We're Going to Cyber Harder". *Gizmodo*, 20. september 2018.
https://gizmodo.com/white-house-were-going-to-cyber-harder-1829209779

Center for Cyber and Information Security. *Årsrapport 2017*. NTNU, 1. marts 2018.
https://www.ntnu.edu/documents/1269858715/1278988725/NTNU+CCIS+2017.pdf/aec1871d-9806-4a49-b9bc-c05c046d90d2

Center for Cybersikkerhed. "Situationscenterets opgaver." *Forsvarets Efterretningstjeneste*, tilgået 2 juli 2019.
https://fe-ddis.dk/cfcs/sitcen/Pages/opgaver.aspx

Center for Cybersikkerhed. "Situationscenterets opgaver". Tilgået 18. juni 2019.
https://fe-ddis.dk/cfcs/sitcen/Pages/opgaver.aspx

Center for Cybersikkerhed. "Udenlandsk aktør spionerer mod danske myndigheder". Forsvarets Efterretningstjeneste, 23. april 2017. https://fe-ddis.dk/cfcs/nyheder/arkiv/2017/Pages/Udenlandskaktoerspionerer-moddanskemyndigheder.aspx

Center for Cybersikkerhed. *Undersøgelsesrapport – Målrettede forsøg på hacking af den danske energisektor*. Forsvarets Efterretningstjeneste, 2018.
https://fe-ddis.dk/cfcs/publikationer/Documents/Undersøgelsesrapport%20%20energisektor.pdf

Centre for Protection of National Infrastructure. "About CPNI". Tilgået 2. juli 2019.
https://www.cpni.gov.uk/about-cpni

Centre for Protection of National Infrastructure. "Security Awareness Campaigns". Tilgået 2. juli 2019.
https://www.cpni.gov.uk/security-awareness-campaigns

Centre for the Protection of National Infrastructure. "Critical National Infrastructure". Tilgået 2. juli 2019.
https://www.cpni.gov.uk/critical-national-infrastructure-0

Chesney, Robert; Citron, Danielle. "Deepfakes and the New Disinformation War – The Coming Age of Post-Truth Geopolitics". *Foreign Affairs, 2019.*
https://www.foreignaffairs.com/articles/world/2018-12-11/deepfakes-and-new-disinformation-war

Cionnaith, Fiachra Ó. "Watchdog wants powers to probe funding of fake news". *Irish Examiner,* 27. november 2018.
https://www.irishexaminer.com/breakingnews/ireland/watchdog-wants-powers-to-probe-funding-of-fake-news-888066.html

City of Helsinki. *Helsinki in the era of hybrid threats – Hybrid influencing and the city.* The European Centre of Excellence for Countering Hybrid Threats, 2018.
https://www.hel.fi/static/kanslia/Julkaisut/2018/hybridirapo-rtti_eng_020818_netti.pdf

Clausewitz, Carl von. *On War.* 1832.

Colliver, Chloe; Pomerantsev, Peter; Applebaum, Anne; Birdwel, Jonathan. *Smearing Sweden: International Influence Campaigns in the 2018 Swedish Election.* Institute for Strategic Dialogue, 2018.
http://www.lse.ac.uk/iga/assets/documents/arena/2018/Sweden-Report-October-2018.pdf

Commission on Fake News and the Teaching of Critical Literacy Skills. *Fake news and critical literacy – The final report of the Commission on Fake News and the Teaching of Critical Literacy in Schools.* National Literacy Trust, 2018.
https://literacytrust.org.uk/documents/1722/Fake_news_and_critical_literacy_-_final_report.pdf

Committee On Foreign Relations United States Senate. *Putin's Asymmetric Assault On Democracy In Russia And Europe: Implications For U.S. National Security.* 2018.
https://www.foreign.senate.gov/imo/media/doc/FinalRR.pdf

Conley, Heather A.; Vilmer, Jean-Baptiste Jeangène. "Successfully Countering Russian Electoral Interference." *CSIS Brief,* 21. juni 2018.
https://www.csis.org/analysis/successfully-countering-russian-electoral-interference

Council of the European Union. "Council Conclusions on the Implementation of the Joint Declaration by the President of the European Council, the President of the European Commission and the Secretary General of the North Atlantic Treaty Organization". 2016.
http://data.consilium.europa.eu/doc/document/ST-15283-2016-INIT/en/pdf

Council of the European Union. "Joint Staff Working Document: EU operational protocol for countering hybrid threats 'EU Playbook'". 7 juli 2016.
http://statewatch.org/news/2016/jul/eu-com-countering-hybrid-threats-playbook-swd-227-16.pdf

Council of the European Union. "Third progress report on the implementation of the common set of proposals endorsed by EU and NATO Councils on 6 December 2016 and 5 December 2017". 31. maj 2018.
https://www.consilium.europa.eu/media/35578/third-report-ue-nato-layout-en.pdf

Cullen, Patrick J.; Reichborn-Kjennerud, Erik. "MCDC Countering Hybrid Warfare Project: Understanding Hybrid Warfare." *Multinational Capability Development Campaign,* 2017. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/647776/dar_mcdc_hybrid_warfare.pdf

Cvetkovska, Saska; Belford, Aubrey; Silverman, Craig; Feder, J. Lester. "The Secret Players Behind Macedonia's Fake News Sites". *The Organized Crime and Corruption Reporting Project,* 18. juli 2018. https://www.occrp.org/en/spooksandspin/the-secret-players-behind-macedonias-fake-news-sites

Delfs, Arne. "Germany Toughens Stance and Blocks China Deal". *Bloomberg,* 1. august 2018. https://www.bloomberg.com/news/articles/2018-08-01/germany-said-to-block-company-purchase-by-chinese-for-first-time

Deloitte. "Cyber risk in an Internet of Things world". Tilgået 2. juli 2019. https://www2.deloitte.com/us/en/pages/technology-media-and-telecommunications/articles/cyber-risk-in-an-internet-of-things-world-emerging-trends.html

Department of Homeland Security. "Homeland Security Presidential Directive 7: Critical Infrastructure Identification, Prioritization, and Protection." 17. december 2003. https://www.dhs.gov/homeland-security-presidential-directive-7

Department of Homeland Security. "National Infrastructure Protection Plan". Tilgået 2. juli 2019. https://www.dhs.gov/cisa/national-infrastructure-protection-plan

Department of Homeland Security. "NCCIC Cyber Incident Scoring System". Tilgået 2. juli 2019. https://www.us-cert.gov/NCCIC-Cyber-Incident-Scoring-System

Department of Homeland Security. *NIPP 2013 Partnering for Critical Infrastructure Security and Resilience.* 2013. https://www.dhs.gov/sites/default/files/publications/national-infrastructure-protection-plan-2013-508.pdf

Department of the treasury. *Re: CFIUS Case 18-036: Broadcom Limited (Singapore)/Quallcomm Incorporated.* 5. marts 2018. http://online.wsj.com/public/resources/documents/cfiusletter.pdf

Devanny, Joe. "Why it's unwise for the UK to boast about its cyber attack capability". *The Conversation,* 13. september 2018. https://theconversation.com/why-its-unwise-for-the-uk-to-boast-about-its-cyber-attack-capability-102870

Dickinson, Steve. "New Restrictions on High Tech Technology Transfers to China". *China Law Blog*, 27. november 2018. https://www.chinalawblog.com/2018/11/new-restrictions-on-high-tech-technology-transfers-to-china.html

Digitaliseringsstyrelsen. *Hovedresultater: ISO 27001-modenhed i staten.* 2018. https://digst.dk/media/18741/hovedresultater-af-iso-maalingen-for-2018.pdf

Economy, Elizabeth C. "The great firewall of China: Xi Jinping's internet shutdown". *The Guardian*, 29. juni 2018. https://www.theguardian.com/news/2018/jun/29/the-great-firewall-of-china-xi-jinpings-internet-shutdown

Elkær, Mads. "Kæmpe cyber-krigsøvelse afslører seriøse problemer". *Computerworld*, 8. november 2013. https://www.computerworld.dk/art/228936/kaempe-cyber-krigsoevelse-afsloerer-serioese-problemer#eodZvMz03G87JFHZ.99

Ellyatt, Holly. "Russia kicks off economic forum, but its wealth is on shaky ground". *CNBC,* 6. juni 2016. https://www.cnbc.com/2019/06/06/russia-kicks-off-spief-as-the-economy-is-on-shaky-ground.html

Europa-Kommissionen. "EU Code of Practice on Disinformation". 2018. https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=54454

Europa-Kommissionen. "Why a new European Agenda on Security". Tilgået 3. juli 2019. https://ec.europa.eu/home-affairs/what-we-do/policies/european-agenda-security_en

Europa-Kommissionen. "Fælles ramme for imødegåelse af hybride trusler – Den Europæiske Unions indsats". 6. april 2016. https://eur-lex.europa.eu/legal-content/DA/TXT/PDF/?uri=CELEX:52016JC0018

Europa-Kommissionen. "Meddelelse fra Kommissionen til Europa-Parlamentet og Rådet: Europæisk energisikkerhedsstrategi /* COM/2014/0330 final */". 2014. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52014DC0330

Europa-Kommissionen. "Sikkerhed: EU styrker indsatsen mod hybride trusler". 6. april 2016. https://europa.eu/rapid/press-release_IP-16-1227_da.pdf

Europa-Kommissionen. *Increasing resilience and bolstering capabilities to address hybrid threats*, 13. juni 2018. https://eeas.europa.eu/sites/eeas/files/joint_communication_increasing_resilience_and_bolstering_capabilities_to_address_hybrid_threats.pdf

Europa-Parlamentet. "Europa-Parlamentets beslutning af 12. september 2013: EU's strategi for cybersikkerhed: Et åbent, sikkert og beskyttet cyberspace (2013/2606(RSP))". 2013. http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+TA+P7-TA-2013-0376+0+DOC+PDF+V0//DA

Europa-Parlamentet. "Europa-Parlamentets og Rådets forordning om et regelsæt for screening af udenlandske direkte investeringer i Unionen". 20. februar 2019. https://data.consilium.europa.eu/doc/document/PE-72-2018-INIT/da/pdf

European Parliamentary Research Service. "Understanding hybrid threats". 2015. http://www.europarl.europa.eu/RegData/etudes/ATAG/2015/564355/EPRS_ATA(2015)564355_EN.pdf

European Regulators' Group for Electricity and Gas. *The lessons to be learned from the large disturbance in the European power system on the 4th of November 2006.* 2007. https://www.ceer.eu/documents/104400/-/-/b4f16360-b355-5d50-bf33-01f8a76fc95a

European Union External Action. "EU launches exercise to test crisis management mechanisms in response to cyber and hybrid threats". 28 september 2017. https://eeas.europa.eu/headquarters/headquarters-homepage/32969/eu-launches-exercise-test-crisis-management-mechanisms-response-cyber-and-hybrid-threats_en

European Union. "Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016, L 194/1". *Official Journal of the European Union*, 19. juli 2016. https://eur-lex.europa.eu/eli/dir/2016/1148/oj

EUvsDisinfo. "Defensive disinformation as decoy flare: Skripal and Flight MH17". 24. marts 2018. https://euvsdisinfo.eu/defensive-disinformation-as-decoy-flare-skripal-and-flight-mh17/

EUvsDisinfo. "Disinformation Cases". Tilgået 2. juli 2019. https://euvsdisinfo.eu/disinformation-cases/

Federal Register. "Review of Controls for Certain Emerging Technologies". *Bureau of Industry and Security*, Commerce, 19. november 2018. https://www.federalregister.gov/documents/2018/11/19/2018-25221/review-of-controls-for-certain-emerging-technologies

Finansministeriet. "Regeringens kasseeftersyn på it-området". 2018. https://www.fm.dk/~/media/files/nyheder/pressemeddelelser/2018/06/kasseeftersyn/regeringens-kasseeftersyn-paa-it_omraadet-2018-_-publikation.ashx?la=da

Finansministeriet. *National strategi for cyber- og informationssikkerhed – 2018-2021*. Regeringen, 2018. https://www.fmn.dk/nyheder/Documents/National-strategi-for-cyber-og-informationssikkerhed-2018.pdf p. 38-40

Finansudvalget. "Samrådsspørgsmål A". *Folketinget,* 9. oktober 2018. https://www.ft.dk/samling/20181/almdel/fiu/samspm/a/index.htm

Finnish Government. "Government resolution clarifies organisation and responsibilities with respect to comprehensive security". 5. december 2012. https://valtioneuvosto.fi/en/article/-/asset_publisher/periaatepaatos-selkiyttaa-kokonaisturvallisuuden-jarjestelyja-ja-vastuita

Foght, Thomas. "Kinesisk firma vil bygge tunnel mellem Danmark og Sverige". *Radio24syv,* 28. november 2018. https://www.24syv.dk/udvalgte-nyhedshistorier/kinesisk-firma-vil-bygge-tunnel-mellem-danmark-og-sverige

Folketinget. "Åbent samråd om regeringens overvejelser om at iværksætte de såkaldte 'investeringsscreeninger'". 28. februar 2019. https://www.ft.dk/udvalg/udvalgene/URU/kalender/42308/samraad.htm

Forsvarsministeriet. *Forslag til Lov om ændring af lov om Center for Cybersikkerhed.* Lovforslag nr. L 215, 2. maj 2019. https://www.ft.dk/ripdf/samling/20181/lovforslag/l215/20181_l215_som_vedtaget.pdf

Forsvarsministeriet. "Offensive cybereffekter". 2019. https://www.fmn.dk/temaer/nato/Documents/2018/Faktaark-cyber-effekter.pdf

Forsvarsudvalget. "Medlem af Folketinget Aaja Chemnitz Larsen (IA) har den 12. februar 2019 stillet følgende spørgsmål nr. 49, som hermed besvares. Sagsnr.: 2019/001068 Dok.nr.: 878959", 12. marts 2019. https://www.ft.dk/samling/20181/almdel/gru/spm/49/svar/1564685/2028492.pdf

French Government. "Livre Blanc Défense Et Sécurité Nationale – 2013". 2013. http://www.livreblancdefenseetsecurite.gouv.fr/pdf/le_livre_blanc_de_la_defense_2013.pdf

Government of Canada. "Guidelines on the National Security Review of Investments". 2016. https://www.ic.gc.ca/eic/site/ica-lic.nsf/eng/lk81190.html

Grigsby, Alex. "Three Takeaways from the French Cyber Defense Review". *Council on Foreign Relations,* 26 februar 2018. https://www.cfr.org/blog/three-takeaways-french-cyber-defense-review

Guess, Andrew; Nagler, Jonathan; Tucker, Joshua. "Less than you think: Prevalence and predictors of fake news dissemination on Facebook". *Science Advances*, Vol. 5, no. 1, DOI: 10.1126/sci-adv.aau4586, 2019.
http://advances.sciencemag.org/content/5/1/eaau4586

Guillaume, Marine. "Combating the manipulation of information – a French case". *Strategic Analysis 2/2019,* Hybrid Centre of Excellence, 2019. https://www.hybridcoe.fi/wp-content/uploads/2019/05/HybridCoE_SA_Combating-the-manipulation-of-information.pdf

Hansen, John; Kjær, Jakob Sorgenfri. "Politikere har kendt Skats ulovlige it-aftaler i 15 år". *Politiken,* 28. januar 2016.
https://politiken.dk/oekonomi/art5609183/Politikere-har-kendt-Skats-ulovlige-it-aftaler-i-15-år

Hao, Karen. "Even the best AI for spotting fake news is still terrible". *MIT Technology Review*, 3. oktober 2018.
https://www.technologyreview.com/s/612236/even-the-best-ai-for-spotting-fake-news-is-still-terrible/

Haynes, Deborah. "Britain to create 2,000-strong cyber force to tackle Russia threat". *Sky News,* 21. september 2018.
https://news.sky.com/story/britain-to-create-2000-strong-cyber-force-to-tackle-russia-threat-11503653

Hern, Alex. "Cambridge Analytica: how did it turn clicks into votes?". *The Guardian*, 6. maj 2018.
https://www.theguardian.com/news/2018/may/06/cambridge-analytica-how-turn-clicks-into-votes-christopher-wylie

Horowitz, Jason. "In Italian Schools, Reading, Writing and Recognizing Fake News". *The New York Times*, 18. oktober 2017.
https://www.nytimes.com/2017/10/18/world/europe/italy-fake-news.html?_r=0

Human Rights Watch. "Germany: Flawed Social Media Law – NetzDG is Wrong Response to Online Abuse". 14. februar, 2018.
https://www.hrw.org/news/2018/02/14/germany-flawed-social-media-law

Jakobsson, André Ken. "Den hybride krig". *Weekendavisen*, 15. juni 2018.
https://www.weekendavisen.dk/2018-24/samfund/den-hybride-krig

Jakobsson, André Ken. "Putins suveræne internet er grænsekontrol i cyberdomænet". *Berlingske,* 10. marts 2019.
https://www.berlingske.dk/kommentarer/putins-suveraene-internet-er-graensekontrol-i-cyberdomaenet

James, William; Piper, Elizabeth; Evans, Catherine. "Britain to set up unit to tackle 'fake news': May's spokesman". *Reuters,* 23. januar 2018.
https://www.reuters.com/article/us-britain-politics-fakenews/britain-to-set-up-unit-to-tackle-fake-news-mays-spokesman-idUSKBN1FC2AL

Janda, Jakub. "The Lisa Case – STRATCOM Lessons for European states". *Security Policy Working Paper*, No. 11/2016, 2016. https://www.baks.bund.de/sites/baks010/files/working_paper_2016_11.pdf

Jensen, Thomas Klose: "Claus Hjort: Vi kan ikke forbyde Huawei". *DR Nyheder*, 22. januar 2019. https://www.dr.dk/nyheder/politik/claus-hjort-vi-kan-ikke-forbyde-huawei

Justitiedepartementet. *Kommittédirektiv – En ny myndighet för psykologiskt försvar.* 2018. https://www.regeringen.se/4a566c/contentassets/b4b90c231b4144e683d5b4a594fe27b1/en-ny-myndighet-for-psykologiskt-forsvar-dir.-201880

Justitsministeriet. *Betænkning om åbenhed om økonomisk støtte til politiske partier – Betænkning nr. 1550.* 2015. http://www.justitsministeriet.dk/sites/default/files/media/Pressemeddelelser/pdf/2015/Betaenkning%20Partistoetteudvalg.pdf

Justitsministeriet. *Forslag til Lov om ændring af straffeloven (Ulovlig påvirkningsvirksomhed).* 14. november 2018. https://www.retsinformation.dk/eli/ft/201812L00095

Justitsministeriet. "Styrket værn mod udenlandsk påvirkning af danske valg og demokratiet". 7. september 2018. http://www.justitsministeriet.dk/nyt-og-presse/pressemeddelelser/2018/styrket-vaern-mod-udenlandsk-paavirkning-af-danske-valg-og

Kaitseliit. "Estonian Defence League's Cyber Unit". Tilgået 2. juli 2019. http://www.kaitseliit.ee/en/cyber-unit

Kaitsepolitseiamet. "Annual reviews". Tilgået 2. juli 2019. https://www.kapo.ee/en/content/annual-reviews.html

Kania, Elsa B. "The PLA's Latest Strategic Thinking on the Three Warfares". *China Brief*, Volume 16 Issue 12, August 22, The Jamestown Foundation, 2016. https://jamestown.org/wp-content/uploads/2016/08/CB_16_13_2.pdf?x25462

Kaska, Kadri; Osula, Anna-Maria; Stinissen, Jan. *The Cyber Defence Unit of the Estonian Defence League*. NATO Cooperative Cyber Defence Centre of Excellence, 2013. https://ccdcoe.org/uploads/2018/10/CDU_Analysis.pdf

Kennan, George. "269. Policy Planning Staff Memorandum". 4. maj 1948. https://history.state.gov/historicaldocuments/frus1945-50Intel/d269

Kjær, Jakob Sorgenfri; Kjeldtoft, Sebastian Stryhn: "Spionagemistænkte Huawei leverer it-udstyr til dansk politi og forsvaret". *Politiken,* 19. februar 2019. https://politiken.dk/indland/art7042686/Spionagemist%C3%A6nkte-Huawei-leverer-it-udstyr-til-dansk-politi-og-forsvaret

Klarskov, Kristian; Bæksgaard, Anders. "Ny lov skal forhindre farlige opkøb i Danmark og pression fra lande som Kina". *Politiken*, 18. november 2018. https://politiken.dk/indland/art6850533/Ny-lov-skal-forhindre-farlige-opkøb-i-Danmark-og-pression-fra-lande-som-Kina

Korteweg, Rem. *Energy as a tool of foreign policy of authoritarian states, in particular Russia.* Policy Department, Directorate-General for External Policies, European Parliament's Committee on Foreign Affairs, doi:10.2861/951739, 2018. http://www.europarl.europa.eu/RegData/etudes/STUD/2018/603868/EXPO_STU(2018)603868_EN.pdf

Krog, Andreas. "Efterretningstjenesten forbereder sig på russisk påvirkning af folketingsvalget". *Altinget,* 28. juni 2018. https://www.altinget.dk/artikel/efterretningstjenesten-forbereder-sig-paa-russisk-paavirkning-af-folketingsvalget

Kruse, Simon. "8.000 embedsmænd skal beskytte det svenske valg mod fremmede magter". *Berlingske,* 9. juni 2018. https://www.berlingske.dk/internationalt/8.000-embedsmaend-skal-beskytte-det-svenske-valg-mod-fremmede-magter

Kruse, Simon; Christensen, Mikkel Fyhn. "Norges svar på PET siger stop for mere cyberovervågning – i Danmark henligger høringssvar i mørke". *Berlingske,* 14. februar 2019. https://www.berlingske.dk/internationalt/norges-svar-paa-pet-siger-stop-for-mere-cyberovervaagning-i-danmark

Larkin, Laura. "Twitter backs new Bill on online political ads". *Independent.ie,* 27. november 2018. https://www.independent.ie/business/technology/twitter-backs-new-bill-on-online-political-ads-37569217.html

Laskai, Lorand. "Why Does Everyone Hate Made in China 2025?". *Council on Foreign Relations,* 2018. https://www.cfr.org/blog/why-does-everyone-hate-made-china-2025

Lavin, Rachel; Adorjani, Roland. "How Ireland Beat Dark Ads". *Foreign Policy*, 1. juni 2018. https://foreignpolicy.com/2018/06/01/abortion-referendum-how-ireland-resisted-bad-behaviour-online/

Lee, John. "China's Trojan Ports". *The American Interest,* 29. November 2018. https://www.the-american-interest.com/2018/11/29/chinas-trojan-ports/

Lindley-French, Julian. "The Revolution in Security Affairs: Hard and Soft Security Dynamics in the 21st Century". *European Security*, 13:1-2, 1-15, DOI: 10.1080/09662830490484773, 2004.

Marsh, Sarah. "US joins UK in blaming Russia for NotPetya cyber-attack". *The Guardian,* 15. februar 2018. https://www.theguardian.com/technology/2018/feb/15/uk-blames-russia-notpetya-cyber-attack-ukraine

McGhie, Steffen. "Trods stigende russisk trussel: Grønland er ubeskyttet mod cyberangreb". *Berlingske,* 21. maj 2019. https://www.berlingske.dk/samfund/trods-stigende-russisk-trussel-groenland-er-ubeskyttet-mod-cyberangreb

McGuinness, Damien. "How a cyber attack transformed Estonia". *BBC News*, 27. april 2017. https://www.bbc.com/news/39655415

Ministry for Foreign Affairs of Finland. "Mikko Kinnunen appointed Finland's first Ambassador for Hybrid Affairs". 30 marts 2018. https://um.fi/press-releases/-/asset_publisher/ued5t2wDmr1C/content/suomen-ensimmaiseksi-hybridisuurlahettilaaksi-mikko-kinnunen

National Cyber Security Center. "About the NCSC". Tilgået 2. juli 2019. https://www.ncsc.gov.uk/information/about-ncsc

National Cyber Security Center. "CyberInvest". Tilgået 2. juli 2019. https://www.ncsc.gov.uk/articles/cyber-invest

NATO. "NATO and the European Union enhance cyber defence cooperation". 10. februar 2016. https://www.nato.int/cps/en/natohq/news_127836.htm

NATO. NATO Strategic Communications Centre of Excellence. *Report for the period from 1 January 2017 to 31 December 2017.* 2017. https://www.stratcomcoe.org/download/file/fid/79624

NATO. "NATO's response to hybrid threats". 17. juli 2018. https://www.nato.int/cps/en/natohq/topics_156338.htm?selectedLocale=en

NATO. "Press statements by the NATO Secretary General Jens Stoltenberg and the EU High Representative for Foreign Affairs and Security Policy, Federica Mogherini". 3. december 2015. https://www.nato.int/cps/en/natohq/opinions_125361.htm

NATO. "Bi-SC Input to a New NATO Capstone Concept for the Military Contribution to Countering Hybrid Threats". 2010. http://www.act.nato.int/images/stories/events/2010/20100826_bi-sc_cht.pdf

NATO. *Warsaw Summit Communiqué,* 9. juli 2016. https://www.nato.int/cps/en/natohq/official_texts_133169.htm#hybrid

NIS Cooperation Group. *Cybersecurity Incident Taxonomy.* Europa-Kommissionen, 2018.
http://ec.europa.eu/information_society/newsroom/image/document/2018-30/cybersecurity_incident_taxonomy_00CD828C-F851-AFC4-0B1B416696B5F710_53646.pdf

Nouwens, Meia. "China's pursuit of advanced dual-use technologies". *IISS,* 18. december 2018.
https://www.iiss.org/blogs/analysis/2018/12/emerging-technology-dominance

NTNU. "Experienced based master´s degree, 3 years, Gjøvik, Information Security". Tilgået 2. juli 2019.
https://www.ntnu.edu/studies/miseb

O'Brien, Ciara. "Facebook bans foreign ads for Eighth Amendment referendum". *The Irish Times,* 8. maj 2018.
https://www.irishtimes.com/business/technology/facebook-bans-foreign-ads-for-eighth-amendment-referendum-1.3487895

Oliker, Olga. "Russian Influence and Unconventional Warfare Operations in the 'Grey Zone': Lessons from Ukraine". Statement before the Senate Armed Services Committee Subcommittee on Emerging
Threats and Capabilities, 29. marts 2017.
https://www.armed-services.senate.gov/imo/media/doc/Oliker_03-29-17.pdf

Pamment, James; Nothhaft, Howard; Agardh-Twetman, Henrik; Fjällhed, Alicia. *Countering Information Influence Activities: The State of the Art.* Swedish Civil Contingencies Agency, 2018.
https://www.msb.se/RibData/Filer/pdf/28697.pdf

Parliament of Canada. "An Act to amend the Canada Elections Act and other Acts and to make certain consequential amendments".
Bill C-76, 13. december 2018.
http://www.parl.ca/DocumentViewer/en/42-1/bill/C-76/royal-assent

Paul, Christopher; Matthews, Miriam. "The Russian 'Firehose of Falsehood' Propaganda Model – Why It Might Work and Options to Counter It". RAND Corporation, 2016.
https://www.rand.org/pubs/perspectives/PE198.html

Peel, Michael. "Fake news: How Lithuania's 'elves' take on Russian trolls". *Financial Times,* 4. februar 2019.
https://www.ft.com/content/b3701b12-2544-11e9-b329-c7e6ceb5ffdf

Politiets Efterretningstjeneste. "Kritisk national infrastruktur". Tilgået 2. juli 2019.
https://www.pet.dk/Forebyggende%20Afdeling/Kritisk%20national%20infrastruktur.aspx

Politiets Efterretningstjeneste. *Årlig redegørelse 2017.* 2018. https://www.pet.dk/~/media/Aarsberetninger/rligredegrelsefor-PET2017WEBpdf.ashx

Politiets Sikkerhetstjeneste. "Høringssvar fra PST – Forslag til ny lov om Etterretningstjenesten". Forsvarsdepartementet, 12. februar 2019. https://www.regjeringen.no/contentas-sets/287d2d52ddb847849cddb49796456129/horingssvar-med-merknader---pst.pdf?uid=PST

Porter, Jon. "Australia's encryption-busting law is 'deeply flawed,' says tech industry". *The Verge,* 7. december 2018. https://www.theverge.com/2018/12/7/18130806/australia-access-and-assistance-encryption-bill-2018-facebook-google-apple-respond

Prime Minister's Office Finland. "Situation Centre". Tilgået 2. juli 2019. https://vnk.fi/en/situation-centre

Quass, Lisbeth; Gram, Kasper Duncan. "Hackerangreb koster Mærsk milliardbeløb". *DR Nyheder,* 16. august 2017. https://www.dr.dk/nyheder/penge/hackerangreb-koster-maersk-milliard-beloeb

Radio Free Europe. "Group Says It Detected Campaign To Suppress Voter Turnout In Macedonia". 27. september 2018. https://www.rferl.org/a/pro-democracy-group-detects-online-campaign-suppress-voter-turnout-macedonian-referendum-name-change-greece/29512150.html

Rambøll. *Analyse af data- og cybersikkerhed. Delrapport 2: Cybersikkerhed.* IDA og FSR – Danske Revisorer, 19. marts 2018. https://ida.dk/media/2389/delrapport_2_-_cybersikkerhed.pdf

Rebouh, David; Gregersen, Benjamin. "Forsker om kinesiske krigsskibe: Kina vil vise militære muskler i Danmark". *DR Nyheder,* 19. Juli 2017. https://www.dr.dk/nyheder/indland/forsker-om-kinesiske-krigsskibe-kina-vil-vise-militaere-muskler-i-danmark

Regeringen. *Forebyggelse og bekæmpelse af ekstremisme og radikalisering: National handlingsplan*. 2016. http://uim.dk/publikationer/forebyggelse-og-bekaempelse-af-ekstremisme-og-radikalisering/@@download/publication

Regeringskansliet. "Stärkt digital kompetens i skolans styrdokument". 2017. https://www.regeringen.se/contentas-sets/acd9a3987a8e4619bd6ed95c26ada236/informationsmaterial-starkt-digital-kompetens-i-skolans-styrdokument.pdf

Riber-Sellebjerg, Thomas; Okholm, Mads Møller. "Afsløring: 86 kommuner hacket". *Ekstra Bladet,* 18. september 2018. https://ekstrabladet.dk/nyheder/samfund/article7221664.ece

Rigsrevisionen. *Rigsrevisionens beretning om statens udbud af it-drift og -vedligeholdelse afgivet til Folketinget med Statsrevisorernes bemærkninger.* 2016.
http://www.rigsrevisionen.dk/media/2104443/sr0816.pdf

Ritzau. "Overblik: Balladen om Grønlands nye lufthavne". 10. september 2018.
https://www.avisen.dk/overblik-balladen-om-groenlands-nye-lufthavne_515199.aspx

Ritzau. "Statens kriseberedskab aktiveret efter togulykke". *DR Nyheder*, 2. januar 2019.
https://www.dr.dk/nyheder/indland/statens-kriseberedskab-aktiveret-efter-togulykke

Ruiz, Monica M. "Is Estonia's Approach to Cyber Defense Feasible in the United States?". *War on the Rocks,* 9. januar 2018. https://warontherocks.com/2018/01/estonias-approach-cyber-defense-feasible-united-states/

Rühle, Michael. "Deterrence: what it can (and cannot) do". *NATO Review Magazine,* 2015.
https://www.nato.int/docu/review/2015/also-in-2015/deterrence-russia-military/en/index.htm

Sandia National Laboratories. "National Infrastructure Simulation and Analysis Center". Tilgået 2. juli 2019.
https://www.sandia.gov/nisac-ssl/

Schjoldager, Jakob. "It-eksperter: Drop Center for Cybersikkerhed til at overvåge Danmark mod hackere: Opret en ny myndighed".
Computerworld, 26. februar 2019.
https://www.computerworld.dk/art/246576/it-eksperter-drop-center-for-cybersikkerhed-til-at-overvaage-danmark-mod-hackere-opret-en-ny-myndighed

Schjoldager, Jakob. "Kritisk infrastruktur er plaget af usikre systemer: 'De er afgjort ikke sikre og vil ikke være det de næste mange år'".
Computerworld, 21. november 2018.
https://www.computerworld.dk/art/245477/kritisk-infrastruktur-er-plaget-af-usikre-systemer-de-er-afgjort-ikke-sikre-og-vil-ikke-vaere-det-de-naeste-mange-aar

Schjoldager, Jakob. "Manglende definition af kritisk infrastruktur i Danmark møder massiv kritik: 'Ser man på FN's liste over lande med den bedste it-sikkerhed, så ligger vi ikke engang i top 10'". *Computerworld*, 26. juli 2018.
https://www.computerworld.dk/art/244156/manglende-definition-af-kritisk-infrastruktur-i-danmark-moeder-massiv-kritik-ser-man-paa-fn-s-liste-over-lande-med-den-bedste-it-sikkerhed-saa-ligger-vi-ikke-engang-i-top-10

Schultz-Nielsen, Jørgen. "Kalaallit Airports: 6 entreprenører får lov at byde på lufthavnsbyggerierne". *Sermisiaq AG,* 26. marts 2018. https://sermitsiaq.ag/node/204638

Selliken, Joachim Kühlmann. "Rigspolitiet har ikke sendt CSC-opgaver i udbud i årevis: System-dokumentation mangler på 19. år". *Computerworld*, 1. december 2015. https://www.computerworld.dk/art/235067/rigspolitiet-har-ikke-sendt-csc-opgaver-i-udbud-i-aarevis-system-dokumentation-mangler-paa-19-aar

Shakir, Taenaz; Raman, Rama Venkat; Schnurr, Leah; Goh, Brenda; Martina, Michael. "Canada blocks Chinese takeover of Aecon on national security grounds". *Reuters*, 24. maj 2018. https://www.reuters.com/article/us-aecon-group-m-a-canada/canada-blocks-chinese-takeover-of-aecon-on-security-grounds-idUSKCN1IO3F2

Somer, Iryna. "Lithuanians create artificial intelligence with ability to identify fake news in 2 minutes". *Kyiv Post,* 21. september 2018. https://www.kyivpost.com/technology/lithuanian-creates-artificial-intelligence-with-ability-to-identify-fake-news-within-2-minutes.html

Standing Senate Committee on Legal and Constitutional Affairs. *Observations to the Twenty-ninth Report of the Standing Senate Committee on Legal and Constitutional Affairs (Bill C-76).* Canadian Senate. https://sencanada.ca/content/sen/committee/421/LCJC/Reports/LCJCC-762018-12-06v7_e.pdf

Statskontoret. *Myndigheternas arbete med psykologiskt försvar. 2017.* http://www.statskontoret.se/globalassets/publikationer/2017/201705.pdf

Stoltenberg, Jens. "Stoltenberg Provides Details of NATO's Cyber Policy". *Atlantic Council*, 16. maj 2018. https://www.atlanticcouncil.org/blogs/natosource/stoltenberg-provides-details-of-nato-s-cyber-policy

Swedish Civil Contingencies Agency. *Countering information influence activities: A handbook for communicators*. 2019. https://www.msb.se/RibData/Filer/pdf/28698.pdf

Sørensen, Heine; Nyemann, Dorthe Bach. *Going Beyond Resilience: A revitalized approach to countering hybrid threats*. The European Centre of Excellence for Countering Hybrid Threats, 2018. https://www.hybridcoe.fi/wp-content/uploads/2019/01/Strategic-analysis-Sorensen-Nyeman-11-2018.pdf

Saalman, Lora. "Little Grey Men: China and the Ukraine Crisis". *Survival,* vol. 58 no. 6, December 2016–January 2017, 2017, 135–156, DOI 10.1080/00396338.2016.1257201. http://cs.brown.edu/courses/csci1800/sources/Little_Grey_Men.pdf

Taksøe-Jensen, Peter. *Dansk diplomati og forsvar i en brydningstid: Vejen frem for Danmarks interesser og værdier mod 2030.* Udenrigsministeriet, 2016.
http://um.dk/~/media/UM/Danish-site/Documents/Udenrigspolitik/Aktuelle%20emner/148396_udredning_indhold_FINAL_PRINTVENLIG.pdf?la=da

Tassy, Agnes; Nielsen, Monika Bille; Jakobsen, Ditte Trier. *It-anvendelse i befolkningen 2018.* Danmarks Statistik, 2018.
https://www.dst.dk/Site/Dst/Udgivelser/GetPubFile.aspx?id=29448&sid=itbef2018

Taylor, Adam. "Mattis compared Xi's China to the Ming Dynasty. Xi might be happy to hear it". *The Washington Post*, 20. juni 2018.
https://www.washingtonpost.com/news/worldviews/wp/2018/06/20/mattis-compared-xis-china-to-the-ming-dynasty-xi-might-be-happy-to-hear-it/?utm_term=.b9d8319be299

The European Centre of Excellence for Countering Hybrid Threats. "Denmark becomes the 14th member of Hybrid CoE". 10. april 2018.
https://www.hybridcoe.fi/news/denmark-becomes-14th-member-hybrid-coe/

The Security Committee. "Security Committee". Tilgået 2. juli 2019.
https://turvallisuuskomitea.fi/en/security-committee/

The Security Committee. "The Finnish Concept for Comprehensive Security". 2017.
https://www.defmin.fi/files/3827/Valtonen_2017_06_14_FI_Concept_for_Comprehensive_Security_Valtonen.pdf

The Security Committee. "The Security Strategy for Society". 2017.
https://turvallisuuskomitea.fi/wp-content/uploads/2018/04/YTS_2017_english.pdf

Thomas, Timothy L. "Russia's Reflexive Control Theory and the Military". *Journal of Slavic Military Studies* 17: 237–256, 2004, DOI:10.1080/13518040490450529.
https://www.rit.edu/~w-cmmc/literature/Thomas_2004.pdf

Thoms, Anahita. "Germany Tightens Rules on Foreign Investments. What are the implications?". *Baker McKenzie,* 2. oktober 2017.
https://www.bakermckenzie.com/en/insight/publications/2017/10/germany-tightens-rules

Thykier, Michael. "PET vil ikke hjælpe – bygherrer må gætte sig til god terrorsikring". *Jyllands-Posten, 5.* november 2017.
https://jyllands-posten.dk/indland/ECE10004235/pet-vil-ikke-hjaelpe-bygherrer-maa-gaette-sig-til-god-terrorsikring/

Transparent Referendum Initiative. Tilgået 18. juni 2019.
http://tref.ie/

Trendall, Sam. "What next for the government's anti-fake news unit?". *PublicTechnology*, 21. december 2018.
https://publictechnology.net/articles/features/what-next-government's-anti-fake-news-unit

U.S. Department of Defense. *Summary of the 2018 National Defense Strategy of The United States of America.* 2018.
https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf

Udenrigsudvalget. "Høring om Magnitsky-listen". Folketinget, 6. juni 2018.
https://www.ft.dk/udvalg/udvalgene/uru/kalender/35571/hoering.htm

United Kingdom Government. *National Cyber Security Strategy 2016-2021.* 2016.
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf

United Kingdom Government. *National Security Capability Review.* 2018.
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/705347/6.4391_CO_National-Security-Review_web.pdf

United States Congress. *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA Patriot Act). Public law 107–56—Oct. 26, 2001* (2001).
https://www.sec.gov/about/offices/ocie/aml/patriotact2001.pdf

UP KRITIS. *Öffentlich-Private Partnershaft zum Schutz Kritischer Infrastrukturen.* Frankfurt: Druck- und Verlagshaus Zarbock GmbH & Co.
KG 2014.
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Kritis/Fortschreibungsdokument.pdf;jsessionid=63AFC8733588446F3B3053D5BEEBFE3E.1_cid341?__blob=publicationFile&v=2

Villesen, Kristian; Kjeldtoft, Sebastian Stryhn. "Offentlige it-projekter går ofte galt. Måske fordi vi privatiserede området i 90'erne og ikke længere har ekspertisen i staten". *Information,* 15. juli 2017.
https://www.information.dk/moti/2017/07/offentlige-it-projekter-gaar-ofte-galt-maaske-fordi-privatiserede-omraadet-90erne-laengere-ekspertisen-staten

Vosoughi, Soroush; Roy, Deb; Aral, Sinan. "The spread of true and false news online". *Science,* Vol. 359, Issue 6380, pp. 1146-1151, DOI: 10.1126/science.aap9559.
https://science.sciencemag.org/content/359/6380/1146

Waterson, Jim. "Google bans Irish abortion referendum adverts". *The Guardian,* 9. maj 2018. https://www.theguardian.com/world/2018/may/09/google-bans-irish-abortion-referendum-adverts

Wessing, Taylor. "German IT security law 2.0 – draft bill of March 2019". *Lexology,* 11. april 2019. https://www.lexology.com/library/detail.aspx?g=8a3936e9-1c10-446d-8179-5e15521a5d3a

Winter, Chase. "EU outlines plans for 'military Schengen zone'". Deutsche *Welle,* 28. marts 2018. https://www.dw.com/en/eu-outlines-plans-for-military-schengen-zone/a-43171043

Young, Zachary. "French Parliament passes law against 'fake news'". *Politico,* 4. juli 2018. https://www.politico.eu/article/french-parliament-passes-law-against-fake-news/