AALBORG UNIVERSITET
STUDENTERRAPPORT
Kandidatspeciale, juni 2023
Cand.scient.soc. i Kriminologi

Udarbejdet af
Kristian Holm
Studienr. 20210774
Uddannelsesinstitution
Det Samfundsvidenskabelige Fakultet, Aalborg Universitet
Studienævn for Kriminologi
Vejleder
Sune Qvotrup Jensen
Antal ord
11478

Misinformation og påvirkningsoperationer:
Et systematisk review af Kina og Irans efterretningsvirksomhed

Abstract

This thesis examines espionage activities, in the form of disinformation and influence operations, conducted by China and Iran. Espionage and counterintelligence operations is a crucial element in every nation's national security. Especially in times of conflict, such as the current Ukraine/Russia conflict, where nation's gets excluded from various cooperation and trading opportunities as a result of political sanctions.

The method in this thesis is based on a systematic review, in order to be able to systematically collect relevant literature on espionage operations carried out by China and Iran, after which the literature is critically assessed and synthesized. The systematic review is based on the guide *Doing a Systematic Review: A Student's Guide* and *Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA)* guidelines in order to conduct a systematic review as accurately as possible.

The literature shows that China and Iran have two different strategies when it comes to espionage, but what they both have in common is that as authoritarian states, they provide their intelligence services with wide authority to conduct these intelligence operations. China and Xi Jinping are primarily focusing on industrial espionage and try to polish the international view of themselves, and appear responsible to their own citizens and allies, where Iran primarily has a defensive strategy to protect themselves from foreign states, mainly the US, dissidents and diasporas Iran perceives as a threat against the regime. The literature shows, that especially cyberoperations sometimes are conducted by non-governmental groups but on behalf of the respective governments.

This thesis concludes, that intelligence operations is conducted by almost every country around the world, even our allies. "Everyone spies" is a common saying in intelligence circles, and especially cyberoperations is an important discipline which is continuously becoming more widespread in intelligence services.

Consequences of espionage operations against Denmark can result in major economic consequences if new technology and knowledge gets stolen, and put the country in a vulnerable position if foreign states use sensitive information as a leverage in international negotiations or if Denmark get dependent on foreign technology such as internet solutions from Chinese tech companies.

Keywords: Systematic review, Iran, China, counterintelligence, influence operations, espionage security

1.0 Indledning **3**

1.1 Problemfelt 4

1.2 Forskningsspørgsmål 5

1.3 Afgrænsning og begrebsdefinitioner 6

1.4 Forskningsdesign 7

2.0 Metode **8**

2.1 Undersøgelsesmetode - litteraturreview som metodologi 8

2.1.1 Indledende søgning 11

2.1.2 Eksklusions- og inklusionskriterier 12

2.1.3 Primær søgning 14

2.2 Analysetilgang 15

2.3 Reducering af bias 16

3.0 Sammenfatning og analyse **17**

3.1 Resultater 17

3.2 Syntese 21

3.2.1 Iran 21

3.2.2 Kina 24

3.3 Delkonklusion 28

4.0 Diskussion **28**

4.1 Metodisk diskussion 28

4.2 Diskussion af resultater 29

5.0 Konklusion **31**

6.0 Litteraturliste **34**

1.0 Indledning

Politiets Efterretningstjeneste (PET) har offentliggjort deres nye Vurdering af Spionagetruslen mod Danmark, Færøerne og Grønland (VSD) hvori de beskriver trusselsbilledet for spionage, samt, at fremmede stater løbende udøver spionage mod Danmark og resten af Rigsfællesskabet (Politiets Efterretningstjeneste, 2023). Ifølge PET kommer spionagetruslen primært fra Kina, Rusland og Iran samt Saudi-Arabien og Tyrkiet, og med den globale udvikling er der opstået et større behov for fremmede stater, for at udføre efterretningsvirksomhed - i form af spionage - mod Danmark (Politiets Efterretningstjeneste, 2023, s. 5). Denne trusselsvurdering er offentliggjort i maj 2023, godt ét år efter Ruslands invasion af Ukraine, hvorfor trusselsvurderingen er mere aktuel end før. Ruslands invasion af Ukraine har ført til sanktioner mod Rusland, som betyder at de i omfattende grad, blandt andet er afskåret fra handels- og samarbejdsmuligheder (Finanstilsynet, 2022), hvorfor de har et større behov for at indsamle oplysninger, om blandt andet den teknologiske udvikling, dansk infrastruktur samt internationale forhold og kapaciteter, hvor de forsøger at undgå sanktioner gennem "frontvirksomheder, skiftende salgsagenter og distributører samt omdirigeringslande" som PET (2023) skriver i sin nye udgave af VSD'en (Politiets Efterretningstjeneste, 2023).

PET nævner i deres VSD, at Kina og de andre lande har det til fælles at de har "vide beføjelser til at udføre spionage mod andre stater" (Politiets Efterretningstjeneste, 2023, s. 7). Kina har eksempelvis, i deres efterretningslov fra 2017, National Intelligence Law of the People's Republic of China (2017), artikel 7 som bestemmer, at *"Kina relativt nemt kan pålægge kinesiske diaspora, altså kinesiske statsborger der er bosat i et andet land, og virksomheder mm. at samarbejde med det kinesiske etpartistyre, hvis det gælder om spørgsmål vedrørende den nationale sikkerhed"* (oversat af PET, Politiets Efterretningstjeneste, 2023, s. 18; også nævnt i Parello-Plesner & Li, 2018, s. 3; National Intelligence Law of the People's Republic of China, 2017). Artikel 7 i den kinesiske efterretningslov, oversat af PET i VSD'en (2023), lyder: *"Enhver organisation og borger skal i henhold til loven støtte, assistere og samarbejde med statens efterretningsarbejde samt beskytte alle hemmelige efterretningsoplysninger, de har fået kendskab til"* (Politiets Efterretningstjeneste, 2023, s. 18).

Kina er et stort land og fylder meget på den internationale scene, og det afspejler sig i, at Kina har ambitioner om at være førende inden for forskellige teknologiske løsninger og sikkerhedspolitiske spørgsmål som også kan medvirke til, at Kina øger deres spionageindsats mod Danmark og resten af Vesten (Sørensen, 2018, s. 18; Politiets Efterretningstjeneste, 2023, s. 16).

Især den kritiske infrastruktur har et særligt fokus når der tales om spionage og kontraspionage. Spionagetruslen retter sig, ifølge PET (2023), blandt andet mod den kritiske infrastruktur som er en vigtig del af vores samfund. Den kritiske infrastruktur kan benyttes som et indflydelsesrigt

virkemiddel i hybrid krigsførelse, hvor blandt andet sabotage er et af virkemidlerne (Poulsen, 2023). Får Kina eller Rusland eksempelvis adgang til - via spionage -, eller viden om kritisk infrastruktur i Danmark, så kan de bruge det til at sabotere forsynings- eller telekabler, eller anvende truslen om dette, til at fordelagtiggøre deres egen sikkerhedspolitiske situation. Det er ifølge PET (2023) derfor vigtigt, at have fokus på disse problemstillinger og have kendskab til principperne i spionage, da det er et vigtigt element i kontraspionageindsatsen, skriver PET i deres nye VSD (Politiets Efterretningstjeneste, 2023, s. 5).

1.1 Problemfelt

O'Flaherty, som er journalist indenfor cybersikkerhed og privatliv, understøtter i en artikel fra Forbes i 2019, at Kinas autoriteter kan pålægge virksomheder at udlevere informationer, der kan være relevante for at nå deres strategiske mål (O'Flaherty, 2019). Hun skriver, at flere netværk, som de amerikanske tele- og teknologiselskaber Verizon og AT&T, har lavet et forbud mod techgiganten Huawei, der fremgik som en sikkerhedstrussel på grund af deres tråde til Kina og kinesiske autoriteter (O'Flaherty, 2019). I artiklen bidrager Timothy Heath, senior international defense research analyst hos RAND Corporation, en delvist offentlig finansieret amerikansk tænketank, og siger, at *"The Chinese state has the authority to demand tech companies like Huawei turn over useful information or provide access to the communications and technologies owned and sold by Huawei"* (O'Flaherty, 2019). Der ses i øjeblikket en lignende problematik med appen TikTok, som med deres udviklervirksomhed, ByteDance, er underlagt den kinesiske efterretningslov da de har hovedkvarter i Beijing og har produkter og services rettet specifikt mod det kinesiske marked (Ørbæk, 2023; ByteDance, u.å.)

Udover, at være i stand til at indsamle viden med det formål at spionere, så udfører nogle nationer også påvirkningsoperationer, spreder misinformation og/eller forsøger at påvirke udenlandske beslutningstagere, for at skabe ustabilitet og usikkerhed, også kaldet "active measures" (Kux, 1985, s. 19). PET (2022) skriver, at der i november 2019 begyndte at florere et brev på forskellige blogs og sociale medier. Brevet var forfalsket, og skulle fremstå som værende fra Grønlands daværende landsstyremedlem for udenrigsanliggender, til USA (Politiets Efterretningstjeneste, 2022, s. 18). I PET's VSD (2022) er det beskrevet, at brevet informerede om, at Grønland snarest muligt ville stemme om uafhængighed fra Danmark (Politiets Efterretningstjeneste, 2022, s. 18). PET (2022) vurderer, at brevet højst sandsynligt var tiltænkt at skabe konflikt mellem Rigsfællesskabet og USA (Politiets Efterretningstjeneste, 2023, s. 33; Svendsen & Larsen, 2019).

Ifølge journalistiske kilder (2022) og PET (2023, s. 17) ser vi også et eksempel fra Kinas side, hvor den kinesisk fødte advokat Christine Lee, som migrerede til Storbritannien som barn, i en årrække var tæt på prominente regeringsfolk og indflydelsesrige personer i forbindelse med hendes virke

som advokat og rådgiver (Politiets Efterretningstjeneste, 2023, s. 17). Det advarede MI5 (Storbritanniens nationale efterretningstjeneste) mod i 2022, hvor der blev udsendt et dokument med billede og navn af Christine Lee (Dahlgaard, 2022). Dahlgaard (2022) oplyser også, at hun nu er beskyldt for, igennem hendes relationer til Storbritannien, at donere betydelige pengebeløb for at kunne påvirke indflydelsesrige personer i det britiske parlament (Dahlgaard, 2022). PET (2023) skriver, at pengene - som i virkeligheden kom fra Kinas kommunistiske parti - forsøgte Christine Lee at sløre, så det så ud som om det kom fra andre britiske organisationer (Politiets Efterretningstjeneste, 2023, s. 17). På den måde, har Kina brugt Christine Lees position - frivilligt eller ufrivilligt - til at skabe magt og eventuelt påvirke britiske embedsfolk, i en retning der er favorabel for Kina.

Spionage er i dag blevet et meget aktuelt emne, både i forhold til Rusland/Ukraine-krisen og konflikten mellem Kina og Taiwan. Den konflikt handler om, at Kinas præsident Xi Jinping mener, at Taiwan bør genforenes med Kina. Taiwan derimod vil beholde deres demokrati og folkevalgte præsident. Aktuelt kører også den såkaldte FE-sag, hvor Lars Findsen, chef for Forsvarets Efterretningstjeneste (FE) er tiltalt for at have lækket højt klassificerede oplysninger og at Forsvarets Efterretningstjeneste har ladet National Security Agency (NSA) aflytte flere europæiske embedsfolk igennem danske internetkabler. Mere om dette er beskrevet i afsnit 2.3. Spionage ses altså fra mange nationer, men der er også forskel på, hvad vi i Danmark accepterer.

Efterretningsarbejdet og spionage er i sagens natur et meget lukket land. Både når der skal forskes, og når der skal efterforskes hændelser med relation til spionage (Redmond, 2010, s. 542). Med den baggrund har specialet altså til formål at skabe en forståelse for, og give indblik i, et ellers forholdsvist underbelyst emne inden for forskningen (Van Cleave, 2013), og bidrage til at give et overblik over, hvad der er af eksisterende litteratur.

1.2 Forskningsspørgsmål

- Hvad er modus operandi i spionageoperationer udført af Iran og Kina, og hvilken betydning kan de have?

1.3 Afgrænsning og begrebsdefinitioner

Redmond (2010) påpeger, at kontraspionage (**C**ounter**i**ntelligence, egen oversættelse til engelsk,) er svær at definere (Redmond, 2010, s. 539). Grundet dets skjulte arbejde, er det et arbejdsområde, der defineres og forklares på forskellige måder fra forskellige synspunkter. Van Cleave (2013) skriver, at kontraspionage er blevet påvirket af både historien, lovgivningen og etik gennem tiden (Van Cleave, 2013, s. 57). Med kontraspionages rødder i både historie, lovgivning og etik forekommer det derfor måske heller ikke så unaturligt, at nogle nationer giver deres efterretningsorganisationer flere beføjelser i deres måde at udføre spionage på, end andre.

Historisk set ændrer efterretningstjenesterne fokus over tid. Under Den Kolde Krig fyldte spionage meget i efterretningstjenesternes arbejde. Det ændrede sig imidlertid med ekspansionen af militante islamister og terrorangrebet på World Trade Center i 2001 og efterretningstjenesterne har siden da haft sit primære fokus på terrorbekæmpelsen. Udgivelsen af PET's første VSD i 2022 og internationale spændinger mellem Vesten og Rusland tyder på, at spionage igen er ved at være en stor del af efterretningstjenesternes opgaveportefølje. Ligeledes når der tales om etik og legitimitet, så nævner Diderichsen (2016), at efterretningstjenesterne har fået tilført betydelige mængde ressourcer og nye magtbeføjelser, som for eksempel PET-loven, i takt med en stigende terrortrussel (Diderichsen 2016, s. 67). Diderichsen (2016) konkluderer dermed, at der synes at være en bred enighed om, at efterretningstjenester er en vigtig brik i forhold til Danmarks sikkerhed (Diderichsen 2016, s. 67). Som jeg introducerede i afsnit 1.3, så kører FE-sagen i øjeblikket, og det skaber nogle problemstillinger for efterretningstjenesterne når vi taler om etik og legitimitet (Diderichsen 2016, s. 67). Lande har derfor med deres forskellige historier, værdier og syn på verden, et forskellige udgangspunkt i hvordan de taler ind i efterretningsarbejdet og hvor mange beføjelser de giver deres efterretningsorganisationer.

Spionage og kontraspionage er to modpoler. Redmond (2010) nævner, at den amerikanske regerings definition af kontraspionage lyder:

> *"Counterintelligence means information gathered and activities conducted to identify, deceive, exploit, disrupt or protect against espionage, other intelligence activities, sabotage or assassination conducted for or on behalf of foreign powers, organizations or persons or their agents, or international terrorist organizations or activities."*
>
> (Exec. Order No. 12333; Redmond, 2010, s. 538).

Kontraspionage handler altså groft sagt om at indhente informationer, så man kan forhindre, at andre nationer indhenter informationer, der kan gøre skade. Kontraspionage skal ses som målmanden i en håndboldkamp, hvor spionage skal ses som spillerne der skal score mål. Det handler om, at få informationer samtidig med at man skal undgå, at modparten får informationer.

I ordene spionage og kontraspionage ligger der adskillige måder at udføre disse discipliner på. Det kan for eksempel være sabotage, terrorisme, påvirkningsoperationer, cyberangreb, modaktioner til at forhindre, at disse spionagemetoder finder sted mod en selv, og så videre. I dette speciale anvender jeg spionage som et paraplybegreb, som omfatter alle de forskellige måder at udføre spionage på. Spionage omhandler dermed også begreberne misinformation og påvirkningsoperationer, som er den form for spionage, specialet ønsker at undersøge.

I artiklen, I Measuring the Effects of Influence Operations som er skrevet af Bateman et al. (2021), beskriver han at forskning baseret på spionage og sikkerhedspolitik fokuserer meget på Ruslands ageren (Bateman, Hickok, Courchesne, Thange & Shapiro, 2021, s. 2). Bateman et al., (2021) skriver, at Rusland er en stor aktør og aktuelt fylder meget i verden med deres invasion af Ukraine, og har ifølge Bateman et al., (2021) "været et stort fokuspunkt i tidligere studier omkring påvirkningsoperationer, selvom det er kendt, at mange andre nationer har kapacitet til at gøre det samme" (Bateman et al., 2021, s. 2). Derfor har jeg valgt, at understøtte og bidrage emnet, ved at inddrage PET's fokuslande fra Vurdering af Spionagetruslen mod Danmark (2022), Iran og Kina, og undersøge deres modus operandi i politiske påvirkningsoperationer og misinformation (Politiets Efterretningstjeneste, 2022).

1.4 Forskningsdesign

Specialets metode vil bestå af et systematisk review til at besvare problemformuleringen, der tager afsæt i specialets afgrænsede problemfelt. Et systematisk review identificerer, udvælger og kritisk vurderer allerede udført forskning med mindst mulig bias. Den systematiske gennemgang følger dermed en klart defineret plan, hvor kriterierne er klart angivet, før gennemgangen udføres for at sikre reliabilitet i undersøgelsen (Andersen, 2010, s. 101; Charles Sturt University, u.å.). Senere i specialet, i afsnit 2.1, vil jeg redegøre for forskellige former for reviews og argumentere for, hvorfor det systematiske review anvendes frem for andre former af reviews.

2.0 Metode

Følgende afsnit vil give en præsentation af specialets metodiske afsæt og hvilke overvejelser der er lagt til grund for, hvorfor et litteraturreview er valgt som metode.

I afsnittet findes flere underafsnit, der hver især vil bidrage til at give specialet den gennemsigtighed, som et litteraturreview kræver. Jeg vil også her argumentere for, hvorfor et litteraturreview er vurderet som den bedst egnede metode i dette speciale. Derefter vil jeg redegøre for, hvilke søgninger der har været startpunktet og hvilke inklusion- og eksklusionskriterier der er blevet fastsat, hvorefter der vil være en præsentation af de databaser og søgeord, der er anvendt til at fremsøge relevant litteratur, der er anvendt i specialet. Afslutningsvis vil jeg diskutere nogle af de opmærksomhedspunkter der findes i et litteraturreview som metode, og hvordan metoden bedst muligt reducerer skævheder i specialet.

2.1 Undersøgelsesmetode - litteraturreview som metodologi

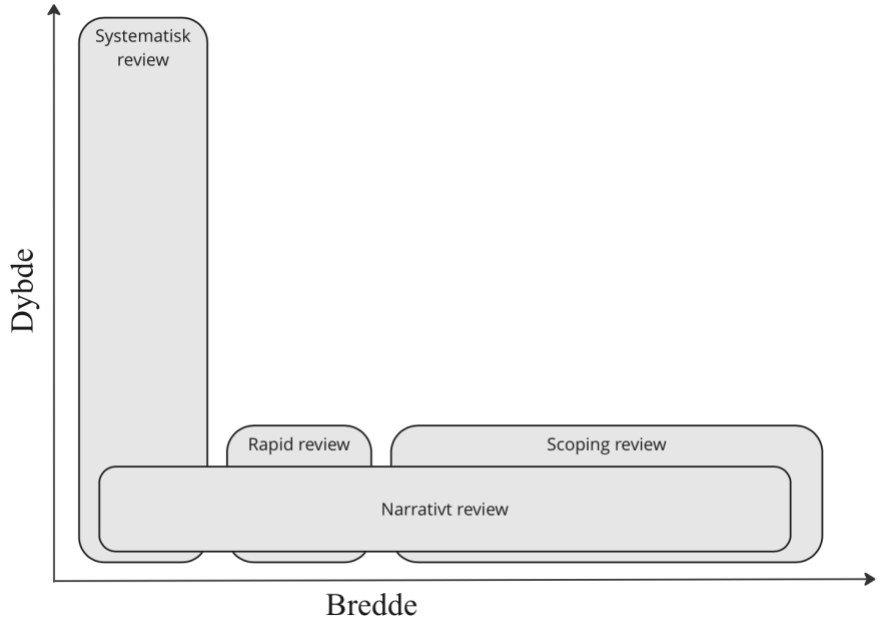
Som ved andre studier, så er det vigtigt at være opmærksom på de faldgruber, der findes indenfor den valgte metode. Litteraturreviews som anvendes i dette speciale kræver, at man anvender præcise, gennemsigtige og detaljerede beskrivelser for den anvendte proces i at lokalisere og udvælge relevant litteratur (Snyder, 2019, s. 334-335; Kugley, Wade, Thomas, Mahood, Jørgensen, Hammerstrøm, & Sathe, 2017, s. 9).

Betegnelsen *litteraturreview* bliver ofte anvendt som et paraply-ord, der dækker over flere former for reviews. At udføre et systematisk review er i sig selv en metode til at reducere bias på, frem for at foretage eksempelvis et narrativt review, rapid review eller et scoping review. De forskellige reviews bygger på samme basis, altså at identificere eksisterende litteratur, men kan være forskellige i selve processen.

Første review jeg vil uddybe er et *narrativt review,* som kan siges at være miniudgaven af et systematisk review og som typisk ikke er så omfattende som et systematisk review. Det kan ifølge Boland et al., (2017) eksempelvis forekomme i et studie, der anvender en anden primær metode, og skal blot præsentere eksisterende litteratur for at fastsætte relevansen af det udførte studie. Narrative reviews bygges således på de samme processer som et systematisk review, for at give læseren et overblik over litteraturen, men uden at forfatteren hævder at reviewet er gennemført (Boland, Cherry & Dickson, 2017, s. 10-12). Andet review er et *rapid review,* eller et *hurtigt* review oversat til dansk, som er et review med en kort deadline (Boland et al., 2017, s. 10-12). Et rapid review kan give et kort overblik over den information man lige nu og her har til rådighed, i situationer der kræver en relativ hurtig beslutning (Boland et al., 2017, s. 10-12). Ifølge Boland et al., (2017), er det derfor accepteret i et rapid review, at man anvender legitime genveje med det

krav, at det er beskrevet i studiet (Boland et al., 2017, s. 10-12). Tredje review er et *scoping review,* som ofte foretages som en mere iterativ proces. Forskere der udfører scoping reviews har ofte det formål at skabe et bredt overblik over litteraturen og de svar der måtte være til bestemte forskningsspørgsmål. Den største forskel mellem scoping reviews og systematiske reviews er altså, at scoping reviews foretages mere iterativt og ikke så dybdegående som et systematisk review (Boland et al., 2017, s. 10-12). Et scoping review kan derfor anvendes som en indledende søgning til en undersøgelse, for at give et overblik over, hvilke undersøgelser og hvilke emner der allerede er undersøgt, inden for det tiltænkte problemfelt.

De forskellige former for reviews er illustreret i figur 1, hvor man kan se hvor meget dybde og bredde, de forskellige former for reviews kræver. Det systematiske review er som nævnt den mest detaljerede og divergerer derfor fra de andre og går mere i dybden. Et rapid review er med dets korte deadline det review, der er smallest og har derfor ikke de samme rigide krav som et systematisk review.



Figur 1. Dybden og bredden af forskellige reviewformer (egen oversættelse fra Boland et al., 2017, s. 13).

Dette speciale anvender derfor et systematisk review, der har nogle strenge og fastsatte retningslinjer for, hvordan det skal udføres, for at kunne identificere litteraturen både i bredden og i dybden samt med henblik på at udføre reviewet så systematisk og detaljeret som muligt.
Boland, Cherry og Dickson udgav i 2017 anden udgave af bogen, "Doing a Systematic Review: A Student's Guide", som kandidatstuderende kan anvende som en step-by-step guide til at anvende systematiske reviews på videregående uddannelser. Dette speciale anvender flowdiagrammet fra "The Preferred Reporting Items for Systematic reviews and Meta-Analyses"

(PRISMA) og gennemgår PRISMA's checkliste for systematiske reviews samt guiden, Doing a Systematic Review: A Student's Guide, for at sikre korrekthed og kontinuitet i afrapporteringen og at metoden bliver anvendt efter gældende retningslinjer (Page et al., 2021).

PRISMA er en anerkendt guide, der blev udarbejdet for at hjælpe forskere med at rapportere og beskrive på en systematisk måde, hvordan deres review er udarbejdet så forskeren kan følge de fastsatte rammer og krav et systematisk review indeholder. Ved at følge PRISMA's guide og checkliste kan jeg sikre, at specialet følger de korrekte retningslinjer for et review (Page et al., 2021). "Doing a Systematic Review: A Student's Guide" skriver mere detaljeret om de forskellige komponenter i et systematisk review og hvordan de udføres. Bogen guider den studerende til, at identificere en problemstilling til reviewet, hvorefter man skridt for skridt kan læse, hvordan man opsætter relevante inklusion- og eksklusionskriterier - som er de kriterier, den fremsøgte litteratur skal overholde for at kunne indgå i reviewet. Det er med til at sikre, at andre efterfølgende kritisk kan gennemgå resultaterne - hvordan man kan udføre sin søgning, hvilke databaser og tidsskrifter der er gode samt en masse gode tips, tricks og råd, der kan bidrage til at udføre et godt review.

I løbet af de seneste tyve år har litteraturreviewet vundet indpas i kriminologien, på trods af at reviews har været anvendt i forskellige videnskaber som metode i mange år forinden. Farrington & Jolliffe (2017) beskriver, at de traditionelle metoder, som blev anvendt i litteraturreviews, har været genstand for en del kritik på grund af deres manglende gennemsigtighed (Farrington & Jolliffe, 2017, s. 2). Det har altså ikke været en klar linje for, hvordan et review skulle udføres, så det kunne genskabes af andre (Farrington & Jolliffe, 2017, s. 2). På baggrund af den problematik blev Cochrane-samarbejdet stiftet i 1993 med fokus på at fastsætte retningslinjer inden for det sundhedsfaglige område (Farrington & Jolliffe, 2017, s. 2; The Cochrane Collaboration, u.å.). Cochrane-samarbejdet er et netværk bestående af blandt andre praktikere og forskere, der udfører forskning indenfor sundhedsvidenskab, med et højt fagligt niveau og engagement. Det er i dag et anerkendt samarbejde, der også publicerer forskningsartikler, der lever op til samarbejdets høje kvalitetskrav.

Når jeg nævner, at reviews i kriminologien har vundet indpas de seneste to årtier, så er det fordi man som følge af Cochrane-samarbejdet stiftede en søsterorganisation i 2000, kaldet Campbell-samarbejdet. Farrington & Jolliffe (2017) nævner, at Campbell-samarbejdet blev stiftet med inspiration fra - og med det samme formål som Cochrane-samarbejdet, at sikre ensartethed i systematiske reviews, blot inden for samfundsvidenskabelige fag såsom kriminologien (Farrington & Jolliffe, 2017, s. 2. Se også Boland et al., 2017, s. 3; Kugley et al., 2017, s. 10).

Typisk udføres et litteraturreview for at evaluere den nuværende viden om et bestemt emne. Det kan med fordel bruges i dette tilfælde, fordi spionage og efterretningsdiscipliner som nævnt, er et underbelyst emne. På den måde er litteraturreviewet nyttigt fordi formålet er, at give et overblik over det valgte forskningsemne, som for eksempel kan være med til at skabe en dagsorden for fremtidig forskning, identificere huller i forskningen, som der kan være mange af i et relativt lukket felt som spionage, eller blot diskutere emnet (Snyder, 2019, s. 334). I dette speciale er formålet, at kortlægge eksisterende litteratur, for at identificere nogle af de videnshuller der måtte være omkring spionage, med henblik på, at informere andre studerende, praktikere og andre interesserede og skabe en baggrund for eventuel fremtidig forskning og give beslutningstagere en baggrundsviden i deres arbejde (Snyder, 2019, s. 339; Boland et al., 2017, s. 2).

I begyndelsen af specialet foretog jeg et scoping review for at skabe et overblik over emnet. Specialet består derfor af to selvstændige søgninger. Et indledende scoping review efterfulgt af hovedsøgningen, det systematiske review som er den bærende metode i specialet.

2.1.1 Indledende søgning

I et review er der naturligt en større mængde litteratur at forholde sig til. For at skabe overblik over, hvilket litteratur der er har været relevant, har jeg anvendt den bibliografiske software Mendeley. Mendeley er en online software, der kan understøtte ved at dele, organisere og gemme litteratur og er i dette speciale anvendt til at kategorisere og gemme litteratur undervejs (Elsevier, u.å.).

Ifølge Dundar og Fleeman anvender scoping-reviewet simple søgeord i kontrast til det primære review, der går i dybden med problemfeltet (Dundar & Fleeman, 2017, s. 63). Det er derfor behjælpeligt til at undersøge nogle af de mest gængse problemstillinger inden for emnet og med til at sikre, at dette speciale ikke undersøger et allerede publiceret reviewspørgsmål, så det bedst muligt kan bidrage til problemfeltet. Reviewspørgsmålet er dermed udformet ud fra en blanding af eksisterende litteratur og deres anbefalinger samt egen interesse og viden i området.

Jeg startede mit scoping review ved at anvende følgende søgeord i Google Scholar: “Espionage”, “Intelligence”,”Influence Operations" og,” counterintelligence”. Søgeordene er valgt ud fra egen viden på området og er afstemt med nogle af de keywords, der oftest fremgår i artikler publiceret i “Policing and Society”, som er en af de mest anvendte tidsskrifter inden for underkategorien Criminology, Criminal Law and Policing, kriminologisk strafferet og politiarbejde” (Google, u.å.).

2.1.2 Eksklusions- og inklusionskriterier

I et systematisk review skal der fastsættes eksklusions- og inklusionskriterier for den litteratur, der kan indgå i selve syntesen. Kriterierne skal bidrage til, at syntesen kun inddrager litteratur der er relevant i forhold til forskningsspørgsmålet samt, at forskere efter noget tid skal kunne foretage et nyt systematisk review med samme udgangspunkt som dette, for at reviewene skal kunne sammenlignes.

Undersøgelser der levede op til kriterierne og kunne inddrages i specialet, er undersøgelser og litteratur, der undersøger og beskriver Kina og Irans metoder ved misinformation- og påvirkningsoperationer. Den inddragede litteratur skal have anvendt kvalitative eller mixed-methods studier i det, at kvantitative studier i form af tal og opgørelser ikke er relevante for besvarelsen af forskningsspørgsmålet. Det er betydningen af modus operandi som dette speciale er interesseret i at undersøge. Litteraturen skal ligeledes være enten dansk- eller engelsksproget. Litteratur skrevet på andre sprog end dansk og engelsk er derfor ekskluderet på grund af sprogbarrieren. Bøger er grundet deres omfang ikke inkluderet. I databasen ProQuest fandt jeg ikke mindre end 103 bøger med anvendelse af mine søgeord, som illustreret i figur 2. Det tyder på, at der findes en relativ bred mængde litteratur om efterretningsarbejdet og spionage, men de er ofte af historisk karakter eller encyclopedias på specifikke geografiske områder eller tidsperioder. Specialet omfatter derfor tidsskrifter, afhandlinger og andre forskningsartikler med det forbehold, at de selvfølgelig overholder de andre inklusionskriterier (Dundar & Fleeman, 2017, s. 66).

Spionage ændrer sig i bølger over tid, alt efter hvordan internationale relationer og sikkerhedspolitik ændrer fokus. Eksempelvis fyldte spionage rigtigt meget under den kolde krig, hvorefter spionagen blev sat i skyggen af terror og truslen fra militante islamister i 00'erne og bliver nu mere og mere aktuelt på grund af blandt andet situationen i Ukraine. Omkring 10 til 20 år tidligere fandt Iran-Irak krigen sted og ændrede for altid politik i området. Det var først i 2013, da Xi Jinping blev præsident i Kina og landet blev mere og mere synlige i deres politik, og hvor indenrigspolitikken handler om, at skolebørn skal vokse op og lære, at være gode borgere i Xi Jinpings styre. Med de historiske begivenheder omkring Iran og Kina, er det besluttet, at litteratur fra før 1990 ikke skal inkluderes.

I planlægningen af søgestrategiens søgeord og inklusions- og eksklusionskriterierne har jeg anvendt" SPIDER-tabellen", som er en måde at bryde forskningsspørgsmålet op, og identificere de forskellige komponenter i forskningsspørgsmålet, hvilket kan bidrage til at beslutte hvilke undersøgelser der skal inddrages i specialet (Methley, Campbell, Chew-Graham, McNally & Cheraghi-Sohi, 2014, s. 2). SPIDER-tabellen er en modificering af "PICO-tabellen", der skal identificere kvantitative studier, til i stedet at identificere kvalitative- og mixed-methods studier

(Methley et al., 2014, s. 2). Cherry et al., (2017) og Methley et al., (2014) viser, at tabellen indeholder begreberne Sample, Phenomenon of Interest, Design, Evaluation og Research Type (Cherry et al., 2017, s. 199-200; Methley, et al., 2014 s. 2-3), og er illustreret med forskningsspørgsmålets identificerede komponenter i figur 2. Design-punktet i tabellen er ikke fastlagt, idet det ikke er vurderet relevant, hvilken måde studierne og litteraturen har indhentet deres kvalitative eller mixed-methods på, da formålet er at identificere modus operandi og betydningen heraf, og ikke hvordan informationen er indsamlet.

Figur 2 som er vist nedenunder, er en illustration af SPIDER-modellen der viser, hvilke komponenter der med fordel kan identificeres i forskningsspørgsmålet for at finde relevante inklusionskriterier. For eksempel står P for "Phenomenon of Interest", og kan være med til at identificere det fænomen i forskningsspørgsmålet, der er relevant at oprette søgekriterier på.

Forskningsspørgsmål	SPIDER	Beskrivelse af SPIDER	Søgeord og trunkering
Hvad er modus operandi i spionageoperationer udført af Iran og Kina, og hvilken betydning kan de have?	**S**ample	Iran og Kina	*"Iran" OR "China"*
	Phenomenon of **I**nterest	Misinformation og påvirkelse	*"Espionage" OR "Intelligence" OR "Counterintelligence" OR "Influence operations" OR "Interference operations" OR "Misinformation"*
			AND
	Design	Ikke fastlagt	
	Evaluation	Modus operandi og betydningen	*"Experience" OR "Modus operandi" OR "Meaning" OR "Consequence"*
			AND
	Research type	Kvalitative og mixed-methods	*Ikke anvendt i søgestreng*

Figur 2: SPIDER-tabel (udarbejdet efter Methley et al., s. 2-4)

Figur 2 illustrerer og viser, hvilke søgeord der indgår i den primære søgning og bidrager til gennemsigtighed i søgningen. Forskningsspørgsmålet er delt op for at identificere emnerne i spørgsmålet, så der kan idenntificeres relevante søgeord. Søgeordene lyder således: "Iran" "China" "Espionage" "Intelligence" "Counterintelligence" "Influence operations" "Interference operations" "Misinformation" "Experience" "Modus operandi" "Meaning" og "Consequence".

Der indgår ikke søgeord relateret til linjen til *research type*. Efter vejledning med en bibliotekar på Aalborg Universitetsbibliotek, blev det frarådet at anvende denne slags søgeord, da det formentlig ville skævvride søgningen. "Research type" er i stedet et af inklusionskriterierne, jeg har med i screeningsprocessen af den fremsøgte litteratur.

Trunkeringsordene "OR" og "AND", er hjælpeord der gør, at databaserne inkluderer de eksakte ord der er sat i citationstegn så søgeordene og de forskellige rækker indgår i litteraturen med søgeord fra de andre kolonner.

2.1.3 Primær søgning

Efter det indledende scoping review har jeg identificeret en række databaser og tidsskrifter inden for kriminologien. Databaserne er fundet ved hjælp af referencer i allerede udfundet litteratur, med vejledning fra universitetets bibliotek samt i den metodelitteratur, specialet anvender, nemlig: Dundar & Fleeman, 2017, s. 67-68; Kugley et al., 2017; s. 14-17. Der er valgt otte databaser og tidsskrifter til den primære søgning og tæller:

Databaser:

- PRIMO
- Campbell Collaboration Crime and Justice library
- Scopus
- Web of Science
- ProQuest

Tidskrifter:

- Policing and Society
- International Journal of Intelligence and CounterIntelligence
- Studies in Intelligence

Ifølge Pilkington og Hounsome (2017) kan det ofte være en fordel at inddrage en informationsspecialist eller lignende, der kan vejlede i effektive søgemåder og databaser (Pilkington & Hounsome, 2017, s. 24). Til den primære søgning har jeg derfor talt med Aalborg Universitet. Jeg kontaktede bibliotekar Jacob von der Hude, der kunne bistå med vejledning til at foretage en korrekt søgning ud fra mine søgeord og kriterier. Til mødet med bibliotekaren anbefalede han, at søge i databaserne Scopus og Web of Science, jeg som studerende har adgang til gennem Aalborg Universitet. Her talte vi om hvordan databaserne er bygget op og hvilken litteratur der kan findes. Efter søgningen i databaserne anvendte jeg selv mine søgeord i de øvrige databaser og journaler jeg har identificeret.

Som nævnt i forrige afsnit, 2.1.2, så er et af inklusionskriterierne, at litteraturen skal være tilgængelig. Det kan variere, hvilke adgange jeg har til forskellig litteratur og i hvilket omfang, alt afhængig af hvilken institution man har et tilhørsforhold til. Det er derfor væsentligt at pointere, at der kan være relevante databaser og dermed relevant litteratur, som det ikke har været muligt at få adgang til (Kugley et al., 2017, s. 13).

Som kandidatstuderende er man naturligt underlagt en deadline på specialet. Det er ifølge Pilkington & Hounsome (2017) derfor essentielt, at det systematiske review bliver planlagt efter, at det skal være klar til en bestemt dato (Pilkington & Hounsome, 2017, s. 23). Det kan sætte nogle begrænsninger, som der normalt ikke vil være i et systematisk review. Som specialestuderende bestræber jeg mig derfor på, at give en begrundelse og forklaring for afvigelser, der eventuelt måtte være fra et udtømmende systematisk review. Det vil ligeledes bidrage til at reducere bias i specialet.

I den primære søgning har jeg undladt at anvende "citation chaining" og "snowball-strategien". Begge strategier handler om, at man undervejs søger relevant litteratur frem, som man finder gennem henvisninger og citationer i den litteratur, der blev søgt frem under den primære søgning (Dundar & Fleeman, 2017, s. 71; Harrits et al., 2010, s. 163). Specialet omfatter altså derfor kun de tidsskrifter, afhandlinger og projekter, der blev fundet i den primære søgning, for at kunne fokusere og gennemgå litteraturen korrekt inden for den fastsatte tidsramme.

2.2 Analysetilgang

Til syntesen af litteraturen, vil jeg anvende "*qualitative meta-narrative"*. Det er blot én metode af mange, der kan anvendes til at analysere kvalitative data i et systematisk review. Cherry et al., (2017) forklarer, at mange af de måder forskere analyserer kvalitative data på i et systematisk review, er baseret på allerede anerkendte analysemetoder, som eksempelvis tematiske analyser (Cherry et al., 2017, s. 203). Cherry et al., (2017) beskriver også, at der bredt set er to måder at kategorisere kvalitativ dataanalyse på i systematiske review. *Integrative approach* som er deduktiv, og *interpretive approach* som er deduktiv (Cherry et al., 2017, s. 204).

Ifølge Cherry et al., (2017) er *Qualitative meta-narrative*-metoden en tilgang, der tillader at sammenfatte og diskutere litteratur med forskellige forskningsdesigns og teoretiske standpunkter (Cherry et al., 2017, s. 206). Reviewets formål er at give et overblik over Kina og Irans misinformations- og påvirkningsoperationer, og kan derfor anvende data uanset hvilket studie det er affodret af. Analysetilgangen kan ud fra denne beskrivelse fremhæve og diskutere Kina og Irans efterretningsvirksomhed, selvom litteraturen har forskellige tematikker og har anvendt forskellige måder fremgangsmåder til at indsamle empirien.

2.3 Reducering af bias

Spionage har i sagens natur et stort politisk fokus. Spionage anvendes netop til at forbedre en nations position i det internationale og sikkerhedspolitiske spil, hvor mange aktører har en interesse. Det er derfor vigtigt, i litteraturudvælgelsen, at være opmærksom på, hvem der har publiceret og skrevet de artikler og den litteratur der anvendes i specialet. Eksempelvis skriver Parello-Plesner og Li (2018) i en artikel udgivet af Hudson Institute, om påvirkningsoperationer begået af det kinesiske kommunistiske parti, og sætter fokus på hvilke modtiltag USA og andre lande kan udføre (Parello-Plesner og Li, 2018). Hudson Institute er en amerikansk tænketank, der vil fremme amerikanske interesser og "*udfordre konventionel tænkning og hjælpe med at styre strategiske overgange gennem tværfaglige studier inden for forsvar, internationale relationer, økonomi, energi, teknologi, kultur og jura"* (egen oversættelse fra engelsk, Hudson Instutite, u.å). Hudson Institute kan derfor have en interesse i at bruge narrativer og informationer, der specifikt taler til fordel for deres interesser, og omvendt kan de bevidst ekskludere positiv information og narrativer, der kan tale til Kinas fordel. At være opmærksom på, hvem der har publiceret udfundet litteratur, er ikke kun et emne bestemt for spionage. Det er også et af kravene, når man foretager et systematisk review, at det er så præcist og processen er så uddybende som muligt.

Det er altså et væsentligt opmærksomhedspunkt i dette speciale, at være kildekritisk og tænke over, hvem de forskellige forfattere og publicerende journaler er. Både på baggrund af emnet i sig selv, og så selvfølgelig fordi et systematisk review kræver, at man kritisk kan vurdere den litteratur, der er inddraget til analysen. Jeg bestræber mig derfor også på, i løbet af specialet, at uddybe, hvem de forskellige forfattere er, og hvilken tidsskrift eller organisation litteraturen er udgivet fra.

Når det gælder spionage handler det om at være dygtigere end sin modstander. Kina er langt fra de eneste, der udfører spionage. USA udfører også spionage i høj grad, hvilket især kom frem i gennem den såkaldte "Operation Dunhammer", som er titelnavnet på den interne undersøgelse, Forsvarets Efterretningstjeneste foretog og afsluttede i 2015. Knudsen (2021) beskriver, at rapporten viste, at amerikanske National Security Agency (NSA), igennem Forsvarets Efterretningstjeneste, "målrettet kunne aflytte og indhente informationer om toppolitikere i Europa" (Knudsen, 2021) og verdens efterretningstjenester samarbejder på kryds og tværs for at dele og få informationer. Den information er vigtig at have in mente i specialet, og især i litteraturudvælgelsesprocessen, så jeg kan undgå, at jeg ekskluderer litteratur, der kan tale imod mit forskningsspørgsmål og dermed kun inkludere litteratur, der kan understøtte specialet. Mit formål er derfor ikke at udfærdige et Kina- eller Iransk-kritisk produkt, men at sætte fokus på, og forstå, den spionage, der aktuelt forekommer fra andre nationer. Når Kina, Iran og Rusland nævnes, er det fordi, det er de lande som Politiets Efterretningstjeneste ser en øget aktivitet fra,

hvilket de nævner i deres Vurdering af Spionagetruslen mod Danmark, Færøerne og Grønland (2023).

Det er også vigtigt at være opmærksom på, hvilken litteratur der indgår i mit review. Et af inklusionskriterier er, at litteraturen skal være enten dansk- eller engelsksproget da jeg ikke læser hverken kinesisk eller persisk, som er modersmålene i de to udvalgte lande. Det giver en naturlig sprogbarriere som ekskluderer litteratur skrevet på andre sprog, men som kunne have været relevant at inddrage i reviewet.

3.0 Sammenfatning og analyse

I følgende afsnit findes en præsentation af resultaterne fra den primære søgning. Afsnittet indeholder en redegørelse for, hvordan litteraturen er fremsøgt, hvor mange resultater der er fundet i hver database, hvilken søgestreng der er anvendt, hvor mange resultater der er screenet og udvalgt, samt en illustration af eksklusionsprocessen. Efterfølgende giver jeg en redegørelse for, hvordan data er blevet kodet og udtrukket fra litteraturen.

Anden del af afsnittet er selve syntesen af den litteratur, der er udfundet. I denne del af afsnittet vil jeg analysere resultaterne og diskutere de forskellige elementer der indgår i litteraturen, som kan bidrage til at besvare mit forskningsspørgsmål. Litteraturanalysen vil tage udgangspunkt i den *qualitative meta-narrative* analysemetode (Cherry et al., 2017, s. 206).

3.1 Resultater

I forbindelse med den primære søgning, har det været nødvendigt at ændre en anelse på den måde, der er søgt på, i de forskellige databaser og tidsskrifter. Den software en database er bygget op omkring er ikke nødvendigvis den samme, og der findes ikke nødvendigvis den samme bagvedliggende struktur i tidsskrifter. Jeg har, hver gang jeg startede en ny søgning, haft udgangspunkt i alle søgeordene, der er illustreret i figur 2. Derefter - hvis der ikke har været nogle resultater - har jeg fjernet et par af søgeordene, en efter en, for at afdække, om der kunne være relevant litteratur der lå inden for eksklusion- og inklusionskriterierne. I og med, at jeg har været nødsaget til at ændre søgestrategi, har jeg derfor, i punktform, indsat en liste over databaser og tidsskrifter med de søgestrenge, hvor resultaterne er fundet ud fra. Jeg har derefter fremhævet hvor mange tidsskrifter, afhandlinger og projekter der har været inkluderet i screeningsprocessen (Dundar & Fleeman, 2017, s. 70). Listen skal dermed bidrage til gennemsigtighed i den primære søgning.

Databaser:

- PRIMO AUB
    - Søgestreng: *Espionage Intelligence Counterintelligence Influence operations Interference operations Misinformation Modus operandi*
    - **2 resultater matcher søgekriterier (til screening)**

- Campbell Collaboration Crime and Justice library
    - Søgestreng: *Intelligence espionage*
    - **0 resultater matcher søgekriterier**

- ProQuest
    - Søgestreng: *espionage Intelligence Counterintelligence Influence operations Interference operations Misinformation Experience Modus operandi Meaning Consequence*
    - **28 resultater matcher søgekriterier (til screening)**

- Scopus
    - Søgestreng: *(TITLE-ABS-KEY (china OR iran)) AND ((TITLE-ABS-KEY (experience OR "Modus operandi" OR meaning OR consequence)) AND (TITLE-ABS-KEY (espionage OR intelligence OR counterintelligence OR "Influence operations" OR "Interference operations" OR misinformation))) AND (LIMIT-TO (SUBJAREA , "SOCI")) AND (LIMIT-TO (LANGUAGE , "English")) AND (LIMIT-TO (OA , "all"))*
    - **57 resultater matcher søgekriterier (til screening)**

- Web of Science
    - Søgestreng: *espionage OR Intelligence OR Counterintelligence OR "Influence operations" OR "Interference operations" OR Misinformation AND Experience OR "Modus operandi" OR Meaning OR Consequence AND China OR Iran*
    - **10 resultater matcher søgekriterier**

Tidsskrifter:

- Policing and Society
    - Søgestreng: *Espionage Intelligence Counterintelligence Influence operations Modus operandi*
    - **0 resultater matcher søgekriterier**

- International Journal of Intelligence and CounterIntelligence
    - Søgestreng: *Espionage Intelligence Counterintelligence Influence operations Modus operandi*
    - **0 resultater matcher søgekriterier**

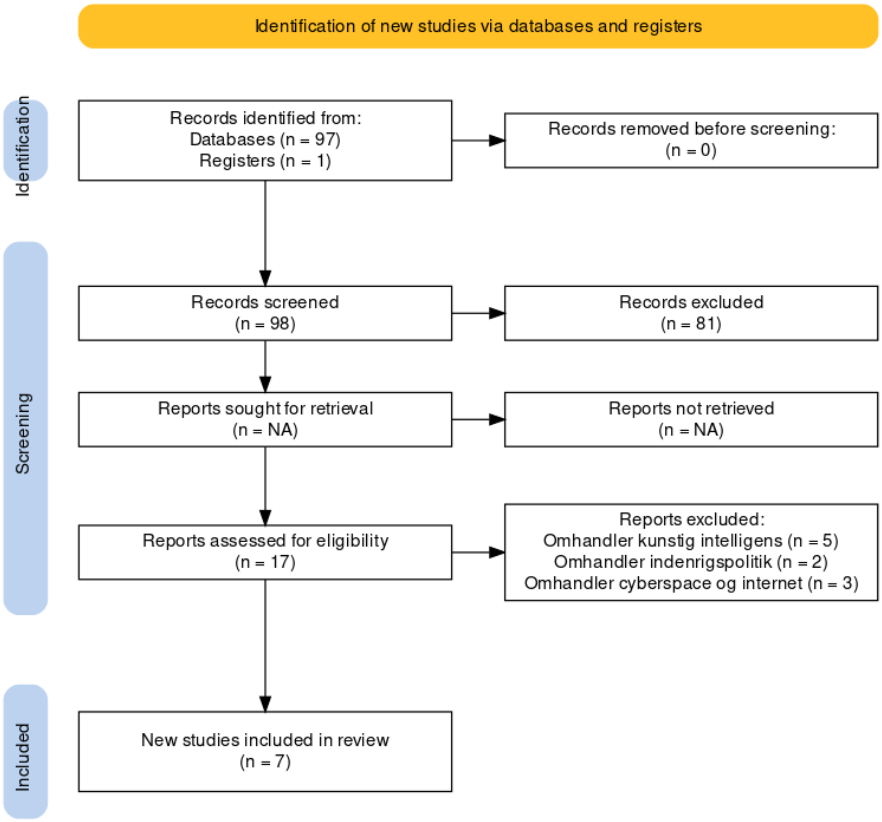
- Studies in Intelligence
    - Søgestreng: *Espionage Intelligence Counterintelligence Influence operations Modus operandi*
    - **1 resultat matcher søgekriterier (til screening)**

Som det ses af listen, identificerede jeg i alt 98 dokumenter. Ud af de 98 dokumenter ekskluderede jeg i screeningsprocessen 81 dokumenter ud fra mine inklusions- og eksklusionskriterier, og endte dermed med 17 dokumenter til gennemgang. Ved screeningen kiggede jeg på titel, abstract og keywords med henblik på at danne et overblik over hvad de enkelte dokumenter omhandlede.

Der fremkommer eksempelvis artikler med overskrifter som *Improving Traffic Safety through Traffic Accident Risk Assessment* og *What Makes a Good Cabman? Behavioral Patterns Correlated with High-Earning and Low-Earning Taxi Driving.* Dem kunne jeg, blot ved hjælp af titel og keywords, vurdere til ikke at handle om efterretningsarbejde eller spionage.

Ud af de 17 dokumenter blev 10 ekskluderet på grund af irrelevans ved nærlæsning. De 10 dokumenter, der blev ekskluderet, omhandlede overvejende kunstig intelligens, cyberspace og indenrigspolitik. Det er dokumenter, der med deres engelske ord *intelligence*, *cyber* og *influence*, ikke blev ekskluderet i screeningen på grund af deres tvetydighed. Der er altså inkluderet i alt syv dokumenter i reviewet.

Nedenstående figur illustrerer, hvor mange dokumenter der er identificeret i henholdsvis databaser og tidsskrifter, hvor mange dokumenter der er screenet og hvor mange der til sidst er inddraget.



Figur 3: PRISMA flow diagram (udarbejdet efter Haddaway, Page, Pritchard & McGuinness, 2022).

Efter at have identificeret de relevante dokumenter, anvendte jeg softwaren NVivo til at udtrække relevante data. Formålet med at udtrække data er at identificere og isolere de informationer, der er vigtige for at kunne besvare mit forskningsspørgsmål (Fleeman & Dunder, 2017, s. 94). Litteraturen der er inkluderet i dette review er valgt, fordi det indeholder data der kan bidrage til besvarelsen af mit forskningsspørgsmål. Den indeholder dog også informationer, som ikke er relevante for dette review.

NVivo er i den forbindelse anvendt til at udtrække og kode de informationer der kan hjælpe med at besvare forskningsspørgsmålet. NVivo er en software, hvori man kan indsætte sit dokument, for derefter at kunne markere de linjer eller afsnit, der vurderes relevant til reviewet. NVivo isolerer efterfølgende de tekststykker man har markeret, så de bliver præsenteret på en kronologisk og overskuelig måde. Overflødigt data bliver derved fjernet.

Jeg har anvendt en deduktiv analysestrategi, til at identificere de tekststykker, der kan bidrage til besvarelsen af mit forskningsspørgsmål og knytte bestemte tematikker til teksten (Jakobsen & Harrits, 2010 s. 177). Forskningsspørgsmålet - med Kina og Irans efterretningsvirksomhed - er allerede forankret i eksisterende viden og begreber forstået på den måde, at jeg ikke med mit forskningsspørgsmål har til formål at generere nye begreber og teorier frem for en induktiv

strategi, hvor hverken teori eller centrale begreber er skrevet på forhånd (Jakobsen & Harrits, 2010 s. 174 - 175, s. 185). Analysestrategien gik således ud på, at kode litteraturen efter koder, der allerede var besluttet på forhånd. De to koder, der blev kodet efter, var Kina og Iran. Ved gennemlæsningen af dokumenterne udtrak jeg altså informationer, der pegede på hvordan enten Kina eller Iran udfører spionage, og hvilke konsekvenser det kan have. På den måde fik jeg en liste over data, der passer til henholdsvis Kina og Iran for et bedre overblik (Jakobsen & Harrits, 2010 s. 182). Listerne over dataudtrækket findes i bilag.

Man kan med fordel være gået mere i dybden med de forskellige koder. Eksempelvis kunne der have været de overordnede koder der hedder *Kina* og *Iran,* samt nogle underkategorier der hver især peger på enten modus operandi eller konsekvenserne, som er de to elementer i forskningsspørgsmålet. Man kan også gå mere i dybden, og kode efter specifikke spionagemetoder som eksempelvis påvirkelse, sabotage eller attentatforsøg, og således kan man fortsætte.

3.2 Syntese

I følgende afsnit, vil jeg præsentere, sammenfatte og analysere den litteratur jeg har fremsøgt i den primære søgning. Afsnittene er delt op, hvor jeg først præsenterer litteraturen på Iran, og dernæst Kina. Slutteligt vil jeg konkludere på syntesen og komme ind på forskelle og ligheder, der ifølge litteraturen er på de to landes efterretningsvirksomhed.

3.2.1 Iran

Infiltration og attentatforsøg

Nogle af de emner der i overvejende grad fylder i litteraturen på Irans efterretningsvirksomhed er spionage af attentatforsøg, infrastruktur og cyberangreb. Der findes flere eksempler på, at Iran har infiltreret netværker og spioneret på eksempelvis forskellige dissidenter og faciliteter rundt om i verden. Dissidenter er en form for systemkritikere. I dette tilfælde med Iran, kan det være en eller flere personer, der åbenlyst kritiserer og taler imod sit lands politiske styre.

Den tidligere efterretningsofficer hos New York Police Department, Ioan Pop og tidligere direktør for samme enhed og nu professor ved Columbia Universitet, Mitchell Silber (2020) skriver, at to mænd med iranske rødder erkendte sig skyldig i at holde øje med to jødiske faciliteter og en gruppe af iranske dissidenter i USA. De arbejdede begge på vegne af den iranske regering (Pop & Silber, 2021, s. 159). Det iranske styre ses så autoritære, at de i sjældne tilfælde planlægger attentatforsøg for at "skille sig af" med den trussel de ser dissidenter som, for at sikre deres succes i hjemlandet uden modstand. Ifølge Pop og Silber (2021), tror man ligeledes, at Iran har

slået flere dissidenter ihjel, herunder Shahpour Bakhtiar, tidligere premierminister i Iran (Pop & Silber, 2021, s. 164).

Et politisk attentat kræver oftest grundig planlægning og informationsindhentning. Iran har ifølge Pop & Silber (2021), i forbindelse med deres indhentning, anvendt efterretningsdisciplinen HUMINT (Human Intelligence). HUMINT handler om at anvende menneskelige kilder, der som regel har en relation til de netværk og miljøer, man har en interesse i at vide noget om. Med andre ord, så infiltrerer Iran forskellige diaspora-netværker for at holde øje med dem, skriver Pop & Silber (2021) (Pop & Silber, 2021, s. 164). Diaspora er en betegnelse, der bliver anvendt om personer eller befolkningsgrupper, der lever i et andet land end deres hjemland, frivilligt eller ufrivilligt. De kan i den forbindelse både være indvandrere eller flygtninge, men er ikke nødvendigvis en systemkritiker som dissidenter.

Der har selv i Danmark været attentatforsøg på iranske dissidenter. I 2018 lukkede politiet hele Sjælland ned, fordi man mente, at der var en konkret trussel mod en gruppe af iranske dissidenter i Ringsted. Det var en gruppe af ASMLA-medlemmer (Arab Struggle Movement for the Liberation of Ahwaz), en oprørsgruppe, som den iranske regering ser som et terrornetværk. Der blev senere anholdt en person, som menes at have planer om dette attentat, men som aldrig nåede at blive udført. Det var en stor sag, som blev endnu mere spektakulær da det senere fremgik i sagen, at alt imens disse eksiliranere var beskyttet af livvagter i PET, blev de sigtet for blandt andet spionage til fordel for Saudi-Arabien (Foght & Fastrup, 2020; Pop & Silber, 2021, s. 167 - 168). Journalistiske kilder påpeger, at den betydelige mængde penge, de fik af den saudiarabiske efterretningstjeneste, skulle være blevet anvendt til terrorfinansiering i Iran (Foght & Fastrup, 2020).

Spionage af infrastruktur

Kritisk infrastruktur bliver mere og mere betydelig i hybridkrig og derfor også et mål for spionage. Ved at lamme kritisk infrastruktur - om det er transport eller forsyningskæden på elektricitet og vand - kan man skabe en ikke ubetydelig uro i et samfund. Krigen i Ukraine har især været med til at rette myndighedernes fokus mod forsyningssikkerheden. Med undersøiske kabler og rør på dansk territorium er vi et populært mål, og myndighederne ser flere og flere hændelser med mistænkelig og spionagelignende adfærd i danske farvande hvor der findes kritisk infrastruktur.

Det er ikke kun i forbindelse med Ukraine og Rusland, at Danmark skal være opmærksom på kritisk infrastruktur. I Pop & Silber (2021) er der beskrevet en række hændelser, hvori de amerikanske myndigheder har fundet mistænkelig adfærd fra iranere eller personer knyttet til Iran. En af de ting som Pop & Silber (2021) nævner er, at der mellem 2002 og 2010 sås iranske diplomater med en underlig og afvigende adfærd. Blandt andet ved at tage billeder og videofilme

rundt i New York (Pop & Silber, 2021, s. 159). To mænd med tilknytning til den iranske FN-mission blev udvist for spionage, efter at have filmet New Yorks metrosystem. Senere blev to mænd opdaget i at videofilme andet offentlig transport og infrastruktur på trods af flere advarsler fra USA (Pop & Silber, 2021, s. 159) og i 2005, 2008 og 2010 var der lignende hændelser hvor fire personer indrømmede at være associeret med den iranske regering. Der var dog ingen, der blev dømt (Pop & Silber, 2021, s. 159).

Der er altså tydelige tegn på, at Iran blandt andet anvender videofilm og billeder i deres dataindsamling for at kortlægge amerikansk infrastruktur. Ved at kortlægge USA's, eller andre landes for den sags skyld, infrastruktur, kan man få indblik i eventuelle svagheder på infrastrukturen. Infrastrukturen er som beskrevet et vigtigt element i hybrid krigsførsel og kan være et effektivt pressionsmiddel i internationale forhandlinger og aftaler.

Ved at stjæle data og teknologi på infrastruktur, kan Iran forhindre USA i at udbrede og eventuelt sælge deres teknologi til andre lande. Ligesom med alle andre virksomheder, er teknologi oftest rettighedsbeskyttet, hvorfor spionage i den forbindelse kan ende som tyveri af forretningshemmeligheder og kan føre til betydelige økonomiske tab hos modparten, i denne forbindelse USA samt en svækkelse af forsyningssikkerheden.

Cyberoperationer

Det er snart ikke længere en nyhed eller overraskelse, at verden bliver mere og mere digitaliseret. Derfor findes der også en øget efterretningsaktivitet i cyberverdenen. Assoudeh (2020), assisterende professor ved Nevada Universitet, skriver i hendes afhandling at Iran løbende bliver mere afhængig af cyberoperationer for at kunne monitorere deres fjender, som blandt andet kunne være dissidenter i både indland og udland. Ifølge Assoudeh (2020 blev Iran i 2012 beskyldt for at stå bag en række cyberangreb på forskellige amerikanske institutioner (Assoudeh, 2020). Hændelser der altså er med til at understøtte påstanden om, at Iran har kapacitet og intentioner om at anvende cyber i deres politiske strategi.

Assoudeh (2020) skriver i sin forskning, at Iran har to typer cybermilits: en offensiv og en defensiv. Den offensive er den der er involveret i cyberaktiviteter sigtet mod andre lande med henblik på at udføre datatyveri, sabotage, spionage og så videre (Assoudeh, 2020, s. 214). Den defensive cybermilits er nok den mest udbredte i Iran. De positionerer sig ifølge Assoudeh (2020) heller ikke offentligt i deres cyberstrategi, og deres cyberstrategi er derfor primært styret af internationale forhold. Et eksempel er USA og Irans atomaftale fra 2015, som den daværende amerikanske præsident, Donald Trump, trak sig ud af i 2018 (Assoudeh, 2020, s. 216). Assoudeh (2020) skriver, at det fordrer, at Iran igangsætter påvirkningskampagner for at beholde en vis

troværdighed over for Irans borgere og allierede (Assoudeh, 2020, s. 216). Den defensive strategi er det, vi i Danmark også udfører - dog med en anden strategi - og kalder kontraspionage.

Iran anvender ifølge Assoudeh (2020) også deres defensive strategi, til at opruste deres cyberaktiviteter som følge af, at Iran er et af de mest hyppige mål for amerikansk spionage (Assoudeh, 2020, s. 218). Som et svar derpå, skriver Assoudeh (2020), at Iranske *Advanced Persistent Threat (APT)* grupper har avanceret sig meget det sidste årti, og har udført avancerede cyberangreb i USA med henblik på at samle information (Assoudeh, 2020, s. 16). Det tyder på, at Iran arbejder målrettet på at dygtiggøre deres spionageoperationer for at forebygge angreb på landet. Og med Irans avancering inden for cyberangreb, er der noget der tyder på, at truslen fra Iran vokser i takt med deres kompetencer på cyberområdet.

3.2.2 Kina

Kinas efterretningsvirksomhed

Der findes lidt mere litteratur om Kinas efterretningsarbejde, end der gør om Irans. I gennemlæsningen identificerede jeg nogle metoder, som går igen i litteraturen om Kinas efterretningsarbejde. De tæller cyber, sabotage, påvirkningsoperationer mv.

En ting der er værd at lægge mærke til, når man studerer Kina og dens efterretningsarbejde, er måden hvorpå de indsamler deres informationer. Aldrich og Kasuku (2012) skriver i en artikel om Kinas efterretningsvirksomhed, om en disciplin de kalder *netspionage* og beskriver samtidig, at sondringen mellem kinesisk efterretningsanalyse og kinesiske tænketanke er forholdsvist tyndt og at den nationale sikkerhed fokuserer meget på forskningsinstitutioner, med forbindelser til statsapparatet (Aldrich & Kasuku, 2012, s. 12). Det ses eksempelvis med China Institute for International Strategic Studies, den kinesiske pendant til Dansk Institut for Internationale Studier (DIIS), som Aldrich og Kasuku (2012) skriver er ledet af den samme person, der leder Kinas militære efterretningsorgan (Aldrich & Kasuku, 2012, s. 12). Der foregår altså et ret tæt samarbejde mellem efterretningstjenesterne og forskningsinstitutioner, som kan have den fordel for Kina, at de har et forholdsvist kort informationsflow, når ekstern forskning finder oplysninger som Kinas regering synes er relevant for deres strategi.

Ifølge Aldrich og Kasuku (2012) er *netspionage* et godt eksempel på kinesisk spionage, hvor man i stor grad, tilsigter at indhente sensitive oplysninger frem for nødvendigvis klassificerede oplysninger (Aldrich & Kasuku, 2012, s. 13). Aldrich og Kasuku (2012) skriver, at Kina i den forbindelse anvender et netværk af blandt andet forskere og forretningsfolk samt cyberangreb, til at indhente oplysninger om teknologi og militær (Aldrich & Kasuku, 2012, s. 13). Det kan være en forklaring på, hvorfor det amerikansk-kinesiske samarbejde på forskningsområdet i en

årrække har været nedadgående. Det tyder på, at der hersker en vis tvivl om, hvorledes landene indhenter følsomme oplysninger fra hinanden gennem deres forskningsprogrammer.

Kinas præsident Xi Jinping har ifølge Crandall (2020), Professor ved Kansas Universitet i USA udtalt, med hans ind i mellem hårde retorik *"government, military, society and schools, North, South, East and West, the Communist Party controls them all"* (Crandall, 2020, s. 5) og nævner i sin afhandling, at ifølge *United States Defense Department's 2019 Report to Congress,* udfører Kina påvirkningsoperationer i USA og andre lande for at stille sig i en bedre position internationalt (Crandall, 2020, s. 5).

Madelyn Ross, Washington Director ved Hopkins-Nanjing Center for Chinese & American Studies, Johns Hopkins University School of Advanced International Studies, bekræfter Crandalls påstand om, at Kina og USA's samarbejde på forskningen, har været anspændt de seneste år. Ross (2021) forklarer, at påvirkningsaktiviteter især under Trump-administrationen, har været et fokuspunkt i henhold til et amerikansk-kinesisk samarbejde på forsknings- og uddannelsesområdet og nævner, at påvirkningsoperationer var begrebet som analytikere startede med at anvende til at beskrive en manipulering af den offentlige mening i udlandet (Ross, 2021, s. 232).

For at vende lidt tilbage til Kinas efterretningslov, som er beskrevet i afsnit 1.0, beskriver Jüris (2020) et projekt, der har til formål at forbinde Europas, Ruslands og Asiens internetbrugere med undersøiske kabler. Dette projekt har et samarbejde med Huawei som leverer den tekniske løsning til projektet (Jüris, 2022, s. 191). Huawei kan derfor, ligesom eksemplet i afsnit 1.1, blive pålagt at samarbejde med de kinesiske efterretningsmyndigheder. Og undersøiske kabler, der forbinder internettet i Europa, Asien og Rusland kan være en guldgrube af oplysninger for ikke bare Rusland og Kina, men stort set alle lande der udfører efterretningsarbejde.

At tappe informationer fra kabler, lyder også som noget vi har hørt før. Amerikanerne har gjort lige præcis dette, som eksemplerne i afsnit 1.1 og 2.3 beskriver. Igen er det vigtigt at huske på, at den litteratur der indgår i dette speciale med al sandsynlighed er meget vestlig orienteret og derfor ikke beskriver vores allieredes efterretningsoperationer så omfattende, som de beskriver Iran og Kinas. Netop ordet "allierede" er et vigtigt element i denne analyse, da litteraturen primært omhandler Kina, Iran og Rusland selvom USA og andre vestlige lande udfører samme efterretningsarbejde. Forskellen er, at USA og Vesten ses som allierede i international politik, hvorimod Kina og Iran ses med en anden dagsorden, hvorfor deres efterretningsarbejde altså kategoriseres som potentielle trusler.

Misinformation og polering af landet

Kina har fået ry for at være et af de hårdeste lande hvad censurering og propaganda angår. Assoudeh (2020) skriver om forskellen mellem strategier på cyberområdet i Vesten og strategierne i lande som Kina og Iran. Mens Vesten ser truslen som en teknisk udfordring, der kræver tekniske løsninger, så er cyberstrategien i Kina og Iran lige så fokuseret omkring misinformation og propaganda og påstår at Vesten ser Kina og Irans strategi som en metode til bevidst at skabe uro eller splid internationalt (Assoudeh, 2020, s. 3).

At Vesten ser Kina og Irans strategi som en metode til at skabe uro er også korrekt, ifølge de danske efterretningstjenester. Forsvarets Efterretningstjeneste (2022) skriver, at blandt andet Kina er i stand til at udføre disse påvirkningsaktiviteter, som kan få landet til at fremstå som en ansvarlig stormagt og bevidst sprede misinformation og anvende falske profiler (Forsvarets Efterretningstjeneste, 2022, s. 32). FE (2022) skriver også, at Kina i forbindelse med COVID-19, har forsøgt at sprede misinformation ved at påstå, at virussen skulle stamme fra amerikanske laboratorier i de gamle sovjetlande (Forsvarets Efterretningstjeneste, 2022, s. 32). Der fremgår altså af litteraturen, at Kina anvender påvirkningsoperationer til, at polere det internationale syn på landet.

Vincent Chang, assisterende professor ved Leiden Universitet, kommer med et eksempel på, at Kina forsøger at fremstå som en ansvarlig stormagt. Chang (2022) skriver i en artikel om Miles Yu, en kinesiskfødt amerikaner, som har skrevet flere Kina-kritiske artikler og var Kina-rådgiver under Donald Trumps administration (Chang, 2022, s. 11). Her beretter han om, hvordan Miles Yu senere blev et mål for mange af Kinas internetbrugere, og blandt andet kaldte ham bedrager og *"The dog who helped the abuser"* (Chang, 2022, s. 11). Det endte ifølge Chang (2022) med, at Kinas Kommunistiske Partis dagblad, People's Daily, startede en hadkampagne mod Miles Yu, som resulterede i, at hans familie fornægtede ham og fik hans navn fjernet fra et monument over ærede forskere (Chang, 2022, s. 11).

Litteraturen viser altså eksempler på, at Kina anvender spionagemetoderne til blandt andet, at fremstå som en ansvarlig supermagt i en international kontekst. Det er også det, som vi ser efterretningstjenesterne skrive om (Forsvarets Efterretningstjeneste, 2022; Politiets Efterretningstjeneste, 2023). Men som Assoudeh (2020) skriver i hendes afhandling, så har Kina blot en anden strategi end vesten, og Kina ser på den anden side helt bestemt vesten - og især USA - som en trussel, der forsøger at forhindre Kinas naturlige udvikling og indflydelse internationalt.

Cyber og sabotage

Cyberspionage og sabotage er - ligesom en del af Irans portefølje - også set i Kinas værktøjskasse af spionagemetoder. Assoudeh (2020) beskriver konkret, hvordan Kina, Iran og Rusland kan anvende cyber til spionage. Assoudeh (2020) beskriver hvordan cyberspionage-operationer er eskaleret, og lande som Kina, Iran og Rusland i 2018 udførte cyberangreb med hjælp fra Advanced Persistent Threat (APT) grupper, og ofte kører med langsigtede strategier. Disse grupper er, ifølge Assoudeh (2020), ofte støttet eller associeret med de respektive lande, de arbejder for (Assoudeh, 2020, s. 2 og 111).

Assoudeh (2020) skriver ligeledes om, hvordan Kinas præsident, Xi Jinping, har planer om at gøre Kina til en supermagt inden for cyber, og foreslog i 2017 andre lande, at de kan drage fordel af Kinas cyberstrategi (Assoudeh, 2020, s. 102). Her kan Kinas påvirkningsstrategier, som Chang (2022) beskriver, også være med til at bidrage til, at Kina fremstår som en ansvarlig stormagt (Chang, 2022, s. 11). Det kan være med til at bekræfte påstanden om, at Kina potentielt kan blive en større trussel inden for cyberområdet, hvis store dele af jordens internetstyring bliver varetaget af Kina, og derved får et større politisk forhandlingsmandat.

Med den teknologi som Kina allerede besidder, påstår Assoudeh (2020), at Kina potentielt set ville kunne forstyrre amerikansk infrastruktur gennem cyberangreb, og selvom det måske er midlertidige forstyrrelser, så kan det medføre betydelige konsekvenser (Assoudeh, 2020, s. 16). Uanset om det er Kina, Rusland, eller USA og andre vestlige lande, der besidder sådanne kapaciteter, så er det potentielt set en trussel for Danmark i og med, at Danmark i høj grad er afhængig af ekstern forsyning og internationalt samarbejde.

Cyberaktiviteter ses at fylde meget i litteraturen. Det kan dels være på grund af digitaliseringen, men kan også være et resultat af, at det er en mere "synlig" form for spionage end HUMINT. Aktivitet på nettet og i cyberverdenen vil altid have et digitalt fodspor, det gælder bare om at skjule det godt nok. Bliver cyber brugt til sabotage i en eller anden form, så bliver man ret hurtigt bekendt med, at det er et angreb der er sket, hvor man ved HUMINT bedre kan operere i det skjulte uden at det bliver detekteret. Det kan være et par forklaringer på, hvorfor der findes mere forskning på cyberspionage, end der gør på eksempelvis HUMINT-aktiviteter.

3.3 Delkonklusion

I sammenfatningen af litteraturen ses der både ligheder og forskelle i Kina og Irans modus operandi i spionageaktiviteter. Begge lande ses at have cyberaktivitet i deres strategier for spionage. Blandt andet for at monitorerer forskellige netværk, beskytte landet mod udefrakommende spionage, og for Kinas vedkommende, til at dele informationer der skal få landet til at fremstå som en ansvarlig stormagt og begrænse ytringsfriheden for systemkritikere og informationer der fremstår kritisk overfor præsident Xi Jinping og Kinas kommunistiske parti. Litteraturen har vist, at for Irans vedkommende, er spionageaktiviteterne blandt andet rettet mod dissidenter og andre trusler, der kan være i mod det autoritære styre. Det er endda beskrevet eksempler i litteraturen, hvori Iran skulle have udført både succesfulde og mislykkede attentatforsøg rundt om i verden. Ved Kina og Irans spionageoperationer kan der være konsekvenser som økonomiske tab samt utryghed og usikkerhed for Danmark.

4.0 Diskussion

Dette afsnit vil diskutere specialets metodiske valg og resultaterne, der er fundet i litteraturen. Syntesen har vist, hvordan modus operandi ser ud, i henholdsvis Kina og Irans spionageaktiviteter. Den metodiske diskussion vil præsentere alternativer til metodevalget, hvor man ved brug af disse, formentlig vil kunne præsentere nogle andre resultater. I diskussionen af resultater, vil jeg bygge videre på emner der allerede er blevet introduceret gennem specialet. Navnligt hvilken litteratur, der er fundet ud fra mine søgekriterier, og hvilken af denne litteratur, der ikke er inddraget i specialet.

4.1 Metodisk diskussion

Gennemsigtighed og præcise regler er nogle af de vigtigste punkter i et systematisk review. Det skal kunne genskabes. I Pilkington & Hounsome (2017) er det nævnt, at hvis man som specialestuderende anvender et systematisk review som den primære metode, så kan der ofte være nogle andre kriterier, fastsat af universitet og format for specialet, som der ellers ikke er i et systematisk review (Pilkington & Hounsome, 2017, s. 23). I den metodiske diskussion vil jeg derfor diskutere nogle af de valg og alternativer, jeg har taget i specialet.

I afsnit 2.1.3 er det beskrevet, at som kandidatstuderende er det nødvendigt at planlægge sit review efter en deadline, som oftest er sat af uddannelsesinstitutionen. Havde der ikke været det, er der en række punkter i specialet, jeg kunne have udvidet og uddybet. Eksempelvis havde *citation chaining*-metoden og snowball-sampling (Dundar & Fleeman, 2017, s. 71; Harrits et al., 2010, s. 163), været ønskelig at udføre i og med, at det kunne have ført mig til litteratur, der ikke nødvendigvis har fremgået i tidsskrifterne eller databaserne jeg har søgt ned i. I den forbindelse, så kunne man med fordel have efterspurgt artikler hos forfatterne selv, hvis ikke de har været

identificeret med *citation chaining*-metoden. Med økonomisk understøttelse ville det også være muligt at få adgang til litteratur, der kræver et betalingsabonnement, hvilket der er op til flere databaser og tidsskrifter, der gør.

Jeg identificerede i flere tidsskrifter, at der var hentet domsdokumenter i forbindelse med hændelser relateret til spionagesager. I dette speciale kunne man også have identificeret de hændelser der har været i Danmark vedrørende spionage og derefter søgt aktindsigt i de relevante domsdokumenter. Med disse domsdokumenter ville det være muligt at kortlægge den præcise metode, som udenlandske efterretningstjenester anvender i spionageoperationer på dansk jord og derved få et mere nøjagtigt billede af modus operandi ved konkrete hændelser. Et opmærksomhedspunkt her er, at når sager omhandler spionage, så vil domsdokumenter ofte være fortrolige idet de omhandler statens sikkerhed.

I planlægningsfasen af dette speciale, havde jeg med i overvejelserne, om specialet skulle være bygget op omkring kvalitative interviews med en induktiv analysetilgang. Ideelt ville semi-strukturerede interviews med fagpersoner, være i stand til at levere førstehåndsviden til forskningsspørgsmålet, hvorefter interviewene kunne være kodet med en induktiv tilgang, så temaer der ellers ikke ville være belyst, kunne identificeres ud fra de respektive interviews (Jakobsen & Harrits, 2010 s. 174 - 175). I et semi-struktureret interview har man muligheden for at afvige fra interviewguiden og få uddybende svar fra informanterne. Det er således muligt at indrette indsamlingen af data efter kontekst (Harrits et al., 2010, s. 144).

Problemet er blot, at efterretningsarbejdet - og især spionage og kontraspionage - som bekendt er et lukket land og de fagpersoner der findes på området, opererer i det skjulte. PET-agenter er som national sikkerhedsmyndighed, der arbejder med klassificerede oplysninger, underlagt "*Cirkulære om sikkerhedsbeskyttelse af informationer af fælles interesse for landene i NATO eller EU, andre klassificerede informationer samt informationer af sikkerhedsmæssig beskyttelsesinteresse i øvrigt"* (Justitsministeriet, 2014). En lov der resulterer i, at de ikke kan stille op til interviews vedrørende deres arbejde. Jeg vurderede derfor, at der ikke ville kunne indsamles nok materiale til at besvare mit forskningsspørgsmål med kvalitative interviewformer.

4.2 Diskussion af resultater

Der er meget begrænset forskning af den lukkede verden efterretningsarbejde er. Det har dog været muligt at finde eksempler på, hvordan Iran og Kina tidligere har udført efterretningsvirksomhed og hvilke strategier der dominerer. Det er vigtigt at være opmærksom på, at litteraturen er baseret på tidligere hændelser og sager, der er kommet frem i offentligheden, og er derfor ikke nødvendigvis et nutidigt billede af, hvordan Kina og Iran i dag udfører spionageoperationer. Spionage er konstant i bevægelse og ændrer sig hele tiden i takt

med, at efterretningstjenesterne bliver afsløret eller opfinder nye metoder til, at udføre deres operationer på. Resultaterne i specialet er derfor et overbliksbillede på, hvordan Kina og Iran førhen har udført spionageoperationer, og ikke et nutidigt billede eller et bud på, hvordan spionageoperationer vil se ud i fremtiden.

Søgekriterierne jeg har sat op til den primære søgning, kan også være med til at farve litteraturen i en bestemt retning. I og med, at et af kriterierne var, at litteraturen skulle være enten dansk- eller engelsksproget, så er der risiko for, at litteraturen jeg har inddraget, er fokuseret omkring Vestens syn på Asien og Mellemøsten og ikke omvendt. Havde jeg været i stand til at inddrage litteratur på kinesisk og persisk, ville jeg være i stand til at fremsætte forskellige synspunkter på samme emne og konklusionen ville formentlig være anderledes.

Med udelukkende engelsksproget litteratur, vil jeg referere tilbage til afsnit 2.3, hvor jeg skriver, at det er vigtigt at være kildekritisk i et systematisk review. Med inddragelsen af udelukkende engelsk litteratur, er en overvejende mængde af litteraturen udfærdiget af amerikanske forfattere og tænketanke, som kan resultere i at litteraturen - bevidst eller ubevidst - er skrevet ud fra amerikanske interesser og data. Et eksempel er Assoudeh (2020), der i hendes afhandling jævnligt refererer til Freedom House, en amerikansk-baseret NGO, der i 2016 modtog 86% af deres finansiering i donationer fra den amerikanske regering (Freedom House Inc., 2016, s. 21). Freedom House kan altså have interesse i at fremme amerikanske synspunkter i deres publikationer, for at sikre sig fremtidige donationer fra den amerikanske regering.

5.0 Konklusion

Verden har ændret sig en del på det sikkerhedspolitiske område det seneste års tid, og spionagetruslen øges. Jeg har derfor foretaget et systematisk review, med det formål at undersøge, hvordan Kina og Iran udfører spionageoperationer, og hvilken betydning disse kan have for Danmark. Det har jeg gjort ved at indsamle relevant litteratur inden for området, hvor efter jeg har identificeret relevant data, og slutteligt lavet en sammenfatning, af de fremsøgte resultater.

Ved at kode litteraturen har jeg fundet, at efterretningsarbejde og spionage er en vigtig del i det internationale sikkerhedspolitiske spil, hvor mange lande har interesse i, at være på forkant. Kina og Iran er to lande, der ses med forskellige strategier på spionageområdet. Litteraturen peger på, at Kina har store ambitioner om at være en ansvarlig stormagt, der har meget indflydelse på teknologiindustrien. Med Kinas ambitioner, og Xi Jinping der sidder tungt på Kinas kommunistiske parti, anvender Kina og de Kinesiske efterretningstjenester overvejende påvirkningsoperationer, censurering og misinformation til at polere det internationale syn på sig selv, så både Kinas egne borgere og deres allierede, ikke kritiserer styret og Xi Jinping.

Iran derimod, har en strategi der overvejende handler om defensive operationer - altså fokuserer på deres kontraspionageindsatser - fordi Iran historisk set har været et populært mål for spionageoperationer udført af især USA. Iran avancerer kontinuerligt deres spionageindsatser, for at være i stand til at beskytte sig selv, hvorimod litteraturen peger på, at Kina arbejder med en offensiv strategi.

Iran er med dets autoritære styre, også fokuseret på systemkritikere, der kan udgøre en trussel for regimet. Litteraturen viser, at der har været flere eksempler på, at Iran har været beskyldt for at udføre attentatforsøg på iranske dissidenter rundt om i verden. Selv i Danmark, har der været en konkret trussel mod iranske AMSLA-medlemmer, der var mål for et attentatforsøg.

Det tyder altså på, at Iran holder et skarpt øje med dissidenter og andre netværk rundt om i verden, for at kunne afværge eventuelle angreb på det iranske styre. Iran benytter i den forbindelse også sabotage og infiltration af forskellige diaspora-netværker til at indsamle informationer de finder relevante. Litteraturen kommer her med flere eksempler på, at Iran har infiltreret dissidenter og spioneret mod jødiske faciliteter.

I dag tales der meget om teknologiske muligheder og cyberangreb, når vi taler om spionage. Forskere skriver mere og mere om cybersikkerhed og at der dagligt sker cyberangreb hos virksomheder rundt om i landet. Det kan konkluderes ud fra litteraturen, på spionageområdet,

at cyberaktiviteter er en overvejende metode, til at udføre sabotage- og spionageoperationer på, i og med, at infrastruktur og daglige gøremål er teknologisk understøttet.

Kina er allerede en stor aktør inden for teknologi, og med Danmarks førende viden indenfor grøn teknologi, kan Danmark være et interessant mål for kinesisk industrispionage, der kan føre til store økonomiske konsekvenser. Hvis vindmøllevirksomheden Vestas eksempelvis får stjålet nyudviklet teknologi, så er risikoen, at de mister den indkomst, de kunne have fået for at sælge teknologien. Andre virksomheder kan også takke nej til fremtidige samarbejder, hvis de ser en risiko for at deres sensitive data bliver stjålet.

Det er vist i litteraturen, at cyber og teknologiske udviklinger får mere og mere indflydelse i spionageaktiviteter. Cyberaktiviteter, kan på grund af digitaliseringen, have enorme konsekvenser for forsyningssikkerheden og kommunikationskanaler i hele verden. Det er ikke nødvendigvis noget man dagligt tænker over, men uden elektricitet og vand i bare 48 timer, kan det blive svært for de udsatte borgergrupper at klare sig.

Når der udføres spionage, om det er cyberaktiviteter, industrispionage, klassisk overvågning eller noget helt fjerde, kan det have store konsekvenser. Udover attentatforsøget på AMSLA-medlemmer i Ringsted, så peger litteraturen ikke direkte på spionagehændelser rettet mod Danmark. Det er alligevel skrevet andre steder, blandt andet i PET's *Vurdering af spionagetruslen mod Danmark, Færøerne og Grønland 2023*, at Danmark står overfor konkrete spionagetrusler samtidig med, at der ifølge medierne har været hændelser i Danmark.

Eksemplerne vi ser fra USA, som fylder meget i litteraturen, peger på at industrispionagen kan medføre betydelige økonomiske tab, hvis der bliver stjålet teknologi hos førende virksomheder. Danmarks fremskridt inden for grøn teknologi, kan det ikke afvises, at den industri er et mål for industrispionage. Spionage kan ligeledes føre til en masse sårbarhed i samfundet. Hvis fremmede nationer skulle forsøge at hacke sig ind i kritisk infrastruktur, eller hvis Kina lykkedes med deres ambitioner om at færdiggøre projekter, der skal binde Asien, Europa og Amerika sammen med internettet, så kan Danmark ende med at blive mere afhængig af fremmede staters teknologi, hvilket kan medføre, at de stater, står i en bedre forhandlingssituation internationalt. Med den førende teknologi, og med Danmarks geografiske placering, er landet altså et strategisk godt mål for spionageaktivitet.

Det kan også konkluderes, at det ikke kun er Kina, Iran og andre fremmede stater, der spionerer. Den primært amerikanske litteratur anvender ofte USA selv som et sammenligningspunkt, når der forskes i spionage og efterretningsarbejde, og her fremgår det at USA i stor grad udfører spionageaktiviteter. Navnlig Operation Dunhammer for eksempel. At verdens

efterretningstjenester samarbejder på kryds og tværs, for at dele, og få informationer er ikke nyt, men en nødvendighed. Når hændelser som Operation Dunhammer kommer frem i offentligheden, kan det skade Danmarks ry i efterretningsverdenen. Hvis andre nationer ser en risiko, ved at dele deres fortrolige informationer med Danmark, så lader de blot være. Det er en af de største konsekvenser for en efterretningstjeneste, at internationale samarbejdspartnere ikke har tillid til dem.

6.0 Litteraturliste

Aldrich, R. J., & Kasuku, J. (2012). Escaping from American intelligence: Culture, ethnocentrism and the Anglosphere. *International Affairs*, *88*(5), 1009–1028. https://doi.org/10.1111/j.1468-2346.2012.01116.x

Andersen, L. B. (2010). Forskningskriterier. I *Metoder i statskundskab* (s. 97–113). Hans Reitzels Forlag.

Assoudeh, M. (2020). *Shaping Cybersecurity Strategy: China, Iran, and Russia in a Comparative Perspective* [Dissertation, ProQuest]. Lokaliseret 20. maj 2023, fra https://objects.scraper.bibcitation.com/user-pdfs/2023-05-24/aed0851b-aae2-4a34-8d3e-8d0e58c4d77a.pdf

ByteDance. (u.å.). *About us*. Inspire Creativity, Enrich Life. Lokaliseret den 2. maj 2023, fra https://www.bytedance.com/en/

Bateman, J., Hickok, E., Courchesne, L., Thange, I., & Shapiro, J. N. (2021). Measuring the Effects of Influence Operations: Key findings and gaps from empirical research. *Carnegie Endowment for International Peace*. Lokaliseret den 25. april 2023, fra https://carnegieendowment.org/2021/06/28/measuring-effects-of-in%E2%80%A6erations-key-findings-and-gaps-from-empirical-research-pub-84824

Boland, A., Cherry, G., & Dickson, R. (2017). *Doing a systematic review: A student's guide* (2nd ed.). SAGE Publications Limited.

Chang, V. K. L. (2022). China's new historical statecraft: Reviving the Second World War for national rejuvenation. *International Affairs*, *98*(3), 1053–1069. https://doi.org/10.1093/ia/iiac021

Charles Sturt University. (u.å.). *Library Guides: Literature Review: Systematic literature reviews*. Library Guides at Charles Sturt University. Lokaliseret den 24. februar 2023, fra https://libguides.csu.edu.au/review/Systematic

Cherry, M. G., Smith, H., Parks, E., & Boland, A. (2017). Reviewing Qualitative Evidence. In *Doing a Systematic Review: A Student's Guide* (s. 193–222). SAGE Publications Limited.

Crandall, C. (2020). *To Cross the Ocean in Full View of the Sun: The Chinese Government's Grand Strategy to Influence Academic Freedom and American University Culture* [Dissertation]. University of South Florida.

Dahlgaard, M. (2022). De bliver kaldt Kinas magiske våben. En spektakulær sag viser, hvordan moderne spioner arbejder. *Zetland*. Lokaliseret den 3. maj 2023, fra https://www.zetland.dk/historie/sOKVBdQ9-aegJ1zvV-86c75

Diderichsen, A. (2016). Om efterretningstjenesternes legitimitet. I K. V. Rønn (Ed.), *Efterretningsstudier* (s. 67–89). Samfundslitteratur.

Dunder, Y., & Fleeman, N. (2017). Developing My Search Strategy. In *Doing a Systematic Review: A Student's Guide* (s. 61–78). SAGE Publications Limited.

Elsevier. (u.å.). *Reference manager - Mendeley*. Elsevier Solutions. Lokaliseret den 7. april 2023, fra https://www.elsevier.com/solutions/mendeley

Exec. Order No. 12333, 52 Fed. Reg. 72 (15. april, 1987). Lokaliseret den 29. marts 2023, fra https://dpcld.defense.gov/Portals/49/Documents/Civil/eo-12333-2008.pdf

Farrington, D. P., & Jolliffe, D. (2017). Special issue on systematic reviews in criminology. *Aggression and Violent Behavior*, *33*, 1–3. https://doi.org/10.1016/j.avb.2017.01.020

Finanstilsynet. (2022). *Sanktioner mod Rusland og Belarus*. Finanstilsynet. Lokaliseret den 2. maj 2023, fra https://www.finanstilsynet.dk/Nyheder-og-Presse/Pressemeddelelser/2022/SanktionerRusland_060322

Fleeman, N., & Dunder, Y. (2017). Data Extraction: Where do I begin? In *Doing a Systematic Review: A Student's Guide*. SAGE Publications Limited.

Foght, T., & Fastrup, N. (2020). Alvorlig mistanke: Ringsted-iranere fik millioner fra Saudi-Arabien til terrorvirksomhed. *DR*. Lokaliseret den 25. maj 2023, fra https://www.dr.dk/nyheder/indland/alvorlig-mistanke-ringsted-iranere-fik-millioner-fra-saudi-arabien-til

Forsvarets Efterretningstjeneste. (2022). *Udsyn 2022: En efterretningsbaseret vurdering af de ydre vilkår for Danmarks sikkerhed og varetagelsen af danske interesser*. Lokaliseret den 8.

marts 2023, fra https://www.fe-ddis.dk/globalassets/fe/dokumenter/2022/udsyn-2022/-fe-udsyn-2022-opslag-.pdf

Freedom House Inc. (2016). *FINANCIAL STATEMENTS, Year ended June 30, 2016, AND INDEPENDENT AUDITOR'S REPORT*. Lokaliseret den 24. maj 2023, fra https://freedomhouse.org/sites/default/files/FINAL_Basic_Financial_Statements_2016.pdf

Google. (u.å.). *Criminology, criminal law & policing - Google scholar-metrics*. Google Scholar. Lokaliseret den 17. april 2023, fra https://scholar.google.com/citations?view_op=top_venues&hl=da&vq=soc_criminologycriminallawpolicing

Haddaway, N. R., Page, M. J., Pritchard, C. C., & McGuinness, L. A. (2022). PRISMA2020: An R package and Shiny app for producing PRISMA 2020-compliant flow diagrams, with interactivity for optimised digital transparency and Open Synthesis. *Campbell Systematic Reviews*, *18*(2). https://doi.org/10.1002/cl2.1230

Harrits, G. S., Pedersen, C. S., & Halkier, B. (2010). Indsamling af interviewdata. I *Metoder i statskundskab* (s. 144–172). Hans Reitzels Forlag.

Hudson Institute. (u.å.). *About*. Hudson. Lokaliseret den 24. april 2023, fra https://www.hudson.org/about

Jakobsen, M. L., & Harrits, G. S. (2010). Kvalitativ analyse: Kodning og dybdegående tekstanalyse. I *Metoder i statskundskab* (s. 173–191). Hans Reitzels Forlag.

Jüris, F. (2022). Sino-Russian scientific cooperation in the Arctic: From deep sea to deep space. I S. Kirchberger, S. Sinjen, & N. Wörmer (Ed.), *Russia-China Relations* (s. 185–202). Springer International Publishing. http://dx.doi.org/10.1007/978-3-030-97012-3_10

Justitsministeriet. (2014). *Cirkulære om sikkerhedsbeskyttelse af informationer af fælles interesse for landene i NATO eller EU, andre klassificerede informationer samt informationer af sikkerhedsmæssig beskyttelsesinteresse i øvrigt*. CIR1H nr 10338 af 17/12/2014.

Knudsen, J. K. (2021). *Danmark lod USA spionere gennem internetkabler: Sådan foregår masseovervågningen.* DR. Lokaliseret den 24. april 2023, fra https://www.dr.dk/nyheder/viden/teknologi/danmark-lod-usa-spionere-gennem-internetkabler-saadan-foregaar

Kugley, S., Wade, A., Thomas, J., Mahood, Q., Jørgensen, A. K., Hammerstrøm, K., & Sathe, N. (2017). Searching for studies: A guide to information retrieval for Campbell systematic reviews. *Campbell Systematic Reviews*, *13*(1), 1–73. https://doi.org/10.4073/cmg.2016.1

Kux, D. (1985). Soviet active measures and disinformation: Overview and assessment. *The US Army War College Quarterly: Parameters*, *15*(1). https://doi.org/10.55540/0031-1723.1388

Methley, A. M., Campbell, S., Chew-Graham, C., McNally, R., & Cheraghi-Sohi, S. (2014). PICO, PICOS and SPIDER: A comparison study of specificity and sensitivity in three search tools for qualitative systematic reviews. *BMC Health Services Research*, *14*(1). https://doi.org/10.1186/s12913-014-0579-0

National Intelligence Law of the People's Republic of China, (2017). Fra Brown University (2019). Lokaliseret den 10. april 2023, fra https://cs.brown.edu/courses/csci1800/sources/2017_PRC_NationalIntelligenceLaw.pdf

O'Flaherty, K. (2019). Huawei security scandal: Everything you need to know. *Forbes*. Lokaliseret den 2. maj 2023, fra https://www.forbes.com/sites/kateoflahertyuk/2019/02/26/huawei-security-scandal-everything-you-need-to-know/?sh=2a13df2073a5

Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., Shamseer, L., Tetzlaff, J. M., Akl, E. A., Brennan, S. E., Chou, R., Glanville, J., Grimshaw, J. M., Hróbjartsson, A., Lalu, M. M., Li, T., Loder, E. W., Mayo-Wilson, E., McDonald, S., … Moher, D. (2021). The PRISMA 2020 statement: An updated guideline for reporting systematic reviews. *Systematic Reviews*, *10*(1). https://doi.org/10.1186/s13643-021-01626-4

Parello-Plesner, J., & Li, B. (2018). *The Chinese Communist Party's foreign interference operations: How the U.S. and Other Democracies Should Respond.* Hudson Institute.

Pilkington, G., & Hounsome, J. (2017). Planning and Managing My Review. In *Doing a Systematic Review: A Student's Guide* (s. 21–41). SAGE Publications Limited.

Politiets Efterretningstjeneste. (2022). *Vurdering af spionagetruslen mod Danmark*. https://pet.dk/-/media/mediefiler/pet/dokumenter/analyser-og-vurderinger/vurdering-af-spionagetruslen-mod-danmark/vurdering-af-spionagetruslen-mod-danmark.pdf

Politiets Efterretningstjeneste. (2023). *Vurdering af Spionagetruslen mod Danmark, Færøerne og Grønland*. https://pet.dk/-/media/mediefiler/pet/dokumenter/analyser-og-vurderinger/vurdering-af-spionagetruslen-mod-danmark/vsd_2023_dk_web.pdf

Pop, I., & Silber, M. D. (2021). Iran and Hezbollah's Pre-Operational Modus Operandi in the West. *Studies in Conflict & Terrorism*, *44*(2), 156–179. https://doi.org/10.1080/1057610x.2020.1759487

Poulsen, N. B. (2023). Hvad er hybridkrig? Forstå Ruslands hybridkrig i Norden [Interview]. In *DR*. Lokaliseret den 2. maj 2023, fra https://www.dr.dk/stories/1288510966/hvad-er-hybridkrig

Redmond, P. J. (2010). The challenges of counterintelligence. I Loch. K. Johnson (Ed.), *The Oxford Handbook of National Security Intelligence* (s. 537–554). Oxford University Press. http://dx.doi.org/10.1093/oxfordhb/9780195375886.003.0033

Ross, M. (2021). US-China higher education links in crisis: Behind the curtain of suspicion. *Asian Perspective*, *45*(1), 225–239. https://doi.org/10.1353/apr.2021.0024

Snyder, H. (2019). Literature review as a research methodology: An overview and guidelines. *Journal of Business Research*, *104*, 333–339. https://doi.org/10.1016/j.jbusres.2019.07.039

Svendsen, J., & Larsen, J. B. (2019). Forfalsket ministerbrev designet til at splitte Danmark og USA spiller hovedrollen i et fake news-angreb. *Politiken*. Lokaliseret den 3. maj 2023, fra https://politiken.dk/udland/art7487699/Forfalsket-ministerbrev-designet-til-at-splitte-Danmark-og-USA-spiller-hovedrollen-i-et-fake-news-angreb

Sørensen, C. T. N. (2018). Kina: Selvsikker og ambitiøs stormagt. *Udenrigs*, *1*, 13–20. https://doi.org/10.7146/udenrigs.v0i1.117687

The Cochrane Collaboration. (u.å.). *About us*. Cochrane. Lokaliseret den 11. maj 2023, fra https://www.cochrane.org/about-us

Van Cleave, M. K. (2013). What Is Counterintelligence? A Guide to Thinking and Teaching about CI. *Guide to the Study of Intelligence*, *20*(2), 57–65. Intelligencer: Journal of U.S. Intelligence Studies. https://www.afio.com/publications/VAN%20CLEAVE%20Pages%20from%20INTEL_FALLWINTER2013_Vol20_No2.pdf.

Ørbæk, K. S. (2023). Forskere advarer om, at Kina kan bruge Tiktok som våben. *TV 2 Danmark*. Lokaliseret den 2. maj 2023, fra https://nyheder.tv2.dk/udland/2023-03-25-forskere-advarer-om-at-kina-kan-bruge-tiktok-som-vaaben