Cybertrusler:

Troppssjefen og soldatene

KRIGSSKOLEN

Calmeyer, Casper Langaas & Heggem, Anders

Militære studier: Ledelse og landmakt

Emne: OPG3201 Syntese

Krigsskolen

2021

Antall ord: 14 966

Publiseringsavtale

En avtale om elektronisk publisering av bachelor/prosjektoppgave

Kadetten(ene) har opphavsrett til oppgaven, inkludert rettighetene til å publisere den.
Alle oppgaver som oppfyller kravene til publisering vil bli registrert og publisert i Bibsys Brage når kadetten(ene) har godkjent publisering.
Oppgaver som er graderte eller begrenset av en inngått avtale vil ikke bli publisert.

Jeg (Vi) gir herved FHS Krigsskolen rett til å gjøre denne oppgaven tilgjengelig elektronisk, gratis og uten kostnader	X Ja	Nei
Finnes det en avtale om forsinket eller kun intern publisering? (Utfyllende opplysninger må fylles ut) Hvis ja: kan oppgaven publiseres elektronisk når embargoperioden utløper?	Ja X Ja	X Nei Nei

Plagiaterklæring

Jeg (Vi) erklærer herved at oppgaven er mitt eget arbeid og med bruk av riktig kildehenvisning. Jeg (Vi) har ikke nyttet annen hjelp enn det som er beskrevet i oppgaven.
Jeg (Vi) er klar over at brudd på dette vil føre til avvisning av oppgaven.

Dato: 15.04.2021

Kadett navn Kadett Anders Heggem

Kadett navn Kadett Casper Calmeyer

Innholdsfortegnelse

1 Innledning 5
1.1 Bakgrunn 5
1.2 Problemstilling 6
1.3 Avgrensninger 6
1.4 Begrepsavklaring 6
2 Metode 7
2.1 Valg av metode 7
2.2 Anvendt metode 9
2.3 Kildevalg og kildekritikk 9
3 Teori 10
3.1 Risiko 10
3.1.1 Trusselaktørene 11
3.1.2 Sårbarhet 14
3.1.3 Verdi 16
3.2 Nye sårbarheter 17
3.2.1 Smarttelefoner 18
3.2.2 Geotagging 18
3.2.3 Internet of Things 19
3.2.4 Big data 19
3.2.5 Mennesket som sårbarhet i systemet 20
3.2.6 Kampen om narrativet i sosiale medier 21
3.3 Digital sikkerhet i Norge i dag 23
3.3.1 Retningslinjer/regelverk 23
3.3.2 Opplæringen i dag 23
3.3.3 Mottiltak og faktorer i Norge 24
3.3.4 Troppssjefen som rollemodell - Hva slags opplæring får kadetten? 26
4 Case-eksempler 27
4.1 Russisk *maskerovka* mot Vesten 27
4.2 Ukraina (2014) 29
4.3 Norge/Stortinget 31
5 Drøfting 33
5.1 Risiko 33
5.1.1 Trusler 33

5.1.2 Verdier 34
5.1.3 Sårbarheter 35
5.1.4 Mottiltak 37
5.1.5 Delkonklusjon 1, risiko 38
5.2 Nye sårbarheter 39
5.2.1 Policyer og dagens opplæring 39
5.2.2 Kampen om narrativet 41
5.2.3 Troppssjefen som rollemodell 41
5.2.4 Mottiltak 42
5.2.5 Delkonklusjon 2, nye sårbarheter 43
6 Konklusjon 44
7 Bibliografi 45

1 Innledning

1.1 Bakgrunn

I forordet til sin nye bok "The Future of War – A History" skriver den britiske historikeren Lawrence Freedman "There is no longer a dominant model for the future of war, but instead a blurred concept and a range of speculative possibilities" (Diesen, 2018, s. 7). Dette innebærer på mange måter å snu på Clausewitz' berømte sitat om at "krig er politikk med andre midler" og si at siden det egentlig hersker en slags kontinuerlig krigstilstand mellom Russland og Vesten, er all politikk krig, også med andre midler enn de tradisjonelle militære (Diesen, 2018, s. 39). I fortiden har kriger i stor grad blitt utkjempet med kinetiske våpen. Med teknologisk innovasjon har det i nyere tid oppstått ett nytt domene å føre krig i, *cyberdomenet*, hvor skillet mellom fred og krig har blitt vagt og utydelig.

Politiets sikkerhetstjeneste (PST) er Norges nasjonale innenlands etterretnings- og sikkerhetstjeneste. I 2020 skrev PST følgende om statlig etterretningsvirksomhet: "Utenlandske etterretningstjenester forventes i 2020 å rette sin spionasje mot politiske myndigheter, mot naturressurser og næringsliv, mot forsvar og beredskap, samt mot forskning og utvikling. Selv om russisk, kinesisk og iransk etterretningsvirksomhet vurderes å ha størst skadepotensial, kan også andre staters fordekte aktiviteter påføre Norge, norske virksomheter og enkeltindivider skade." (Politiets sikkerhetstjeneste, 2020a, s. 3).

Som PST, gir også E-tjenesten ut sin årlige trusselvurdering. E-tjenesten er Norges etterretningstjeneste utenlands. I E-tjenestens trusselvurdering for 2020 blir Kina, på lik linje med Russland, pekt på som et land med "interesse av å utfordre den USA-dominante verdensordenen". Et premiss for dette er Kinas strategi "Den nye silkeveien". "Videre legger «Den digitale Silkeveien» grunnlaget for en storstilt, global etterretningskapasitet. Kontroll over 5G-nettverk, fiberkabler og smartby-systemer gir muligheten til å samle inn enorme datamengder. Silkeveiprosjektene gjennomføres som regel av kinesiske virksomheter, som etter kinesisk lov er pålagt å dele informasjon med myndighetene i Beijing. Kinesiske teknologiselskaper etablerer nye tekniske standarder og inntar en stadig mer dominerende posisjon innenfor digitale tjenester." (Etterretningstjenesten, 2020, s.10). At kinesisk lov pålegger virksomheter å dele alt av informasjon, er bekymringsverdig sett opp mot innsamling og kartlegging av enorme mengder data om enkeltpersoner verden

over. Dette peker derfor i retning av at moderne, mer vanlige krigshandlinger foregår i en gråsone i cyberdomenet, hvor spionasje og etterretning forventes mot blant annet Forsvaret, og skade kan påføres enkeltindivider.

1.2 Problemstilling

Cyberdomenet er det eneste domenet som er menneskeskapt, og det er i stadig vekst. Mange er fortsatt usikre på hvordan en skal forholde seg til dette domenet, med utfordringer og muligheter. Marius Bekkevang skrev i 2017 en bachelor om hvorvidt det er sannsynlig at Norge blir utsatt for cyberangrep fra en statlig aktør. Han konkluderte med at det er vanskelig å si hvorvidt det vil inntreffe, men at det er potensiale for et slikt angrep (Bekkevang, 2017, s. 28). Russland har i en årrekke drevet med cybersabotasje mot tidligere sovjetstater som Estland, Litauen, Georgia og Ukraina. Dette gir en pekepinn på hva som kan forventes av cyberoperasjoner i fremtiden (Kroghrud, 2019, s. 54). I denne oppgaven vil vi ta for oss truslene som våre soldater, og dermed vår operative evne, står ovenfor. Vi vil også se på hvilke mot-tiltak som gjennomføres i dag og utforske hvorvidt disse er gode nok.

Problemstillingen vår blir derfor følgende:
Hvordan kan vi som troppssjefer beskytte egne soldater mot dagens cybertrussel?

1.3 Avgrensninger

- Vi ser på handlinger i cyberspace som del av hybrid krig.
- Vi ser ikke på IT-sikkerhet teknisk i form av kryptering og andre defensive tiltak rundt beskyttelse av persondata og lignende, og tekniske verktøy Forsvaret bruker i dag.
- Vi ser i hovedsak på utdanning og rammer/regelverk i Hæren.

1.4 Begrepsavklaring

Hybrid krig: "...The synchronized application of political, economic, informational, CEMA [cyber electromagnetic activities] and military effort, for strategic objectives, that minimizes the risks that accompany conventional war" (Johnson, 2018, s. 158). Denne definisjonen appellerer til forskjellige domener, eksempelvis informasjonsdomenet, som kan innebære både propaganda og cyber-domenet. En lavere risiko for konvensjonell krig blir også vektlagt. En sentral del i hybrid krig er derfor gråsonen mellom krig og fred.

Cyber: Prefiks som viser at det ordet prefikset benyttes sammen med henviser til noe i cyberdomenet. F.eks. cyberangrep eller cybertrussel (Forsvarsdepartementet, 2014, s. 5).

Narrativ: Et narrativ er kort fortalt en fortelling. Det er en side av saken, altså en måte å fremstille noe på, som fremstilling av samfunnet eller verden. Når vi snakker om å kontrollere narrativet, snakker vi om å kontrollere oppfattelsen av fortellingen (Språkrådet, n.d.).

Aktør: Aktør er brukt for å referere til en person eller organisasjon, inkludert statlige og ikke-statlige enheter, innenfor det internasjonale systemet med kapabilitet eller ønske om å påvirke andre i forfølgelsen av dens interesser og mål (AJP-2(A), 2016, pkt. 1-3).

Informasjon: Ubehandlet data over alle beskrivelser som kan bli brukt i produksjon av etterretning (Etterretningsdoktrinen vedlegg C, 2013, vedlegg C s. 4).

Etterretning: Systematisk innhenting og bearbeiding av informasjon som angår utenlandske forhold, ervervet med åpne og fordekte metoder i en statlig legal ramme. Produktene skal redusere usikkerhet, skape forståelse og har ofte en prediktiv karakter. Begrepet brukes om produktet, aktiviteten og organisasjonen som utøver aktiviteten (Etterretningsdoktrinen vedlegg C, 2013, s. 4).

2 Metode

2.1 Valg av metode

"Metodevalg og problemstilling skal gå hånd i hånd" (Røkkum, 2016). Det vi ønsket å undersøke i denne oppgaven var hvorvidt dagens utdanning, retningslinjer og reglementer holder mål sett opp mot de nye sårbarhetene som følger med utviklingen i cyberdomenet. I tillegg er vinklingen hvilke muligheter troppssjefen har til å sikre soldatene, og dermed vår operative evne, mot slike trusler. Problemstillingen gjorde det naturlig å benytte flere typer kilder. Vi har sett på sentral teori rundt cyberdomenet og eksempler på utnyttelsen av cyberdomenet til både defensive og offensive handlinger. I tillegg har vi sett på nye sårbarheter og brukt eksempler fra virkeligheten rundt hvordan disse ble og stadig kan bli utnyttet. Vi har da sett på hvilken risiko vi står ovenfor, ved å bruke risikoanalyse som

metode. Hva trusselen er, hvilke sårbarheter som gjelder våre soldater og hvilken verdi disse sårbarhetene kan ha for en utnyttende part. Dette har det da vært gunstig å sette opp mot hvilken praksis som gjennomføres innen utdanning og kompetanseutvikling både hos våre soldater og våre offiserer. Vi har også sett på hva slags utdanning som gjennomføres for troppssjefer på Krigsskolen i dag. Dette måtte da settes opp mot hvilke nye sårbarheter som har utviklet seg i den siste tiden og hvorvidt dagens praksis tar høyde for dette. E-tjenesten og PST sine risikovurderinger var også sentrale i denne oppgaven for å kartlegge trusler, sårbarheter og risiko.

Samfunnsvitenskapelig metode "... dreier seg om å samle inn, analysere og tolke *data*, og dette er en sentral del av *empirisk forskning*. De viktigste kjennetegnene ved metode/empirisk forskning er systematikk, grundighet og åpenhet" (Johannesen, Tufte & Christoffersen, 2010, s. 29). Forskjellen mellom naturvitenskap og samfunnsvitenskap er at naturforskeren er en tilskuer til det han eller hun studerer. Det er ikke mulig å kommunisere med det som studeres, eksempelvis gener og atomer. Det er typisk det vi forbinder med eksperimenter og forskningslaboratorier (Johannesen, Tufte & Christoffersen, 2010, s. 30). Det samfunnsforskeren studerer er mennesker med deres oppfatninger og meninger, om andre og seg selv. Dette mangfoldet av meninger er under konstant endring. "Samfunnsforskeren er en deltaker i samfunnet, og kan ikke bare være en tilskuer til det han studerer" (Johannesen, Tufte & Christoffersen, 2010, s. 31). Dette betyr at eventuelle avdekninger som blir gjort, og som videreformidles til samfunnet, kan resultere i endringer blant folk, meninger og i samfunnet i sin helhet.

Metoden vi brukte var en kvalitativ tilnærming, da dette resulterte i mer nyansert og detaljert informasjon rundt problemstillingen vår (Johannesen, Tufte & Christoffersen, 2010, s. 32). Dataene vi analyserte var i stor grad tekst (Johannesen, Tufte & Christoffersen, 2010, s. 37). Metoden for oppgaven var også dokumentanalyse av relevante retningslinjer, trusselvurderinger, utdanningsplaner og deres målsettinger. Dokumentanalyse er en metode som tar for seg kvalitative data fra dokumenter, og setter dette opp mot problemstillingen (Johannesen, Tufte & Christoffersen, 2010, s. 165). Vi har analysert teori og relevante artikler rundt historiske eksempler og trender vi ser i dag. I tillegg har vi benyttet en anonym informant som forskningsobjekt til eget materiale.

2.2 Anvendt metode

Vi har valgt å fokusere på cyber-siden av hybrid krig-scenario. Ettersom dette temaet er relativt nytt, men stadig mer relevant med tanke på utviklingen i samfunnet, mener vi vinklingen for oppgaven er svært interessant og dagsaktuell. Det er også flere nyhetsartikler vi har sett de siste årene som tyder på at det er både sårbarheter det muligens ikke tas høyde for i gjeldene utdanning, og et behov for at troppssjefen tar større ansvar for å bidra til soldatenes digitale robusthet. Vi som kadetter på Krigsskolen har også fått erfare skolens utdanningsprogram innenfor cyber-sikkerhet, og vil derfor kunne si noe om utgangspunktet offiserer i dag får til å kunne bidra i soldatenes utdanning og sikkerhet i cyberdomenet.

For å besvare problemstillingen har vi fordypet oss i trusselbildet gjennom PST og E-tjenestens trusselvurderinger, historiske eksempler og nyhetsartikler om avdekte digitale sårbarheter. Vi har sett på hvilke aktører som kan være relevante trusler, deres kapasiteter og motivasjon. Hvilke sårbarheter som er aktuelle for våre soldater er også noe vi har kartlagt. Dette har vi funnet mye om gjennom nevnte trusselvurderinger, eksempler og artikler om avdekte sårbarheter. I tillegg har vi undersøkt hvilken verdi som kan trekkes ut av disse sårbarhetene. Videre har vi fordypet oss i hva som praktiseres i dag hva gjelder retningslinjer, reglementer, utdanning og praksis, både for soldater og offiserer. Dette er vårt teorigrunnlag for drøfting opp mot problemstillingen.

2.3 Kildevalg og kildekritikk

“Forskeren må være seg bevisst at han er en utvelgende aktør, og at data som brukes, ikke er uavhengige av hans forhåndsoppfatninger” (Johannesen, Tufte, & Christoffersen, 2010, s. 40). Dette prinsippet var i stor grad gjeldene for oss når vi skulle svare på problemstillingen. I vårt makkerpar er det flere års erfaring fra tidligere arbeid med IT-sikkerhet i privat sektor. Som kadetter uten tidligere befalsutdanning og med annen bakgrunn enn tidligere offiserer, besitter vi også sannsynligvis mer og annen erfaring med cyberdomenet enn våre forgjengere. Vi har dermed flere og andre forutinntatte syn, meninger og erfaringer enn det som er vanlig i vår utdanning på Krigsskolen. For å forholde oss så nøytrale som mulig, satt vi oss ned sammen og ble enige om hvilke kilder vi i hovedsak ønsket å bruke. Vi landet tidlig på å basere oss på trusselvurderinger fra regjeringen, dagens gjeldende reglementer, retningslinjer og utdanning, samt historiske eksempler og artikler om avdekte digitale sårbarheter. Vårt syn er dog farget av å være

kadetter i Hæren.

"Kildekritikk handler om å vurdere en kildes troverdighet, objektivitet, nøytralitet og egnethet" (Enstad, 2016, s. 14). Disse fire prinsippene benyttet vi når vi valgte artikler med eksempler på avdekte sårbarheter og historiske eksempler. Vi var da spesielt skeptiske til hva agendaen bak artikkelen var. Videre var kildene våre i stor grad dokumenter og artikler fra Forsvarets forskningsinstitutt (FFI), Forsvaret, PST og E-tjenesten. Når vi valgte kilder fra nyhetsmedier benyttet vi i hovedsak anerkjente og tradisjonelle kilder, som NRK og BBC. Når det gjelder artikler og fakta rundt cyberdomenet brukte vi kun anerkjente aktører som kilder, som IT-sikkerhetsfirmaene AVG og Kaspersky. Spesielt kritiske var vi til hvorvidt målsettinger for utdanningsprogram, retningslinjer o.l. faktisk når sine mål.

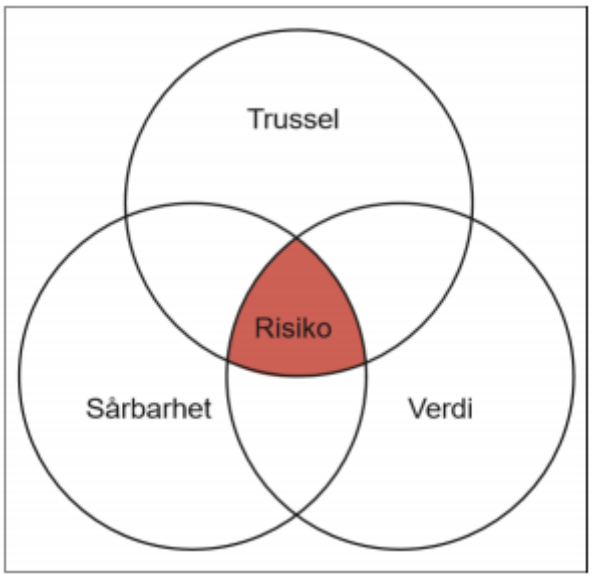
En utfordring for oppgaven var at vi fortsatt ikke har sett relevante aktører i en eksistensiell krise, og det er rimelig å anta at disse aktørene har kapasiteter innenfor cyberdomenet vi ikke vet noe om i dag. En sentral kilde i denne oppgaven vil var H. R. McMaster. Kilden er tydelig farget av å ha vært amerikansk general og sikkerhetsrådgiver for tidligere president Donald Trump, men han har doktorgrad i militærhistorie og hans bøker er akademisk sterke (Hoover.org, n.d.). Der vi har vært skeptiske til hans påstander eller kildehenvisninger har vi gått inn og sjekket opp mot andre kilder, og kun brukt det vi har fått bekreftet fra andre parter.

3 Teori

3.1 Risiko

For å finne ut av hva slags sikkerhetsarbeid vi troppssjefer kan gjøre for å beskytte egne soldater fra cybertrusler, må vi først finne ut av hva slags *risiko* som foreligger for slike trusler. Risiko er bestående av *sannsynlighet* og *konsekvens*. Når vi omtaler sannsynligheten for eksempelvis et cyberangrep må vi se på begrepet *trussel*. Dette er hvilken evne (kapasitet) og vilje (intensjon) som ligger til grunn for at uønskede handlinger kan gjennomføres for å oppnå spesifikke mål (Norges offentlige utredninger, 2012, s. 68). En trussel kan eksempelvis være sabotasje, spionasje eller terror. Det en også kan se på her er *tilstedeværelse* av en eventuell aktør, *historie* - hvorvidt lignende har skjedd tidligere, og om *målvalget* tyder på at noe kan skje snart (Brusmundrud, Maal & Kiran, 2015, s. 32). Her må aktører som har en interesse av å gjennomføre operasjoner

identifiseres, samt deres evne. Konsekvensen av uønskede handlinger avhenger av *verdien* til det som angripes, i tillegg til dens motstandskraft for avvik og påkjenninger. Dette kalles *sårbarhet* (NOU, 2012, s. 68).



Figur 1: Samspillet mellom trussel, verdi og sårbarhet (Norges offentlige utredninger, 2012, s. 68).

For å identifisere *verdien* til det som angripes kan vi se på "hvor kritisk er bortfallet av verdi X for de ulike konsekvensklassene" (Brusmundrud, Maal & Kiran, 2015, s. 32). Disse konsekvensklassene kan være *økonomi, omdømme, operativ evne, informasjon og liv og helse*. Hvis vi da kommer frem til at tap eller reduksjon av liv og helse til soldater har store konsekvenser, er verdien *høy*. Når det kommer til vurdering av *sårbarhet*, må vi se på hvorvidt en aktør kan gjennomføre uønskede handlinger vellykket. Det som påvirker dette er ressursene til aktøren, sikringstiltak som eksisterer eller kan iverksettes, og muligheten aktøren har til å forbigå sikringstiltakene (Brusmundrud, Maal & Kiran, 2015, s. 32-33).

3.1.1 Trusselaktørene

Samtidig som teknologien har utviklet seg, har også aktører og brukere i cyberdomene ekspandert. I 2018 var det tilkoblet 2.4 enheter til internett for hver bruker. Dette vil øke til 3.6 enheter i 2023. I 2020 fantes det 4.5 milliarder internettbrukere, noe som vil øke til omtrent 5.3 milliarder i 2023. Det vil tilsvare 66 prosent av verdens befolkning (Cisco, 2020). De mest avanserte, velorganiserte og ressurssterke aktørene er statlige, og ofte

tilknyttet etterretningstjenester. Disse har tilgang på mye personell og avansert teknologi. Statlige aktører bruker cyberdomenet først og fremst til spionasje mot andre stater, eller for å avdekke svakheter i deres systemer og nettverk som kan utnyttes (Norsk utenrikspolitisk institutt, 2011). Russland var en av de første statene som begynte med cyberoperasjoner. Så tidlig som 1996 drev amerikansk FBI etterforskningen med navnet *Moonlight Maze* rettet mot russiske styresmakter. Her ble det avdekket spionasje mot et titalls organisasjoner, inkludert teknologiselskaper, energisektoren og forsvarssektoren (Rid, 2016).

Andre ikke-statlige aktører er blant annet kriminelle, som hovedsakelig ønsker å innhente informasjon om bedrifter og enkeltmennesker for å lure til seg penger. Hacker-aktivister, som eksempel *Anonymous*, ønsker å skape politisk oppmerksomhet og fremme sitt syn på saker gjennom hacking av nettsider. Terrorister ønsker å lamme deler av cyberdomenet for å skape frykt og forsøke å fremtvinge sitt politiske syn (NUPI, 2011).

Kina er en av hovedsakelig to stater som truer Norge med hybride virkemidler. En del av irregulære virkemidler i hybrid krigføring er bruken av cyberdomene. Et kjennetegn ved dette er at en kan påvirke over lange avstander uten fysisk tilstedeværelse. For at vi skal kunne se på en stat som en mulig trussel, må vi kombinere militær rekkevidde, institusjonelle forutsetninger og geopolitisk interesse (Diesen, 2018, s. 42). Kina har vist stor interesse for nordområdene, med forskningsstasjoner på Spitsbergen og Island, og observatører i Arktisk råd. Interessene dreier seg om transport, ressursutnyttelse og forskning. I tillegg har landet anskaffet en betydelig flåte av isbrytere. Når det kommer til ressursutnyttelse har Kina formidlet at kyststatene ikke kan begrense andre lands utnyttelse av havressurser, og mener bruk av militærmakt er legitimt for ivaretagelse av disse interessene. Til tross for dette tilsier ikke dagens politiske situasjon at kinesiske interesser i Nordområdene er så sterke at det er sannsynlig at landet vil bruke militærmakt ovenfor Norge for å ivareta disse (Diesen, 2018, s. 42).

Både kinesiske og russiske etterretningstjenester utfører dog spionasje på norsk petroleumssektor, som omfatter både norske og utenlandske virksomheter i Norge. Sivile selskaper i petroleumsbransjen utvikler teknologi som har flerbrukspotensiale, teknologien kan også brukes til militære formål. I et verstefallsscenario kan fysisk eller digital sabotasje av undersjøiske gass- og oljerørledninger svekke troverdigheten til norsk

leveranseevne, øke andre lands militære kapasiteter og evner, svekke norsk krisehåndtering og dermed gi både konsekvenser for nasjonal sikkerhet, økonomi og Forsvaret (PST, 2020b, s. 3). I 2014 ble Olje- og energidepartementet (ODIR) samt over 50 olje- og gassvirksomheter i Norge utsatt for et omfattende nettverksangrep. "Etterforskningen av hendelsen viste at trusselaktørene hadde kartlagt og målrettet angrepet mot nøkkelfunksjoner og nøkkelpersoner i sektoren. Hensikten med slike angrep er ofte å installere skadevare i datasystemene til et selskap, som senere kan brukes til å utføre ulike handlinger" (PST, 2020b, s. 2-3).

Russland er den mest innlysende trusselaktøren. Dette skyldes den geografiske nærheten, deres autoritære politiske syn, formidlet interesse av nordområdene og det de har vist av evne til å utføre irregulære og regulære militære operasjoner (Diesen, 2018, s. 43). "In recent years, Russia's hybrid war against Ukraine has encompassed both cyber attacks and manipulation of information. Information operations are a critical component of modern warfare" (Nye, 2018). Russlands forståelse av krigens natur har forandret seg, da russiske eliter ser på informasjonskrig og politisk subversjon som viktige metoder for moderne krigføring. Ettersom informasjonskrig og politisk subversjon er under grensen for væpnet vold, har også skillet mellom fred og krig blitt utydelig. Russiske toppledere har, siden 2011/2012, ansett at Russland er i krig med USA og deres allierte, vel og merke med ikke-voldelige midler (Jonsson, 2019). Skillet mellom hva som regnes som informasjonskrig og cyberkrig er mer utydelig i Russland enn i vestlige land (Limnéll, 2015, s. 524). Selv om Russland ikke har publisert en offentlig doktrine med beskrivelser av cyberkapasitetene deres, har de vist evne og vilje til å gjennomføre cyberoperasjoner.

Russland er regnet som ett av tre land i verden som er dyktigst, mest erfarne og i best stand til å utføre cyberoperasjoner. De har opprettet Cyber Command, et senter for å utføre propagandaoperasjoner og cyberangrep. For å fremme deres globale interesser, har Russland implementert cyber-spionasje som del av deres overordnede strategi (Limnéll, 2015, s. 528). Å styre narrativet er en del av propaganda- og påvirkningsoperasjoner. "... Russian disinformation is designed to shake citizens' belief in their common identity and in their democratic principles, institutions, and processes by manipulating social media, planting false stories, and creating false personas. The repetitive nature of these narratives is intended to portray a certain point of view as a popular perception." (McMaster, 2020, s. 41).

3.1.2 Sårbarhet

Som tidligere beskrevet, kan sårbarheter forstås som en begrenset evne til å motstå påkjenninger som kan resultere i negative avvik fra normal funksjon. En sårbarhetsvurdering er hvorvidt en aktør kan gjennomføre uønskede handlinger uten å bli stanset (Brusmundrud, Maal & Kiran, 2015, s. 33). Vår kjennskap til sårbarheter kan bli delt opp i fire deler: Known-knowns (kunnskap), unknown-knowns (påvirkningen er ukjent, men at den finnes er kjent, dvs. ubenyttet kunnskap.), known-unknowns (Vi erkjenner at det er sårbarheter vi ikke vet om.) og unknown-unknowns (Vi vet ikke at det finnes sårbarheter vi ikke vet om) (Kim, 2012).

De mest kjente, og vanlige cyberangrep på nettverk, er:

- *Denial of Service (DoS):* Aktøren overvelder nettverkets kapasitet og lammer det ved å unytte svakheter i nettverket eller sender et stort antall forespørsler som nettverket ikke tåler. Dette forhindrer andre i å få tilgang til nettverket (NUPI, 2011).

- *Distributed Denial of Service (DDoS):* En type DoS-angrep hvor aktøren tar kontroll over et stort antall slavemaskiner i cyberspace for å sende et samordnet og synkront angrep mot et nettverk (NUPI, 2011).

- *Skadevare/Malware:* En samlet betegnelse for diverse virus, ormer og trojanske hester. Disse inneholder skadelig kode som ofte har til hensikt å forstyrre prosesser over tid, eller skade omdømmet til offeret. Malware kan komme i nettverket gjennom USB-minnekoder, hacking eller epostvedlegg/lenker som den mottakende part trykker på. Skadevaren kan eksempel få datasystemet til å utføre selvødeleggende handlinger, få nettverket ut av drift eller samle inn sensitive opplysninger og informasjon (NUPI, 2011).

Ettersom cyberdomenet har ekspandert og antall enheter tilkoblet internett har økt, har også cyberkriminalitet økt. I februar 2020 utgav NorSiS rapporten “Trusler og trender 2019-2020" som tar for seg de ti største digitale truslene (NorSiS, 2020). Disse er:

- *Løsepengevirus:* Viruset kommer inn på offerets datamaskin via infiserte nettsider eller lenker og vedlegg i e-poster og krypterer filene. Deretter kreves det løsepenger for å få filene tilbake.

- *ID-tyveri:* Dette kan gjøres gjennom phishing, hvor offeret får tilsendt en e-post hvor du blir bedt om å oppgi informasjon, gjennom hacking eller datalekkasjer hos tjenesteleverandør. Offerets ID-bevis blir benyttet av en aktør for eksempel å bestille tjenester, eller påføre tap av omdømmet for enkeltperson, organisasjon eller virksomhet.

- *Falske trusler og utpressingskrav:* Eksempel her er pornosvindel. Aktøren har ofte fått noe informasjon om deg igjennom større datalekkasjer. Denne lille informasjonen, som telefonnummer, brukernavn eller passorddetaljer blir brukt mot deg.

- *Phishing:* Offeret får som oftest tilsendt en e-post fra noen som fremstår som en reell virksomhet, eksempel en bank. Den angripende part blir lurt til å oppgi sensitiv informasjon ved eksempel å klikke seg inn på en lenke for å logge inn. Dette kan bli brukt til svindel, utpressing, ID-tyveri eller videreselges.

- *Ekte utpressing:* Dette finnes det mange varianter av. Eksempelvis seksuell utpressing eller datingsvindel. I førstnevnte klarer aktøren å få tak i bilder eller videoer. I den neste blir man kjent med noen over nettet, før uforutsette hendelser skjer, som fører til at offeret betaler penger for å hjelpe til.

- *Kontohacking:* En persons personlige konto overtas. Dette kan skje ved datalekkasjer eller at bruker har blitt fralurt eller delt påloggingsinformasjon, eksempelvis ved phishing.

- *Datainnbrudd:* Aktøren kan ha angrepet sårbarheter i et datasystem eller at ondsinnet programvare har blitt lastet ned og gitt aktøren adgang til systemet. Målet kan være personopplysninger eller forretningshemmeligheter til sabotasje og spionasje. Dette kan bli brukt for videre angrep mot samarbeidende eller større virksomhet eller organisasjon, eksempel forsvaret.

- *Menneskelig feil:* Etter hvert som systemer blir mer komplekse og enheter øker, øker også faren for at enkeltpersoner gjør feil som en aktør kan utnytte.

- *Krenkelser:* Gjennom sosiale medier og andre nettsider kan hets, trusler, mobbing og trakassering rettes mot virksomheter og enkeltpersoner.

- *Verdikjedeangrep:* Angrepet rettes mot en usikret IoT-enhet (Internet of Things), underleverandør eller tredjeparts dataprogramvare. Verdikjeden som leder til målet blir angrepet, ikke målet i seg selv. Dette er for å gi aktøren adgang til en virksomhets datasystemer, ved å utnytte svakheter (NorSiS, 2020).

Selv om dette er de mest vanlige, er ikke dette de eneste sårbarhetene og cybertruslene. Mer rettet mot enkeltsoldater og Forsvaret, kan geolokalisering og kartlegging av soldater være blant de mest fremtredende cybertrusselene. Det er flere eksempler hvor geolokalisering på eksempelvis appene "Tinder" og "Strava" har avslørt soldaters lokalisering og identitet. For en aktør kan dette være nyttig informasjon, som kan brukes til eksempelvis sabotasje og spionasje. Tinder har allerede blitt brukt til å lokalisere norske soldater under en brigadeøvelse (Karlsen, 2019). Norske, danske og amerikanske soldater har blitt identifisert og lokalisert i krigssoner med appen Strava (Lied & Svendsen, 2018).

Russiske soldater har fått forbud mot å bruke smarttelefon og å legge ut meldinger i sosiale medier når de er i tjeneste eller strid, etter at russiske soldater, som angivelig skulle være i Russland på øvelse, ble avslørt som deltakende i strid i Øst-Ukraina i 2015 (Aale, 2019). Amerikanere må enten slutte å bruke en del apper eller skru av geolokalisasjon, etter en instruks ble sendt ut som pekte på risiko knyttet til dette (Garamone, 2018). Forsvaret har i utgangspunktet som hovedregel at soldater ikke skal ha med mobiltelefon i felt, og det er en streng policy på ikke å ha mobil med ut i internasjonale operasjoner (Karlsen, 2019). En annen sårbarhet er knyttet til sosiale medier, og hva som blir lagt ut. Personlig informasjon kan i verste fall bli brukt av en aktør til å manipulere, true, sette press på soldater eller verve personell til å være insidere. For flere aktører gjøres 80% av etterretning igjennom cyberdomenet (Herland, 2020).

3.1.3 Verdi

Verdivurdering handler om å identifisere hva vi ønsker å beskytte, altså verdien, for så å estimere hva slags skade uønskede hendelser kan få for verdien (Norges offentlige utredninger. 2015, s. 31). Disse verdiene kan eksempelvis være *liv og helse, informasjon, personopplysninger, infrastruktur* eller *materiell.* Som tidligere beskrevet finnes det mange

digitale trusler, som kan få store konsekvenser. Oppgavens problemstilling gjør at verdiene vi fokuserer på er våre soldaters liv og helse, informasjon og personopplysninger. Tidligere beskrevne trusler virker direkte inn på soldaters psykiske helse, tap av omdømme, eller i verste fall liv. "Forsvarets forskningsinstitutt (FFI) mener evnen til å ta i bruk ny teknologi vil ha stor betydning for forsvarsevnen fremover. En viktig forutsetning for å lykkes er å ha personell med riktig kompetanse innenfor både teknologi, operative behov og anskaffelsesregimet" (Svendsenutvalget, 2020, s. 14). Uønskede hendelser som fører til tap av liv har derfor store konsekvenser, og verdien *soldaters liv og helse* har svært høy verdi.

"Russia does not have the defense budget to compete with the US and its NATO allies, either in advanced conventional weaponry or in the ability to conduct integrated land, aerospace, maritime and cyberspace operations (joint warfighting). But just as the internet and social media provided opportunities to revise 'maskirovka' (tactical deception and disguise), Russia has integrated disruptive technologies into its military to exploit perceived US and NATO vulnerabilities." (McMaster, 2020, s. 56). For at Norge skal ha et forsvar og beskytte norsk suverenitet, må også Forsvaret kjempe om mennesker med kloke hoder på lik linje med det sivile næringslivet (Svendsenutvalget. 2020, s. 5). For at Norge også skal ha som ambisjon om å være blant de beste på innovasjon og utnyttelse av ny teknologi, må vi også utnytte synergien mellom det sivile samfunnet og Forsvaret (Svendsenutvalget. 2020, s. 14). Det er derfor viktig at tilliten mellom styresmakt og folket opprettholdes, og at Forsvaret beholder opinionen til sine soldater og befolkningen. Siden informasjonskrig og politisk subversjon er blitt en så stor del av Russlands hovedstrategi, vil derfor *informasjonen* som skaper Norges narrativ være en verdi vi ønsker å beskytte.

3.2 Nye sårbarheter

De siste årene har vi sett en ekstrem økning i bruk av teknologi og nettverk. Det har dukket opp nye muligheter for ikke-kinetisk krigføring. Nyhetsdekningen har blitt global og hele verden får oppdateringer i sanntid. Sosiale medier gjør det enkelt for uformelle grupper å organisere seg eller å nå ut til et stort publikum raskt. Militær teknologi spres enkelt og sivil teknologi tilpasses til bruk i militære formål. Kunnskap og informasjon om slikt ligger tilgjengelig, ofte gratis, for alle og enhver (Diesen, 2018, s.3).

3.2.1 Smarttelefoner

Ifølge SSB bruker 100% av befolkningen i aldersgruppen 16 til 24 år smarttelefon privat i dag. I gruppen 25 til 34 år bruker 99% smarttelefon privat (SSB, 2020). Over 90% av disse oppgir at de bruker sosiale medier daglig, eller nesten daglig (SSB, 2019). Vi bruker smarttelefonen til alt av dagligdagse gjøremål. Med tale, tekst, bilder og videoer kommuniserer vi med andre. Den brukes til å lese nyheter, handle, spille spill, se filmer og som kart med GPS. Den er konstant koblet til internett, gir fra seg stråling og enorme mengder av informasjon om brukeren. Dette skal vi se videre på i dette kapitlet. Når en enhet er koblet til internett er den også tilgjengelig for misbruk gjennom denne forbindelsen. Hacking og tekniske mottiltak innenfor IT-sikkerhet vil ikke være hovedfokus i denne oppgaven, men det er likevel viktig å nevne at det uansett er en risiko for enheter koblet på internett. I år ble det nok en gang avdekket en rekke sårbarheter i en chip Android-smarttelefonene bruker (Muhammad, 2020). Det er rundt 400 sårbarheter og disse kan utnyttes til å få tak i alt av informasjon som ligger på telefonen, kontroll over kamera, mikrofon og høyttaler. I tillegg kan telefonene enkelt saboteres ved å stenge tilgangen til nettverk.

3.2.2 Geotagging

Mange er ikke klar over hvor mye informasjon som faktisk deles "skjult" gjennom sosiale medier. Når en tar et bilde med en smarttelefon lagres det mye tilleggsinformasjon i bildefilen, såkalt *exif*-data. Dette er en ekstra komponent med informasjon som lagres sammen med bildefilen. Dersom GPS-data er tilgjengelig, noe det ofte er, lagres koordinatene bildet er tatt fra sammen med bildefilen. Når dette lastes opp på internett er dette tilgjengelig for hvem som helst (AVG, 2015). En aktør med tilgang til disse filene vil kunne kartlegge hvem som var hvor, og når.

Flesteparten av de mest populære sosiale media-appene tilbyr og oppfordrer til å dele GPS-lokasjonen direkte. På Snapchat er det en funksjon som deler din GPS-lokasjon i sanntid og fremstiller dette på et kart som viser hvor du er, eller sist var når appen var på nett, til enhver tid. Instagram oppfordrer til å “tagge” bildene du laster opp med en lokasjon og gjør dette så enkelt som mulig for brukeren. På denne måten trenger ikke en aktør å gå inn i *exif*-dataene for å se GPS-koordinater, det blir direkte servert til alle som måtte komme over bildet. Facebook tilbyr også muligheten til å “sjekke inn” på alle mulige steder i verden, som også da publiserer informasjon om hvem, hva, hvor og når (Silkstream,

2016). Smartklokker og treningsklokker bruker ofte GPS for å hente inn data som løperuter.

3.2.3 Internet of Things

Tilgangen til internett har blitt enklere de siste tiårene. Kostnaden for internettbruk synker og flere og flere "ting" blir skapt med muligheter for tilkobling til nett, og prisen på teknologi synker (Morgan, 2014). "*Internet of Things*" (IoT) brukes som begrep om alt av enheter som kobles på internett. Dette er blitt et begrep som følge av at internett-tilkobling ikke lenger i hovedsak er for datamaskiner og telefoner. I dag kan alt fra vaskemaskiner til kjøleskap og garasjeporter kobles til og styres gjennom smarttelefonen, via internett. Analyser tilsier at det i 2020 vil være over 26 milliarder tilkoblede enheter på internett (Morgan, 2014). Norges vassdrag- og energidirektorat besluttet at innen 1. januar 2019 skulle alle norske hjem få smarte strømmålere (NVE, 2015). Disse strømmålerne er også koblet til nettet og sender inn data om strømforbruket. Dette er data som vil kunne vise når brukeren er hjemme, sovende, drar på jobb eller er på ferie (Datatilsynet, 2018). Informasjon fra strømmåleren kan du også få rett inn på smarttelefonen via en app (Istad, 2019).

3.2.4 Big data

Big data er i utgangspunktet ment som noe som gir fordeler for enkeltindividet. Det er samling av strukturert, semistrukturert og ustrukturert data utført av organisasjoner, som kan brukes til å generere informasjon og profiler, og prosesseres av avanserte analysesystemer (Rouse, 2019). Det er mange måter disse dataene samles inn. Kredittkort gir f.eks. informasjon som lagres rundt hvilke kjøp som gjøres når, og det gir detaljert data som kan brukes til å lage en profil med brukerens preferanser og handlemønster. Denne profilen kan så selges videre. Mange organisasjoner utvikler apper som henter inn geo-data i bytte mot å gjøre bruken enklere. Flere epost-leverandører henter også data fra postkassene til brukere og lager slike profiler. Sosiale medier er også en enorm kilde for *big data*, det samme er alt av geotagger og data fra IoT. Alle disse dataene mates inn i system og analyseres for å lage profiler som omhandler alt av hva en person er interessert i, dagsmønsteret til personen, hva den jobber med osv. (Rybkin, 2018). Dette brukes i hovedsak til markedsanalyser og skreddersydd reklame til hver enkelt bruker. I lys av etterretningsvirksomhet er *big data* en god kilde for informasjon, med andre ord

ubehandlet data som kan bearbeides og bli omgjort til etterretninger for å skape bedre forståelse og minske usikkerhet (Etterretningstjenesten, 2013).

Selv anonymisert data er ikke nødvendigvis sikret mot å bli korrekt koblet til en persons *big data*-profil (Rouse, 2014). I 2018 innførte Norge GDPR (General Data Protection Regulation), en lov som stiller nye krav til behandlingen av person-data i EU- og EØS-land (Regjeringen, 2018). Denne loven har blitt kritisert av bl.a. Næringslivets Hovedorganisasjon for å være generell og vag, og legge opp til at bedrifter selv skal vurdere hvordan loven skal etterfølges (NHO, 2017). En ondsinnet aktør kan helt lovlig kjøpe de personlige profilene til individer de måtte være ute etter informasjon om. NRK gjorde slike kjøp i fjor, og skrev artikkelen "Norske offiserer og soldater avslørt av mobilen" (Gundersen, Skille, Lied, Grafsrønningen & Jansson, 2020), hvor de klarte å kartlegge mye om hvem som gjorde hva i bl.a. Forsvarets Spesialkommando (FSK) og andre operative enheter. Kina er også verdt å nevne i forbindelse med det sosiale mediet TikTok. Ettersom kinesisk lovgivning pålegger private virksomheter og enkeltpersoner å overlevere alt av informasjon til myndighetene vil da alt av data som bilder, lyd, geodata, brukerprofiler osv. samles opp og kunne brukes fritt av kinesisk etterretning og andre statlige organer (Kampsæter, 2020).

3.2.5 Mennesket som sårbarhet i systemet

Det er flere måter menneskelig svikt kan forekomme, enten ved uhell, manglende forståelse eller ved direkte ignoranse (Kaspersky, 2017). Det viser seg også at det er manglende forståelse og/eller kunnskapsløshet om regler, rutiner og retningslinjer som er årsaken til flest sikkerhetshendelser, gjennom *phishing*- og *malware*-hendelser (Kaspersky, 2017). Manglende forståelse for risikoen en tar ved å klikke ukritisk på lenker eller åpne filer en får tilsendt er, ifølge Kaspersky, den største kilden til sikkerhetshendelser globalt (Kaspersky 2017). De viser videre til at bakgrunnen for denne mangelen kan være at IT-sikkerhetspolicyene som settes inn ikke er nok. En policy alene vil ikke beskytte mot trusler, både fordi policyer ofte ikke følges, eller fordi de er vanskelige å forstå. I tillegg kan ikke en policy dekke hver eneste potensielle risiko. "Instead of communicating risks, dangers and good practices in clear and comprehensive instructions, businesses often give employees multipage documents that everyone signs but very few read – and even less understand." (Kaspersky, 2017).

Dette understøttes av Daniel Osen, sikkerhetsmedarbeider i Militærpolitikompaniet. Han mener at policyer blir for vagt. “Jeg våger å påstå at policyer oppfattes som en «bør»-sak, kontra en «må»-sak." (Kampsæter, 2020). Videre sier han at informasjonssikkerhet er et lederansvar, selv om brukerne er ansvarlig for eget bruk. Det må være tydelige ordrer, ikke policyer og retningslinjer fra ledelsen, mener han. Rekrutter som ble intervjuet i forbindelse med artikkelen “Rekrutter vil ha tydeligere føringer for sosiale medier” svarer at de eneste føringene de har fått er at det ikke er tillatt med bilder av våpen eller bilder på enkelte steder i leir (Kampsæter, 2020). “Alt i alt så har vi ikke fått noen god pekepinn på hva som er greit eller ikke” legges det til. I NRKs artikkel “Norske offiserer og soldater avslørt av mobilen” spørres Viseadmiral Elisabeth Natvig, sjef Forsvarsstaben, om hvorfor Norge ikke har klare retningslinjer for deling av data (Gundersen et al, 2020). “Vi har jo en policy og retningslinjer knyttet til bruk av sosiale medier og en del slike ting, men dere henviser spesifikt til dette med stedstjenester. Det er nok noe vi bør være mer bevisst på hvordan vi skal regulere” svarer hun.

3.2.6 Kampen om narrativet i sosiale medier

En annen side av saken er kampen om narrativet og informasjonsdominans. Dagens situasjon er at moderne informasjons- og kommunikasjonsteknologi er tilgjengelig for alle (Diesen, 2018, s. 22). Kontroll over sivilbefolkningen er gått over til å bli en kamp om påvirkningen av sinnene. Dette har ført til at irregulære operasjoner som geriljakrigføring er blitt erstattet av påvirkningsoperasjoner som søker å påvirke holdninger og vilje (Diesen, 2018, s. 23). Kampen om narrativet avgjøres gjennom å være det folk flest oppfatter at stemmer best med virkeligheten, eller som appellerer best til folkets følelser, fordommer eller preferanser (Diesen, 2018, s. 23). Den mest sannsynlige bruken av cyberdomenet for militære formål vil være som en plattform for kampen om virkelighetsbeskrivelsen. Denne kampen vil da dreie seg om å skape et narrativ som er gunstig og som målgruppene finner mest i samsvar med det de selv ser og opplever (Diesen, 2018, s. 24). Dette omhandler da både å nedkjempe motstanderens forsøk på å ta kontroll over narrativet, men også å beskytte sitt eget narrativ. Måtene dette kan gjøres på er mange, og et enkelt eksempel er tjenestenektelsesangrep (DoS) som kan hindre tjenester eller nettsider å fungere, og dermed hindre en aktør i å nå ut med sitt budskap eller informasjon. Slike angrep må en også kunne forsvare seg mot (Diesen, 2018, s. 24).

Fremveksten av sosiale medier har skapt en ny dimensjon i kampen om narrativet. Disse mediene er ofte helt foruten noen form for redaksjonelt ansvar for innhold som også har en ekstrem spredningshastighet. Dette er dermed et svært kraftig våpen i denne kampen, og spesielt kraftig når kampen om narrativet er tidskritisk (Diesen, 2018, s. 25). Det kan være enkelt å rette på en forvrengt fremstilling av virkeligheten, men om denne forvrengningen har til hensikt å påvirke en bestemt hendelse, slik som et politisk valg og spredning av misinformasjon om enkelte kandidater, er det stor sjanse for at det ikke vil kunne rettes opp i tide. En annen utfordring rundt slik spredning av falsk informasjon i sosiale medier er at brukerne selv kan velge bort alt av informasjon som ikke er i tråd med deres ønskede eller etablerte oppfatning av sannheten. Spredning av misinformasjon og propaganda, eller hindring av eksempelvis staten Norge i å komme ut med sitt narrativ, kombinert med militære aksjoner fra en aktør vil i stor grad kunne skape kaotiske tilstander og påvirke sinnene i både sivilbefolkningen og soldatmassen (Diesen, 2018, s. 25).

Sosiale medier har en svakhet grunnet business-modellen til de sosiale medienes firmaer. Firmaene fokuserer på å vise brukeren hva den ønsker å se, og gjør det de kan for å holde brukeren på plattformen lenger, i den hensikt å tjene mer penger på bl.a. å vise brukeren reklame (McMaster, 2020, s. 47). Fokuset til disse firmaene er i hovedsak på brukeropplevelsen og funksjonalitet. Det er ikke fokus på hvordan plattformen kan misbrukes av ondsinnede aktører, eller på å ha kontroll over at informasjonen som spres er korrekt. Algoritmene som avgjør hva som presenteres til brukeren fører ofte til mer ekstreme meninger og dermed polarisering (McMaster, 2020, s. 47). Et eksempel her er når YouTube foreslår hvilke videoer du også bør se om du har vært inne på én type videoer, brukeren ledes så videre ut til ekstremt og polariserende innhold, fordi det er det brukere oftere klikker på, og hva en brukers profil generert gjennom *big data* sannsynligvis vil være interessert i (McMaster, 2020, s. 47).

Dette er noe Russland har identifisert som en lav-kostnad og lav-risiko metode for å svekke forholdene mellom de vestlige statene og skape splid innad i landene (McMaster, 2020, s. 48). Dette skal vi se mer på i et senere kapittel. Valerey Gerasimov, sjef GRU (General Staff of the Armed Forces), sa i 2013 “The very ‘rules of war’ have changed. Non-military means of achieving political and strategic goals have grown and, in many cases, exceeded the power of force of the weapons in their effectiveness.” (McMaster, 2020, s. 40). Denne nye typen *maskirovka* (russisk uttrykk for taktisk villedning og kamuflering) på nett

innebærer integrering av forstyrrende teknologier i militære system i den hensikt å utnytte sårbarheter i andre land (McMaster, 2020, s. 56).

3.3 Digital sikkerhet i Norge i dag

3.3.1 Retningslinjer/regelverk

Forsvarets sikkerhetsavdeling (FSA) er det organet som står for Forsvarets policyer rundt bruk av sosiale medier. I mai 2020 kom det en oppdatert versjon av dette dokumentet. I policyen nevnes det at sosiale medier er nyttige verktøy, men også noe som kan utnyttes av fremmed etterretning, terrorister og andre kriminelle rundt innhenting av informasjon om Forsvarets personell (Herland, 2020, s. 3). I punktet om publisering av personlig informasjon står det at dette lett kan utnyttes til å videre fremskaffe informasjon av større verdi, og at Forsvarets personell må være bevisst på dette. Det nevnes også i en setning at denne informasjonen kan brukes for å "påvirke deg, dine nærmeste eller Forsvaret på en negativ måte." (Herland, 2020, s.4).

Policyen tar også for seg delingstjenester som Facebook, Instagram og Snapchat. Det oppfordres der til å sette seg inn i risikoene og gjøre vurderinger basert på dette. "Bli kjent med tjenesten, les vilkårene og sett deg inn i hvilke sikkerhetsmessige utfordringer dette kan by på for deg. Vurder hvilke muligheter du har for å ivareta personvernet for deg selv og de rundt deg, og bruk sikkerhetsinnstillingene aktivt." (Herland, 2020, s. 5). Stedstjenester, som geotagging og lignende, tas også opp. Det beskrives kort hva det er, og nevnes at dette kan være interessant informasjon for aktører interessert i å skade deg eller Forsvaret. Det nevnes så at denne informasjonen, koblet sammen med offentlig tilgjengelig informasjon og informasjon fra andre sosiale medier kan avdekke mye detaljert informasjon om en person. "Vurder å slå av disse stedstjenestene for å redusere skadepotensiale mot deg og Forsvaret." (Herland, 2020, s. 6). Det er lite konkrete eksempler eller klare føringer, ord som går igjen i hele policyen er "vær klar over" og "vurder selv".

3.3.2 Opplæringen i dag

Vi har fått innsyn i dagens opplæring av soldater innenfor IT-sikkerhet gjennom et sentralt fagmiljø, som av operative hensyn holdes anonymt. Dagens opplæring er utdatert, ikke oppdatert siden 2017, og det finnes ikke klare leksjonsmål, eller kunnskapsmål, for

opplæringen (anonym informant, 2020, 14. desember). Likevel oppfattes opplæringen som fungerende, til en viss grad. Dette skyldes mye at dagens soldater er unge og teknologisk flinke, men naive i møtet med sosiale medier og hva de deler om seg selv. Føringene som gis rundt bildedeling av materiell og fra innsiden av leire følges til en viss grad. Utdanningen gir forståelse hos soldatene for at det er sosiale medier og smart-telefoner som utgjør den digitale sårbarheten, både for dem selv og organisasjonen. Det er kun egen bruk av sosiale medier og smart-telefon utdanningen tar for seg. Hovedutfordringen med dagens utdanningsprogram er at soldatene får opplæringen tidlig i tjenesten, og deretter minimalt med påfyll, oppfriskning eller oppdateringer. En annen utfordring er at utdanningsprogrammet er utdatert, og ikke tar for seg andre aktuelle kapasiteter andre aktører har og potensielle sårbarheter som følger med eksempelvis big data og kampen om narrativet.

3.3.3 Mottiltak og faktorer i Norge

Det er satt inn flere tiltak for å redusere sårbarheten til Forsvarets personell og sivilbefolkningen generelt på nett. Vi skal se på noen av de mest relevante tiltakene for denne oppgaven, samt noen av de relevante faktorene som er til stede i Norge som påvirker sårbarheten for disse nye truslene. Et av tiltakene er sikkerhetsklarering og personopplysningsblankett (POB). Sikkerhetsklarering innebærer at klareringsmyndigheten (Nasjonal sikkerhetsmyndighet, NSM) tar en avgjørelse rundt hvorvidt en person er skikket til å ha innsyn i og behandle sikkerhetsgradert informasjon (Nasjonal sikkerhetsmyndighet, 2014). Hensikten bak dette er å beskytte virksomheter, som for eksempel Forsvaret, som er omfattet av sikkerhetsloven mot organisasjoner eller enkeltindivider som kan være en trussel mot nasjonale sikkerhetsinteresser. Dette er da et tiltak mot sårbarhet i form av utpressing, fristelser og lignende som kan føre til at en person begår sikkerhetstruende handlinger (NSM, 2014). Prosessen for å motta en sikkerhetsklarering inkluderer utfylling av personopplysningsblanketten (POB). Denne blanketten skal avdekke om det er forhold rundt personens pålitelighet, lojalitet og dømmekraft i forbindelse med behandling av sikkerhetsgradert informasjon (NSM, 2014). Den ber søkeren erklære forhold som gjeld, affiliasjoner til diverse miljøer, familieforhold, lovbrudd, forhold til rus og en rekke andre faktorer som kan gjøre en person sårbar for utpressing (NSM, 2019b). Gjennom dette garderer søkeren seg mot for eksempel at en aktør presser personen ved å avdekke pinlige forhold rundt rusutfordringer eller andre faktorer, ettersom dette allerede er informasjon personen har meldt ifra om. Denne informasjonsinnhentingen kan også hjelpe NSM med å

kartlegge hvilke personer som kan være sårbare for eksempelvis bestikkelser eller økonomiske fristelser ut ifra hvem som har gjeldsproblemer, og ta dette med i vurderinger rundt sikkerhet og skikkethet.

NSM har også andre ansvarsområder. De er tilsyns- og fagmyndighet innenfor forebyggende sikkerhet iht. sikkerhetsloven og er det organ med sertifiseringsmyndighet for IT-sikkerhet i produkter og systemer i Norge, dette gjelder også systemer og produkter i Forsvaret (NSM, 2019a, s.3). NSM har dessuten ansvar for å produsere risikobildet innen forebyggende sikkerhet og rapportere om tilstanden og trusselvurderingene til Etterretningstjenesten og Politiets sikkerhetstjeneste, samt foreslå tiltak for å forbedre sikkerhetstilstanden. De har spesielt ansvar for å vedlikeholde risikobildet for digital sikkerhet rundt statssikkerhet, samfunnssikkerhet og individsikkerhet, samt foreslå tiltak og stille krav til digital sikkerhet i samfunnet og følge opp dette. Det er også NSMs jobb å bidra til samfunnets kunnskap, forståelse, evne og motivasjon til å ivareta digital sikkerhet (NSM, 2019a, s. 4). Nasjonalt cybersikkerhetssenter (NCSC) er underlagt NSM og har i oppgave å detektere, analysere og håndtere dataangrep i Norge (NSM, 2020).

Faktorene som spiller inn i Norge rundt digitale trusler og polarisering av befolkningen som følge av ekstern påvirkning er flere. Sosiologien er relevant å nevne, da det mangler politiske og sosiale forutsetninger som undertrykte befolkningsgrupper på landsbasis. Det eneste potensialet for dette ville vært i form av mindre grupperinger innad i større byer som etableres som en kunstig "motstandsbevegelse" av eksterne aktører, eller utviklet fra kriminelle gjengmiljøer (Diesen, 2018, s. 25). Den politiske demokratiske situasjonen i Norge er også en faktor som styrker Norges motstandsevne mot slik påvirkning. I Norge er det lite distanse mellom politikerne og befolkningen, og det medfører en høy grad av tillit mellom disse (Diesen, 2018, s. 44). Myndighetene vil da kunne nytte seg av informasjonskampanjer og andre tiltak for å bevisstgjøre befolkningen og forberede dem på hva slags virkemidler de vil kunne møte i en konflikt, og hvordan de da skal forholde seg. Pressen i Norge har også strenge krav å forholde seg til ift. kildekritikk. Dette gjør det vanskelig for en aktør å manipulere virkelighetsbildet til befolkningen, spesielt rundt saker som omhandler sikkerhetspolitikk (Diesen, 2018, s. 45). Sistnevnte faktorer gjør det også enklere for myndighetene i Norge å ha kontroll over narrativet.

3.3.4 Troppssjefen som rollemodell - Hva slags opplæring får kadetten?

3 år etter påbegynt bachelor skal Krigsskolekadettene bli offiserer og lede sin egen tropp i avdeling. Kadetten blir da utdanningsleder, som innebærer å planlegge utdanningen og drive med noe utdanning selv. For kull 18-21 på operativ linje ble den eneste opplæringen relatert til cybertrusler gjennomført i delemnet "Militær teknologi og innovasjon" som del av emnet "Kontekst landoperasjoner" (Forsvarets høgskole, 2020). Ut ifra delemnebeskrivelsen er ferdighets- og kunnskapsutbytte knyttet til teknologi som et bredt begrep. Innholdet rettet mot cyber er:

- Emnet tar for seg signaturer som fanges opp av sensorer, eksempelvis elektromagnetisk signatur og sensorer.
- Emnet tar for seg etterretningsanalyse i forhold til big data.
- Risikoanalyse, samt oppnå en forståelse for sårbarhet, trussel og verdi.

I tillegg til dette er det fem relevante artikler til cyber:

- *Greenberg, A. (2017). How an entire nation became Russia's test lab for cyberwar*, som tar utgangspunkt i Ukraina og hvordan Russland utnyttet skadevare for å kutte strømnettet til Ukraina.
- *FFI* rapport (2016) med *Teknologien Forsvaret trenger*, som tar for seg informasjonsteknologi, smarttelefon, Internet of Things og cyberforsvar.
- *Adams, M. (2015). Cybergeddon Military Technology,* som omhandler cyberspace rettet mot cyberkrig, hacking, spionasje og kriminalitet.
- *Aven, T. (2012). Risikotenkningen er fullstendig foreldet*
- *Symon, P. B. & Tarapore, A (2015) Defense, Intelligence Analysis in the Age of Big Data*, som tar for seg etterretning og big data.

Det er med andre ord relativt lite pensum og kompetansemål rettet mot cyberdomenet med digitale trusler og datasikkerhet (Forsvarets høgskole, 2020). I *NOU 2015: 13 Digital sårbarhet – sikkert samfunn* foreslår Lysne-utvalget at "IKT-sikkerhets- og personvernrelaterte problemstillinger måtte få en større plass i relevant høyere utdanning" (Justis- og beredskapsdepartementet. 2018, s. 1). Deretter ble det fastsatt av Kunnskapsdepartementet 18. mai 2018 at generell kompetanse i bachelorutdanningen av ingeniører gjør at "Kandidaten kan identifisere sikkerhets-, sårbarhets-, personverns- og datasikkerhetsaspekter i produkter og systemer som anvender IKT" (Kunnskapsdepartementet, 2018, s. 2).

4 Case-eksempler

4.1 Russisk *maskerovka* mot Vesten

Selv om Russland aldri har innrømt å drive en informasjonskrig på nett mot Vesten er det mye bevismateriale for nettopp dette, og mange hendelser som linkes til Russland. Russiske cyber-angrep og informasjonskampanjer rettet mot europeiske valg, samt det amerikanske presidentvalget i 2016, er bare deler av det store bildet i Russlands nye strategi. Målsettingen er å skape splittelse mellom USA og Europa, mellom land i Vesten og mellom folkegrupper innad i disse landene. Dette søkes oppnådd gjennom polarisering av folkegrupper på sosiale medier, samt undergraving av myndighetene og den politiske prosessen (McMaster, 2020, s. 26).

Russisk propaganda kan beskrives som en massiv røykskjerm av misinformasjon som konstant blir større. Målet med denne røykskjermen er å få innbyggerne i land Russland anser som konkurrenter til å stille spørsmål ved absolutt alt. Dette skal skade tilliten mellom befolkning og regjering, samt mellom folkegrupper, og skape splittelser samtidig som det svekker samfunnene i sin helhet. Dette gjøres gjennom å gå til angrep på innbyggernes felles identitet, demokratiet og nasjonens institusjoner ved å manipulere sosiale medie-plattformer med falske historier og personer (McMaster, 2020, s. 41).

I 2004 opplevde Ukraina russisk innblanding i landets presidentvalg. Den pro-russiske presidentkandidaten Yanukovych lå an til å tape valgkampen til tross for 300 millioner dollar i støtte fra Russland (McMaster, 2020, s. 42). Den mer Russland-kritiske Yushchenko var mer populær blant folket, og ble da forgiftet slik at han ikke var i stand til å stille (BBC, 2018). Yanukovych vant valget, men dette førte til revolusjon i Ukraina, og han ble avsatt etter kort tid. Yanukovych prøvde igjen i 2010 og han ble da valgt som president. Gjenvalget i 2014 ble forsøkt påvirket av Russland, men dette lyktes de ikke med, og Yanukovych ble igjen avsatt tross russiske cyberangrep mot stemmesystemene (McMaster, 2020, s. 42). Selv om disse forsøkene på innblanding ikke nødvendigvis nådde de direkte målene, bidro de til å skape uro i sivilbefolkningen og rundt den demokratiske prosessen. Lignende forsøk på innblanding i valg ble også gjennomført rundt 2015 mot land som Storbritannia, Tyskland, Nederland, Italia, Frankrike, Tsjekkia og en rekke flere vest-europeiske stater (McMaster, 2020, s. 43).

Over tid har Russland lært å skreddersy misinformasjons-kampanjene til spesifikke land og folkegrupper. Dette ble synlig i Montenegro i 2016. På denne tiden var Montenegro på vei inn i EU og NATO, og landet var den siste biten av Adriaterhavskysten som ikke var under kontroll av NATO. Russland gjorde alt de kunne for å hindre Montenegro i å bli med i både EU og NATO. Politiske partier som var EU-kritiske ble støttet finansielt. Misinformasjonskampanjer på sosiale medier og cyberangrep mot nyhetsmedier og regjeringens nettsider ble gjennomført (McMaster, 2020, s. 43-44). I tillegg var russiske agenter på plass til å gjennomføre statskupp dersom EU-vennlige Dukanovic skulle vinne, men disse ble avslørt og stanset (BBC, 2019).

Russland identifiserte også store demografiske skiller mellom presidentkandidatene i USA i forkant av valget i 2016. De var da raskt ute med å utnytte dette og startet arbeidet med å utvikle polariseringen i samfunnet videre. Russiske Internet Research Agency (IRA), en underavdeling av GRU, brukte sosiale medier til å publisere propaganda og misinformasjon. Frem til valget nådde de over 126 millioner brukere med disse postene (McMaster, 2020, s, 46-47). Postene omhandlet problemstillinger som skapte splittelser i befolkningen og var ment til å drive disse befolkningsgruppene til stadig mer ekstreme sider av disse problemstillingene. Noen av postene var også ment som støtte for amerikanske policyer som var gunstige for Russland, som for eksempel uttrekning av amerikanske militære styrker fra Syria og Afghanistan. IRA tok også i bruk såkalte "*click farms*", som får poster til å virke mer populære enn de er og således trekker oppmerksomhet, og dermed utnytter svakheter i sosiale medier som plattform for nyheter og informasjon (Pastoor, 2019). Problemstillingene som her ble fokusert på av GRU var bl.a. våpenregulering i USA, klimaendringer, rase og innvandring (McMaster, 2020, s. 48).

Black Lives Matter-bevegelsen (BLM) ble en del av hovedinnsatsen til IRA. Som nevnt er rase noe av det som polariserer den amerikanske befolkningen i størst grad. IRA kjøpte over 3000 annonser på Facebook som omhandlet BLM og rettet disse både mot folkegrupper som ville bli provosert og folkegrupper som ville sympatisere. Dette ble muliggjort gjennom *big data*-genererte profiler (Entous, Timberg & Dwoskin, 2017). IRA publiserte både artikler og videoer rundt BLM og politivold mot fargede, men også propaganda for "hvite militser" som motsats for ytterliggere å polarisere befolkningen.

Over 1000 videoer relatert til BLM og politivold ble publisert av IRA forkledd som nyhetskilder og lignende (McMaster, 2020, s. 48-49).

Uttrykket *"fake news"* kom også i denne perioden. Det var minkende tillit til tradisjonelle kilder for informasjon, som de tradisjonelle mediene i USA, og dette gjorde manipulering av nyhetsbildet og narrativet enklere for GRU. At presidentkandidat Trump var kritisk til de tradisjonelle mediene, og stadig brukte begrepet *"fake news"*, gjorde at befolkningens tillit til informasjonen som ble utgitt stadig sank (McMaster, 2020, s. 49). På denne måten klarte Russland å få det amerikanske folket til å bli skeptiske til absolutt alt av informasjon. De tradisjonelle mediene endte også ofte opp med å styrke russisk-skapte konspirasjoner og misinformasjon gjennom å forsøke å avkrefte dem. Med så mye motstridende informasjon, manglende tillit mellom folk, regjering og tradisjonelle medier, ble mediene ofte ikke trodd og dermed bidro de mest til å spre konspirasjonene og misinformasjonen ytterliggere (McMaster, 2020, s. 49).

Cyberangrep var også en stor del av denne kampanjen rundt presidentvalget. I mars og april 2016 ble presidentkandidat Clinton, The Democratic National Committee (DNC) og The Democratic Congressional Campaign Committee (DCCC) hacket. GRU plantet *malware* ved å utnytte den menneskelige sårbarheten i de ansatte og hentet ut eposter og andre dokumenter. Gjennom DCLeaks og Wikileaks publiserte GRU nesten 20.000 eposter og over 8000 vedlegg fra disse ansatte, noe som førte til synliggjøring av mye lobbyvirksomhet og ufint spill mellom kandidatene og instansene (McMaster, 2020, s. 50). Dette igjen bidro da til ytterliggere misnøye, mistillit og polarisering av befolkningen.

Denne samlede innsatsen for å polarisere samfunnet gjennom bruken av cyberdomenet med misinformasjon, propaganda og manipulering av sosiale medier klarte å skape denne røykskjermen Russland var ute etter i USA. Utnyttelsen av brukerprofiler skapt av *big data* forenklet målutvelgelses-prosessen for GRU, i forhold til hvilke folkegrupper som ville bli påvirket av hva. Det førte til at befolkningens tillit til både tradisjonelle medier og til regjeringen ble sterkt svekket.

4.2 Ukraina (2014)

Som nevnt i forrige case-eksempel ble det Ukrainske presidentvalget i 2014 forsøkt påvirket av Russland. Noen dager før valget ble datasystemet til Ukrainas sentrale

valgkommisjon (CEC) utsatt for et cyberangrep. CEC klarte å gjenopprette systemet igjen før valget, men på valgdagen ble nettsiden igjen utsatt for angrep. Det ble lagt ut et bilde av en kandidat fra høyresiden som angivelig hadde vunnet valget. Russisk rikskringkasting sendte fortløpende den falske historien med bilde av den angivelig nyvalgte ukrainske presidenten som var hentet fra den angrepne nettsiden. Ukrainsk etterforskning fant i etterkant *malware* i valgkommisjonens system. Dette ble sporet tilbake til aktøren *Fancy Bear*, også kalt *APT28 (Joselow, 2016).* Angrepet ga ikke utslag for valgresultatene, men kan fortsatt ha oppnådd målet deres med å undergrave valget og forstyrre prosessens integritet og kredibilitet. Selv om Russland benekter innblanding, var deler av koden i skadevaren skrevet på russisk, og den ble laget i russisk arbeidstid. Det er også et nært bånd mellom Fancy Bear sin aktivitet, nyheter i Russland og sosiale medier. Når en lekkasje forekommer, er nyheten allerede klar til å bli publisert i Russiske globalt-rekkende medier (Joselow, 2016).

I forkant av dette valget begynner det å skje mye i Øst-Ukraina. Etter et par måneder med demonstrasjoner og uro i befolkningen forsvinner president Yanukovych den 22. februar 2014 (BBC, 2014b). 27. Februar inntar "pro-russiske opprørere" nøkkelbygninger i hovedstaden på Krim-halvøya. Uniformerte soldater, uten flagg eller andre distinksjoner, begynner å dukke opp flere steder på Krim. 1. mars godkjenner det russiske parlamentet bruk av militære midler til å beskytte russiske interesser i Ukraina. 16. mars erklærer Krim seg som en del av Russland, etter å ha gjennomført avstemning, hvor 97% av stemmene var for separeringen fra Ukraina. Vesten anerkjenner ikke dette valget. Opptøyer over store deler av Ukraina fortsetter gjennom våren og sommeren. Kampene pågår mellom Ukrainske militærstyrker og "pro-russiske opprørere" frem til 5. september. 24. september rapporterer NATO at store russiske styrker trekker ut av Øst-Ukraina. All form for militær innblanding benektes av russiske myndigheter (BBC, 2014b).

I denne væpnede konflikten mellom "opprørere" og Ukrainske militære styrker er det spesielt to momenter som er relevante for denne oppgaven. Under de pågående kampene lager en ukrainsk artilleri-offiserer en app til mobiltelefoner som kalkulerer innstillingene til Howitzer-kanonene deres (Martin, 2016). Denne bruken av relativt enkel teknologi senker tiden mellom avfyring på kanonene fra minutter til sekunder. Informasjon om appen og bruken ble publisert av ukrainerne på YouTube, noe russisk etterretning raskt fikk med seg. Appen ble hacket, og spor fra hackingen ledet tilbake til Fancy Bear. Russland fikk

dermed full tilgang til all informasjon fra telefonene denne appen var installert på, og kunne dermed lede artilleri-ild rett mot disse målene gjennom geodata (Shankland, 2016).

Det andre relevante momentet er de russiske styrkenes personlige bruk av sosiale medier i denne perioden. President Vladimir Putin gikk klart og tydelig ut og avkreftet at det var noen form for russisk militært nærvær i Øst-Ukraina (Trujillo, 2014). Russiske soldaters bruk av sosiale medier forteller en annen historie. Geodata fra en av soldatenes Instagram-bilder avslører at han var i Øst-Ukraina i denne perioden, mer spesifikt i landsbyene Krasna Talycha og Krasny Derkul, som på det tidspunktet ble kontrollert av disse "pro-russiske opprørerne" (Szoldra, 2014). I Russland brukes en plattform som kalles VKontakte (tilsvarende Facebook). På denne plattformen er det en rekke poster fra den aktuelle perioden, postet av russiske soldater, med titler som [oversatt fra russisk] "På vei til Ukraina" og "Vi bombet Ukraina hele natten" med bilder av russisk militært utstyr (Szoldra, 2014).

4.3 Norge/Stortinget

Som tidligere belyst, er det mange cybertrusler og metoder som kan benyttes i nettverksoperasjoner. I august 2020 ble Stortinget rammet av en større cyberoperasjon. Etterforskningen utført av PST, Etterretningstjenesten og Nasjonal sikkerhetsmyndighet viser at aktøren brukte en metode som kalles *passord-bruteforcing* i den hensikt å skaffe brukernavn og passord (PST, 2020c).

Brute force angrep er en prøving- og feilingsmetode for å gjette alle mulige kombinasjoner i innloggingsinformasjon. Brute force gjøres gjerne fra et program på en maskin, for å trenge seg inn i kontoer. Dette er en enkel, men fortsatt effektiv og populær metode blant aktører. Metoden avhenger av passordets lengde og kompleksitet, og kan ta alt ifra sekunder til år å bryte igjennom. Så vel som passordets lengde, avhenger innbruddstiden også av maskinens prosessorkraft og tid til disposisjon (Kaspersky, 2020) For å beskytte seg mot slikt kan både administratoren av et nettverk og brukeren gjøre tiltak som gjør det vanskelig for en aktør å lykkes. En administrator kan eksempelvis kreve to-faktor-autentisering, som gjør at en må godkjenne innlogging på to måter, eller begrense antall innloggingsforsøk som kan benyttes. Brukeren kan benytte seg av lengre passord i kombinasjon med tegn og tall. I tillegg burde flere komplekse og usammenhengende ord benyttes sammen. Brukeren bør holde seg unna vanlige passord, og benytte forskjellige

passord på forskjellige nettsider. Disse tiltakene kan gjøre at det tar mange år før et *brute force* angrep vil lykkes (Kaspersky, 2020).

Brute force-metoden ble benyttet mot et stort antall brukere i e-post systemet til Stortinget. Aktøren har vellykket skaffet seg gyldig innloggingsinformasjon, og benyttet dette til å logge seg inn på noen brukerkontoer, hvor ble det hentet ut sensitiv informasjon og innhold. Aktøren har videre forsøkt å ta seg inn i Stortingets datasystemer, uten å lykkes. Etterforskningen viser at aktøren bak cyberangrepet sannsynligvis var *Fancy Bear*, også omtalt som *APT28* og er tilknyttet GRU, som er Russland militære etterretningstjeneste. Angrepet var en del av en større kampanje som har pågått siden 2019, både internasjonalt og nasjonalt (PST, 2020c). Samme aktør kan knyttes til angrepet mot Demokratene i USA, 2016 (Ertesvåg & Persen, 2020). Etterforskningen avsluttes og henlegges fordi det er vanskelig å ta ut en tiltale for brudd på straffeloven § 121 (PST, 2020c).

"Som Norges lovgivende forsamling utgjør Stortinget et sterkt symbolmål, og er en av de viktigste bærebjelkene for integriteten til norsk suverenitet og til de demokratiske prosessene mellom norske folkevalgte. I tillegg forvalter Stortinget helt konkrete, til dels sensitive verdier som er kritisk for Norge, og som er av stor interesse for flere fremmede stater sine etterretningstjenester" (PST, 2020c). Dette gjør Stortinget til en *verdi* Norge ønsker å beskytte, da deler av *trusselaktørens* strategi er informasjonskrig og politisk subversjon, med andre ord undergravelse. Kjennskapen til *sårbarheten*, altså *brute forcing*, er en *unknown-known*. Vi vet at dette er en metode aktører kan benytte, men hvorvidt den vil påvirke oss er ikke kjent. Stortinget har heller ikke benyttet seg av kunnskapen om sårbarheten, da risikoen for et slikt angrep kunne blitt avverget ved hjelp av sikkerhetsmekanismer som to-faktor-autentisering og bedre brukerkunnskap rundt innloggingsinformasjon (PST, 2020c). Dette kan derfor sees på som *menneskelig svikt* som skyldes *manglende forståelse.*

5 Drøfting

5.1 Risiko

5.1.1 Trusler

Hvis vi går ut ifra at Russland anser seg selv i en informasjonskrig med Vesten (Jonsson, 2019), vil det ikke være kinetiske angrep som er den mest nærliggende trusselen knyttet til neste krig. Den statlige trusselaktøren Russland har kapasiteter til å drive cyberoperasjoner ettersom de har opprettet Cyber Command (Limnéll, 2015, s. 525), og dessuten har formidlet interesse for nordområdene (Diesen, 2018, s. 43). Russland har med andre ord både evne og vilje til å drive informasjonskrig og politisk subversjon, noe vi eksempelvis har sett i Norge, Ukraina og USA (McMaster, 2020), (Joselow, 2016), (PST, 2020c). En annen ikke-statlig trusselaktør er kriminelle (NUPI, 2011), som for eksempel gjennom phishing begår ID-tyveri, utpressing og datainnbrudd for å skaffe sensitiv informasjon og svindle til seg penger (NorSiS, 2020).

Når vi ser på konkrete trusler ovenfor soldater, og det som kan påvirke forholdet mellom soldaten og Forsvaret, vil vi trekke frem ID-tyveri, ekte utpressing, datainnbrudd (NorSiS, 2020), geolokalisering (Karlsen, 2019), (Lied & Svendsen, 2018), (Aale, 2019), (Garamone, 2018) og narrativpåvirkning gjennom sosiale medier som de største truslene (Diesen, 2018, s. 25), (McMaster, 2020, s. 48-49). Vi har sett at Russland gjentatte ganger forsøker å styre narrativet. Eksempelvis gjennom publisering av falske nyheter om vinneren av Ukrainas presidentvalg (Joselow, 2016), eller innblanding i det amerikanske valget i 2016. Sosiale medier, som Facebook, ble da brukt til å poste misinformasjon og propaganda gjennom falske brukere som nådde 126 millioner mennesker (McMaster, 2020, s. 47).

I et oppdiktet scenario kan en aktør drive utpressing av soldater med grobunn i informasjon som ligger på sosiale medier. Utpressingen kan gi nyttig informasjon for en aktør, og i verste fall kan soldater bli vervet som insidere (Herland, 2020). Skulle aktøren også begå vellykkede datainnbrudd, kan en aktør få tak i viktige organisasjonshemmeligheter og gradert informasjon som kan bli brukt til et videre angrep på organisasjonen (NorSiS, 2020). Ved hjelp av geodata fra apper som Snapchat, Facebook, Tinder og Strava, kan en aktør kartlegge hvor soldater og annet Forsvarspersonell oppholder seg, og hvem de er (Silkstream, 2016), (Lied & Svendsen, 2018). Ved å utnytte sosiale medier, kan en aktør

skape usikkerhet og uro i befolkningen, og styre narrativet til ens fordel (Diesen, 2018, s. 25). Utsettes soldater eller andre personer med høy tillit i samfunnet for ID-tyveri, kan en aktør utnytte dette til å spre propaganda. Dette kan en aktør som Russland gjennomføre for å oppnå målsettinger om å skape splittelse i befolkningen (McMaster, 2020, s. 26).

Gjør vi en trusselvurdering rundt hvorvidt det er sannsynlig at Russland vil gjennomføre cyberoperasjoner mot Norge, kan vi se at Russland har erfaring og kapasitet til å gjennomføre angrep (FFI, 2015, s. 32), (Rid, 2016), (Limnéll, 2015, s. 525). På grunn av deres autoritære politiske syn, umiddelbare nærhet, interesse for nordområdene (Diesen, 2018, s. 43) og ønsket om å skape splittelse i befolkning og politisk undergraving (McMaster, 2020, s. 26) kan en si at det er høy sannsynlighet for at de har en intensjon og vilje til å gjennomføre angrep. I lys av case-eksemplene fra USA, Ukraina og Norge tilsier historien at slik bruk av cyberdomenet har skjedd før, og sannsynligvis vil skje oftere i fremtiden. Det er derfor sannsynlig at også norske soldater blir utsatt for cybertrusler.

5.1.2 Verdier

Verdier som vi ønsker å beskytte, vil kunne endre seg ut ifra konteksten vi er i. Verdier er det vi ønsker å beskytte, og bortfallet av disse kan få ulike konsekvenser (NOU, 2015, s. 31). For troppssjefen og soldaten er oppdraget en verdi. For å kunne løse oppdrag effektivt, er samhold, tillit og troverdighet viktig. Både horisontalt og vertikalt samhold. Samhold er ikke bare hvorvidt mennesker knytter seg til hverandre, men også hvorvidt de forplikter seg til oppdraget. En konsekvens av at vi ikke løser våre tildelte oppdrag kan være at nasjonal sikkerhet trues. I ekstreme situasjoner vil posisjonsdata kunne ha høy verdi, og lekkasjer vil kunne ha store konsekvenser og ringvirkninger. Hvis en fiendtlig aktør allerede vet hvor vi er, kan vi enten bli omgått, eller bli forhåndsuttatte mål. En fiende med denne informasjonen vil også kunne forstå vår manøver og vi vil miste all form for overraskelse. Om en fiende vet hvor vi angriper, med hvor mange og når, vil dette kunne få fatale konsekvenser for både oppdraget og våre soldater.

Når det kommer til trusselen rundt narrativstyring i sosiale medier, er tillit mellom Forsvaret som organisasjon og personellet en viktig verdi. Hvis en aktør klarer å så tvil mellom personell innad i Forsvaret, vil dette igjen gå på bekostning av oppdraget. For soldater har også samfunnets syn på Forsvaret en direkte påvirkning på moralen. Hvis befolkningen ikke er enig i hvordan Forsvaret blir brukt, vil personellet tvile på om det de

gjør er rett. Dette kan da ha innvirkning på moralen, og hvorvidt personell ønsker å tjenestegjøre i Forsvaret (Diesen, 2018, s. 25).

For en troppssjef er troverdighet viktig for å kunne påvirke holdninger og motivasjon til underordnede og stab, og skape en felles retning. Det er de daglige gjerningene til troppssjefen som vil være grunnlaget for hans troverdighet når ekstreme situasjoner inntreffer. Når situasjonen er ekstrem er det færre ting som skal gå galt før en sjef mister sin troverdighet, og dermed sjefens evne til å ha innflytelse på soldatene. Dette har konsekvenser for narrativet soldater står igjen med, som igjen har innflytelse på hvordan oppdraget blir løst. I Forsvaret er oppdragsbasert ledelse den grunnleggende ledelsesteorien. For at denne ledelsesteorien skal fungere effektivt må det foreligge tillit. Sjefen må kunne stole på at underordnede handler etter intensjon i et skiftende situasjonsbilde.

For en fiende vil også forskjellige stillinger og funksjoner i Forsvaret ha ulik verdi. Eksempelvis vil en etterretningsoffiser ha større verdi enn en vernepliktig infanterist. Det samme gjelder hva slags rolle soldaten har i striden, hvor for eksempel bortfallet av et sambandslag kan ha større konsekvenser for striden enn et infanteristlag, da alle infanterister er avhengig av samband for å samhandle med hverandre og skape synergi. I casen Norge/Stortinget ble det påpekt at Stortinget er Norges nasjonalforsamling, og en bærebjelke som behandler "til dels sensitive verdier som er kritisk for Norge, og som er av stor interesse for flere fremmede stater sine etterretningstjenester" (PST, 2020c). Siden Stortinget er av høy verdi for Norge og andre aktører, gjør dette Stortinget til et attraktivt mål (PST 2020c).

5.1.3 Sårbarheter

Det er en del sårbarheter knyttet til cyberdomenet. En del av disse er kjente for brukerne av domenet, og det har blitt gjennomført tiltak for å være resistente mot angrep (known-knowns) (Kim, 2012). Et eksempel på dette er graderingen av informasjon, slik vi har i Forsvaret, som vi ønsker å beskytte (verdi). For at denne informasjonen skal være enkelt tilgjengelig for personell i Forsvaret ligger denne på et nettverk. Det er sårbarheter ved nettverk, da det finnes metoder for å få tak i informasjon som er digital, eksempelvis ved bruk av malware (trussel). Derfor har Forsvaret et lukket nettverk for gradert informasjon. Men igjen er det måter å få skadevare, selv på lukkede nettverk. Derfor er det for eksempel

ikke lov å bruke USB-pinner i datamaskinene som er på dette nettverket. Det er også områder vi brukere vet og erkjenner at vi ikke har identifisert alle sårbarheter, men det er nødvendigvis heller ikke her den største bekymringen ligger, da vi konstant prøver å finne sårbarheter for å motvirke dem (known-unknowns) (Kim, 2012).

Bekymringen ligger der vi har identifisert sårbarheter, men ikke vet påvirkningen av dette, og heller ikke har valgt å benytte oss av kunnskapen vi innehar for å gjøre tiltak (unknown-knowns) (Kim, 2012). Et eksempel på dette er cyberangrepet rettet mot Stortinget, hvor dette enkelt kunne blitt avverget ved å innføre to-faktor-autentisering på innloggingsinformasjonen (PST, 2020c). Vi vet at passord-brute forcing er en metode for å anskaffe seg gyldig innloggingsinformasjon, og at to-faktor-autentisering er et fungerende sikkerhetstiltak for å holde uønskede aktører unna. Likevel ble det valgt å ikke ta dette i bruk (Kaspersky, 2020).

De aller fleste har hørt uttrykket "ikke tro på alt du leser på nettet". Men fortsatt benytter mange brukere all informasjon på nettet som sannheter. Russland har interesse av å skape mistillit og splittelse blant folk og styresmakter i andre land. Propaganda er blitt implementert som del av hovedstrategien, og vår påstand er derfor at det florerer av misinformasjon på nettet. Uviten inkompetens (unknown-unknowns) (Kim, 2012) er muligens den farligste tilstanden, fordi brukere ikke vet at det finnes sårbarheter, ei heller søker etter feil. Dette kan i verste fall føre til tap av store verdier, både for Norge, Forsvaret og enkeltpersoner. Terje Aven kritiserer risikotenkning og mener den er utdatert fordi på punkter hvor kunnskapen er lav og usikkerheten stor, blir sannsynligheten og konsekvensen av faktorer vurdert til lav, og dermed lav risiko. Et eksempel på dette er risiko for soloterrorisme (Aven, 2018, s. 2).

For soldater er bruk av sosiale medier og apper, med og uten geolokalisering, en sårbarhet. Grunnen til dette er at sosiale medier er en høyst aktuell plattform for en aktør som ønsker å spre tidskritisk informasjon raskt (Diesen, 2018, s. 25). Dette kan være misinformasjon, propaganda, eller informasjon med små, nærmest umerkbare forandringer for å påvirke narrativet. Alle soldater og mennesker har blir servert et narrativ som gjør at de tar stilling til eksempelvis hvorvidt en vil tjenestegjøre for landet sitt, eller løse gitte oppdrag. Skulle en aktør lykkes med å påvirke narrativet til soldatene i stor grad med misinformasjon og propaganda, eller hindre Norge i å dele sitt narrativ med befolkningen, vil dette kunne

skape kaos (Diesen, 2018, s. 25). Når soldater bruker apper som Tinder, som deler posisjonsdata, vil dette være en annen inngangsvei for en aktør til å spionere, skaffe etterretning og utføre sabotasje eller andre angrep (Karlsen, 2019). På den andre siden bør en heller ikke frata soldater retten til å bruke sosiale medier eller apper så lenge det gjøres varsomt og med kløkt. Begrensninger vil frata soldatene deres evne til å holde seg oppdatert i samfunnet, samt forbindelse med venner og familie. Slike tiltak påvirker soldatenes trivsel.

5.1.4 Mottiltak

I profesjonsutdanning er kompetansen en tilegner seg rettet inn mot hva en skal jobbe med. Vi som kommende offiserer på operativ linje på Krigsskolen skal arbeide med mennesker, og øver i fredstid på å lede mennesker i krise og krig. Ettersom nesten alle mellom 16-34 år bruker smarttelefon (SSB, 2020), har de aller fleste mennesker i Norge et forhold til internett. Tidligere kriger har i stor grad blitt utkjempet med kinetiske våpen, men ettersom dagens forståelse av krigens natur er i forandring (Jonsson, 2019) (McMaster, 2020, s. 40), vil vi påstå at vi trener på gårsdagens krig, istedenfor å se frem og trene mot en ny, moderne krig. Det har allerede blitt påpekt at kunnskapsløshet blant brukere av cyberdomenet er grunn til de største sårbarhetene. Derfor bør all høyere utdanning i Forsvaret inkludere IT-sikkerhet i utdanningen slik det er gjort i ingeniørutdanningen (Kunnskapsdepartementet, 2018, s. 2).

For at vi skal verne om verdiene som forsvarspersonell setter høyt, må soldaters holdnings- og kompetansedannelse starte med troppssjefen. Dette for å kunne gjøre mottiltak ovenfor sårbarheter når trusler fra en aktør er sannsynlig. Ved å gi offiseren tilstrekkelig med utdanning innen IT-sikkerhet, vil troppssjefen kunne gi soldatene opplæring i hvordan bruke data- og nettverksenheter på en sikker måte. Dette minsker mulighetene en trusselaktør har til å forsere sikkerhetstiltak, vår evne til å motstå påkjenninger øker og sårbarhetene våre blir færre (FFI, 2015, s. 33).

Soldater kan selv gjøre mange mottiltak som har stor betydning. For det første bør det benyttes lengre passord, bestående av uregelmessigheter i ord, forskjellige og merkelige kombinasjoner av ord, tegn og tall. Dette kan gjøre at det tar mange år å gjette passord for en aktør, gjennom passord-brute forcing, som kan føre til at han gir opp (Kaspersky, 2020). For det andre bør en bli kjent med applikasjoner som lastes ned gjennom å lese vilkårene

grundig. Deretter bør soldater skru av stedstjenester på apper (Herland, 2020, s. 6). For det tredje bør det vurderes nøye, og være svært kritisk til, hvor mye og hva som legges ut på sosiale medier (Herland, 2020, s. 4). All dataen som gjøres tilgjengelig på nett vil kunne bli brukt til å opprette profiler og kartlegge individene gjennom big data. Dette kan i verste fall bli brukt mot brukeren og dens nærmeste for å drive utpressing eller som planleggingsgrunnlag for andre typer angrep, også kinetiske. For det fjerde må en være kritisk til hva en leser på nettet. Det kan være misinformasjon eller propaganda, laget i den hensikt å fremme en aktør sitt narrativ eller skape splid mellom grupper (Diesen, 2018, s. 25). For det femte må en være kritisk til vedlegg og linker en får tilsendt. Dette kan være phishing (NorSiS, 2020).

5.1.5 Delkonklusjon 1, risiko

En god måte å beskytte egne soldater mot cybertrusler på, er bevisstgjøring rundt risikoen soldater står ovenfor. Når vi snakker om risiko, må vi se på sannsynlighet og konsekvens. Sannsynligheten er knyttet til trussel, og konsekvens er knyttet til verdi og sårbarhet (FFI, 2015, s. 32). Russland kan anses som en trussel som både har evne og vilje til å rette cyberoperasjoner mot soldater for å så splid og svekke Vesten ved å kontrollere narrativet. Hensikten er å utnytte sårbarheter som vi enten ikke har kjennskap til, eller ikke innehar nok kompetanse om, som kan gi en fordel. Aktøren har eksempelvis interesse av geolokaliseringen til soldater som kan brukes til etterretning og videre angrep. Videre er det interesse for personopplysninger, som kan gi tilgang til sensitiv informasjon i deres jakt etter gode etterretninger. Det er derfor vesentlig sannsynlighet for cybertrusler rettet mot norske soldater.

Soldater og troppssjefer har verdier vi ønsker å beskytte. Verdiene varierer ut ifra kontekst, men verdier som oppdraget, posisjonsdata, troverdighet og samhold er noe som vil ha store konsekvenser ved tap. Bruken av sosiale medier og apper med geolokalisering er sårbarheter, fordi det er kanaler som kan brukes til å spre misinformasjon, som igjen er en måte å kontrollere narrativet på. Geolokaliseringen er en måte for en aktør å anskaffe nyttig informasjon. Det er sannsynlighet for russiske cybertrusler rettet mot norske soldater, og konsekvensene kan være store. Det er derfor risiko for cybertrusler rettet mot soldater med rolle av større betydning, som etterretnings- og sambandssoldater.

Et mottiltak som har stor effekt og gir soldater gode holdninger til IKT-sikkerhet, er opplæringen i IT-sikkerhet rettet mot troppssjefen. Dette for å gi utdanningslederen den riktige kompetansen for å kunne videreutdanne soldater, noe som vil minske risikoen mot cyberangrep. Det er flere mottiltak som er iverksatt, og mange enkle mottiltak kan soldaten iverksette selv. Eksempler på dette er å skru av stedstjenester på apper og vurdere om det brukeren legger ut på sosiale medier kan være av interesse for en aktør. Det kan også være å begrense mengden av informasjon en gir fra seg. Videre kan brukeren være kildekritisk, benytte lange passord og være kritisk til tilsendte lenker og vedlegg. Dette handler også om holdningsdanning. Troppssjefen må selv inneha, samt være i stand til å videreformidle til soldatene, de riktige holdningene til IT-sikkerhet.

5.2 Nye sårbarheter

Det opprettes enorme mengder data fra alt av enheter vi har tilkoblet nett, som vil kunne gi mye detaljert informasjon om enhver bruker. Dette kan misbrukes om det havner i feil hender. Særlig mobiltelefonen har vi sett at er en enorm kilde til data, gjennom geotagging og sosiale medier. Utfordringene rundt *big data* er flere, og den mest relevante utfordringen for denne oppgaven er at det er svært vanskelig å gjøre noe som helst digitalt uten at en persons digitale signatur linkes til handlingen (Rouse, 2019). EU har innført GDPR-loven som tiltak mot dette, men som nevnt er det svakheter også i den. I tillegg gjelder ikke denne loven selskaper i land basert utenfor EU, som Facebook, Snapchat og Instagram, som alle er amerikanske og dermed ikke underlagt GDPR-loven (Regjeringen, 2018).

I utgangspunktet er dette et problem først når en ondsinnet aktør bryter seg digitalt inn et sted og henter ut alle disse dataene. Men det kan være enklere for en aktør enn som så. Mange firmaer samler og selger data som er samlet for å lage profiler som tidligere nevnt, og dette er det lite kontroll eller begrensninger rundt utenfor EU. Selv innad i EU kan dette misbrukes, tross GDPR, slik som vi så i NRK-artikkelen “Norske offiserer og soldater avslørt av mobilen” (Gundersen et al, 2020).

5.2.1 Policyer og dagens opplæring

Når vi ser på Forsvarets policyer for bruk av sosiale medier må vi stille spørsmål rundt hvorvidt denne er hensiktsmessig og tydelig nok. Så godt som alle retningsgivende

setninger i denne policyen handler om at enhver bruker selv må sette seg inn i risikoen og gjøre egne vurderinger (Herland, 2020). Policyen oppfordrer til selvrefleksjon og individualitet, noe som kan være gunstig i et komplekst cyber-miljø. Men dette fordrer at enhver vernepliktig og ansatt i Forsvaret innehar kompetansen nødvendig for både å kunne forstå hva risikoen er, og å kunne ta gode vurderinger på selvstendig grunnlag. Dagens opplæring av soldatene innenfor dette temaet består av et sett med leksjoner, som gir forståelse for sårbarhetene hovedsakelig ved egen deling i sosiale medier, og ved bruk av smart-telefon (anonym informant, 2020, 14. desember). Den største svakheten i denne utdanningen er at den gjennomføres tidlig i tjenesten til soldatene, og deretter får lite fokus. Dette kan føre til at soldatene glemmer hvilke føringer som gjelder, eller at det oppfattes som lite viktig ettersom det ikke tillegges mer tid til repetisjon, oppdateringer eller påfyll.

Uansett hvor godt et system er sikret mot cyberangrep utenfra vil det oftest være mennesket som er den største sårbarheten i systemet. Det er også denne sårbarheten, mennesket, som troppssjefen kan påvirke. Eksemplene vi har sett på understøtter argumentet om at det er menneskelig svikt som er den største sårbarheten. Uhell er menneskelig, mennesker gjør feil, det kommer vi ikke unna. Det Forsvaret kan gjøre noe med er å rette fokus mot forståelse og holdningene til IT-sikkerhet. Det vi også har sett fra eksemplene er at det ikke er uhell som er kilden til de fleste sikkerhetshendelsene. Det er manglende forståelse og kunnskapsløshet om retningslinjer som er den den største kilden (Kaspersky, 2017). Dette er det mulig å gjøre noe med, gjennom blant annet tydeligere retningslinjer, bedre opplæring og fjerning av vage policyer. Holdningsdannelse er også svært viktig for at brukere faktisk setter seg inn i risikoen og sårbarheten som følger med digitale tjenester. Dette er det svært lite fokus på i utdanningen soldater og offiserer får i dag.

Rekrutter som har blitt spurt om dette temaet har svart at de ikke føler de har fått noen god opplæring i hva som er tillatt og ikke, og ønsker tydeligere føringer (Kampsæter, 2020). Dette er i tråd med kritikken fra Daniel Osen om at policyer blir for vagt og oppfattes mer som en "bør"- sak (Kampsæter, 2020). Når vi ser dette opp mot Forsvarets policy for bruk av sosiale medier, hvor det legges opp til at brukeren selv må vurdere eller kun være klar over farene, er det forståelig at rekruttene føler det ikke er klare rammer (Herland, 2020). NRK-artikkelen hvor offiserer og soldater ble kartlagt, og artikkelen om at soldater kunne spores opp via geodata fra apper er gode eksempler på at praksisen og

opplæringen i dag ikke tar nok høyde for disse nye sårbarhetene for ansatte i Forsvaret (Gundersen et al, 2020). Vi har også sett eksempler fra Ukraina 2014 hvor slike sårbarheter utnyttes med stor effekt, hvor Russisk artilleri kunne skyte mot måldata levert av ukrainske mobiltelefoner (Shankland, 2016). Alle disse eksemplene viser at selv om slike enkle policyer, som å ikke ta med mobiltelefoner inn på graderte områder, eller ut i strid, brytes da det sannsynligvis ikke er et fokus på slikt i den daglige driften. Vår personlige erfaring er også at policyene nevnes noen få ganger, det gjennomføres et foredrag i et par timer, og så glemmes det.

5.2.2 Kampen om narrativet

Som nevnt er det et problem at data havner i feil hender, og det er stort potensiale for å utnytte dette til militærstrategiske formål. Denne faktoren kombinert med kampen om narrativet og fremgangen for sosiale medier har skapt en arena som kan legge til rette for polarisering innad i befolkninger så vel som mellom land eller innad i allianser.
I 2017 ble det klart at Russland førte en aggressiv strategi digitalt i den hensikt å undergrave vestlige demokratier. Russiske cyber-angrep og informasjonskampanjer rettet mot det amerikanske valget i 2016, og europeiske valg rundt samme periode, viste seg å kun være en del av en større strategi som søkte å utnytte splittelser mellom folkegruppene gjennom propaganda, misinformasjon og politisk undergraving (McMaster, 2020, s. 26). Dette viser at det er en reell trussel også mot samfunnet i Norge i forhold til informasjonskrigføring. Den plattformen det er mest sannsynlig at Norge blir utsatt for informasjonskrig gjennom er åpenbart sosiale medier. Likevel nevnes ikke dette i Forsvarets policy for sosiale medier, og er heller ikke en del av opplæringen til soldater eller offiserer. En kan derfor spørre seg om dagens utdanningsprogram treffer godt nok på det faktiske trusselbildet.

5.2.3 Troppssjefen som rollemodell

Det er heller ikke noe fokus på troppssjefen i forhold til IT-sikkerhet. Som nevnt er det troppssjefen som er utdanningsleder etter bestått Krigsskole. Dette innebærer da å både kontrollere, planlegge og bidra i utdanningen. Det eneste som er en del av troppssjefens utdanning innenfor IT-sikkerhet er elektromagnetiske sensorer, etterretningsanalyse i forhold til big data og generell risikoanalyse (Forsvarets høgskole, 2020). Spørsmålet blir da hvorvidt troppssjefen i det hele tatt er i stand til å danne riktige holdninger og

engasjement rundt IT-sikkerhet for sine soldater. Troppssjefen er i stand til å skape oppslutning om avgjørelser tatt ovenfra, som Forsvarets policy for bruk av sosiale medier, men hjelper det når den forståelsen som kreves for å kunne bruke et slikt dokument ikke er til stede hverken hos troppssjef eller soldatene? Vi mener, på bakgrunn av de historiske eksemplene, dagens policyer og trusselbilde, at troppssjefen ikke får et godt nok utgangspunkt gjennom utdanningen på Krigsskolen til å kunne skape forståelse for IT-sikkerhet, og å sørge for at soldatenes opptreden i cyberdomenet blir så sikker som mulig.

5.2.4 Mottiltak

Det er dog flere av dagens mottiltak og faktorer i Norge som reduserer noe av sårbarheten. Personopplysningsblanketten som må fylles ut i forbindelse med sikkerhetsklarering er et godt tiltak for robustheten mot utpressing og lignende (NSM, 2014). I en situasjon hvor trusselaktører og deres metode blir identifisert vil NSM være i stand til å identifisere hvilke personer som vil være mest utsatt og kunne fatte tiltak. I tillegg er NSM tilsyns- og fagmyndighet innenfor forebyggende sikkerhet, og de har ansvar for å bidra til samfunnets kunnskap, forståelse, evne og motivasjon til å ivareta digital sikkerhet (NSM, 2019a, s.4). Det vil derfor være naturlig at Forsvaret henvender seg til NSM i forbindelse med å skulle utarbeide et forbedret og oppdatert utdanningsprogram både for soldater og offiserer.

Polarisering av det norske samfunnet som følge av ekstern påvirkning er lite sannsynlig, men ikke umulig. Som nevnt gjør dagens sosiologi i Norge det vanskelig fordi vi har få undertrykte befolkningsgrupper. Det er dog mulig å skape sosial uro gjennom etablering av kunstige "motstandsbevegelser" eller utvikle kriminelle gjengmiljøer, spesielt i byene (Diesen, 2018, s. 25). Den politiske demokratiske situasjonen er også en faktor som styrker Norges robusthet mot slik påvirkning, men det er verdt å merke seg at Norge allikevel ikke blir oversett av Russland, noe hackingen av Stortinget i 2020 viste. Ettersom Norge er en del av NATO, og dermed i målgruppen for russisk informasjonskrig, er det sannsynlig at det både pågår og vil komme informasjonsangrep i fremtiden, og dette er Forsvaret nødt til å være forberedt på. Viktige motmidler vil da både være informasjon fra myndighetene og fra Forsvaret, for å ikke miste kontroll over narrativet (Diesen, 2018, s. 44-45).

5.2.5 Delkonklusjon 2, nye sårbarheter

Vi vurderer trussel og verdi som likt fra forrige drøfting, og denne delkonklusjonen tar derfor kun for seg nye sårbarheter. Ut ifra dette vil vi konkludere med at det må bli større oppmerksomhet på de nye truslene rundt sosiale medier, informasjonskrigføring og big data, i Forsvaret. Det legges ikke vekt på dette i verken policyer i Forsvaret eller utdanningsplaner. Det legges i dag for stor vekt på at brukere selv skal skaffe seg den forståelsen som trengs for å ta gode vurdering i forhold til disse nye sårbarhetene. Når dagens trusselbilde ser ut som det gjør mener vi offiserer og soldater ikke får et godt nok utgangspunkt til å kunne klare dette selv. Policyene må bli tydeligere og utdanningen må ha større fokus på trussel rundt informasjonskrigføring. Forståelse for at big data kan utnyttes av en ondsinnet aktør og at GDPR og lignende tiltak ikke fjerner risikoen må også bli en del av utdanningen. Opplæringen av menneskene må få riktig fokus ettersom de er den største sårbarheten i systemet.

I tillegg må det være et økt fokus rundt dette i den daglige driften. Det holder ikke å gå gjennom et utdanningsopplegg i et visst antall timer og deretter regne med at dette sitter og blir husket på i det daglige, uten noen form for oppfølgning. Det er troppssjefen som er rollemodellen til soldatene og den som har anledning til å følge opp at sikkerheten ivaretas gjennom forståelse og holdninger. For å være i stand til å gjøre dette trenger troppssjefen et bedre utgangspunkt for å kunne skape riktige holdninger og forståelse for IT-sikkerhet. Her mener vi at utdanningen på Krigsskolen må skape forståelse for dagens trusselbilde og kunnskap om cyberdomenet, noe den i dag ikke gjør i tilstrekkelig grad. Kampen om narrativet på nett og forsterket polarisering innad i samfunn påført av eksterne aktører må også soldater og offiserer være klar over at er en aktuell trussel. Dagens utdanning treffer ikke det faktiske trusselbildet på en god nok måte verken for soldater eller offiserer. Ettersom NSM har ansvar for å bidra til å øke befolkningens kunnskap, forståelse, evne og motivasjon til å ivareta digital sikkerhet, vil vi se det som naturlig at Forsvaret henvender seg til NSM for å få utbedret dagens opplæring.

Faktorene og mottiltakene i Norge i dag, som reduserer sårbarheten, bør videreføres. Dette er tiltak som POB og sikkerhetsklarering. De politiske og demokratiske forholdene i Norge reduserer risikoen for at en ekstern aktør kan skape eller forsterke polarisering innad i befolkningen. Likevel må Forsvaret, og Norge som stat, være forberedt på å stå ovenfor slike inngrep og ha mottiltak klare. Dette vil være mottiltak i form av informasjon ut til

soldater og øvrig befolkning i den hensikt å ikke miste kontroll over narrativet. For å kunne gjøre dette må det være robuste nok systemer som kan levere denne informasjonen, som vil fungere når de trengs og ikke enkelt kan settes ut av spill av en ondsinnet aktør.

6 Konklusjon

En trusselaktør har til hensikt å utnytte sårbarheter som vi enten ikke har kjennskap til, eller innehar nok kompetanse om. Dette kan være å styre narrativet, misbruke informasjon fra geolokaliseringen til soldater, eller deres personopplysninger. Det er flere muligheter for troppssjefen til å beskytte egne soldater mot dagens cybertrussel. For å implementere mottiltak som har effekt og gi soldater kunnskap og gode holdninger til IT-sikkerhet, må først utdanning av IT-sikkerhet rettes mot troppssjefen. Dette for å gi utdanningslederen den riktige kompetansen for å kunne videreutdanne soldater, noe som vil minske risikoen mot cyberangrep. Det er mange gode mottiltak som er iverksatt, og mange enkle mottiltak soldaten kan iverksette selv. Eksempler på dette er å skru av stedstjenester på apper og vurdere om det brukeren legger ut på sosiale medier kan være av interesse for en aktør. Det kan også være å begrense mengden av informasjon en gir fra seg. Videre kan brukeren være kildekritisk, benytte lange passord og være kritisk til tilsendte linker og vedlegg. Dette handler også om holdningsdanning. Troppssjefen må selv inneha, samt være i stand til å danne, de riktige holdningene ovenfor IT-sikkerhet hos soldatene.

Videre vil vi konkludere med at det må bli større oppmerksomhet på de nye truslene rundt sosiale medier, informasjonskrigføring og big data i Forsvaret. Det legges ikke vekt på dette i verken policyer, utdanningsplaner eller daglig drift. Policyene må bli tydeligere og utdanningen må ha større fokus på trusselen rundt informasjonskrigføring. Opplæringen av menneskene må få riktig fokus ettersom de er den største sårbarheten i systemet. Utdanningen på Krigsskolen må skape forståelse for dagens trusselbilde og kunnskap om cyberdomenet, noe den i dag gjør i liten grad. Kampen om narrativet på nett og forsterket polarisering innad i samfunn påført av eksterne aktører må også soldater og offiserer forstå at er en aktuell trussel. Forsvaret og Norge må være forberedt på å stå ovenfor slike inngrep, og da være i stand til å fatte effektive mottiltak. Dagens utdanning treffer ikke det faktiske trusselbildet på en god nok måte verken for soldater eller offiserer. Vi ser det som naturlig at Forsvaret henvender seg til NSM for å få utbedret dagens opplæring.

7 Bibliografi

Aale, P. K. (2019, 6. mars). *Slik ble Russlands militæroperasjoner avslørt. Nå blir det mye vanskeligere*. Hentet fra: https://www.aftenposten.no/verden/i/p6oAvo/slik-ble-russlands-militaeroperasjoner-avsloert-naa-blir-det-mye-vanskel

Adams, M. (2015). Cybergeddon? *Military Technology*, *39*(11), s. 67-70. Monch Publishing Group.

Aven, T. (2012, 20. august). *Risikotenkningen er fullstendig foreldet. Aftenbladet*. Hentet fra: https://www.aftenbladet.no/meninger/i/PEdl5/risikotenkningen-er-fullstendig-foreldet s.2

AVG. (2015, 7. oktober). *The dangers of geotagging via photos and social media.* Hentet fra: https://now.avg.com/the-dangers-of-geotagging-via-photos-social-media

BBC. (2014, 1. april). *Viktor Yushchenko: Ukraine's ex-president on being poisoned.* Hentet fra: https://www.bbc.com/news/av/world-europe-43611547

BBC. (2014, 13. november). *Ukrainian Crisis: Timeline.* Hentet fra: https://www.bbc.com/news/world-middle-east-26248275

BBC. (2019, 9. mai). *Montenegro jails 'Russian coup plot' leaders.* Hentet fra: https://www.bbc.com/news/world-europe-48212435

Beazer, M., & Robin, P. (2017, 18. oktober). *Stuxnet*. Hentet fra: https://www.research-collection.ethz.ch/handle/20.500.11850/200661

Brusmundrud, O., & Maal, M., & Kiran, J. H., & Endregard, M. (2015, 8. juni). *Tilnærminger til risikovurderinger for tilsiktede uønskede handlinger. FFI-rapport 2015/00923.* Hentet fra: https://publications.ffi.no/nb/item/asset/dspace:2503/15-00923.pdf

Cisco. (2020, 9. mars). *Cisco annual internet report (2018-2023) White paper*. Hentet fra: https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-

internet-report/white-paper-c11-741490.html

Datatilsynet. (2018, 21. juni). *Automatisk strømmåling.* Hentet fra: https://www.datatilsynet.no/personvern-pa-ulike-omrader/overvaking-og-sporing/strommaling/

Diesen, S. (2018, 26. april). *Lavintensivt hybridangrep på Norge i en fremtidig konflikt.* Hentet fra: https://www.ffi.no/publikasjoner/arkiv/lavintensivt-hybridangrep-pa-norge-i-en-fremtidig-konflikt

Enstad, K. (2016). *Hvordan skrive en god tekst*. Oslo: Krigsskolen.

Entous, A., & Timberg, C., & Dwoskin, E. (2017, 25. september). *Russian operatives used Facebook ads to exploit America's racial and religious divisions.* Hentet fra: https://www.washingtonpost.com/business/technology/russian-operatives-used-facebook-ads-to-exploit-divisions-over-black-political-activism-and-muslims/2017/09/25/4a011242-a21b-11e7-ade1-76d061d56efa_story.html?tid=sm_tw&utm_term=.9aa3481a6620

Ertesvåg, E. R., & Persen, K. (2020, 8. desember). *Dataangrep mot Stortinget ferdig etterforsket – mener "Fancy Bear" stod bak.* Hentet fra: https://www.tv2.no/a/11825244/

Etterretningstjenesten. (2013). *Etterretningsdoktrinen*. Oslo: Forsvaret.

Etterretningstjenesten. (2020, 10. februar). *Fokus 2020: Etterretningstjenestens vurdering av aktuelle sikkerhetsutfordringer.* Oslo: Forsvaret. Hentet fra: https://www.forsvaret.no/aktuelt-og-presse/publikasjoner/fokus

FFI. (2016, februar). *Teknologien forsvaret trenger.* Hentet fra: https://www.ffi.no/publikasjoner/arkiv/teknologien-forsvaret-trenger , s. 47.

FN. (2020, 11. februar). *Ukraina*. Hentet fra: https://www.fn.no/Konflikter/Europa/ukraina

Forsvarsdepartementet. (2014, 1. mars). *Forsvarsdepartementets retningslinjer for informasjonssikkerhet og cyberoperasjoner i forsvarssektoren. FDs*

cyberretningslinjer. Oslo, Norge: Forsvarsdepartementet.

Forsvarets Høgskole. (2020). *Utdanning ved forsvarets høgskole: OPS2201 kontekst landoperasjoner.* Hentet fra: https://utdanning.forsvaret.no/nb/program/bachelor-i-milit%C3%A6re-studier-med-fordypning-i-ledelse-og-landmakt/studieplan/436

Garamone, J. (n.d.). *New DoD Policy Prohibits GPS-Enabled Devices in Deployed Settings.* Hentet fra: https://www.jcs.mil/Media/News/News-Display/Article/1594821/new-dod-policy-prohibits-gps-enabled-devices-in-deployed-settings/

Greenberg, A. (2017, 20. juni) *How an entire nation became Russia's test lab for cyberwar, Wired.* Hentet fra: https://www.wired.com/story/russian-hackers-attack-ukraine

Gundersen, M. & Skille, Ø. B., & Lied, H., & Grafsrønningen, M., & Jansson, H. K. (2020, 18. mai). *Norske offiserer og soldater avslørt av mobilen*. Hentet fra: https://www.nrk.no/norge/xl/norske-offiserer-og-soldater-avslort-av-mobilen-1.14890424

Herland, H. K. (2020, 20. mai). *Policy for bruk av sosiale medier*. Hentet fra: https://forsvaretsforum.no/files/2020/08/28/Policy%20for%20bruk%20av%20sosiale%20medier.pdf

Hoover.org. (n.d.). *H. R. McMaster*. Hentet fra: https://www.hoover.org/profiles/h-r-mcmaster

Istad, M. (2019, 1. mars). *Data fra HAN-porten på smarte strømmålere (AMS) kan gi deg verdifull informasjon.* Hentet fra: https://blogg.sintef.no/sintefenergy-nb/han-porten-smarte-strommalere-ams/

Johannesen, A., Tufte, P. A., & Christoffersen, L. (2010). *Introduksjon til samfunnsvitenskapelig metode*. Oslo: Abstrakt forlag AS.

Johnson, O. (2019): *The Russian understanding of war. Blurring the lines between war and peace.* Washington DC: Georgetown University press

Johnson, R. (2018). *Hybrid war and its Countermeasures: A Critique of the literature, Small Wars & Insurgencies,* 29:1, 141-161. DOI: 10.1080/09592318.2018.1404770

Joselow, G. (2016, 3. november). *Election Cyberattacks: Pro-Russia Hackers Have Been Accused in Past.* Hentet fra: https://www.nbcnews.com/mach/technology/election-cyberattacks-pro-russia-hackers-have-been-accused-past-n673246

Justis- og beredskapsdepartementet. (2018, 19. februar). *Høring - Justering av forskrift om rammeplan for ingeniørutdanning.* Hentet fra: https://www.regjeringen.no/no/dokumenter/horing-forskrift-om-ingeniorutdanning/id2578866/

Kampesæter, S. (2020, 11. september). *Rekrutter vil ha tydeligere føringer for sosiale medier*. Hentet fra: https://forsvaretsforum.no/cyber-sosiale-medier-teknologi/rekrutter-vil-ha-tydeligere-foringer-for-sosiale-medier/158307

Karlsen, J. (2019, 26. mars). *Soldaters Tinder-bruk på øvelse bekymrer.* Hentet fra: https://forsvaretsforum.no/soldaters-tinder-bruk-pa-ovelse-bekymrer/104826

Kaspersky. (2017). *The Human Factor in IT-Security.* Hentet fra: https://www.kaspersky.com/blog/the-human-factor-in-it-security/

Kaspersky. (2020). *Brute force attack: Definition and examples.* Hentet fra: https://www.kaspersky.com/resource-center/definitions/brute-force-attack

Kim, S. D. (2012). *Characterizing unknown unknowns.* Artikkel presentert ved PMI Global Congress 2012-North America, Vancouver, British Columbia, Canada. Newtown Square, PA: Project Management institute.

Kristoffersen, M. J. (2018, 7. august). *Amerikanske soldater får app-nekt.* Hentet fra: https://www.abcnyheter.no/nyheter/verden/2018/08/07/195421858/amerikanske-soldater-far-app-nekt

Kroghrud, P. E. (2019, mai). *Russisk cybersabotasje – Forsmak på fremtidens cyberkrig?* (masteroppgave). Institutt for sammenliknende politikk: Universitetet i Bergen.

Kunnskapsdepartementet. (2018, 18. mai). *Forskrift om rammeplan for ingeniørutdanning.* Hentet fra: https://www.regjeringen.no/contentassets/389bf8229a3244f0bc1c7835f842ab60/ny-forskrift-om-rammeplan-for-ingeniorutdanning-fastsatt-18.05.18.pdf

Lied, H., & Svendsen, C. (2018, 30. januar). *Slik røper soldater fra Norge, Danmark og USA hvem de er og hvor de trener i krigssoner.* Hentet fra: https://www.nrk.no/urix/slik-roper-soldater-fra-norge_-danmark-og-usa-hvem-de-er-og-hvor-de-trener-i-krigssoner-1.13891513

Limnéll, J. (2015). *The Exploitations of Cyber Domain as Part of Warfare: RussoUkrainian war. International Journal of Cyber-Security and Digital Forensics.* Finland: Aalto University

Martin, D. (2016, 22. desember). *Russian hacking proves lethal after Ukrainian military app hijacked.* Hentet fra: https://www.cbsnews.com/news/russian-hacking-proves-lethal-after-ukrainian-military-app-compromised/

McMaster, H.R. (2020). *Battlegrounds - The Fight to Defend The Free World. Free World.* London: HarperCollinsPublishers

Morgan, J. (2014, 13. mai). *A Simple Explanation of 'The Internet of Things'.* Hentet fra: https://www.forbes.com/sites/jacobmorgan/2014/05/13/simple-explanation-internet-things-that-anyone-can-understand/?sh=6e7abb2e1d09

Muhammad, Z. (2020, 8. august). *Hundreds of Vulnerabilities Found in Vast Majority of Android Smartphones.* Hentet fra: https://www.digitalinformationworld.com/2020/08/hundreds-of-vulnerabilities-found-in-vast-majority-of-android-smartphones.html

Nasjonal Sikkerhetsmyndighet. (2014, 12. juni). *Slik blir du sikkerhetsklarert.* Hentet fra: https://nsm.no/fagomrader/personellsikkerhet/sikkerhetsklarering/slik-blir-du-sikkerhetsklarert/

Nasjonal Sikkerhetsmyndighet. (2019, 3. mai). *Hovedinstruks for Nasjonal sikkerhetsmyndighet.* Hentet fra: https://nsm.no/getfile.php/134519-1606830131/Demo/Dokumenter/instruks-for-nsm.pdf

Nasjonal Sikkerhetsmyndighet. (2019, 28. juni). *Veiledning til utfylling av personopplysningsblankett for sikkerhetsklarering.* Hentet fra: https://nsm.no/getfile.php/133488-1592225719/Skjemaer/veiledning-til-utfylling-av-pob-for-sikkerhetsklarering---28.-juni-2019--.doc%20%281%29.pdf

Nasjonal Sikkerhetsmyndighet. (2020, 24. juni). *Hendelseshåndtering.* Hentet fra: https://nsm.no/fagomrader/digital-sikkerhet/nasjonalt-cybersikkerhetssenter/handtering-av-dataangrep/hendelseshandtering

NATO (2016). *AJP-2(A) Allied joint doctrine for intelligence, counter-intelligence and security.* Brussel: NATO

Norges offentlige utredninger 2012: 14. (2012). *Rapport fra 22. juli-kommisjonen.* Oslo: Departementenes servicesenter.

Norges offentlige utredninger 2015: 13. (2015) *Digital sårbarhet - sikkert samfunn.* Oslo: Departementenes sikkerhets- og serviceorganisasjon.

Norges vassdrag- og energidirektorat. (2015, 10. desember). *Smarte strømmålere (AMS).* Hentet fra: https://www.nve.no/stromkunde/smarte-strommalere-ams/

NorSiS. (2020, 4. februar). *Få en tryggere digital hverdag: Trusler og trender 2019-2020.* Hentet fra: https://norsis.no/trusler-og-trender-2019-2020/

Norsk utenrikspolitisk institutt. (2011, 8. mai). *Nye sikkerhetstrusler: Cyberangrep.* Hentet fra: https://www.nupi.no/Skole/HHD-Artikler/2011/Nye-sikkerhetstrusler-cyberangrep

Nye, J. (2018, 13. november). *Protecting Democracy in an Era of Cyber Information War*. Hentet fra: https://www.hoover.org/research/protecting-democracy-era-cyber-information-war

Næringslivets Hovedorganisasjon. (2017). *Hva er personvernforordningen (GDPR)?* Hentet fra: https://arbinn.nho.no/forretningsdrift/personvern/personopplysningsverktoy/personvernforordningen/

Oxford Learner's dictionaries. (2020). *Geotracking.* Hentet fra: https://www.oxfordlearnersdictionaries.com/us/definition/english/geotracking

Pastoor, I. (2019, 29. april). *A look behind the scenes of click farms.* Hentet fra: https://www.diggitmagazine.com/articles/look-behind-scenes-click-farms

Politiets sikkerhetstjeneste. (2020, 4. februar). *Nasjonal trusselvurdering 2020.* Hentet fra: *https://www.pst.no/alle-artikler/trusselvurderinger/nasjonal-trusselvurdering-2020/*

Politiets sikkerhetstjeneste. (2020, 5. november). *Etterretningstrussel mot norsk petroleumssektor.* Hentet fra: https://pst.no/globalassets/artikler/utgivelser/2020/etterretningstrusselen-mot-norsk-petroleumssektor.pdf

Politiets sikkerhetstjeneste. (2020, 8. desember). *Datainnbruddet mot Stortinget er ferdig etterforsket.* Hentet fra: https://pst.no/alle-artikler/pressemeldinger/datainnbruddet-mot-stortinget-er-ferdig-etterforsket/

Regjeringen. (2018, 26. juni). *Personvernforordningen (GDPR).* Hentet fra: https://www.regjeringen.no/no/sub/eos-notatbasen/notatene/2014/aug/forslag-til-personvernforordning/id2433856/

Rid, T. (2016): *Rise of the Machines: A Cybernetic History. WW Norton & Company.* London: King's College.

Rouse, M. (2014, 1. august). *10 Big Data Analytics Privacy Problems.* Hentet fra: https://www.secureworldexpo.com/industry-news/10-big-data-analytics-privacy-problems

Rouse, M. (2019, oktober). *Big Data.* Hentet fra: https://searchdatamanagement.techtarget.com/definition/big-data

Rybkin, Y. (2018, 5. oktober). *How is Big Data collected?* Hentet fra: https://codeit.us/blog/how-is-big-data-collected

Røkkum, N. (2016, 3. desember). *Metodisk inngang - én eller flere?* Hentet fra: https://sosiologen.no/student/metodisk-inngang-flere/

Shankland, S. (2016, 22. desember). *Russian Android malware tracked Ukrainian military: Report.* Hentet fra: https://www.cnet.com/news/russian-android-malware-tracked-ukrainian-military-report/

Silkstream. (2016, august). *Geotagging on Social; Media: Beware of the risks.* Hentet fra: https://www.silkstream.net/blog/2016/08/geotagging-social-media-risks.html

Språkrådet. (n.d.). *Narrativ: Bruk og genus.* Hentet fra: https://www.sprakradet.no/svardatabase/sporsmal-og-svar/narrativ-bruk-og-genus/

Statistisk sentralbyrå. (2019). *Fakta om internett og mobil.* Hentet fra: https://www.ssb.no/teknologi-og-innovasjon/faktaside

Statistisk sentralbyrå. (2020). *Bruk av IKT i husholdningene.* Hentet fra: https://www.ssb.no/statbank/table/12344/tableViewLayout1/

Su, X. (n.d.). *Introduction to big data.* Hentet fra: https://www.ntnu.no/iie/fag/big/lessons/lesson2.pdf

Svendsenutvalget. (2020, 24. juni). *Økt evne til å kombinere menneske og teknologi: Veier*

mot et høyteknologisk forsvar. Hentet fra: https://www.regjeringen.no/contentassets/374492dfae2f41a18f9b01e8678b468a/svendsen-utvalget--okt-evne-til-a-kombinere-menneske-og-teknologi.pdf

Symon, P. B., & Tarapore, A. (2015) Defense, Intelligence Analysis in the Age of Big Data. *Joint Force Quarterly*, *79*(4), s. 4-11. Washington: National Defense University

Szoldra, P. (2014, 1. august). *Without Realizing It, Russian Soldiers Are Proving Vladimir Putin Is Lying About Eastern Ukraine.* Hentet fra: https://www.businessinsider.com/russian-soldiers-social-ukraine-2014-7?r=US&IR=T

Trujillo, M. (2014, 17. april). *Putin denies troops are in eastern Ukraine.* Hentet fra: https://thehill.com/policy/international/203740-putin-denies-russian-troops-are-in-eastern-ukraine