FORSVARET

Forsvarets høgskole

Russisk EK

Hvordan Russland utnytter det elektromagnetiske spektrum for å forberede oppkjøringen til strid?

Thorbjørn Wiig

Masteroppgave

Forsvarets høgskole

Vår 2022

Sammendrag

Russland har gjennom perioden fra Berlin-murens fall, frem til angrepet på Ukraina i 2022, bygd opp en god evne til gjennomføring av operasjoner innen elektronisk krigføring. Russland hadde økonomiske problemer, men ønsket å bli en stormakt igjen. Gjennom å øke forsvarsbudsjettene og å studere USAs krigføring på 1990-tallet så så de hvilke kapasiteter amerikanerne hadde og la der listen for hva de selv måtte jobbe mot. Dette resulterte i flere våpensystemer og systemer for elektronisk krigføring som skulle kunne motstå amerikanernes teknologi- og våpensystemer.

Denne oppgaven tar for seg bruken av russisk elektronisk krigføring i Øst-Ukraina (2014-2022) og Syria (2015-2022) og hvordan disse innsatsene eventuelt skilte seg i innsats, med bakgrunn i at mesteparten av utstyret er likt i de to operasjonene. Det er flere kommentatorer som tar for seg den teknologiske utviklingen Russland har gjennomgått innen elektronisk krigføring og at de trolig har rykket fra USA og NATO. Russland har bevist i Ukraina og Syria at de har kompetente avdelinger innen EK-operasjoner. De har rullert personellet mellom de to operasjonene og trening på hjemmebase. Personellet har derfor bred erfaring innen operasjonsmiljø og motstandere.

Oppgaven ser på gjennomføringen og metodene av EK de russiske styrkene har benyttet i operasjonene. Hvordan de benytter EK mot sivilbefolkningen i Øst-Ukraina og hvordan de er et viktig bidrag i det større «information warfare»-oppdraget. De deployerte EK-styrkene fikk her mye trening i et aktivt operasjonsmiljø og videreutviklet bruken av kapasitetene deres. Styrkene i Øst-Ukraina fikk god trening i bruk av slike systemer for effektivt å ramme en motpart, uten å ha et stort fotavtrykk i stridsområdet. I samme periode har de utnyttet sitt militære engasjement i Syria for uttesting av EK-materiell i roller innen baseforsvar og nærsikring.

Russland har evnen til å gjennomføre liknende oppdrag mot Norge og den norske befolkningen. En slik innsats vil fortone seg annerledes da den vil ligge som grunnlaget for en eventuelt kommende konflikt. En hybrid krigførings-operasjon med mål om å forberede russiske styrker for hva de eventuelt vil møte i Norge samt en kartlegging av norske svakheter. Det vanskeligste for Norge i en slik operasjon vil være å avdekke at den er i gang. For norske myndigheter å sammenstille informasjonen som avslører at Russland har iverksatt en hybrid operasjon mot Norge gjennom bruk av elektronisk krigføringsmidler.

Summary

After the tearing down of the Berlin Wall and until the attack on Ukraine in 2022, Russia has built a good ability to carry out operations in electronic warfare. Russia experienced economic problems, but aspired to become a great power again. By increasing defense budgets and studying US warfare in the 1990s, they saw the capabilities the Americans had at their disposal. This became the goal line of what they had to work towards, and go beyond. This resulted in several weapon systems and electronic warfare systems that could withstand and match the American systems.

This thesis deals with the use of Russian electronic warfare in Eastern Ukraine (2014-2022) and Syria (2015-2022) and how these efforts may differ in effort, based on the fact that most of the equipment is similar in the two operations. There are several commentators addressing the technological development that Russia has undergone in electronic warfare. Some of these commentators think that Russia have probably surpassed the United States and NATO. Russia has proven in Ukraine and Syria that they have a competent force for conducting EW-operations. They have moved the personnel between the two operations and home base to maximise operations time for the personnel. The personnel therefore have extensive experience in the complex operating environments and different opponents.

The thesis looks at the implementation and methods of EW that the Russian forces have used in the operations. How they use EW against the civilian population in Eastern Ukraine and how they are an important contribution to the larger information warfare mission. The EW-forces deployed, received a lot of training in an active operational environment to further developed the use of their capabilities. The forces in Eastern Ukraine received good training in the use of such systems to effectively hit an opponent, without leaving a large footprint in the area of operations. During the same time period, they have used their military involvement in Syria to test EW materiel in roles of base defense and force protection.

Russia has the ability to carry out similar missions towards Norway and the Norwegian population. Such an operation will be different as it will be the foundation for Russian action in case of a future conflict. This would be a hybrid warfare operation with the aim of preparing Russian forces for what they may encounter in Norway. Also as a mapping of Norwegian weaknesses. The most difficult thing for Norway in such an operation will be to uncover that it is underway. Norwegian authorities will need to be able to compile and analyse the information that reveals Russia`s intent and that they have launched a hybrid operation against Norway, through the use of electronic weapons.

Innholdsfortegnelse

1 Innledning

"electronic warfare: Military action that exploits the electromagnetic energy to provide situational awareness and achieve offensive and defensive effects" (NATO, 2019, Lex-7).

Allerede i 1956 satte Sovjetunionen opp egne bataljoner for jamming av fiendtlig radar- og kommunikasjonssystemer (McDermott, 2017, s. 9). Etter murens fall sto Russland igjen med store deler av det gamle sovjetiske forsvarssystemet. De slet med dårlig økonomi og det var ekstra viktig for Russland å få mest mulig forsvar for pengene. Russland måtte derfor finne sine satsningsområder utover bare det å pusse opp og vedlikeholde arven fra Sovjet-tiden. Russland fulgte nøye med på USAs krigføring på 1990-tallet. Der så de hvordan USA utnyttet og fokuserte på utviklingen og bruken av systemer innen det elektromagnetiske spektrum (EMS). Russlands militærteoretikere la brikkene på plass og konkluderte med at elektronisk krigføring (EK) var en «*force multiplier*»; resultatet av militærinnsatsen var større når den ble kombinert med EK. Innen russisk strategi ble EK nå regnet inn som en viktig part av utviklingen av eget nettverksbasert forsvar samt i forsvaret mot motstanderes utnyttelse av EMS (McDermott, 2017, s. 9). EK er en viktig militær kapasitet som stadig må utvikles i takt med teknologisk utvikling da det er de nyeste systemene EK er ute etter å ramme hos motstanderen. Fram til fullskalakrigen i Ukraina i 2022 ga de to kamparenaene, Ukraina og Syria, Russland et stort spillerom for utvikling og uttesting av nye våpen- og sensorsystemer. De har testet ut nye missil-, luftvarsling-, EK- og våpensystemer (Jaber, 2021). EK vil på en annen side være et middel en utøver kan benytte både i det skjulte og i det åpne for å påvirke eller overvinne en motstander. EK alene vil ikke vinne striden, men kan vippe balansen til egen fordel.

Definisjonen på elektronisk krigføring har som alle andre definisjoner innen krigsmakt endret seg etter hvert som utviklingen skjer. Russlands bruk av EK startet med krigen mellom Russland og Japan i 1904 der russiske enheter klarte å motta japanske radiomeldinger for deretter å jamme frekvensen. I dag er EK blitt til et bidrag i hacking av telefoner og kommandosystemer hos motstanderen. Elektronisk krigføring kan i denne oppgaven kort defineres som påvirkning av det elektromagnetiske spektrum. EK består av evnen til å utnytte signaler i det elektromagnetiske spektrum i egen favør, både aktivt og passivt. Forsvarets forskningsinstitutt definerer EK kort inn i tre hovedfunksjoner a) Identifisere en motstanders bruk av det elektromagnetiske spekteret, b) Redusere eller forhindre motstanderens bruk av det elektromagnetiske spekteret, og c) Tiltak for å sikre egne styrkers bruk av det elektromagnetiske spekteret (Forsvarets Forskningsinstitutt)

Mulighetene for utnyttelse av EK-kapasiteter innen et lavintensitets stridsmiljø er stor i dag. Siden tidlig 2000-tallet har det vært et økt fokus på såkalt *hybrid krigføring* eller *New generation warfare*. Selv om det ikke finnes en omforent definisjon benyttet NATO selv en definisjon på NATOs toppmøte i Wales 2014 med: «*a wide range of overt and covert military, paramilitary, and civilian measures are employed in a highly integrated design*» (NATO, 2014, pkt 13). Denne definisjonen viser hvor stort emnet hybrid krigføring kan defineres inn i og hvor mange spillere det kan være på «slagmarken» samtidig uten noen form for klare spillerdrakter. Elektronisk krigføringsmidler passer godt inn i et slikt miljø. Enkle elektroniske midler kan spille en stor rolle i skjulte miljøer.

Elektronisk krigføring består av flere komponenter og disse spenner fra svært enkle å produsere og utnytte til andre mer kompliserte og kompetansekrevende. Verdien av å beherske hele kompetansespennet av virkemidler innen EK er stor. Dette gir evnen til ikke bare å jamme ut signaler og lamme motstanderens kommunikasjon eller posisjoneringssystemer, men det gir også evnen til å sende inn feilinformasjon og feilposisjonering i motstanderens K2-system. Det gir muligheten til å sette i gang motstanderens reaksjonshandlinger gjennom å ødelegge deres situasjonsforståelse og tro på egne systemer. Russland brukte tiden godt mens NATO-landene var i krig i Afghanistan uten seriøs EK-motstand. Russiske styrker har i henhold til uttalelser fra amerikanske EK personell bevist at de gode på fagfeltet elektronisk krigføring (Brimelow, 2018; McLeary, 2015). De besitter utstyr for jamming av sambandssystemer på enorme avstander, både på bakken og mot satellitter. De beviser jevnlig at de spoofer GPS-signaler i den hensikt å avverge anslag av GPS-styrte våpen, og de lammer telekomnettverk og radarer for å kunne forflytte egne tropper uten deteksjon fra motstandere (C4ADS, 2019, s. 26). Dette er kapabiliteter og taktikker sett brukt av russiske styrker i både Ukraina og Syria. Basert på Russlands utnyttelse av slike kapasiteter i stridsmiljøer gir det en pekepinn på at det vil være viktig å ikke legge all kompetanse hos egne styrker i elektroniske systemer, men fortsatt trene på «offline» operasjoner. I miljøer der russiske styrker opererer må det ses som sannsynlig at elektroniske systemer kan være korrumpert eller kompromittert.

Nasjonene i NATO har hatt en enorm utvikling innen elektroniske støttemidler i militæroperasjoner og K2 siden 2. verdenskrig. Mye er basert på kommunikasjon over store distanser og det er stor utvikling av ubemannede farkoster i alle domener, der K2 bedrives over satellittkommunikasjon. Denne kommunikasjonen er verdifull for eieren av utstyret og signalene, men den er like fullt verdifull for motstanderen. Både for innhenting av dataene og kanskje mest av alt å kunne ødelegge kommunikasjonen og dermed utnyttelsen av f.eks. droner. Slik forstyrrelse av kommunikasjons- og posisjonssignaler er et fokusområde for Russland og deres innsats i stridsmiljøer (McCrory, 2021, s. 36), da det gir Russland muligheten til å slå ut formidable krigssystemer med enkle midler fremfor å måtte fremstille egne tilsvarende systemer og mulig havne i en rustningsspiral.

1.1 Problemstilling

Gjennom flere år har Russland utviklet og testet nye evner innen bruk av det elektromagnetiske spektrum. Utviklingen innen bruken av det elektromagnetiske spektrum er for Russland både for forsvar av egne ressurser, men like viktig er muligheten for nektelse av motstanderes bruk av det samme spektrum. Russland har i perioden fra 2014 vist et enormt potensial i nektelse av motstanderens bruk av elektromagnetiske signaler over eteren. Dette dreier seg om alt fra jamming av signaler, spoofing av signaler og planting av falsk informasjon i motstanderens *kommando og kontroll*-system.

Problemstillingen i studien er:
Hvordan utnytter Russland det elektromagnetiske spektrum for å forberede oppkjøringen til strid?

Forskningsspørsmål: Hvordan utnytter Russland EK i Syria og Ukraina? og hva skiller innsatsene?
Forskningsspørsmål: Hvordan kan Russland utnytte sine EK-kapabiliteter mot Norge før en strid?

Innen det elektromagnetiske spektrum finnes det flere metoder å hindre eller begrense en motstanders bruk av egne midler. Ved å bruke midler innen det elektromagnetiske spektrum kan det skapes usikkerhet og avledninger som fører til et overtak for den utøvende part. I denne studien vil jeg se på hvordan Russland har utnyttet EMS for å fremme egne operasjoner og hvilken usikkerhet deres bruk av EMS kan skape, for Norge eller tilsvarende land. Oppgaven vil se på forholdene fra russisk perspektiv. Dette for å sørge for at oppgaven ikke blir gradert i henhold til Sikkerhetsloven og holdt opp mot norsk beredskapsplanlegging.

Oppgaven vil ta for seg artikler og dokumenter som dokumenterer Russlands bruk av EMS-midler og hvordan disse skaper trusler og usikkerheter for deres motstandere. Oppgaven vil også se på hvilket signal russisk bruk av disse midlene signaliserer til deres andre «småstatsnaboer».

1.2 Avgrensning

Information Warfare (IW) fungerer som en paraplykategori der stadig flere grener av operasjoner implementeres. Paraplyen dekker over alt fra Stratcomoperasjoner til offensive angrep på en motstanders sambandssystemer. Det som er ønskelig å oppnå med IW kan deles inn i fire kategorier: 1) Degradere (*Degrade)*: målet er å ødelegge eller avspore motstanderens informasjonskommunikasjon gjennom jamming eller begrensning av motstanderens evne til bruk av EMS.
2) Korrumpere (*Corrupt)*: gjennom å plassere falsk informasjon inn i motstanderens situasjonsforståelse (eks spoofing av radar/GPS eller PSYOPS) kan det oppnås forvirring og usikkerhet om situasjonsbildet hos motstanderen.

3) Nekte (*Deny*): å aktivt nekte motstanderen evnen til å utnytte egne sensorer gjennom fysiske tiltak (eks: laserjamming, hackerangrep, etc).
4) Utnytte (*Exploit*): samle inn og bygge egen forståelse av motstanderens bruk av EMS for senere å utnytte dette mot dem (eks: bygge EOB ved hjelp av ELINT/SIGINT) (Borden, 1999).

Denne oppgaven vil fokusere seg mot EK, men bidraget fra EK i IW kan være så stort at EK-operasjoner ofte vil kunne utføre flere roller. Elektronisk Krigføring (EK) kan begrenses til å være krigføringsoperasjoner innen det elektromagnetiske spektrum (EMS). EK kan brukes sammen med flere av de andre krigføringsområdene innen IW, men EK begrenses til aktive og passive tiltak innen elektromagnetiske utsendelser gjennom eteren. Det er EK som vil omhandles i denne oppgaven og andre områder innen IW kan nevnes, dog ikke omhandles. EK er i seg selv et fagområde som inneholder mange typer bruk av EMS, men her i denne oppgaven vil jeg fokusere på typer av førsteinnsats-EK. Med førsteinnsats mener jeg utnyttelse av EMS der Russland kan påvirke en annen part gjennom midler som ligger under terskelen for væpnet angrep. Dette kan være forstyrrelser av mobilnett, GPS eller andre sambandtyper. Påvirkninger som rammer både sivilt hverdagsliv og forsvar.
Studien vil primært ta for seg dokumenter og artikler som omtaler Russlands bruk av elektronisk krigføring i de to stridsområdene: Ukraina og Syria. Russland har bedrevet stridsoperasjoner i flere områder siste 20 år, men Ukraina og Syria er to områder der det er god dokumentasjon for hva som har vært gjort tidlig i operasjonene og hvordan de fortsatt opererer. Russland har gjennomført andre stridsoperasjoner de siste tiårene (eks: Tsjetsjenia og Georgia), men mengden av dokumentasjon som foreligger for innsatsen i Ukraina og Syria er større og mer omfattende. Studien begrenses til å ta for seg utnyttelsen av teknologi og utstyr som er kjent per i dag. Oppgaven vil ikke ta for seg hvordan bruk av ny teknologi i utstyr som er på forskningsstadiet kan påvirke fremtidens stridsfelt, men kort nevne noen av de mest nevnte kommende teknologier.
Oppgaven har blitt skrevet i en periode med store endringer i Russlands bruk og fremstilling av sine EK-kapasiteter. De har gått fra en stillingsstrid i Ukraina og en testkriging i Syria til å gå til fullt angrep på Ukraina. Oppgaven vil derfor ta for seg Russlands teoretiske EK stridskapasiteter slik de har vært fremstilt frem til invasjonen av Ukraina i februar 2022 og inneha kommentarer på situasjoner de har fremvist gjennom sine operasjoner i angrep på Ukraina i feb 2022. «Cut-off-date» for tilfang av informasjon er derfor ikke tilbake i tid, men går helt frem til starten av april 2022, men med tynnere kildegrunnlag for de siste hendelsene.

1.3 Definisjoner og terminologi

Det er mange som har forsøkt å definere hva Elektronisk krigføring (EK) innebærer. Det eksisterer ikke en felles anerkjent definisjon da det gjerne vektlegges litt forskjellige sider av fagområdet avhengig av

hva forskere ønsker å poengtere. Jeg starter her med noen utdrag som viser alt fra NATOs svært forenklede til Forsvarets detaljerte.

Den første er den enkle formen som Hoehn bruker i rapport til kongressen i USA som omhandler emnet elektronisk krigføring:

> *EW generally refers to operations that use the electromagnetic spectrum (i.e., the "airwaves") to detect, listen to, jam, and deceive (or "spoof") enemy radars, radio communication systems and data links, and other electronic systems (Hoehn, 2019)*

Hoehn sin definisjon er en forkortet versjon av Don E. Gordon sin fra hans bok «Electronic warfare» fra 1981:

> *Electronic warfare includes all actions in the entire electromagnetic spectrum to intercept, analyze, manipulate, or suppress the enemy's use of the spectrum as well as to protect friendly use of the spectrum from similar attack by an enemy. The electromagnetic spectrum includes both the visible and invisible ranges, measured in megahertz, of the spectrum. The use of signals intercepting, locating, identifying, detecting, jamming, disrupting, deceiving, protecting, analyzing, and cryptanalyzing is electronic warfare (Gordon, 1981).*

NATO har, i sin publikasjon AJP-5, en svært kort tekst der de har klart å forene alle alliansens nasjoner til å bli enige i definisjonen på EK som:

> *Military action that exploits the electromagnetic energy to provide situational awareness and achieve offensive and defensive effects (NATO, 2019).*

NATOs korte tekst viser til hva de ønsker å oppnå mer enn hva de faktisk utnytter innen det elektromagnetiske spekteret.

Definisjonen brukt i Forsvarets fellesoperative doktrine (FFOD) er en kombinasjon av de ovennevnte og definerer det slik:

> *Elektronisk krigføring (EK) er definert som militære tiltak for å kunne kontrollere, beherske og utnytte det elektromagnetiske spektrum. Fellesoperasjoner er avhengige av det elektromagnetiske spekteret til kommunikasjon mellom hovedkvarterer og ulike deler av den fellesoperative styrken. Moderne våpensystemer er avhengige av det elektromagnetiske spektret til posisjonering, navigasjon og tidssynkronisering, til måloppdagelse, målfatning og målstyring. Elektronisk krigføringskapasitet er derfor helt avgjørende for evnen til å opprettholde egen stridsevne og samtidig forhindre, forstyrre eller redusere en motstanders stridsevne (Forsvaret, 2019a, pkt 05175).*

Definisjonen på elektronisk krigføring kan se ut til å være detaljert etter hvilket publikum det er ønskelig å treffe. Alt fra NATOs enkleste form som skal forklare det overliggende for et enhetlig forsvarssamarbeid og ned til fagpersoner som Gordon sin definisjon. Publikummet for definisjonen er i de to tilfellene forskjellig, og derfor blir definisjonen mer detaljert i sistnevnte som adresserer EK-fagpersonell.

EK vil være en viktig ressurs i en stridsoperasjon, og EK benyttes av begge sider i en strid samtidig. Mens den ene siden i striden vil utnytte aktive elektromagnetiske stridsmidler i en offensiv utnyttelse for å ødelegge for motstanderen vil den andre siden utnytte passive midler for å kunne motvirke motstanderens aktive midler. Bruken av EK-midler vil endre seg avhengig av posisjonen parten har i striden, den angripende eller den defensive. Disse rollene kan skiftes etter hvert som striden går fremover. Som en russisk forsvarspublikasjon omtaler elektronisk krigføring:

> *"It aims to "reduce the effectiveness" of enemy forces, including command and control and their use of weapons systems, and targets enemy communications and reconnaissance by changing the "quality and speed" of information processes. In reverse, EW in defence protects such assets and those of friendly forces" (McDermott, 2017, s. 3)*

Elektronisk Krigføring (EK): Terminologien omfatter flere innsatsområder. Det er både aktive og passive aktiviteter innenfor betegnelsen. Aktive midler er der en part påvirker motstanderens sensorer og systemer med egne midler. Passive midler kan beskrives som innsamling av motstanderens utsendte signaler for analyse og senere utnyttelse i en aktiv handling eller for å bygge egne databaser over motstanderens utnyttelse av det elektromagnetiske spektrum (NATO, 2020, s. 47)

Aktive EK-midler kan defineres som midler som aktivt forsøker å ødelegge motstanderens systemer innen K2 eller *Intelligence, Surveillance and Reconnaisance* (ISR). Dette for å blinde eller forvirre motstanderen gjennom deres systemers virkelighetsbilde. Dette kan gjøres både gjennom aktiv bruk av utsendelser innen EMS eller gjennom midler som deployeres f.eks. chaff eller flare (NATO, 2020, s. 47).
Passive midler vil være systemer der det benyttes materiell for å motvirke de aktive sendernes påvirkning. Dette kan være alt fra mekaniske chaff, for å motvirke fiendtlig radar i å oppnå korrekt målbilde, til elektroniske støttetiltak (ESM) for situasjonsforståelse og opparbeidelse av bibliotek over fiendens faktiske bruk av det elektromagnetiske spektrum (NATO, 2020, s. 47).

Drone: Drone er et ubemannet luftfartøy som kan kontrolleres med fjernstyring eller fly autonomt ved hjelp av programvare, sensorer og GPS (Tandberg & Jarslett, 2020)

EMS: Det ElektroMagnetiske Spektrum. Elektromagnetisk stråling er energi som overføres gjennom det tomme rom eller gjennom materie i form av elektromagnetiske bølger. Synlig lys, radiobølger og røntgenstråling er eksempler på EMS (Universitetet i Bergen, 2020).

GNSS: Global Navigational Satellite System. Dette er en samlebetegnelse på de forskjellige satellitt navigasjonssystemene som er tilgjengelig, enten globalt eller regionalt. Eksempler på GNSS er GPS (USA), Galileo (EU), GLONASS (RUS) og BeiDou (Kina).

Jamming: Med vilje å sende ut elektromagnetiske signaler for å ødelegge andres leselighet av ønsket signal eller for å forfalske dette (NATO, 2020, s. 72).

K2D: Kommand og Kontroll Desorganisering. Peonget med desorganisering av en motstanders Kommando og kontrollsystemer er å hindre denne i en tidsriktig og korrekt rapportering. Og dermed ha dårligere styring av sine styrker (Thomas, 2019, s. 6-1).

Satcom: Kommunikasjon over satellittbærende samband.

Spoofing: Å aktivt forvirre en motstander gjennom å sende feilinformasjon eller endre deres signal til å gi feil situasjonsinformasjon (NATO).

Som en evne for kampinnsats så er elektronisk krigføring (EK) svært godt egnet til de fleste stridsmiljøer. I et scenario med hybride midler vil EK være en godt tilpasningsdyktig evne der det er mulig å tilpasse intensitet og påvirkning etter hva det er ønskelig å få ut av situasjonen (McCrory, 2021, s. 36). EK kan lamme hele systemer innen EMS eller begrenses til å påvirke og forvirre mottakerens bilde/signal. Dette kan gjøres for alt fra GNSS til K2-systemer. Russland har siden krigen i Georgia, i 2008, utviklet sine evner innen EK og tilpasset dem til aktiv påvirkning av motstanderes systemer samt innsamling av motstanderens utsendelser i EMS. Elektronisk krigføring i denne oppgaven vil ta for seg områdene innen utnyttelse av EMS fra russisk side der de påvirker en motstander aktivt med elektromagnetiske utsendelser. Jeg vil ikke ta for meg innsamling av signaler da det er vanskelig å se hva som utføres i et passivt system og prosesseringen internt i systemet, men jeg vil nevne viktigheten av å samle inn og hvordan de kan utnytte noe av den innsamlede informasjonen. Aktive midler er derimot lettere å påvise gjennom hvordan egne systemer blir påvirket og annen innsamlet informasjon i det elektromagnetiske spektrum.

Hybride trusler er av NATO definert som en type trussel som kombinerer konvensjonelle, irregulære og asymmetriske aktiviteter i tid og rom (NATO, 2020, s. 64). Terminologien Hybrid krigføring fikk feste i NATO etter Russlands angrep på Ukraina, i 2014. Begrepet har derimot ikke en entydig definisjon, men tar inn i seg flere operasjonskonsepter utenfor en tradisjonell lineær krigføring (Giles, 2016b, s. 6). En hybrid trussel mot kyststaten Norge vil effektiv kunne gjennomføres fra sjøen. Norge har en kyststripe som rekker hele landets lengde og det er vanskelig for norske myndigheter å ha kontroll over et så langstrakt område. Russland har store amfibiske styrker med god evne for innsetting i norske kystområder. Det er også mange russiskflaggede fartøyer som seiler i norsk farvann. Disse fartøyene har

i sammen en evne til førsteinnsats gjennom fordekt innsetting av spesialkapasiteter og deretter landgang med amfibiske styrker (Metrick & Hicks, 2018, s. IV). Metrick og Hicks tar i sin bok «Contested Seas» opp problemet Russland kan utgjøre gjennom utnyttelse av forskjellige metoder. Russland kan sende inn spesialstyrker med utstyr på sivile fartøyer for deretter å svekke norske kystsystemer for situasjonsforståelse og bildebygging. Neste skritt vil kunne være å utnytte elektronisk krigføring for å lamme deler av kommunikasjonsnettverkene og påvirke sikker navigering gjennom GPS-forstyrrelser som jamming og spoofing (Metrick & Hicks, 2018). Ved bruk av hybrid krigføring er det bare fantasien som setter grenser for hva som kan settes inn som virkemiddel for å forvirre motstanderen fra å se det korrekte bildet. Et av hovedmålene for skjult førsteinnsats er å holde seg under terskelen for væpnet angrep og å unngå å bli attribuert angrepet. Denne oppgaven skal ikke omhandle hybrid krigføring som emne, men elektronisk krigføring spiller en viktig rolle innen hybrid krigføring. Hybrid krigføring er som nevnt i avsnittet en terminologi som tar for seg operasjoner utenom en tradisjonell militær-innsats med en lineær operasjonsplan. I samme kategori havner krigføringstyper som *asymmetrisk krigføring* og *New generation warfare*. Det er ikke noe nytt i noen av disse, men mer et behov for å ha en boks-betegnelse for å plassere operasjonsinnsatsene i.

Begrepet A2/AD (Anti Access/Area Denial) brukes som samlebetegnelse på innsats for å nekte en motstander innpass og bruk av områder. Uttrykket er NATO-generert og i Russland har de ikke dette begrepet i sine publikasjoner. I Russland omtaler de samme type operasjoner for «desorganisering» (Thomas, 2020b). Dette begrepet benytter de i forbindelse med motstanderens «Kommando og Kontroll» (K2) og «informasjonsledelse». Russiske EK-styrker spiller absolutt en rolle innenfor operasjoner for å nekte en motstander operasjonsfrihet i gitte områder eller fri bruk av det elektromagnetiske spektrum (EMS) til gjennomføring av deres operasjoner. Russiske EK-avdelinger har utstyr som dekker mange oppgaver og kan bidra til en økt sikkerhet for «andre egne» i fellesoperasjoner. Som Smith poengterer i sin artikkel om russisk EK: «*EW can also play a role in Russian anti-access/area denial efforts (A2/AD), where EW can be used as a "stand-off weapon" that "can turn areas falling within [its] range into strategically and operationally isolated 'bubbles.*"» (Smith, 2020, s. 3).

2 Metode

Som Dag Ingvar Jacobsen skriver i sin bok: «*Forskerens formulering av forskningsspørsmål og valg av metode vil forme hva slags informasjon som samles inn, noe som igjen vil bestemme hvordan virkeligheten fremstår, og dermed hvordan forskeren oppfatter den*» (Jacobsen, 2015, s. 22). Det er avgjørende at forskeren har et oppriktig mål om å fremme oppgavens med mål om å legge frem troverdig og gyldig kunnskap om virkeligheten (Jacobsen, 2015, s. 15). I denne oppgaven ønsker jeg å fremme en balansert og kunnskapsbasert vinkling basert på varierte rapporteringer og tolkninger. Jeg ønsker å se på hvordan Russlands bruk av elektronisk krigføring (EK) er rapportert gjennomført samtidig som jeg ønsker å frembringe mulig bruk av deres EK-ressurser mot Norge og NATO , som en førsteinnsats i en mulig fremtidig situasjon. Jeg ønsker også å få frem utnyttelsen av EK fra russiske tropper i Ukraina og Syria og forsøke å balansere dette opp mot situasjon og nytte.

Valg av metode for oppgaven

Denne studien er en kvalitativ dokumentstudie med en tilnærming og mål om å frembringe en fortolkning og fremstilling av en situasjon (Jacobsen, 2015, s. 133).

Den nyanserte fremstillingen det forsøkes på kan påvirkes av det tidkrevende arbeidet med informasjonsinnsamling. Det vil alltid kunne argumenteres med tidspress og evig søken etter mer, men analysen blir gjennomført på informasjonstilfanget innen «cut-off-date» (Jacobsen, 2015, s. 132).

Det vanskeligste med denne oppgaven har vært å få en følelse av å ha et godt nok informasjonsgrunnlag. Samtidig som mengden av informasjon har vært stor har det hele tiden vært mer å finne. Ikke alltid det mest relevante, men likevel innenfor temaet. Som Friedrich von Hayek snakket om i sitt foredrag som Nobel-vinner er ikke all forskning like enkel. Forskning innen realfag har en enklere vei til «fasiten» enn andre fagområder, som samfunnsvitenskap (Von Hayek, 1974). Det vil neppe være slik at to uavhengige forskere tolker alle uttalelser og oppførsler likt dersom de forsøker å gjenta et samfunnsvitenskapelig forskningsspørsmål, slik som man vil dersom en foretar en ren realfagsoppgave. Det er mye som ikke lar seg måle direkte og heller må tolkes og satt i sammenheng. Dermed blir det vanskelig å vite om alle nødvendige data er tatt med og at det ikke er glemt noen aspekter. Det vil alltid kunne være en usikkerhet om grunnlaget er godt nok. Poenget vil være at det er viktig å være åpen på hva som er tatt med og hvorfor noe eventuelt er utelatt. Det er nær umulig å få med alle faktorer da noen kanskje ikke en gang lar seg måle. I slike forskningsspørsmål er det komplekse situasjoner med mange potensielle utfall og som von Hayek sier i sitt foredrag er det ikke lett å på forhånd si hvilke faktorer som spiller inn en slags binding i informasjonen. For å finne de rette påvirkningene er det ikke bare å innføre en forenklet modell og analysere. Det vil ofte kreve store og viktige komplekse situasjoner med et mulig stort utfall. Som von Hayek poengterer vil det alltid være noe mer man kunne tatt med, men

det er like viktig å sette grensene for hva som skal med som for hvordan det vil være mulig å omhandle alle dataene. Mer informasjon vil i mange tilfeller heller kunne tåkelegge og forkludre analysen og tolkningen. Usikkerheten vil forbli hos forskeren om det var noen faktorer som skulle vært med eller om emnet er belyst godt nok. Etterrettelighetен i arbeidet må også være god da det i slike studier vil være mange som kan degradere arbeidet basert på faktorer de mener burde vært med og dermed diskreditere arbeidet.

Valgte data, deres gyldighet og pålitelighet

Dokumentundersøkelse innebærer at informasjonen er samlet og utgitt av andre personer i et tidligere arbeid. For å motvirke problemstillingen at all innsamlet informasjon er preget av like tanker og meninger må jeg samle inn informasjon fra forskjellige kilder og sammenligne deres resultater. Det er forskjell på hvordan kommentatorer ser på emnet jeg skal studere, og det innsamlede materialet viser at begge sider, mer eller mindre, ser negativt på eget ståsted og skryter opp motparten. Det blir derfor viktig å ikke bare se på de største navnene innen forskningen, men også ta inn mindre kjente som sitter nærmere det taktiske nivå med fingeren på pulsen innen emnet. Det er selvsagt et problem at Russland har strammet inn på tilganger til deres nettsider. Det er likevel mange som tidligere har dokumentert russiske kilders tanker om tematikken. Jeg har gjennom oppgaveskrivingen sett at det er svært mange som omtaler og kommenterer emnet i forskjellige sammenhenger. Ved å sammenstille mange av disse utgivelsene vil det muliggjøre en mer objektiv tolkning enn om antallet utvalgte artikler er lite. Gjennom å sammenligne både vitenskapelige verker med avisreportasjer og nyhetsbulletiner så blir det totale bildet relativt mer objektivt. Det er mange kilder som peker i samme retning, men nok andre kilder som peker på problemstillinger innen samme teoretiske bilde til at det er mulig å se en større sammenheng. Fordelen med skriftlige kilder er at det som er offisielt skrevet er sjelden spontant og kan regnes som mer gjennomtenkt og reflektert (Jacobsen, 2015, s. 172). Ikke at det dermed blir en endelig sannhet, men i det minste mer troverdig enn spontane utsagn. Derimot vil spontane utsagn kunne være blottet for «politiske» begrensninger og heller gi direkte meninger.

Det er nødvendig å ta stilling til påliteligheten til grunnlagsinformasjonen benyttet i en dokumentundersøkelse. Kjenner vi forfatterens motiver for artikkelen eller avhandlingen? Hvordan kan vi avgjøre om det er hold i påstander og konklusjoner? Det er mange ting som påvirker en kildes pålitelighet og det er vanskelig å ikke fremheve artikler og dokumenter som passer inn i egne holdninger etter hvert som undersøkelsene går fremover. Kildekritikk og siling av kilder som skal velges inn blir derfor en viktig prosess som må tas hensyn til av forskeren. Det kan i mange situasjoner være problematisk å få tak i førstehåndskilder og det er da nødvendig å ta til takke med andrehånds- eller i siste fall tredjehåndkilder. Problemet med kilder som er enda lenger unna primærinformasjonen er at alle ledd gjør sine utvalg og tolkninger i det de presenterer sine funn (Jacobsen, 2015, s. 188-189). I denne oppgaven har jeg blitt stilt over flere av disse problemstillingene. I denne sammenhengen har det derfor vært viktig å fokusere på kildenes hensikt og primærpublikum. Samtidig som jeg har måttet se på

informasjonen som er presentert har det også vært viktig å se etter andre kilder som omtaler og rapporterer innen samme tema og om det er avvik i rapporteringen. Dette omtaler også Jacobsen i sitt kapittel 9 under vurderinger av kilder (Jacobsen, 2015, s. 187-194). Det er mange mennesker og grupperinger som mener og føler sterkt for temaet denne oppgaven omhandler. Det er derfor mye informasjon å samle inn på, men da jeg ikke snakker russisk selv og emnet er innenfor et tema det kan være viktig for partene selv å holde reelle evner skjult for andre så er det vanskelig å verifisere påstander om kapasitetene.

3 Russisk EK

3.1 Bakgrunn

Det sovjetiske synet på elektronisk krigføring, i henhold til deres militære oppslagsverk fra 1984 (Kjellén, 2018, s. 20), endret seg ettersom tiden og teknologien har skridd frem. Det var i nevnte publikasjon definert som tiltak med EK-utstyr iverksatt for å identifisere og deretter nekte motstanderens elektromagnetiske utsendelser. Dette ble i henhold til definisjonen gjort for å beskytte egne styrker. Kjellén omtaler i sin rapport hvordan definisjonen i den sovjetiske marinens oppslagsverk, i 1990, endret til å spesifisere mer direkte egne styrkers evne til å detektere og nedkjempe fiendens utsendelser samt utnytte informasjonen til å lede ild mot fiendens styrker. EK ble sett og definert som en stridsstøttefunksjon (Kjellén, 2018, s. 20)

Det russiske forsvarets styrker innen elektronisk krigføring definerer i dag EK som evnen til å oppdage, nedkjempe, angi mål-data og å kunne angripe bakenforliggende systemer. I definisjonen har de implementert datasystemene bak emitterne og K2 systemene, brukt av fienden (Kjellén, 2018, s. 21).

Elektronisk krigføring har en lang historie i det russiske forsvaret. Russland regner starten på sin EK-historie tilbake til krigen mellom Russland og Japan i 1904. Da gjennomførte russiske fartøyer en jamming av japanske styrkers radioer før de klarte å gjennomføre en beskytning av russiske styrker (Smith, 2020). Elektronisk krigføring startet som forstyrrelse av motstanderens radiosamband. Etter hvert som utviklingen gikk og radar ble et viktig virkemiddel i krigføring ble det viktig å kunne jamme både samband og radar. I Kjelléns rapport fra 2018 referer han til sovjetisk militært oppslagsverk fra 1984:

> *«Electronic warfare is a set of measures taken in order to identify and subsequently use radioelectronic suppression on adversarial radioelectronic equipment and systems, and in order to protect own forces' radioelectronic equipment and systems» (Kjellén, 2018, s. 20).*

Sovjetiske EK-styrkers definisjon viser fokuset på radiofrekvenser og jamming av disse. Dette for å beskytte egne kapasiteter og ødelegge for motstanderen. Etter vært som teknologien gjorde fremskritt utvidet også russiske EK-styrker sin tolkning av hva de skulle innebære. Kjellén viser videre til russiske styrkers definisjon fra 2017:

> *«Electronic warfare is a set of coordinated activities and actions encompassing radioelectronic attack on adversarial radioelectronic and information-technical objects, radioelectronic protection of radioelectronic and information-technical objects, countermeasures against technical reconnaissance and radioelectronic information support measures» (Kjellén, 2018, s. 21).*

Som definisjonen nå viser så har russerne beveget seg fra den sovjetiske definisjonen av EK som dekket påvirkning av radiofrekvenser til å omhandle innsamling og påvirkning. Det er ikke lenger et forsøk på å motvirke motstanderens signaler, men skal nå også inneholde passive innsamlinger og aktive tiltak mot både utsendelser og systemene bak.
Da Russland gikk inn i Georgia, i 2008, merket de raskt at de ikke hadde hverken kapasitet eller evne til å motvirke georgisk luftvern. De klarte heller ikke å jamme ut georgisk samband i områder der stridighetene forgikk. Etter Georgia-operasjonen gikk Russland gjennom erfaringene av operasjoner og besluttet at elektronisk krigføring var et stridsområde de var avhengig av å håndtere bedre enn sine motstandere. President Putin startet oppbyggingen av EK-brigader i alle militærdistrikter. I tillegg til en EK-brigade underlagt hvert militærdistrikt bygde det russiske forsvaret også opp en egen selvstendig manøverbasert EK-brigade som ble underlagt Generalstaben. Landstyrkene er tungt EK-oppsatt, og forsvaret innførte også egne kompanier innen elektronisk krigføring i samtlige luftlandestyrkebrigader, egne EK-sentre i marineflåtens hovedbaser og EK-bataljoner i luftstyrkene (Kjellén, 2018, s. 33-40). EK-kompanier er i dag en særdeles viktig del av landstyrkene, og EK-styrkene har kapasiteter for EK innen taktisk, operasjonelt og strategisk nivå (Grau & Bartles, 2016, s. 288, 289).

En tradisjonell tankegang rundt EK er ofte bundet opp mot jamming av radar og radio. Dette er en veldig forståelig tankegang da slik jamming ofte blir eksemplifisert i diskusjoner innen EKs evner. I denne oppgaven vil jeg heller fokusere mer mot bruken av EK i en førsteinnsats-rolle. Elektronisk krigføring som en asymmetrisk funksjon med evner under terskelen for krigsangrep. Slike operasjoner kan benyttes i en «initial period of the war» (Osflaten, 2021, s. 110-111). Som Osflaten forklarer i sin artikkel er den initielle perioden der kapasiteter utnyttes i det skjulte for å oppnå en evne på et senere tidspunkt. Russland ønsker å påvirke i det skjulte for å legge til rette for en utnyttelse av et område ved senere anledning.

3.2 Elektronisk krigførings-styrker i Russlands Forsvar

Russland fokuserer på hvor viktig evnen er til å gjennomføre elektronisk krigføring i enhver operasjon. Det ble i perioden 2008-2009 gjennomført en restrukturering av forsvaret i Russland. Russland omorganiserte til de nåværende militærdistriktene. Med erfaringene fra Georgia 2008, om mangler i EK-kapasiteter, ble det samtidig gjort en endring i struktureringen av EK-styrkene. Viktigheten av elektronisk krigføring ble poengtert i Georgia og organiseringen av disse styrkene skulle vektlegges. Ikke bare ble det opprettet, som tidligere nevnt egne EK-brigader i hvert militærdistrikt, men disse brigadene skulle ha som oppgave å stille med EK-kapasiteter til støtte for gjennomføring av større operasjoner. Disse EK-brigadene ble opprettet i 2009 som et resultat av behovet for kraftsamling av

kapasitetene innen operasjonelt og strategisk nivå for å sørge for korrekt bruk og kompetanse. Kapasitetene var allerede til stede i landstrukturen, men den var spredt og ikke under en enhetlig kommando. EK-Brigadene ble derfor opprettet for en kraftsamling av denne evnen i militærdistriktene. Hver av disse brigadene inneholder fire EK-bataljoner og ett kompani (McDermott, 2017, s. 6). Nordflåten er et nyopprettet militærdistrikt og har ennå ikke egen brigade underlagt, men har egne EK-kompanier i sine bataljoner.

EK som en komponent i de militære styrker har i henhold til uttalelser fra sjefen fra de russiske EK styrker, Generalmajor Yuriy Lastochkin, en helt klar rolle og fordel:

> *«There is nothing surprising that in the current circumstances, EW—as a relatively inexpensive and easily implemented means to disrupt the functioning of an enemy's radar and other systems and to defend one's own similar systems from interference—is emerging as a priority and a focus for development. In certain circumstances, use of EW approaches can be viewed as asymmetric measures that negate the benefits of an adversary's highly sophisticated systems and means of armed combat"(McDermott, 2017, s. 3).*

Russiske landstyrker er definitivt størst i de væpnede styrkene i Russland. Sjø og luft har også EK-styrker, men det er selv i disse grenene flere EK-kapasiteter på land enn på sjø- og luftenhetene. På landenhetene i russiske EK-styrker har de fem primærområder de jobber innen og EK-brigadene er derfor oppsatt med egenskaper slik at de innehar evnen til påvirkning og utnyttelse av signalmiljøet. De fem operasjonsområdene er EK mot 1) bakkestyrker, 2) luftbårne systemer, 3) satellittbaserte systemer, 4) terroraktiviteter og 5) komplekse systemer (K2D) (Kjellén, 2018, s. 31-40). På fartøyer i Marinen vil det være systemer som kan gjøre mange av de samme operasjonene som landavdelingenes systemer, men primært vil slike systemer om bord fungere som selvforsvarssystem mer enn en aktiv påvirkningsoperasjon.

De nevnte EK-brigadene er satt opp med flere kapasiteter der de kan deployere kombinasjoner med effektorer som kreves til forskjellige oppgaver. Russiske militære styrker sendes ikke ut i operasjoner uten bidrag fra elementer fra disse EK-brigadene for nærsikring og operasjonsstøtte. Disse kapasitetene har systemer som kan gjennomføre jamming av HF på en distanse opp til 5000km, radarer, samband og K2-systemer, GPS, GSM og satellittsamband (McDermott, 2017; Thomas, 2020b, s. 17). Det russiske forsvaret har flere nyutviklede kapasiteter som utnytter en motstanders behov for bruk av EMS. Russerne legger opp til problemer for deres motstandere gjennom å ha kapasiteter til å lamme motstanderens evne til internkommunikasjon mellom avdelinger over distanse. Slik koordinerende kommunikasjon mellom egne avdelinger er viktig innen K2 for utnyttelse av kapasiteter og styrke-enheter.

Russlands bruk av EK i militære kampanjer er godt kjent blant deres motstandere. EK utnyttes også som et virkemiddel i deres operasjoner der de ønsker å fremstå med en lavere eller ikke-eksisterende militær tilstedeværelse. Kapasiteter innen elektronisk krigføring inneholder en evne som kan utnyttes til å forvirre eller tåkelegge situasjonen mer enn å ramme motstanderen tradisjonelt militært. Det å benytte EK til å skape usikkerhet hos motstanderen om situasjonen og hva som skjer, er en del av *hybride trusler* (NATO, 2020, s. 64). En slik uryddig krigføring kalles også for asymmetrisk krigføring eller ikke-lineær krigføring. EK kommer innunder denne betegnelsen på grunn av sin rolle som «stridførende», men likevel uten kinetisk energi. EK-styrker vil utnytte radiosignaler eller annen elektromagnetisk utsendelse som kan påvirke materiell, ikke mennesker, og dermed kunne operere skjult. Ikke minst kan de oppnå en mulighet for å nekte skyld (plausible deniability) (McDermott, 2017, s. 25). Russland har fokus på at krigføringen ikke skal være lineær, men innebære en usikkerhet/tvetydighet (ambiguity) i utførelsen. Under et foredrag i 2013 la Forsvarssjefen i Russland, General Valery Gerasimov, frem sine synspunkter på moderne krigføring. Han la da frem et syn om at krigføring ikke kan bestå av rene konvensjonelle styrker, da det å seire vil kreve mer enn bare ren maktbruk. Ved å benytte «usynlige» virkemidler som EK, cyber og spesialsoldater (hybride styrker) som undergraver og forvrenger virkelighetsbildet hos motstanderens befolkning, vil en kunne påvirke deres motstandsvilje (Galeotti, 2014; Monaghan, 2015). Det er ikke noe nytt at en makt benytter andre midler for strid enn rene militære styrker. Det kan derimot sies at slike ikke-lineære midler alltid har vært til stede. En «hybrid» motstander vil ofte være til stede i motstanderens land på forhånd og planlagt striden med sine undergravende midler.

Etter Sovjetunionens fall lå det russiske forsvaret økonomisk i en bølgedal, men da Vladimir Putin kom inn som president i 2000 ble forsvarsbudsjettet styrket, og det var fokus på økt satsing på moderne våpensystemer. Putin innførte en 10 års langtidsplan for det russiske forsvaret i 2010 (GPV-2020). Russland spesifiserte i GPV-2020 at deres materiellbeholdning ved enden av planen skulle bestå av 70% moderne våpensystemer (Connoly & Boulegue, 2018, s. 5). Dette målet har vist seg å være høyt prioritert innen flere typer våpensystemer. De mest åpenbare er nok de konvensjonelle og nukleære systemene som Russlands president gjentatte ganger har promotert i media; hypersoniske missiler, cruisemissiler, interkontinentale missiler (ICBM) og nukleær undervannsdrone (Osborn, 2018). Putin har også lagt vekt på å vise frem konvensjonelle våpensystemer i pågående stridigheter. Russland ser ut til å benytte Syria som en enorm «showcase» for sine systemer og bruken av våpensystemene i strid legges ut som nyhetssaker og glad-saker for egen befolkning. Pressedekningen fungerer også som en salgsfolder til regimeledere i Russlands venne-sfære. Filmer av missilskytinger inn i Syria fra fartøyer i Middelhavet legges ut av forsvarsministeriet kun timer etter gjennomførte aksjoner. Helt siden russiske styrker offisielt ble part i striden i Syria har de utnyttet situasjonen som et våpentestsenter av russiske systemer (Kofman & Rojansky, 2018, s. 18). Dette gjelder alle slags våpen og soldater. Det russiske forsvaret rapporterte at de har testet flere hundre våpensystem-utviklinger for å bekrefte design i stridsmiljøer. De våpenprosjektene som ikke besto gitte målsetninger har blitt terminert, mens godkjent

utstyr har blitt videreutviklet og videreført i det russiske forsvarets portefølje (Jaber, 2021; Petkova, 2020).

Det ble i løpet av de første årene av Ukraina-krisen sjelden rapportert fra ukrainske styrker om jamming GLONASS-signaler. Russland prioriterte antakeligvis sin jamming primært mot vestlige systemer da disse er absolutt mest utbredt. Russiske styrker viste også at de hadde mulighet til å «fjerndestruere» ukrainsk materiell, som var russiskprodusert. Denne «destruksjonen» ble trigget av russiske EK-styrker (Trevithick, 2019). Slike *killswitcher* i militært eksportmateriell er vanskelig å detektere av kjøperne, men gir en sikkerhet for eksporterende land om å slippe krig mot *eget* utstyr.

3.3 Russisk utnyttelse av elektronisk krigføring

Russlands våpenutvikling og testing har gjennom de siste tiårene fokusert på flere høyprofilerte våpensystemer, spesielt innen missilteknologi. Samtidig som de har videreutviklet flere systemer innen elektronisk krigføring. Det har vært flere store oppslag om nye missiler og deres testskytinger. De siste 5 årene har det vært tydelig gjennom Russlands gjennomføringer av skytinger med KALIBR-missiler (SS-N-30A Sagaris[1]) fra fartøyer plassert i Middelhavet og inn i Syria (Michaels & Stanglin, 2015; Reuters, 2017). Samtidig med de mediefokuserte våpenprogrammene har nye elektroniske krigføringssystemer blir testet og benyttet i praksis, både i Ukraina og Syria, uten samme promotering.

Russland har flere EK-systemer utplassert for beskyttelse av egne styrker både i felt og leirområder. Russiske styrker har flere EK-systemer som rammer alt fra GSM, radio-samband, link-systemer, satellittkommunikasjon, GNSS, radar og optiske enheter (Smith, 2020). Det er flere av russernes EK-systemer som rapporteres til stede når det forekommer jamming av forskjellige systemer i Øst-Ukraina. GPS og GSM utsettes ofte for jamming, men også andre sambandssystemer rammes i områder der russiske styrker opererer. GSM-jammingen skal ikke påvirke militære operasjoner, da GSM ikke er primærsamband for taktiske avdelinger. Men ved jamming av andre militære kommando-samband så ender mobiltelefon som eneste gjenværende samband. Det er rapportert fra ukrainske styrker i stridsområdene at russiske styrker raskt bombarderer deres stillinger dersom soldatene slår på sine telefoner i stridsområdene. Russiske EK-kapasiteter benytter triangulering av GSM-utsendelser som målangivelse for egne styrkers artilleriild (Collins, 2018; Trevithick, 2019).

Jamming av GPS-signaler vil i mange tilfeller være en effektiv måte å sette motstanderens systemer ut av spill. Russland benekter at de jammer GPS i Øst-Ukraina da de ikke har regulære styrker i området.

[1] SS-N-30A Sagaris er NATO-betegnelsen på det russiske kryssermissilet 3M-14

Når Organisasjonen for sikkerhet og samarbeid i Europa (OSSE) rapporterer jamming av sine droner i Øst-Ukraina legger Russland skylden på Ukraina. OSSE opplever jevnlig problemer med posisjonering på sine droner grunnet frafall av GPS- og radiosignaler for kontroll med droner, i Øst-Ukraina. Disse situasjonene rapporteres gjennom pressemeldinger og i løpet av tre måneder på våren 2021 meldte de inn seks situasjoner der deres droner måtte avbryte oppdrag grunnet jamming (OSCE SMM, 2021). Slike signaltap har medført at droner har styrtet og gått tapt. Russland på sin side anklager offisielt Ukraina for jammingen av dronene til OSSE (TASS, 2021). Til tross for Russlands anklager mot ukrainske styrker for jamming mot OSSE sine droner har OSSE selv gått ut med anklager mot Russland i disse tilfellene, da de rapporterer russiske EK-styrker i områdene jammingen forekommer (OSCE, 2021). Russland nekter for OSSEs attribuering av EK-innsatsen til Russland, gjennom å benekte kjennskap til handlingene og avkrefte egne styrker i området.

3.4 Russisk påvirkning på GSM-samband

GSM er ikke et primærnett for militære styrker og burde derfor ikke være et fokusområde for EK. Det som derimot viser seg, er at det er mye en militærstyrke kan oppnå gjennom å påvirke GSM i et område der de gjennomfører en militæroperasjon. Evnen til å bidra i IW-operasjoner mot GSM-enheter i stridsområdene er derfor en av oppgavene til russiske EK-styrker. En annen, er deres kapasiteter til å utnytte jamming av militærstyrkenes sambandssystemer og dermed tvinge ukrainske soldater til å benytte mobiltelefoner. Som nevnt i forrige kapittel, bruker russiske styrker ukrainske soldaters mobiltelefoners posisjon som målangivelse for ildgiving (Smith, 2020, s. 4; Trevithick, 2019). De utnytter EK sammen med Cyber og utfører ganske kompliserte scenarioer der de kobler sammen ukrainske soldater i operasjonsområdet mot deres familier, gjennom hacking av telefoner og bruk av cyber. Deretter gjennomfører de kommunikasjon mellom soldatene og deres familier for å skape frykt, redsel og tap av tro på egne evner til motstandskamp (Collins, 2018). Collins viser til noen tekstmeldingers innhold som seendes fra soldatens telefonnummer til familie: "surrounded and abandoned", etterfulgt av meldingen: "Your son is killed in action". Motsatt vei sendes meldinger som: "retreat and live", før artillerigranatene kommer. Slike demoraliserings operasjoner kan virke undergravende på motstandsviljen i befolkningen, i Ukraina.

Operasjonene nevnt over er ikke kompliserte, men utnyttelsen viser effektiviteten til bruken av EK i fellesskap med andre IW-innsatser. Det er ikke bare til innsamling av informasjon fra motstanderen og deres bruk av EMS som er interessant, men også motstanderens følte behov for telefonkommunikasjon grunnet påvirkningsoperasjoner. Personenes behov for å berolige familie utnyttes som målangivelse, og dermed for bekjempelse av dem selv. Mobiltelefoner er bare en type av utsendelser som kan peiles med godt EK-utstyr. US Army sin *Asymmetric Warfare Group* ga ut en håndbok til amerikanske soldater for

hvordan forholde seg til *New Generation Warfare*. Håndboken tar for seg flere emner innen russisk krigføring og deres evner. Den nevner også spesifikt russisk EK innen GSM-påvirkning:

> *"Electronic warfare devices allow Russian Forces to broadcast … messages directly against opposing Ukrainian forces with cellular text messages," "These can be very specific and directed at individuals, such as by threatening their wives and children by name, or generic and sent to entire units as was the case in Ukraine." (Assymmetric Warfare Group, 2016, s. 30)*

Elektronisk krigføring kan utnyttes som en effektiv part av information warfare (IW). Gjennom bruk av EK kan en part påvirke store deler av styrkene i et stridsområde. Russlands EK-styrker utnytter ikke bare evnen til å ødelegge eller påvirke signalgangen, men de infiltrerer og gir direkte informasjon til ønskede telefoner. EK er en viktig pilar i IW gjennom oppstarten av en strid og gjennom opprettholdelsen av IW sin evne til å påvirke motstandere gjennom striden over tid. Både gjennom deres evne til å 1) Degradere (*Degrade)*, 2) Korrumpere (*Corrupt)*, 3) Nekte (*Deny*) og 4) Utnytte (*Exploit*) sambandsmidlene i et område og påvirke stridsområdets EMS til sin favør (Assymmetric Warfare Group, 2016; Borden, 1999).

I Syria har motstanderne vært mindre teknologisk utviklede og deler av jammingen av mobilnettverk har derfor vært for egenbeskyttelse mot GSM-armerte IED-er og droner med styring mot mobilsignaler plassert inne på basene (Thomas, 2020a, s. 16). En slik lammelse av mobilnettverk på og rundt basen hindrer også spredning av uønsket informasjon fra leiren. Russisk ledelse forsøker å holde narrativet på styrkenes situasjon og ønsker derfor ikke fri flyt av ukontrollert informasjon (The Moscow Times, 2018).

Russiske EK-styrker i Ukraina har bevist gjennom 8 år at de er gode på GSM-påvirkningsoperasjoner. Derimot har de under angrepet på Ukraina i februar 2022 vært mindre synlige. En grunn til at det ble registrert mindre GSM-operasjoner kan være at det i de første åtte årene ble gjennomført påvirkning av GSM i et klart definert område med få mennesker foruten soldater (Eversden & Gill, 2022). I totalkrigen blir en hel befolkning blandet sammen i områder pakket med soldater og sivile i samme område. Påvirkningsoperasjonene blir da mer utfordrende og mindre målrettet. En måte de kan utnytte sine ressurser innen påvirkning av mobiltelefoner i en slik folkemasse er spredning av masseutsendte «SMS-flyveblader», med propaganda, til alle telefoner gjennom falske basestasjoner.

3.5 Russisk utnyttelse av GNSS-påvirkning

Etter USAs oppstart av GPS (1993) som globalt posisjoneringssystem for sivile og militære systemer har viktigheten av systemets tilstedeværelse blitt godt poengtert gjennom alle systemer som i dag benytter GPS-signaler for tids- og posisjonskontroll. Systemet ble opprinnelig ikke lagd for å være jammeresistent, men robust mot interferens og utilsiktede forstyrrelser gjennom flere parallelle

frekvensbånd som økte posisjoneringsnøyaktigheten. Signalet fra satellittene er så svakt at det på bakken er lett å overstige signaleffekten med enkle midler og dermed jamme ut satellittsignalet. En GPS-jammer med signalstyrke som en GSM-telefon kan fra et fly jamme GPS signaler innenfor flere titalls kilometer. Selv mot en GPS som allerede har låst posisjonssignalet kan denne tvinges av posisjonssignalet på 10km avstand fra jammeren (Glomsvoll, 2014, s. 24). I løpet av de siste 10 årene har det blitt opprettet andre GNSS systemer tilsvarende GPS. Innen gruppen GNSS ligger i dag systemer som GPS (USA), GLONASS (Russland), GALILEO (EU) og BeiDou (Kina). Alle systemene har ikke god dekning over hele kloden, men alle kan brukes av militære systemer og kapasiteter, og alle har hemskoen med svake signaler på sine frekvensbånd. GNSS blir benyttet av svært mange aktører i hele verden og på verdensmarkedet har GPS den definitivt største andelen brukere.

Bruk av EK som kapasitet innen degradering av en motstanders GNSS er svært effektivt. Den amerikanske hærens gruppe for asymmetrisk krigføring har sett avhengigheten av GNSS som så alvorlig at de har gitt ut en publikasjon med poengtering at det i en strid ikke vil være mulig å stole på satellittsignaler for navigasjon. Kart og kompass må derfor være primærkunnskaper for personell i felt:

> *Units should anticipate attacks on their electronic assets during the planning for any operation. The performance and reliability of electronic navigation will deteriorate, cease to function entirely, or provide incorrect data to the user through false information inserted by an opposing force. The ability to maneuver could be reduced to non-electronic navigation aids (compass, military map) or other aids… (Assymmetric Warfare Group, 2016, s. 35)*

Russiske styrker utnytter ofte bruk av GNSS-jamming i sine operasjoner. I Europas grenseområder mot Russland registreres det GNSS-jamming jevnlig. I 2018 gjennomførte NATO en stor øvelse i Norge og det ble gjennom hele perioden registrert jamming av GPS-frekvensene i grenseområdet mellom Russland og Norge (Nilsen, 2019; Regjeringen, 2019). Denne jammingen er primært satt opp som et selvforsvar for russiske baseenheter, men vil også fungere som en jamming av norske områder. Det at russiske styrker dermed også rammer sivil luftfart i nabolandene er en signalering om at Russland prioriterer en EK «beskyttelsesparaply» mot eventuelle langtrekkende presisjonsvåpen, fremfor sivile behov. Russland annonserte i 2016 at de ønsket å plassere 250.000 GPS-jammere i mobilmaster, rundt om i Russland, for effektivt å kunne beskytte mot angrep fra cruise-missiler (Goward, 2019). En slik bruk av GPS jammere passer godt inn med rapporterte problemer blant drosjesjåfører i Moskva. De melder at deres GPS kartfunksjoner ikke fungerer i området rundt Kremlin da posisjonen i disse navigasjonssystemene plasserer dem 20 kilometer utenfor Moskva. Slik bruk av signalforstyrrelser brukes ikke bare i Moskva. Det er et betydelig antall situasjoner der fartøyer i kystområder, spesielt i Svartehavet, befinner seg langt inne på land i sine kartplottere (Nilsen, 2017). Russiske styrker benytter også en slik jamming og spoofing av GNSS for sikring av VIP-mennesker i lederapparatet (BBC, 2019). Det er ikke vanskelig å forstå hvorfor russiske styrker gjennomfører slike spoofing-operasjoner. Russiske EK-styrker som gjennomfører oppdrag med VIP-mennesker og viktige områder er en

signalering der de viser for dem som kan detektere dette at de har kontrollen og ikke møter uforberedt. Å påvirke alle andres hverdags-hjelpemidler og andre nasjoners områder på en slik måte er en markør for makt.

Alle sjøgående næringsfartøyer bruker GPS som posisjoneringsverktøy og sender automatisk fartøyets posisjon, kurs og fart til alle andre fartøyer i området, gjennom AIS[3], for å unngå kollisjon. Gjennom Spoofing av GPS-signaler vil en aktør kunne endre fartøyers seilingsruter og ikke minst påvirke om de seiler i internasjonalt eller nasjonale farvann. Dersom det skulle bryte ut en uenighet mellom Russland og en annen kyststat vil det være nødvendig for Russlands motstander å være klar over Russlands bruk av EK-midler som kan gjøre stor skade. Russland kan i en eventuell oppbygging av situasjon deployere enkle GPS jammere eller spoofingmateriell på sivile fartøyer for deretter å true kyststatens næringsliv gjennom å potensielt sende fartøyer på grunner eller land gjennom falske posisjonsdata.

Organisasjonen for sikkerhet og samarbeid i Europa (OSSE) opprettet i 2014 en spesialgruppe for å holde oversikt over situasjonen i øst-Ukraina. I perioden etter 2014 har Russland gjennom sin GPS-jamming i østlige Ukraina satt flere av OSSE sine overvåkingsdroner ut av spill. Gjennom jamming av deres kontroll og posisjonssignaler har de sørget for at disse har totalhavarert eller nødlandet ved hjemmebase (DFRLab, 2018; OSCE, 2021). Slike EK-operasjoner følger de opp med IW-operasjoner gjennom å plante russiske narrativer i media der de anklager Ukrainske myndigheter for å jamme OSSEs droner i sine oppdrag i Øst-Ukraina (TASS, 2021). Russland har vist at de er dyktige på totaliteten i den type operasjoner og ikke minst hvordan de kan påføre motstanderen problemer med påvirkning av både GSM og GPS i kampområdene.

3.6 Jamming av K2

Et av de viktigste forholdene for opprettholdelse av kommando og kontroll (K2) vil være kommunikasjonsmidler mellom ledelse og styrker. Et K2-system vil optimalt sett være gjennomført på faste kanaler via fiberkabler eller andre nedgravde kabelsystemer som er ute av syne for fienden. Dette lar seg derimot ikke gjøre i en styrke som skal operere i et krigsteater med stadig forflyttinger og mekaniserte avdelinger. Da er det sambandsbærere gjennom eteren med RF-signaler som benyttes. For landavdelinger med sentralisert ledelse og ordregiving vil slike K2-samband være relativt enkle å finne, da det i slike organisasjoner vil bli mye trafikk til og fra sentralisert kommandoplass. I krigen i Ukraina viser de ukrainske styrkene å ikke operere med sentraliserte ledd, men heller desentraliserte noder der det blir mindre trafikk og dermed også vanskeligere for motstanderen å finne K2-ledelsen (Osborn,

[3] AIS – Automatic Identification System. Anti kollisjonssystem på fartøyer

2022). På land er det mulig for styrkene å utnytte geografiske strukturer for å dekke sine utsendelser og hindre motstanderen fra å detektere utsendte signaler, mens det for sjøstyrker er vanskeligere. Så fort fartøyer i marinen er utenfor skjærgårder og områder med øyer blir det store områder der de kan peiles og jammes. Russiske EK-styrker har på strategisk nivå systemer som er kapable til å jamme store områder som dekker både land- og sjøområder. Murmansk BN er et slikt system. Det kan gjennomføre informasjonsinnsamling av signaler for etterretninger og i tillegg jamme RF-signaler i HF-båndet ut til 5000km i havet (Thomas, 2020b, s. 17). Det sender enorme mengder med støy ut i eteren og vil degradere signalmiljøet så kraftig at de kan hindre motstandere til effektiv K2 i store områder. Slike systemer vil potensielt jamme alt i sitt område. Ikke bare motstanderens, men også ens egne systemer som opererer i HF-båndet.

En av utfordringene som vil treffe USA og NATO, i tilfelle en krise mellom NATO og Russland, er jamming av satellittkommunikasjon (satcom). NATO, med USA i spissen, har bygd opp store deler av sitt K2 nettverk rundt satcom (Bendett et al., 2021, s. 67). Denne typen kommunikasjonssignaler er noe Russland har fokusert på og har effektive EK-systemer for å ta ut (Bendett et al., 2021, s. 43). Amerikanske styrker i Syria rapporterer hvordan russiske systemer jammer deres nettverk og kommunikasjon mellom land og luftstyrker (Keller, 2019)

En annen viktig egenskap for EK er innsamling av parameterdata fra motstanderes emittere. Gjennom montering av utstyr for innsamling av RF-signaler som benyttes i kystnære områder vil en aktør kunne sørge for forhåndsprogrammerte systemer som kan påvirke slike radar- og linksystemer langs kysten i en eventuell konflikt. Det vil enkelt kunne monteres på diverse type skip som ferdes i andre lands territorier for deretter å bli brukt i erfaringsdatabaser i russisk EK-programmering. Slik innsamling vil kunne benyttes for programmering og testing av nye systemer med KI. Kunstig intelligens vil i slike systemer kunne avgjøre hvilken type emittere og hva slags meldinger som formidles (Andås, 2020, s. 33). Dette vil kunne utnyttes for å samle inn informasjonen, påvirke forsendelsene gjennom tilførsel av falske data eller nekte signalene gjennom jamming.

3.7 Hovedfunksjoner for EK-kapasiteter

Russland bruk av EK faller inn under kategorien støttefunksjon i operasjoner. En slik karakteristikk av kapasiteten gir ikke EK den fulle respekten den fortjener. Russland har spesifikt satset på faget EK de siste tiårene og legger vekt på utvikling og kompetanse innen denne militærkapasiteten som EK utgjør (McLeary, 2015). Elektronisk krigføring som funksjon er definert som en styrkemultiplikator. Styrkemultiplikator-rollen er noe som har utviklet seg over tid. Ikke bare hos russiske styrker, men i militære forsvarsstyrker generelt. EK er planlagt brukt for å hindre motstanderen i å utnytte EMS i en

operasjon, mens for egne styrker skal EK fungere som en garantist for unnvikelse fra fiendens systemer og oppdagelse. Dette krever selvsagt at EK-avdelingene har flere systemer som dekker flere bruksområder, og multiple frekvensbånd. Som McDermott (2017) tar opp i sin bok så vil EK bli utviklet til mer enn en støttefunksjon i det russiske forsvaret. EK vil få økte bevillinger og oppgraderes til egen våpengren. Dette vil gi EK en viktigere rolle innen planlegging av militæroperasjoner for å effektivt sørge for fiendtlig K2D (McDermott, 2017, s. 10).

EK er delt inn i tre hovedgrupper. Elektronisk støtte (ES) gjennom utnyttelse av innsamlingsmidler for oppbygging av biblioteker og etterretninger fra en motstanders utsendelser. Dersom det skulle bli detektert utsendelse fra en fiendtlig emitter så kan elektronisk angrep (EA) benyttes for å uskadeliggjøre fiendens utstyr. Skulle det være et fiendtlig EK-angrep mot egne systemer vil det være nødvendig å bruke elektronisk beskyttelse (EP) mot dette for egenbeskyttelse av egne systemer.

For EK er funksjonen elektronisk støtte en av de viktigste gjennom en operasjon. Det er selvsagt viktig å gjennomføre angrep og påføre en fiende problemer, men innsamling av motstanderens bruk av EMS gir mye kunnskap. I en passiv funksjon vil en kunne samle inn informasjon fra samband om fiendens intensjoner og situasjon, men også samle inn mengder av metadata fra deres systemer. En viktig utvikling av EK-systemer er dets evne til automatisering og evnen til å få vekk «man in the loop» og heller gå over til «man on the loop» (Andås, 2020, s. 32). I nye stridsmiljøer er mengden data benyttet i EMS så stor at det er vanskelig for mennesker å mestre dette. Dersom EK-systemet selv kan ta avgjørelser basert på kunstig intelligens og erfaringsdata så vil det være svært verdifullt. Det er først i denne sammenhengen at en EK-operasjon virkelig kan bidra til å utmanøvrere en motstanders OODA-loop (Richards, 2020). Slike innsamlinger av erfaringsmateriale vil foregå kontinuerlig. Russisk innsamling av EMS-data er ikke berammet til et område i en stridshandling, men derimot gjennom kontinuerlig innsamling mot NATOs styrker og enheter. Russland har flere stasjoner på grensene mot NATO gjennom hele Europa og ikke minst egne innsamlingsfartøyer som opererer inne i NATO-fartøyers øvingsområder. Gjennom å ha et etterretningsfartøy (AGI) liggende i nærheten av en NATO-fartøygruppe så vil de sitte igjen med en mengde data på NATOs bruk av samband, sensorer og manøvrering. Dette er kunnskap som potensielt går inn i erfaringsdatabaser for opplæring og testing av kunstig intelligens som kan implementeres i EK-systemer på fartøyer, fly eller landenheter. Kunstig intelligens er absolutt et satsningsområde innen EK-utviklingen og jo bedre og mer realistisk erfaringsdata et slikt system har å bli opptrent i desto bedre egnet blir det til automatiserte beslutningsprosesser i reelle operasjoner (Thomas, 2020b, s. 15). Slike innsamlingsaksjoner er det mange av i løpet av et år. Det er vanlig for russiske fly å fly langs Norges kyst jevnlig og ikke minst er det ofte fartøyer med innsamlingskapasiteter som regelmessig oppholder seg i farvann utenfor store NATO-baser. Det er ikke mye utstyr som skal til, men en god digital radio med opptaksmulighet vil kunne gjenskape gode nok data for erfaringsutnyttelse av slike data.

Ved å se på russisk behov for innsamling av sambandsdata og linksystemer vil det være nyttig for russiske myndigheter å plassere slike innsamlingskapasiteter på fartøyer uten militær betydning for så å samle inn «hverdagsdata» for å si noe om normalsituasjonen i et område. Dette kan så legges inn i systemer for rapportering av unormal sambands- og datatrafikk i et område. Et slikt datasett vil spille direkte inn på russiske styrkers mål om K2D og kapasiteten for å ramme NATO-lands internkoordinasjon. EK-styrkers roller kommer her inn i funksjonen hybrid krigføring og hvordan de kan bidra til å skape forvirring i starten/opptakten til en konflikt. Det vil for begge parter i en konflikt være viktig å komme først til skudd på motstanderens K2 for å få forsprang inni konflikten. Politiets spesialtjeneste (PST) har a mottatt bekymringsmeldinger fra personell i Los-tjenesten om russiske sjømenn som sa det var ønske fra russiske myndigheter at de fikk farledsbevis for å kunne sile fritt i norske farvann og dermed kunne bemanne russiske fartøyer i tilfelle krise/krig (Doksheim, 2015).

3.8 Russisk bruk av EK i operasjoner

Russland angrep Ukraina i 2014 da de angrep østlige Ukraina og tok Krim-halvøya. Soldatene de benyttet var ikke konvensjonelle soldater, men de ble kalt separatister og utga seg for å være Ukrainere med ønske om selvstendighet. Russland hadde flere fordeler da de startet denne kampen. De møtte et uforberedt ukrainsk forsvar som hverken var mentalt eller militært forberedt. Russland satte raskt inn militære kontraktører med leveranser til separatistene som hurtig koordinerte innsatsen på bakken. Ikke minst sendte Russland inn EK-materiell for bruk mot ukrainske styrker i grenseområdene. Disse EK-kapasitetene hadde som hovedoppgaver å sørge for sabotasje mot russiskproduserte samband brukt av ukrainske styrker, innsamling av sambandstrafikk, jamming og spoofing av GPS og sambandsstasjoner samt angrep på informasjonsteknologiske hjelpemidler. Sistnevnte ble veldig synlig gjennom russiske systemers evne til hacking av telefoner, masseutsendelser av meldinger i flere medier (GSM, mail, radio) for undergraving av ukrainske myndigheter og folkets motstandslyst (Sukhankin, 2020, s. 6). Gjennom bruk av disse systemene, som det russiske forsvaret stilte til disposisjon, kunne styrkene på bakken jamme ukrainske styrkers bildebygging i stridsområdene samt sette deres radiosamband ut av spill. Russisk-støttede styrker i Ukraina benyttet seg av hele spekteret innen sine tildelte kapasiteter av EK. En viktig metode russiske styrker benytter seg av er påvirkningsoperasjoner av sivilbefolkningen gjennom tradisjonelle media og sosiale media. Emnet informasjonskrigføring (IW) innen påvirkningsoperasjoner er svært viktig for å holde presset oppe om situasjonens fordeling av skyld. Gjentakende formidling av et budskap har vist seg meget effektivt for å vinne folkets oppfatning av situasjonen, både på hjemmebane og i stridsområdene. I slike operasjoner er såkalt «fake news» et viktig virkemiddel. Gjennom massegjentakelse av budskapet nok ganger så må selv motstanderen adressere usannhetene for å ikke virke skyldig. Russland har hatt fokus på IW-operasjoner tilbake til lenge før

internett. De brukte da andre lands aviser og media som bærere av sine budskap mens de i dag utnytter mer moderne og spredningsvennlige former for påvirkning (Cunningham, 2020).

GPS-jamming er ikke et komplisert område innen EK. Signalene fra satellittene er svært svake, og de ble ikke utviklet med tanke på å være motstandsdyktige mot jamming. Signalene er fordelt på forskjellige frekvenskanaler for bedre å unngå naturlig interferens, men for noen som ønsker å sette signalene ut av spill er det enkelt. For jamming av GPS-signaler er det bare å ha en sender i samme frekvensbånd som overstiger GPS-satellittenes signalstyrke. Russland har flere systemer for jamming av GPS-signaler distribuert i det russiske forsvaret. I Ukraina-konflikten er det diverse aktører som benytter systemer for overvåking og kontroll av konfliktens parter. Organisasjonen for Samarbeid og Sikkerhet i Europa (OSSE) er en av disse aktørene. OSSE jobber på et mandat fra Europarådet for å holde kontroll på hva som blir gjort og hvem som gjennomfører hvilke handlinger. Som en del av dette arbeidet benytter de langtrekkende flygende droner (UAV-er). OSSE har flere ganger opplevd jamming av GPS-signaler for styringen av sine droner. De har gjentatte ganger rapportert dette og vært i situasjoner der droner har nødlandet på alternative plasser eller så vidt kommet seg ned. Den 17. mai klarte de derimot ikke å motstå denne jammingen og dronen styrtet (OSCE, 2021). Da de sendte to droner for å våke over krasjstedet ble også disse jammet og kom aldri frem til krasjstedet (OSCE, 2021). I denne saken ble det sendt ut fem pressemeldinger fra OSSE om GPS-jammingene av deres droner. Som tilsvar på dette sendte Russland ut en pressemelding gjennom den statlige medieaktøren TASS der de anklagde myndighetene i Ukraina for jamming av OSSE sin drone i oppdrag over øst-Ukraina (TASS, 2021).

Jamming av GPS er som nevnt ikke komplisert, men det som krever mer innsikt og utstyr er å spoofe slike signaler. Da er det ikke bare å overdøve satellittenes signaler, men nye signaler skal genereres og distribueres til mottagere som skal lese de nye signalene som gyldige tidssignaler. Gjennom disse falske signalene vil den aktive parten forlede alle GNSS-mottagere i sitt område til å tro at de er plassert et annet sted enn de i virkeligheten er. Russland har utviklet mobile og effektive EK-systemer til disse formålene (DFRLab, 2018; Thomas, 2020b). Kjent bruk av slike systemer utenom stridsområder er som deployerte luftsikring-«paraplyer» mot innkommende GNSS-styrte missiler mot høyverdige mål, f.eks.: Kremlin og president Putin på reise. Det er ved flere anledninger rapportert om fartøyer som på sine navigasjonssystemer får oppgitt at de befinner seg langt inne på land. Disse fartøyenes navigasjonssystemer har da blitt utsatt for spoofing. Slik spoofing av fartøyer er også godt dokumentert da globale AIS-bildedistributørers systemer plutselig plasserer fartøyer på land i slike stridsområder (BBC, 2019). En av de tydeligste incidentene av slik spoofing var da president Putin besøkte Krim og Kerchstredet. Det var da tydelig at han hadde en «GNSS-paraply» som passet på ham (C4ADS, 2019, s. 26). En slik paraply vil kunne beskytte mot droner, missiler og GNSS-styrt ammunisjon. Det er ikke

ufarlig med en slik bruk av jamming/spoofing av GNSS-systemer. Skipstrafikk og luftfarten er helt avhengig av GNSS-systemer for sikker navigasjon. Deres pålagte anti kollisjonssystemer er basert på automatisk posisjonering og sending av varsel til andre enheter i samme område om egen posisjon, kurs og fart. Dermed vil jamming/spoofing av GNSS ramme posisjonssignaler for automatiserte systemer for sikker navigasjon, og risikoen for kollisjoner og havari vil øke. Operasjoner som medfører risiko for sikkerheten til sjøs og i lufta er noe som tas på alvor i internasjonal luftfart og skipsfart, og påvirkning av disse systemenes pålitelighet blir raskt rapportert og håndtert opp mot de ansvarlige. Russland har derfor flere ganger blitt utsatt for søkelys i forbindelse med GNSS-jamming både i Arktis og Svartehavet (Hambling, 2017; Regjeringen, 2019). Slik forstyrrelse av signaler rammer derimot ikke bare ens motstandere. Den rammer derimot også egne styrker og vil derfor kunne være til fordel for en del av egne operasjoner, men absolutt kunne medføre problemer for andre deler av egne operasjoner. Ukrainske styrker opplevde lite jamming av sine satellittsamband. Dette var samme samband brukt av russiske styrker. Derimot opplevde de at Russland hadde en «kill switch» de aktiverte i russiske samband som spredte seg som et slags virus og satte sambandssystemene ut av spill (Trevithick, 2019). De samme ukrainske styrkene opplevde og så at russiske styrker forstyrret signalene fra amerikanske GPS, men at de samtidig jammet og spoofet eget GLONASS signal. Trusselen ved påvirkning av GNSS-signaler vil være selvsagt for de som benytter dem for sikker navigasjon. Trusselen vil derimot kunne være mye større og farligere gjennom spoofing av signalene enn av jamming. Der jamming vil sørge for at GNSS-systemet om bord ikke vil vise noen posisjon så vil spoofing sørge for å vise feil posisjon. Denne posisjonen kan være lite grann av slik at Russland kan påvise at andre benytter deres territorium ulovlig eller de kan settes langt ut av faktisk posisjon for således å skape farlige situasjoner med styringssystemer med autopilot.

En viktig erfaring Russlands fikk fra stridsoppdragene i Syria var evnen til å opprettholde K2 og evne å ødelegge for motstanderens K2. De erfarte i Syria at motstanderen var mindre teknologisk utviklet, men de opererte svært dynamisk og russisk evne til å opprettholde overtaket i situasjonsforståelse og evne å utnytte EK-systemene til å bedrive K2D mot motstanderen samtidig som de opprettholdt egen K2 (Clark, 2021).

Russland benytter de samme EK-systemene i Syria som i Ukraina. Styrkene innen elektronisk krigføring i Russland rullerer mellom de forskjellige stridsmiljøene for å bygge erfaring fra både Ukraina og Syria. Forskjellen er derimot stor i hvordan EK-styrkenes innsats promoteres til omverdenen. Mens Ukraina er et oppdrag der de benekter egne styrkers innblanding og at det er ukrainske styrker som gjennomfører jamming og signalforstyrrelser er derimot Syria et utstillingsvindu der russiske styrker deler sin erfaring i utført arbeid. Russlands Forsvarsminister, Sergei Shoigu, uttalte i 2019 at han mener russiske EK-styrker og systemer er i en særklasse. Et av eksemplene som da trekkes frem er fra Syria der et russisk

EK-system (Krasukha-4) jammet amerikanske Tomahawk-missiler. Russland mener de jammet missilene slik at 36 av 59 misset på sine mål (McDermott, 2021a). Amerikanske styrker benekter dette. Det er vanskelig å finne troverdige kilder som objektivt vil kunne si hva sannheten er. Amerikanske styrker vil nødig offentlig anerkjenne russiske enheter som overlegne deres egne og russiske styrker vil selvsagt hevde at deres systemer er langt forbi kapasitetene hos sine motstandere. Sannheten vil nok ligge et sted imellom, men LtGen Ben Hodges uttalte i et intervju at russiske taktiske styrker har: «*electronic warfare capability at a tactical level that we absolutely don't have*» (Brimelow, 2018) og «*Russia has developed a significant electronic warfare capability*» (Nilsen, 2017).

På tidspunktet, der Russland gikk inn i Syria og aktivt tok part i en borgerkrig, hadde Russland allerede problemer på hjemmebane med internasjonale handelsrestriksjoner etter angrepet på Krimhalvøya og østre Ukraina. Mange militærprosjekter ble forsinket da de ikke fikk importert materiell til sine nybygg. Frankrike kansellerte også eksporten av Mistral hangarfartøyer til Russland. Det var lite å vinne for Russland annet enn å ta et standpunkt for regionen og sørge for å forbli en regional og strategisk maktfaktor som motvekt mot NATO og USA (Kofman & Rojansky, 2018, s. 10).

Russland startet tidlig med våpenbruk inn mot mål i Syria. Borgerkrigen ble raskt brukt for testing av nye missiler i Kaliber-systemet (Michaels & Stanglin, 2015; Reuters, 2017). Missilene ble avfyrt fra fartøyer plassert i Det kaspiske hav, med flyrute over Iran og Irak før de slo ned i diverse områder i Syria. Russland var godt kjent med stridighetene og hva de ønsket å bidra med og de hadde flere nye systemer de ønsket å teste i reelle stridsmiljøer (Brown, 2017; Jaber, 2021). Stridsmiljøet viste seg gunstig for utplassering og testing av nye anti luft-systemer (Smura, 2016), langtrekkende landmålsmissiler avfyrt fra marinefartøyer og ubåter (Reuters, 2017). For at angrepene skal kunne gjennomføres og ikke minst lykkes er det nødvendig for russiske styrker å ha kontroll på eventuelle motstanderes sensorer og potensielle motmidler. Det vil være nødvendig med sensorer for markering av mål gjennom koordinater på forhånd eller personell på bakken med markeringsutstyr. En erfaring russiske styrker dro med seg fra krigen i Georgia, 2008, var behovet for situasjonsoversikt i stridsmiljøet. De igangsatte derfor prosjekter for utvikling av feltdroner for bygging av situasjonsbilde og kommando og kontroll. De endte opp med flere typer droner, men den dronen de benyttet mest er en lett drone som kan deployeres og bemannes av en til to personer. Dronen heter Orlan-10 og gir evne til foto/video, radiorelè, signalinnsamling, EK og målangivelse (Grau & Bartles, 2016, s. 372).

Russisk bruk av EK i Syria ble primært sett opp mot egenbeskyttelse mer enn som en «showcase»: ”Russian EW systems deployed in Syria were focused on base and force protection, rather than serving as a chance to show off systems in a wider effort to send “strategic messages” (McDermott, 2017, s.

22). Syria har likevel vist seg å være en velegnet plass for test av nye EK-systemer og deres ytelser i et aktivt stridsområde. EK-systemene russiske forsvaret har brakt med seg til Syria har vært til plage for både amerikanske styrker vel som for Israelske. Amerikanske styrker ble i henhold til General Raymond Thomas: "*everyday Russia is knocking our communications down*" og Syria ble omtalt som: "*the most aggressive EW environment on the planet*" (Smith, 2020, s. 8). De amerikanske troppene rapporterte at selv droner med krypterte kommandosignaler og anti jamme-utstyr ble jammet av russisk EK-materiell.

Russland har brukt Ukraina som en testarena for sine EK-systemer. Russland så tidlig fordelen med å kunne jamme en motstanders utsendelser og samband for å motvirke deres evne til å koordinere og motta ordrer. De så også fordelen med å kunne sørge for at motstanderen heller ikke visste hvor de var. Gjennom jamming av motstanderens samband- og posisjonssignaler vil de potensielt oppnå et fortrinn.

3.9 Hva skiller EK i Ukraina og Syria

En viktig forskjell i hvordan Russland opererer forskjellig i Syria og Ukraina er åpenhet om operasjonene. I Øst-Ukraina har Russland gjennomført operasjoner under dekke av at det ikke var regulære russiske soldater, men ukrainske separatister som ville ha selvstendighet. Dette gjaldt på Krim-halvøya samt i Donbass området øst i Ukraina. Russland har i de åtte årene etter annekteringen av Krim nektet for å ha regulære styrker i områdene, men de har støttet russisk-ukrainske separatister som kjemper for sine rettigheter (Qiblawi et al., 2022). Russland benekter egne styrker i området tross bred rapportering om både russisk utstyr og offiserer i østlige Ukraina (Qiblawi et al., 2022).

På den andre siden har Russland i Syria hatt en åpen rolle. De gikk med i krigen på President Assads side i 2015 og har etter det åpenlyst gjennomført massive stridstiltak. Gjennom sin åpne krigføring i Syria fant de en enorm arena for å vise seg til vennligsinnede om hva de evner på slagmarken. Gjennom flere år har de gjennomført storstilt våpentesting. De har som nevnt tidligere brukt store deler av sine kapasiteter og evner innen EK i Syria. Det som derimot har skilt seg mest fra EK-bruken i Ukraina er at de primært har bedrevet sikring av egne baser og styrker. I Ukraina har de russiske EK-styrkene gjennomført aktive EK-operasjoner mot militære og sivile. I Syria har de samme kapasitetene primært gjennomført operasjoner for sikring av egne styrker (McDermott, 2017, s. 21). Som McDermott tar opp i sin bok (2017) var det i Syria få trusler mot russiske styrker. Deres EK-avdelinger ble derfor satt til A2/AD-oppgaver og beskyttelse av egne styrker. I henhold til McDermott ble det ikke fokusert fra russisk side på en trussel om krig med NATO, i Syria. Russland konstaterte tidlig i konflikten at det var svært liten lufttrussel fra opprørsgruppene Russland skulle bekjempe. Manpads var trusselen og dette ble motvirket gjennom å fly høyere (Clark, 2021, s. 25). EK ble derfor rettet mot å slå ut opprørsgruppenes mobilnett og sørge for å lamme deres mindre robuste K2-nettverk ved å fjerne kommunikasjonslinjene gjennom GSM-jamming og falske basestasjoner.

3.10 Har Russland evnen innen EK som de påstår

Mange kommentatorer er enige om Russlands kapasiteter og evner innen moderne EK. Det er ikke kapasiteten i seg selv som er viktig. Det er derimot evnen til å utnytte kapasiteten i en faktisk operasjon som avgjør en evne. Evnen kan oppnås når kapasiteten klarer å gjennomføre oppdrag sammen med andre styrker i et fellesoperativt scenario (Clark, 2021). Noe av problemet med forskning på EK er at kapasitetens faktiske evner er skjermingsverdig informasjon og det blir derfor åpent registrerte data som blir grunnlaget for en vurdering. Hva russiske systemer evner å prosessere internt er vanskelig å kommentere uten tilgang til systemets indre, men målte parametere og registrerte egenskaper gjennom deres bruk av systemene gir et godt grunnlag for hva som kan ventes. Derimot er det usikkert hvor mange «ekstra-nummer» slike systemer kan produsere utover tidligere registrerte evner.

Russland har gjennomført mange EK-operasjoner i både Ukraina og Syria. Der har de med sitt EK-materiell tilpasset innsatsen etter behov i stridsoppgavene. I østlige Ukraina har de i flere år gjennomført EK-operasjoner mot både sivilbefolkningen, og de militære, gjennom bruk av mobile kommandovogner og droner. En effektiv metode russiske styrker har benyttet er angrep mot GSM-nettverk og målrettet påvirkningsoperasjoner mot soldater og sivile etter å ha hacket deres telefoner og deretter sendt meldinger med rettet innhold (Collins, 2018; DFRLab, 2017). Derimot har det etter angrepet på Ukraina i februar 2022 ikke vært samme intensitet i bruk av disse systemene. Det kan være flere grunner til dette. En av grunnene kan være at russiske styrker ikke har gjennomført fullskala operasjoner i flere dimensjoner og derfor slitt med effektuering av oppdrag for flere styrker samtidig, i samme område. Det er i tillegg ikke alle systemer som egner seg like godt for stadig fremrykking med taktiske avdelinger samtidig som systemene skal yte støtte

I en artikkel fra 2017 gjengir Keir Giles et sitat der Andrew Monaghan tar for seg russisk EK og vestens syn på dette:

> *While some Western military observers are painting a picture of a "2030 future" in which Russia has developed a "new generation" warfare, one in which Russian ground forces would rely on massive salvoes of precision rocket and artillery fire, targeted by UAVs and cyber and electronic warfare capabilities designed to blind NATO, we do not have to look as far ahead as 2030 to see precisely that capacity taking shape. This emphasizes the point that the Western understanding of the evolution of Russian military, already playing catch-up in the wake of Russia's annexation of Crimea, should not fall behind either (let alone both) of the twin Russian curves of re-equipment and lesson learning (Giles, 2017, s. 5-6)*

Det ble i mange år satset på EK i vesten, men mye av satsingen ble fokusert mot hva vestens soldater hadde behov for i krigene i Afghanistan, Irak og Syria. Det var i disse krigsområdene få, til ingen, EK-systemer med kapasitetene som Russland utviklet i samme periode for sine fremtidige scenarioer. Russland fokuserte sin utvikling på hva de hadde registrert av amerikanske erfaringer under krigene på 90-tallet samt hvilke styrker og svakheter de fokuserte på i dagens stridssituasjoner. USA og vesten satset på nettverksbaserte K2-systemer og høyteknologiske løsninger med store krav til kommunikasjon

underveis i operasjonene. Disse nye K2-løsningene baserte seg på direkte-linker og satellittkommunikasjon. Russland så det som mer lønnsomt å angripe vestens høyteknologiske kommunikasjon enn å ta opp kampen om kvantitet (Giles, 2017). USA så russisk utvikling av systemer for jamming av deres satellittkommunikasjon sammen med GNSS som en trussel mot amerikansk krigføring. Ikke minst så USA en reell trussel dersom Russland delte sin nyutvikling med andre stater som kunne ønske USA vondt (Clapper, 2016). USA har utvilsomt verdens mest kapable militæravdelinger med evner innen alle typer krigføring. Likevel er de helt avhengig av god kommunikasjon for koordinering av alle sine styrker i kompliserte krigføringsområder for å unngå angrep på egne styrker. Det er denne kommunikasjonen Russland ønsker å påvirke. Gjennom en slik K2D sørger de for å senke amerikanske styrkers evne til hurtighet og automatikk i styringen.

Ukraina sine forsvarskapasiteter var i 2014 ikke noen utfordring for russisk EK. Systemene var gamle og russiske systemer var nye. Russiske styrker jammet lett ut sambandssystemer hos det ukrainske forsvaret. Trolig var NATO publikummet Russland var ute etter å «underholde» med sine nye systemer og kapasiteter. Russiske styrker jammet også flere av OSSE sine droner som opererte i samme område i Ukraina (McLeary, 2015). OSSEs hendelsesrapporter ble naturligvis videreført til NATO, og Russlands evner innen EK ble satt på dagsorden. I 2020 satt den statsvennlige nettavisen politexpert.net (Nikiforov, 2020) opp en liste med de tre viktigste teknologiene som Russland hadde utviklet: 1) stille og moderne ubåter, 2) hypersoniske missiler og 3) effektiv elektronisk krigføringskapasitet. Det er ikke tvil om at russisk EK har tatt store steg i forhold til NATO sine medlemsland. Det er mange NATO-land som har god forskning og utvikling innen EK, men Russland har kapitalisert og produsert forskningen til faktisk operativt materiell. Deres utstyr er i bruk og viser at de er effektive i strid per tid. Som General Raymond Thomas sa om russisk EK i Syria: "*everyday Russia is knocking our communications down*" (Smith, 2020, s. 5).

Russland har mange forskjellige EK-systemer tilgjengelig for bruk til forskjellige situasjoner. Noen er spesialisert mot GSM, GNSS, Satellitt-kommunikasjon, RF-samband og andre mot radarer og linksystemer. Sistnevnte er noe som gjør seg gjeldende i forhold til NATOs overvåkingsfly og ubemannede droner. Russland påstår i media at de har en evne til jamming av slike systemer, men det er lite rapportering fra NATO i åpne kilder som tilsier at dette stemmer. Russland er derimot svært åpne om sitt utstyrs egenskaper i slike miljø. De har spesifikt lagd et system, Divnomorye-U, spesielt for høy-effekts jamming av luftbårne kommandoplattformer fra NATOs medlemmer (McDermott, 2021b). Systemet er satt opp med automatisk K2 og kunstig intelligens for hurtig å kunne tilpasse nødvendig jammekonfigurasjon mot innkommende luftbårne sensorplattformer.

I Syria har russisk EK vært en sikkerhet for egne styrker. De har gjennomført samme type EK-operasjoner som i Ukraina, men har i tillegg gjennomført mer sambandsjamming på et høyere, og mer synlig, nivå. Synligheten har primært vært på grunn av Russlands avgjørende rolle for EK i Syria. De

har derimot ikke sendt kapasitetene i større formasjoner mot frontlinjen for støtte i operasjonene. De har heller blitt satt til baseforsvar og trygging av egne områder (McDermott, 2017, s. 21). EK-styrkene har vært et viktig A2/AD-bidrag (anti access/area denial). I motsetning til i Øst-Ukraina der de russiske styrkene hadde testet ut og «felt-sertifisert» sine systemer ble engasjementet i Syria mer en operasjon der de skulle yte EK-støtte til egne operasjoner og baser mer enn et utstillingsvindu for russisk EK til verden (McDermott, 2017, s. 21). Det var flere situasjoner der russisk EK bidro til egne styrkers sikkerhet. Det er utvilsomt at de russiske styrkene har kapasiteter som overgår mange av deres motstandere. De har brukt mye ressurser i oppbyggingen av slike systemer og utnytter alle situasjonene der de kan få trening og praksis for sine styrker. De roterer styrkene mellom trening hjemme og operasjoner i Ukraina og Syria. Dette gir EK-styrkene god praksis og trening med ekte systemer og faktiske oppdrag med risiko for materiell og personell. Dette gir Russland et godt rutinert strids-personell. Problemet for disse soldatene er derimot at de er i områder med lite direkte motstand. I Ukraina har det vært operasjoner i Donbass-regionen med grenseområder og begrensede trefninger, mens i Syria har EK-styrkene primært blitt brukt i baseforsvar og mindre utsatte posisjoner. I begge stridsområder har Russland vist frem sine evner innen EK. De har rammet OSSE sitt drone-arbeid i Ukraina og de har i operasjoner i Syria jammet Israelsk luftrom (Gross, 2019).

Til tross for at russiske EK-operasjoner har vist at de er flinke innen områdene de viser frem så er det vanskelig å si at de lykkes som de ønsker. Poenget med en EK-operasjon er ikke å vise frem hva de kan klare, men å målrettet degradere motstanderens evne til fritt å benytte egne systemer. Optimalt sett skal ikke motstanderen forstå hvorfor ens systemer ikke fungerer. Det er hevet over enhver tvil at Russland har bygd opp et fungerende og kompetent EK-system. Derimot er det usikkert hvordan de vil fungere i et mer dynamisk miljø med totalstyrkene i alle dimensjoner. Russland har ikke mye erfaring med slike store kampanjer, men heller små begrensede operasjoner uten veldig mange involverte avdelinger.

3.11 Oppsummering

Russland har helt siden 90-tallet bygd opp sin evne innen elektronisk krigføring. De fokuserte på hvilke kapasiteter USA viste frem og brukte deretter disse som rettesnor for hvor de selv trengte å gå. Etter krigen i Georgia i 2008 startet arbeidet med å omorganisere forsvaret og opprettelsen av EK-brigader i alle militærdistrikter. Det blir også opprettet egne EK-avdelinger i marinen og luftforsvaret. En av oppgavene som russiske forsvaret har er å gjennomføre hybride angrep. Dette er EK-styrkene en del av. De skal være bidragsyter til fordekte operasjoner og påvirke motstanderen både direkte på militæravdelinger, men også påvirke sivile personer i nærheten til motstanderens militære styrker. EK er en del av styrken som Russland vil benytte i en «initial phase of the war» gjennom påvirkning av

motstanderens systemer og informasjonskrigføring. Noen av de mest brukte påvirknigene er påvirkning av GNSS, mobilnettverk og K2. Innen påvirkning av K2 er det K2D som er målet for Russland. Målet er å redusere motstanderens K2 så mye at de ikke evner å gjennomføre sine planlagte operasjoner. Disse påvirkningsoperasjonene skal sørge for at sivile og militære mister tiltroen til egne systemer og styresmakter. Elektronisk krigføring som kapasitet er en billig innsats i forhold til å sende inn stridende enheter. EK evner å stå på avstand og blokkere motstanderens innsatser og dermed en billigere innsats med færre tap av personell og materiell.

Russland har en helt klar holdning til hva de har som målsetning og hvordan de skal ramme motstanderen gjennom å lamme K2 og infiltrere deres kommandonett gjennom hacking. Det er derimot stor usikkerhet hos USA og NATO om dette faktisk er noe de evner. Russland og NATO har ikke vært i direkte strid og det er derfor russisk propaganda som påstår at de har gjennomført slike operasjoner allerede. Dette er selvsagt avkreftet av NATO og USA. I tillegg til russiske operasjoner i Ukraina og Syria er det mange eksempler på deres bruk av A2/AD inne i Russland. Der benytter de slike GNSS-bobler for å beskytte president Putin, på reiser inne i Russland.

En av de store forskjellene mellom EK-innsatsen i Ukraina og Syria er stillingskrigen i Ukraina der Russland har prøvd å skjule sin egen innsats mens de i Syria har vært godt synlige i sin utførelse. Likheten ligger i at det begge steder har vært lite dynamisk krigføring med større forflytninger.

4 Analyse

4.1 Russisk påvirkning av GSM/Mobilnett

Russland har i stillingskrigen i Ukraina hatt tid på seg til å teste ut og forbedre sine operasjoner mot ukrainske sivile og militære. Ved å studere russiske operasjoner i Ukraina er det mulig å se hvordan en slik kapasitet kan utnyttes i et hybrid angrep på andre nasjoner. Russland har evnen til å utplassere falske basestasjoner for overtakelse eller påvirkning av GSM-nett, i ønskede områder. En slik basestasjon vil ikke nødvendigvis bli benyttet for å angripe eller trakassere personer, men kan gjerne benyttes for å bygge nettverksoversikt over hvem som snakker med hvem. Dersom de i tillegg kan få ut tale og datatrafikken i nettverket vil det gi ekstra mye. Et område av høy verdi for russiske avdelinger å benytte slike kapasiteter kan være i områder rundt et annet lands nasjonalforsamling. Gjennom å avlytte telenettverket i slike plasser vil de kunne få stor påvirkning på beslutningstakere hos motstanderen. Slik tilgang kan benyttes for uthenting av viktig informasjon. Andre steder av interesse for slike basestasjoner vil være i nærheten av militære hovedkvarter eller baser. På den måten kan de lage seg «targeting lister» for hvem de skal påvirke i en tilspisset situasjon. Ved å samle inn informasjonen om hvilke telefoner som tilhører de øverste ledere så kan kunnskapen utnyttes for følging av de samme menneskene gjennom andre deler av samfunnet elektronisk. I grenseområder vil det også være mulig for Russland å skru opp effekten på sine egne kontrollerte telenettverk og overdøve sendere i nabolandet for deretter å få mobiltelefoner og andre GSM-enheter til å koble seg mot deres. En slik metode vil kunne gi samme evne for påvirkning som en falsk basestasjon.

Påvirkning av en motstanders GSM-nett og muligheten for masseutsendelse av meldinger og sette opp samtaler gir russerne en evne til påvirkning av andre nasjoners innbyggere. GSM-nettet kan dermed utnyttes for å bedrive propaganda gjennom meldinger med løgner og undergravende budskap. Et av systemene russiske styrker har benyttet for slike GSM-operasjoner er et system som heter Leer-3. Systemet består av en mobil EK kommandosentral som gjennom sin antennepark og tre droner kan gjennomføre operasjoner over større områder. Dronene er av typen Orlan-10 som også benyttes innen flere andre operasjoner i det russiske forsvaret (McDermott, 2017; Thomas, 2020b). Gjennom påvirkning av en så viktig ressurs som GSM er for sivilbefolkningen, og soldater, vil det være svært krevende for personell som mottar meldinger eller oppringinger fra nummer de kjenner, å adressere disse som falske. Meldinger sendt fra «kjente» nummer kan spille på følelsene hos mottaker. Slike meldinger kan gjøres i en personlig stil eller det kan sendes som «opplysningsmeldinger» fra en teleleverandør. I desember 2015 angrep Russland en ukrainsk kraftleverandør og sendte deretter ut en falsk melding fra leverandøren til kundene om at de holdt på med reparasjoner og at de ikke ønsket telefoner med feilmeldinger til sentralbordet. Resultatet ble et lengre brudd i energileveransen og en mistro til offisielle meldinger hos befolkningen (Giles, 2016a, s. 72). Russiske EK-styrker er med sitt utstyr også

en viktig rolle i Russlands IW-operasjoner i området i øst-Ukraina. EK-styrkene har sendt sms-er til ukrainske soldater der de skriver: *«Soldier of Ukrainian Army – Better stay alive than becoming dead here»* (McCrory, 2021) og *«Leave and you will live»* (DFRLab, 2017; Smith, 2020). Slike operasjoner mot motstanderens soldater i felt eller mot deres familier kan være med på å demotivere soldatene og sørge for mindre støtte i befolkningen på hjemmebane (Collins, 2018). Dette fungerer som en moderne form av flyveblader. Meldingene vil likevel være mer effektive da de treffer menneskene på et viktig kommunikasjonsmiddel i bukselommen heller enn en lapp på bakken.

Gjennom å benytte seg av falske basestasjoner og droner for økt dekning vil det tilsi at mange av de sivile i områdene av stridighetene blir innlemmet i en slik EK-operasjon. Slike kapasiteter gir russiske styrker en mulighet til å utnytte mobiltelefoner som et moderne flyveblad og dytte ut propaganda til menneskene i område de ønsker å påvirke. Slike meldinger trenger ikke være aggressive eller kontroversielle, men de kan spille på frykten hos befolkningen og spille dette inn som meldinger fra folkets egne myndigheter. Dette er også noe russiske spesialsoldater kan gjennomføre i norske områder. Dersom de innsettes gjennom sivile russiske fartøyer og deretter setter opp falske basestasjoner for overvåking og undergraving. Det vil være nyttig for Russland å plassere ut falske basestasjoner i diverse områder i Norge for å kunne kartlegge brukere og kommunikasjonsrelasjoner.

4.2 Russiske erfaringer med påvirkning av GNSS

Russland har mange erfaringer innen bruk av GNSS-påvirkningsoperasjoner. Slike operasjoner har flere bruksområder for russiske styrker og er med på å sørge for trygghetsfølelse hos russiske ledere. Dette gjøres gjennom oppsetting av A2/AD-bobler i områder der lederne befinner seg (C4ADS, 2019). Det at russiske EK-styrker iverksetter slike GNSS jammebobler kan være effektivt mot droner, men mot missiler vil det være lite effekt. De fleste seriøse cruise-missiler har treghetsnavigator samt en form for søkehode som finner korrekt mål. Derimot vil en slik boble si noe til allmennheten om hva Russland er villige til å utsette lokal for gjennom å fjerne GPS for deres del.

Signalforstyrrelsen, av de tidligere nevnte dronene til OSSE, er god trening for russerne til å overta kontroll over dronene og eventuelt infiltrere dronenes K2 system. Russland har i Ukraina frem til angrepet i 2022 vært overlegen ukrainske styrker innen EK, men derimot kan det se ut til at noe har sviktet i planleggingen ved invasjonen av Ukraina. Russiske styrker ser ut til å mangle evnen til å få EK-systemene frem i riktig posisjon. Eller så kan mangelen på EK i stridsområdene være frykt for å jamme egne styrker i samme operasjon (Pomerleau, 2022). Hva det faktiske problemet har vært for russisk EK i krigen mot Ukraina i 2022 er vanskelig å si, men basert på vestlige medier med direkterapportering fra fronten ser det ut til at evnen, Russland tilsynelatende har, innen EK ikke blir utnyttet. Det vil være utfordrende for EK-styrkene i en stridssituasjon der de mangler luftherredømme eller kontroll over stridslandskapet. Ikke alle EK-enhetene er lagd for å være til stede i en dynamisk

situasjon med stadig flytting av interesseområde og ildgiving fra begge sider. Kapasitetene har evnen til å yte støtte, men den hurtig endrede situasjonen og svært dynamiske fremrykninger kan gjøre det vanskelig å utnytte potensialet i EK-kapasitetene .

Russiske styrkers evner innen jamming eller spoofing av GNSS vil absolutt være en kapasitet som kan ramme norske interesser og sikkerhet. En GPS-jammer vil kunne sette ut av spill en del systemer og trafikkavvikling innen luft- og skipsfart, men en slik jamming av signalet vil raskt bli oppdaget og varslet videre. En spoofing av slike posisjoneringssignaler vil derimot kunne sørge for mer skade gjennom utvidet bruk av autopiloter på både fly og fartøy. Slike signalforstyrrelser emittert i et flaskehals-område på sjøen eller ved innflyvinger til flyplasser vil kunne være svært skadelig. Dette vil gjelde både for GNSS innen posisjonssikkerhet og mobilnettverk for varsling og koordinering.

4.3 Russisk desorganisering av Kommando og kontroll

Da Russland i 2014 annekterte Krim utnyttet de EK til å avskjære ukrainske styrker fra K2, med Kyiv. Dette var effektivt og sørget for en tåkelegging av det faktiske situasjonsbildet for militærkommandoen i Kyiv (Osflaten, 2021, s. 122). Da angrepet på Ukraina startet ble det rapportert om jamming av samband i deler av operasjonen, men det kom ikke frem av rapporteringen om deres egne systemer også ble jammet. Med tanke på Russlands overordnede strategi om å hindre motstanderens K2 er det vanskelig å se for seg at den manglende offensive bruken av EK skyldes at de også rammer egen K2. Samtidig som russiske operasjonslederne skal sørge for et koordinert angrep så deler Ukrainske styrker seg i mindre enheter. Russland har satset mye på evnen til å degradere motstanderes sambandssystemer heller enn å utmanøvrere motstanderen i mengde soldater og materiell (Assymmetric Warfare Group, 2016). Jamming og spoofing av en motstanders militære enheter vil derfor være en viktig evne for å oppnå et fortrinn. Degraderingen av sambandet skaper usikkerhet og svekker deres tiltro til egne systemer. For å bøte på dette har deler av det ukrainske forsvaret har også blitt tilført sambandsutstyr fra vestlige land, som ikke nødvendigvis er like enkle å detektere, for russiske systemer. Likevel benytter mange soldater mobiltelefoner, og russisk EK utnytter deteksjon av ukrainske soldaters bruk av telefoner for krigstiltak. Etter angrepet på Ukraina er disse telefonene blandet inn med alle sivile telefoner i samme område. Det er derfor vanskelig å diskriminere militære fra sivile (Eversden & Gill, 2022).

Planen til russisk elektronisk krigføring er å ramme motstanderens evne til kommando og kontroll. Det er viktig å lamme beslutningsprosessen og dermed være overlegen i situasjonsforståelse og utmanøvrere motstanderen. Dette er akkurat den samme målsetningen som motstanderen har og disse styrkene står derfor mot hverandre med mye av de samme midlene. Oppgaven til EK er derfor å først ute med sine midler for å sette motstanderen ut av spill. Detter er noe russiske styrker har trent på, men i deres operasjonsmiljø har de vært i en statisk stillingskrig i Ukraina og primært som baseforsvar i Syria. Det

vil derfor være utfordrende for disse styrkene å endre sine operasjonsprosedyrer til et mer dynamisk stridsmiljø.

Gjennom flere artikler og utgivelser har vestlige offiserer uttalt seg om hvor høy kvalitet det er på russisk EK i motsetning til vestens. GenLt Ben Hodges, sjef for US Armys tropper i Europa, uttalte i et intervju med en journalist fra Foreign Policy at russisk EK, i Ukraina, var «*eye-watering*» (McLeary, 2015). Russland har de siste tiårene oppgradert sitt EK-materiell og tilført kapasiteter som utfyller hverandre i stridsområder, fra taktisk til strategisk nivå. Perioden etter angrepet på Krim i 2014 har Russland vist sin evne til å forme stridsmiljøet gjennom bruk av EK-systemer. Russland har gjort inntrykk på amerikanske styrker i Syria. Som Keller skriver i sin artikkel har erfaringer fra russisk jamming av amerikanske overvåkingsfly og desorganisering av deres K2, så har den amerikanske Kongressen satt utnyttelse av EMS på dagsordenen (Keller, 2019)

Det har vært mindre fokus på tradisjonell EK (radar og radio) og mer opp mot signaltyper som GSM/mobilnett, GNSS og kommunikasjon-/link-samband (K2). Gjennom EK-operasjoner innen GSM, som nevnt i kapittel 3.4, klarer de å innføre usikkerhet blant befolkningen i stridsområdene samtidig som de evner å gjennomføre operasjoner mot ukrainske forsvarstillinger. De fleste i vesten som kommenterer på russisk EK er enige om at deres satsning innen nye kapasiteter har gitt dem et godt forsprang på sine motstandere. Selv om erfaringer hos amerikanske styrker i Syria viser at de blir jammet av russiske EK-systemer (Varfolomeeva, 2018) så er fortsatt amerikanske styrker operative. De blir ikke satt mer ut av spill enn at de må benytte alternative metoder for kommunikasjon. Selv om russiske styrker setter inn alle sine evner til å jamme amerikanske og NATOs styrker så er disse så erfarne innen store fellesoperasjoner at de fortsatt evner å gjennomføre sine oppdrag. Bare med mindre oppløselighet innen billedbygging og tregere K2 enn ved normaldrift. NATO skal følge godt med på hva russisk utvikling er innen nye EK-kapasiteter, for å finne alternativer til å omgå deres midler. Som Thomas skriver i sin rapport fra 2019:

> Russia's disorganization effort aims to disrupt/jam adversary C2 links, whether by soft (REB, cyber, etc.) or hard (physical destruction) means. The concept has been under discussion since at least the early 1990s. Disorganizing an opponent's C2 can collapse his ability to coordinate and integrate nearly every aspect of his plans, whether it be logistic support, the use of fire support means, or his command over troops in the field (Thomas, 2019, s. 64)

Denne planen fra Russland om å lamme motstanderen gjennom å fjerne deres K2 er vist gjennom deres operasjoner i både Ukraina og i Syria. Derimot er det ikke vist at EK har klart å videreføre denne evnen når operasjonsmiljøet gikk fra en statisk situasjon som i Donbass og Krim til å bli en dynamisk innsats i angrepet på Ukraina i sin helhet (Eversden & Gill, 2022). Russland ser ut til å ha manglet evnen på høyere nivå til å samordne alle styrkens komponenter til samhandling, og heller fokusere på enkeltdeler av operasjonen. Årsaken til at det blir rapportert lite bruk av elektronisk krigføringsstyrker i fremrykningen i Ukraina kan også skyldes redselen for å ramme egne systemer. Ikke minst har ukrainske

styrker omgått en del av eventuell jamming gjennom mottak av enheter for bruk av selskapet Space-X` satellittbaserte internett Starlink (Outlook web desk, 2022). Det er med andre ord ikke nødvendigvis Russland som ikke jammer. Det kan være Ukraina som unngår å bli jammet. Russland benytter fortsatt mye eldre utstyr og det er samme type teknologi som Ukraina benytter i mange av sine avdelinger. Dette kan være en forklaring på manglende jamming av diverse kapasiteter.

Til tross for rapportering i vestlige medier om hvor gode Russland har blitt innen EK og hvilke evner de har til å svekke vestlige styrkers operasjonsfrihet, så er det ikke like sikkert hos en del russiske skribenter. Clark (2021) beskriver i sin bok russiske militæranalytikere og hvordan de ser problemer med å hevde evnen til K2D-operasjoner i fremtiden. Dette begrunner de med at det ikke er grunnlag for å nedkjempe fiendens K2 gjennom å ha en konkret operasjonsavdeling for dette med dedikert utstyr. Det er behov for et gjennomgående fokus på dette i hele styrken (Clark, 2021, s. 23-24). Det er nok ikke tvil om at det er stor forskjell på det som presenteres i media, som et strategisk bilde på hva ledelsen ønsker skal være situasjonen, og hva den reelle situasjonen er for de på bakken. Russland har bevist i flere situasjoner i både Syria og Ukraina at de evner å sette motstanderens utstyr ut av spill, jamme K2-linker og ødelegge situasjonsbilde. Likevel må det huskes at dette har vært statiske kriger over små avstander og begrenset med motstand. En viktig ting Russland mangler er erfaring innen store operasjoner mot en fiende med store teknologiske ressurser.

4.4 Russiske erfaringer med disponering av EK

Erfaringer fra russiske operasjoner i Syria viser at EK ikke er disponert i fremste rekke i operasjonsområdene, men heller utplassert i leire for styrkebeskyttelse og baseforsvar. Dmitry Adamsky beskriver i sin artikkel om Russlands innsats i Syria at lederskapet i russisk forsvar er skyld i store deler av mangelen på effektiv bruk av styrker i større operasjoner: «*There is an inherent tension between the notion of operational creativity, which implies a certain delegation of authority, and the concept of the integral strategist, which epitomises centralisation*» (Adamsky, 2020). Det byr på problemer når de militære lederne ikke forstår godt nok kompleksiteten i militæroperasjoner med så mange forskjellige styrker og kapasiteter som det russiske angrepsforsvaret består av. Som sitatet sier så er det en dragkamp mellom sjefens operasjonelle kreativitet for bruk av styrkenes egenskaper og forventningen av sentralisert ledelse som ikke ønsker delegert ledelse nedover i rekkene. Det er ikke meningen å si at russiske generaler og offiserer ikke er dyktige på krigføring, men de er oppfostret i et forsvar der alle øvelser er scriptet og operasjoner er styrt fra sentralt hold. Det er en tradisjon for at alle venter på øverste sjefs ordre om iverksettelse (Adamsky, 2020). Det er lite rom til å trene sjefers operasjonskunst (Forsvaret, 2019a, s. 243).

Etter angrepet på Ukraina i februar 2022 er det mulig å trekke slutningen om at russiske ledere ikke var forberedt godt nok på kompleksiteten med en så stor operasjon og alle de bevegelige delene i en

angrepsstyrke av den størrelsen (Beale, 2022). Russiske generaler har trent på mange operasjoner gjennom øvelser på hjemmebane, men reelle stridsoperasjoner i et annet land med store styrker har det vært få av. Kompleksiteten blir så stor at ved frafall av enkelt-strukturer så blir alt annet også stående i bero. Det vil ikke være enkelt for det russiske forsvaret å endre en slik struktur der det er innebygd en sterk detaljstyring fra toppen og ned. Å kritisere Russlands manglende bruk av EK i fremste linje under angrepet på Ukraina vil være et feilskjær. Det kan være flere rasjonale for dette. Det vil ikke gagne russiske styrker dersom de lammer sitt eget samband gjennom jamming av motstanderens, eller at de må binde opp fremrykkende styrker for nærforsvar av disse EK-enhetene. Vestlige styrker kan se på russisk bruk av EK i Ukraina, mellom 2014 og 2022, som effektivt og godt. Der var situasjonen stabil og russiske EK-styrker rullerte mellom hjemmebase, utstasjonering i stridsoppdrag i Ukraina og stridsoppdrag i Syria. Angrepet på Ukraina i 2022 har ikke gått etter planen til den russiske ledelsen. EK-styrkene, som frem til angrepet hadde ødelagt for motstanderens samband, ble ikke observert i særlig bruk i de fremrykkende styrkene på fronten. Jeg ser for meg tre mulige scenarioer i denne situasjonen: a) de russiske EK-styrkene opererer riktig og forstyrrer spesifikke radio-sett/-nett og ikke hele spektrum, men ukrainske styrker ikke ønsker å innrømme svakhet og rapporterer derfor ikke om manglende samband, b) russiske EK-styrker evner ikke «ild-og-bevegelse» og yter derfor ikke sin rolle i en fremskutt stilling og blir av den grunn holdt tilbake fra fronten og opprettholder EK-evnen i bakre linjer, eller c) russiske sjefer ble jammet ned av eget og ukrainsk EK og trakk derfor sine EK-styrker tilbake for å kunne opprettholde K2 på egne styrker. Uavhengig av hvorfor det meldes om manglende russisk EK i fremrykkingen i Ukraina så er personellet i EK-avdelingene godt trent i stridsoperasjoner og kyndig på elektronisk krigføring i forskjellige miljø. Et tettpakket EMS-miljø med jamming og påvirkning vil være i forsvarende styrkes favør. Den angripende part må organisere og koordinere sine grupper, mens den forsvarende som sitter i sine forhåndsbygde forsvarsverk kan skyte på det som rører seg i teig.

Russiske ledere er frempå og krever anerkjennelse på egne EK-styrkers vegne. Gjennom bruk av samme systemer i både Ukraina og Syria sikrer det russiske forsvaret en erfaringsdatabase på hva som fungerer og ikke fungerer i de forskjellige stridsområdene. Disse erfaringene er basert på forskjellige stridsmiljøer, motstandere, motstanders materiell og taktikker.

Russland har gjennom sine operasjoner i Ukraina og Syria skaffet seg en effektiv læringsarena for sine militære styrker. Operasjonsmiljøene er forskjellige, men det er bare med på å gi soldatene et bredere erfaringsgrunnlag for gjennomføring av operasjoner i nye miljøer på senere tidspunkt.

4.5 Hva er russisk EKs målsetting

Sjefen for Russlands styrker innen elektronisk krigføring, Generalmajor Yuriy Lastochkin, sa i et intervju: «***The disorganization of enemy troop and weapons command and control*** *and the reduction of the effectiveness of the conduct of reconnaissance and weapons employment by them* ***is the primary***

goal of the conduct of electronic warfare» (Thomas, 2020b, s. 10). Basert på Generalmajor Lastochkins utsagn vil det kunne sies at det første som kan ventes ved et angrep er EK-innsats mot motstanderens K2. Russiske styrker har i sine oppdrag i Syria fokusert motstanden mot væpnede grupper. De har gjennom område-jamming mot en gruppeleders oppholdsområde, eller gjennom punktangrep mot lederens kommunikasjonsenheter, demoralisert og forvirret gruppene så mye at de ikke har evnet å gjennomføre sine aksjoner mot russiske styrker (Thomas, 2019, s. 6-2, 6-3). En slik bruk av K2D sørget for at gruppene falt fra hverandre da de mistet evnen til kommando og kontroll. Thomas tar i sin artikkel for seg russiske artikler som omhandler emnet K2D. Disse viser til viktigheten av å kunne påføre motstanderen en desorganisering av deres kommando og kontroll. Som de russiske artiklene sier er det ikke nødvendigvis en total krasj i motstanderens system som er målet. Det at motstanderen får tidsforsinkelser og usikkerhet i korrektheten i det som kommer inn gjør nok til at deres omsetningstid øker så mye at de henger etter en motstanders handlinger (Thomas, 2019, s. 6-4).

Et suksesskriterium for styrker i strid er fungerende kommando og kontroll. Dette vil i mange tilfeller kreve kommunikasjon over avstander. Russland ser derfor ut til å ha en større plan enn bare å være til bry for NATO gjennom sine krigføringsprogrammer. Gjennom satsing på EK for jamming av kommunikasjonssatellitter, eller i verste fall å skyte dem ned med missil, vil Russland kunne hindre USA og NATOs K2 gjennom satellittkommunikasjon. USA er NATOs absolutt viktigste medlem og er de som vil måtte støtte Europa med styrker i tilfelle krig i NATO øst. Det vil være av kritisk viktighet at det er god kommunikasjonslinje mellom Europa og USA for en felles situasjonsforståelse og koordinering. Dersom Russland blokkerer kommunikasjonssatellitter vil det neste steget for Russland være å kutte de transatlantiske kommunikasjonskablene på havbunnen, gjennom sine spesialubåter. Som NATOs tidligere militærsjef, Admiral Stavridis, sa «*We've allowed this vital infrastructure to grow increasingly vulnerable and this should worry us all*» (Beale, 2017). EK er ikke et middel for å skade de transatlantiske internettkablene, men EK vil være den gjenværende faktoren for effektivt å hindre NATOs K2 mellom USA og Europa.

> *"Future wars will be launched by electronic warfare (EW) forces, which will protect friendly forces, block foreign propaganda disinformation, and strike at enemy EW forces and assets, blending with strategic and aerospace operations, with the latter augmented by cruise missiles and reconnaissance assets (UAVs, robots) delivering strikes and fires" (Giles, 2016a, s. 69)*

Russiske styrker har gjennom stridigheter i både Ukraina og Syria bevist at de effektivt kan gjennomføre operasjoner innen jamming av flere typer signaler. Det er derimot ikke like sikkert at effektiviteten til alle deres systemer er på linje med russiske myndigheters propagandabilde. Russland ønsker å fremstå som ledende innen forsvarsteknologi. Krigføringen i Syria må derfor kunne ses også med PR-briller. Russiske styrker leverer langtrekkende presisjonsild (LPI), flyangrep i store mengder og skryter av deres egenskaper innen sikring av styrker med sine EK-system. I Syria må det være mulig å se kampene som et stort salgsskilt, mens det i Ukraina har vært testing og utvikling av konsepter og utstyr. Like viktig

som sitt bidrag innen nye LPI-våpen så er evnen til å kunne motvirke USAs og NATOs kapasiteter minst like viktig. Dette kan ses gjennom Russlands bruk av GNSS-jamming/spoofing for villedning av disse NATO-LPI-ene i deres avsluttende flukt.

En av de viktigste oppgavene til russisk EK er noe som kan kalles Kommando og kontroll desorganisering (K2D). Dette er en oppgave russiske EK-styrker har som mål. Påvirke motstanderens kommunikasjon og systemer for kommando og kontroll gjennom jamming, spoofing og desinformasjon. Gjennom sine passive systemer bygger de situasjonsoversikt og et situasjonsbilde for deretter å sende ut falske data til motstanderen for å ødelegge deres bilde (McCrory, 2021). Dette er en taktikk som fungerer veldig godt i en situasjon som i Ukraina. Det er en aktivitet utøveren kan bedrive relativt fordekt og uten bruk av kinetiske våpen. Eneste skade påført er midlertidig nekting av kommunikasjon mellom motstanderens enheter og kommandoledd. Russland har egenskapen for slike operasjoner gjennom bruk av både landenheter og luftenheter i samspill. Russland har utviklet en drone de benytter som sensor og rele for sine operasjoner. Landstasjonen Leer-3 og dens Orlan-10 drone (UAV) kan i samspill dekke et stort område for både innsamling og utsendelse av nødvendige signaler for K2D-operasjoner. Ses situasjonen fra en annen vinkel vil det være klart at et slikt system også selv vil være sårbart for mye av det samme, men ukrainske styrker har så langt ikke vist evnen til å sabotere de russiske styrkenes evner og kapasiteter på samme måte. Russiske styrker har gjennom sine operasjoner i Ukraina vist at de gjennom et godt situasjonsbilde evner de å utnytte egne ressurser til å ramme motstanderens operasjonskanaler. Samtidig bruker de samme kapasiteter til å sette motstanderens «tilsvarende» kapasiteter ut av spill gjennom å nekte dem sannferdige navigasjonsdata gjennom jamming og spoofing av GNSS-systemer. Bare mellom 2015 og 2017 mistet ukrainske styrker rett under 100 droner grunnet jamming og spoofing av dronenes navigasjonssystemer (McCrory, 2021, s. 36). Samtidig som russiske styrker lykkes med sine EK-operasjoner, er det vanskelig å se for seg at de ville hatt et like klart overtak i EMS på samme måte dersom de hadde en mer likeverdig motstander i stridsområdene. Russland har hatt stort fokus på utviklingen, men det er fortsatt bare systemer for å ødelegge signalgangen for motparten. Situasjonen ville vært en helt annen dersom det var to likeverdige parter som kjempet mot hverandre med tilsvarende evner. Problemet blir et helt annet dersom scenarioet blir Russlands EK-kapasiteter og evner satt opp mot NATOs kamp-enheter. Vil et slikt system kunne yte like godt mot et AWACS eller mot en BMD-Destroyer fra USA? Russland har skrytt på seg evnen til å ha en slik kapasitet, men problemet for NATO er i slike situasjoner at Russland benytter seg av hele sitt IW-apparat når de planter disse oppslagene i media. Til tross for at NATOs egne styrker benekter slike resultater har Russland satt i gang et slikt apparat av løgner/falske sannheter at media tar «første mann til mølla» historier, da dette selger mer enn sannferdige data (Nimmo et al., 2017).

4.6 Oppsummering

En absolutt likhet mellom Ukraina og Syria er det russiske forsvarets fokus på EK-styrkenes kompetanse. Begge stridsmiljøene har blitt brukt som arenaer for opplæring og erfaringsbygging. Russiske EK-styrker har gjennom åtte år i Ukraina og sju år i Syria jevnlig rullert personellet mellom kampområdene og sørget for at de får jevnlig prøvd seg på forskjellige situasjoner. Selv om Ukraina og Syria er forskjellige miljøer og med forskjellige trusler vil det være en styrke for operatørene å få «trene» i realistiske miljøer med relativt lav trussel mot egne styrker. Derimot skiller situasjonene i Syria og Ukraina seg diametralt fra hverandre på andre områder. Metodene utnyttet er sammenlignbare, men derimot få likheter i utførelsen av de fleste operasjonene. Der Syria fungerer som et utstillingsvindu for Russlands kapasiteter og evner, står Ukraina igjen som et operasjonsområde der Russland er ute etter å spille et skyggespill. I Ukraina forsøker Russland å benekte sin faktiske innsats og heller gi separatister midler og æren for motstanden mot den undertrykkende ukrainske staten. Selv om Russland har flere operasjoner i Svartehavsregionen er deres handlinger i østre Ukraina primært basert på å bistå landstyrker som skal motarbeide de ukrainske styrkene i området. Utstyret er i de to kampområdene mye det samme, men utnyttelsen og promoteringen har vært forskjellig. En annen grunn til at russiske EK-styrker og deres innsats blir så belyst er selvsagt at i Syria er USA en part i konflikten. Disse rapporterer åpent om hvilke kapasiteter de ser hos russiske styrker i samme område og bygger dermed oppunder Russlands rykte som en stormakt innen elektronisk krigføring.

> *So ultimately, what Moscow publicly acknowledges in Syria and doesn't acknowledge in Ukraine is a consequence of their different goals in each country. They not only want to negotiate with the west and advertise their arms in Syria, but they also want to be seen as a power player in the Middle East. They want to be a power player in the Baltics too, especially Ukraine. But they only want the right people to know about it (Brown, 2017)*

For russiske styrker er det positivt at USA deltar i Syria. Det gir russiske EK-kapasiteter muligheten til å teste sitt utstyr mot amerikanske stridssystemer og kan måle sin egen ytelse opp mot disse. Amerikanske styrker har rapportert om effektiv jamming av deres systemer og etterlyst bedre resistens imot russiske kapasiteter. Her har også russerne en fordel i at situasjonen er statisk og dermed finne beste tid og situasjon for desorganisering av amerikanske styrker. Det er likevel ikke uten risiko russiske styrker tester ut sine evner. Det kan resultere i respons fra styrker som føler seg truet og dermed medfører skarpe situasjoner. Både Ukraina og Syria fungerer som krigsutdanningsoperasjoner og Russland utnytter situasjonen maksimalt for sine styrker. Russiske styrker målsetting er å lamme beslutningsprosessen til motstanderen gjennom K2D. Ved å hindre motstanderens kommunikasjon og situasjonsforståelse vil det være vanskelig for denne å gjennomføre vellykkede operasjoner. Handlingslammelse er en målsetting og EK er et viktig middel for å nå dette. Skulle alle fastlinjer være brutte mellom sentral og perifer ledelse er det opp til EK-styrkene å motarbeide sambandet på den ene siden og å forsvare det på den andre.

5 Kan Russland utnytte EK mot Norge

5.1 Hva er trusselen mot Norge

Schnelle tar i sin masteroppgave opp problemstillingen vedrørende russisk utnyttelse av hybrid krigføring i Norges kystområder (Schnelle, 2018). Han tar for seg hvordan russiske styrker kan utnytte sivil shipping for innsetting av styrker i strategiske punkter. Det er utvilsomt en viktig ressurs Russland har i alle sine sivile fartøy som seiler langs norskekysten. Det er både handelsfartøy og fiskeri fartøy. Ved hjelp av slike fartøy har Russland muligheten til å frakte med seg nødvendig personell og utstyr for å kunne gjennomføre aksjoner innen EK i Norge. Det har vært en stor økning innen farledsbevis i Norge utstedt til russiske navigatører. Det er ikke nødvendigvis en sikkerhetsrisiko i seg selv at russiske sjømenn har farledsbevis. Om bord er det også annet personell som har bakgrunner vi ikke kjenner til. I sin artikkel beskriver Østensen personellet om bord fartøyene med russiske farledsbevis-kapteiner. Kysten er lang og hverken forsvaret eller politi har mulighet til å kontrollere hva disse fartøyene gjør på hele sin ferd. Disse får fri tilgang til kysten. Problemet er at de kan samle inn etterretninger for bruk på et senere tidspunkt om viktig infrastruktur og områder langs Norges kyst (Østensen, 2020). Trusselen for bruk av kunnskapen er ikke nå, men på midlere og lengre sikt (Ure, 2021, s. 6).

Påvirkning av GNSS er en enkel måte for russiske EK-styrker å kunne gjøre stor skade på norske områder. Skulle de gjennomføre jamming vil det enkelt bli detektert av fartøyer som rapporterer inn manglende posisjonssignal. Dette vil deretter varsles videre og dermed etterforskes av norske myndigheter. Skulle de derimot gjennomføre spoofing av GPS i kystnært farvann eller flaskehalsområder kan de skape farlige situasjoner som det kan være vanskelig for fartøyene å oppdage før det er for sent. Det er ikke sikkert at en navigatør vil få med seg at posisjonen fra GNSS forflytter seg fra deres faktiske posisjon, før en eventuell kollisjon. Slik bruk av GPS-spoofing er ikke nytt. Det er likevel effektivt. Iran har utnyttet samme taktikk for å arrestere fartøyer i Hormuz stredet. De spoofet GPS og arresterte et britisk fartøy, som hevn for britisk aksjon mot et iransk fartøy i Middelhavet, da fartøyet lot seg lure ut av farleden og inn i iransk territorialfarvann (Cozzens, 2019). Påvirkning av GPS langs norskekysten vil ikke gi Russland et fortrinn i Norge i seg selv. Det vil derimot kunne gi Russland en brikke for undergraving av tilliten til sikker navigasjon i Norge. Russland vil kunne benytte slike situasjoner til å hevde at Norge med vilje vanskeliggjør det for russiske fartøy å seile i Norge.

Sivile russiske fartøyer er til kai i Norge jevnlig. Det nødvendige utstyret for slike operasjoner kan pakkes i kofferter med en batteripakke, og fjernstyring kan benyttes for tidvis å bedrive spoofing/jamming. Det vil også være mulig for fartøyer i norsk farvann å bringe med seg utstyr for påvirkning av mobilnettverk og falske basestasjoner. Falske basestasjoner og påvirkning av mobiltelefon-nettverk er noe russiske styrker kan gjennomføre i «klandestine» operasjoner langs norskekysten. Utstyret vil kunne fraktes inn gjennom enkle løsninger og plasseres slik at de når de

ønskede nettverk. I tilfelle en politisk krise mellom Norge og Russland skulle oppstå vil det være i Russlands interesse å påvirke Norge negativt, men under terskelen for en NATO-artikkel 5 hendelse. Russland kan benytte fiskefartøyer eller handelsfartøyer for å frakte utstyr i posisjoner for påvirkning av norske områder. Som Duncan McCrory sier: «*Russian offensive EW tactics are particularly well suited to hybrid warfare, as EW systems can be tuned to deliver subtle and less escalatory non-kinetic effects in a relatively covert manner, such as temporarily denying communications*» (McCrory, 2021, s. 36).

Gjennom å tidvis eller delvis lamme mobilnettverk i norske områder så fjerner de russiske styrkene en av bærebjelkene i norsk kommunikasjon da staten også legger opp til mobilnettverkene som grunnlaget for nødnett i Norge (Prop. 14 S (2020)). Falske basestasjoner kan være vanskelig å oppdage og operasjoner på norsk jord for å forvirre og skape usikkerhet blant befolkningen vil derfor kunne gjøre stor skade på Norge. Et argument mot en påvirkning av mobilnett i Norge kan være at 4G er kryptert, og nesten all mobilnett-trafikk i Norge er 4G. Dersom det oppstår en krisesituasjon i et geografisk område vil alle mobilnett-tilbydere som dekker dette måtte prioritere å slippe gjennom såkalte «prioritetsabonnement» (NKOM, 2021). Slike prioritetsabonnementer er kun for kritisk personell innen helse, sikkerhet og infrastruktur. Ved overbelastede basestasjoner, i krisesituasjoner, vil samtalene i mobilnettet automatisk flyttes fra 4G til 2G, som er et ukryptert nett. Påvirkning av mobilnettet vil dersom en krise oppstår i et område kunne gi flere muligheter for en fiendtlig aktør å øke krisens omfang. Slike operasjoner vil kunne skape en stor påvirkning innen sivil K2 i kriseløsningen. Russland har i sine landavdelinger utstrakt bruk av droner for å utvide sin operasjonsrekkevidde på systemer. Dette benytter de også på fartøyer. De tidligere nevnte Orlan 10-dronene er testet ut på fartøyer og selv korvetter er utstyrt med dronen for passiv EK, stillbilde/video, signal relé og målangivelse (Navy Recognition, 2018). Dette er også materiell som kan utstyres på sivile fartøyer og benyttes for operasjoner langs norskekysten både for passiv og aktiv EK.

Russland vil benytte EK som et asymmetrisk middel for å kontre andre høyteknologiske land skriver Bendett i en forskningsrapport (Bendett et al., 2021). Dette tilsier at Norge vil møte russisk EK som et av midlene Russland kan iverksette for å få overtak i tilfelle krise mellom landene.

5.2 Hva ser vi i dag

Det vil være viktig for en EK-avdeling å kunne ødelegge for en motstanders evne til å bygge bilde for sin situasjonsforståelse. Jamming og spoofing av radarer er en effektiv metode for å sette ned en motstanders evne til hurtige operasjoner og situasjonsforståelse. Gjennom å degradere et sensorsystems evne til å fremstille omgivelsene korrekt gjør at tilliten til systemene minsker.

Hittil i denne oppgaven har det vært snakket mest om Russlands EK-avdelinger på land og deres operasjoner. Russland har også mange av de samme kapasitetene på sine marinefartøyer og ikke minst

har de mulighet til å plassere materiell midlertidig på sivile fartøyer dersom det er behov. I Russlands EK-inventar har de marine-systemer som dekker evnen til påvirkning innen GNSS-jamming/spoofing, påvirkning av radiosamband, radarer, linksystemer eller mobilnett/GSM. I noen tilfeller er det nesten samme utstyr og evner som de benytter på land, men de er tilpasset marinen. I tillegg er det. Det er derimot få rapporteringer om aktiv jamming fra russiske fartøyer til tross for at de innehar evnen. Det er mange rapporteringer om russisk jamming fra land, som rammer norske områder (Regjeringen, 2019), men marinefartøyene ser ut til å holde tilbake jammingen/spoofingen. Det kan hende russiske fartøyer bruker jamming av GNSS og andre former for EK aktivt, men det vil da ofte bli rapportert i sikkerhetsgraderte kanaler og derfor ikke delt videre. Fordelen med slike systemer montert på fartøyer er muligheten for deployering i hele verden. Utstyr montert på en mobil land-plattform fordrer tilgang til landområdene utstyret er tiltenkt brukt, mens fartøys- eller luftenhetsmontert utstyr kan benyttes i alle områder i internasjonalt sjø- og luftterritorium. En slik bruk vil gi mulighet for påvirkning av et kystområde fra en slik «perifer» posisjon. Utstyr montert på fartøyer vil være til nytte for spoofing av GNSS i naturlig flaskehalsområder for å skape usikkerhet og forsinkelser i en forsyningslinje. Likevel vil trusselen for norskekysten være materiell montert om bord sivile fartøy. Disse kan gjennomføre operasjoner i perioder korte nok til at de ikke blir tatt, men skaper nok uro. Det vil da være naturlig at de selv spiller offerrollen og rapporterer problemer på lik linje med andre berørte. Det er stadig rapporteringer om GNSS-jamming i Norge, som ikke stammer fra Russland. I de fleste tilfeller dreier dette seg om kjøretøyer med mål om å jukse med kjørelogger, og har GPS-jammer i bilen for å skjule sine faktiske bevegelser. Falske basestasjoner er enkle å distribuere da de kommer i koffertstørrelse med batteripakke. Dette er en godt kjent trussel mot samfunnet og i et intervju med Dagbladet forteller Tore Lunestad, i NKOM, at de gjennomfører stikkprøver av biler samt kjører rundt for å kontrollere mobilnettsignaler for å avdekke slike (Halvorsen, 2022). Disse forebyggende kontrollene har tiltatt i forbindelse med Russlands angrep på Ukraina og den økte trusselen for etterretning mot Norge.

Samtidig som Russland utgjør en trussel mot Norge innen EK har de samtidig evnen til å gjennomføre skjulte operasjoner mot Norge, under vann. Det er flere russiske fartøyer langs norskekysten til enhver tid. Ståle Ulriksen, ved Sjøkrigsskolen, kaller disse for spionskip i et intervju med Dagens Næringsliv (Kibar, 2021). Det er vanskelig å se på Russlands innsats mot Norge som enten eller. De benytter alle muligheter og bygger et situasjonskart over Norges infrastruktur og sårbarheter. Dette gjennomføres både som fordekte og helt åpenlyse innsamlinger. Russland benytter egne militære forskningsskip eller sivile fartøyer som seiler oppsiktsvekkende sakte gjennom militærøvelser og forbi viktige infrastrukturpunkter langs norskekysten (Forsvarets Forskningsinstitutt, 2019). Skulle en krisesituasjon mellom Norge og Russland oppstå vil norsk infrastruktur være i fare. Russland har kartlagt Norges sårbarheter på kysten og under vann, og de vil utnytte disse sårbarhetene ved behov. Dersom Russland ønsker å gjennomføre en aksjon mot norske interesseaktiviteter så kan det være nyttig å kunne effektuere

en avledningsmanøver gjennom EK-kapasiteter. Dette for å sørge for mindre omtale av deres faktiske operasjon.

Norges kyst er langstrakt, og Russland kan utnytte dette i sin favør på flere måter. I oppbyggingen av en stridssituasjon vil radar-spoofing forvirre en radaroperatør eller et overvåkingssystem gjennom å legge inn flere kontakter enn det som reelt er til stede. Gjennom å påvirke overvåkingsbildet slik at det ikke stemmer med reell posisjonering av kontakter vil de degradere et systems troverdighet og undergrave Norges evne til kontroll av egne områder. Gjennom påvirkning av GNSS og radarer samtidig vil dette kunne medføre store konsekvenser med en relativt liten innsats fra russiske enheter.
Russisk EK langs Norges områder med sivile fartøy vil ikke minst være viktig med tanke på innsamling av signaldata. Passiv EK for å kunne bygge bibliotek over signalmiljøet i Norge vil være av viktighet for å vite hvilke EK-tiltak som må benyttes hvor i tilfelle en situasjon skal oppstå. En slik innsamling av signaldata, kunnskap om områdets EMS-bruk, kan utnyttes som trening for moderne EK-materiell med integrert kunstig intelligens (se kap 6). Informasjonen vil kunne bidra til at russisk automatisert jammesystem vil kunne tilpasse innsatsen i henhold til signalmiljøet basert på erfaringsdata fra tidligere innsamlinger. Ved en eventuell konflikt vil alle Norges sårbarheter bli utnyttet av Russland, og disse sårbarhetene er allerede kjent når situasjonen utvikler seg.

5.3 Hvordan kan vi oppdage russisk hybrid angrep

Russiske styrker har gjennom flere år fått god trening i operasjonsområder med høyintensitets EK-miljø. Norge har gjennom flere år rapportert om forstyrrelser av GNSS, fra Russland, i norske områder som rammer både luftfart og landområder (Nilsen, 2019; Regjeringen, 2019). Slike rapporteringer har ofte kommet i forbindelse med større NATO-øvelser. Russisk bruk av GNSS-jamming kan relateres øvelse i russiske styrker eller for baseforsvar og sikring av viktig infrastruktur på Kola. Norge er NATOs grense til Russland i nord, og Norge er derfor i en utsatt stilling for å bli påvirket av russiske tiltak innen påvirkningsaksjoner. Dette kan gjøres som EK operasjoner, både innen GNSS, GSM eller andre RF-systemer.

> *«EW can also play a role in Russian anti-access/area denial efforts (A2/AD), where EW can be used as a "stand-off weapon" that "can turn areas falling within [its] range into strategically and operationally isolated 'bubbles» (Smith, 2020).*

Gjennom rapportering fra Syria er det kjent at Russland benytter A2/AD-bobler for sikring av egne baser. Dette kan overføres til Kola og hvordan GPS-jamming øker ved tilstedeværelse av amerikanske fartøyer i nord (Regjeringen, 2019). Ved deteksjon av jamming av spesifikke frekvenser, rapporteres disse videre til NATO. Skulle bruk av slike russiske systemer skje et annet sted enn ved grenseområdene

kan det være vanskelig å detektere hva som faktisk blir utført og av hvem. Det er flere måter påvirkninger kan gjennomføres: GSM/mobilnett med falske basestasjoner eller signaljamming, spoofing eller jamming av GNSS, degradering av kystradarer og bildebyggingsenheter, eller forstyrrelser av andre sambandssystemer. Mange systemer vil kunne detektere slike forstyrrelser og melde fra, men det er vanskelig å si noe om hvor lang tid slike operasjoner ville kunne påvirkes før en eventuell operasjon kunne blitt avslørt. En slik type operasjon ville falt inn under Russlands bruk av hybrid krigføring og kunne degradert tiltroen til egne systemer nok til at de kunne gjennomført skjulte aksjoner inn under terskelen av deteksjon. I et slikt hybrid scenario vil det være mulig å utplassere systemer for påvirkning flere steder langs kysten og spesifikt ramme systemer for infrastruktur. Problemet er til slutt hvem som sitter på sentralen for å analysere og finne de anomale tegnene, for deretter å sammenstille bildet og alarmere om et hybrid angrep. Som Forsvarssjefen skrev i sitt fagmilitære råd i 2019:

> *Evnen til å håndtere hybrid krigføring i en konfliktsituasjon er for liten, og det trengs kompetanseheving og bevisstgjøring fra taktisk til strategisk nivå, både i sivil og militær sektor. Håndteringen av enkelthendelser vil først og fremst foregå sektorvis og gjerne på lavere nivå. Hovedutfordringene er derfor å oppdage, forstå og attribuere eventuell hybrid virkemiddelbruk og vurdere sammenhenger og intensjon. Det er et behov for å forbedre evnen til tverrsektoriell situasjonsforståelse, informasjonsflyt og samarbeidsmekanismer. Kommunikasjonsløsninger og liaisonfunksjoner må utvikles videre (Forsvaret, 2019b, s. 83)*

Store deler av kritisk infrastruktur er eid og driftet av sivile selskaper. Det er derfor ikke en instans for oppdagelse og kontroll på eventuelle trusler. I en hybrid operasjon er det bare fantasien som setter grenser for hvordan en usikkerhet kan påføres motstanderen og dermed få fokus vekk fra det en faktisk forsøker å oppnå. Hybride operasjoner er ikke noe som blir funnet på i farten. Hybride operasjoner vil være planlagt hos russiske myndigheter og bestå av innsats over tid. Slike operasjoner kan gjennomføres i lang tid i forveien av en eventuell konflikt. Hybride operasjoner er med på å berede området for innsats dersom striden skulle komme.

Russland har et stort propaganda-apparat som kan mobiliseres for å bygge en ønsket narrativ i media og offentligheten. Denne typen «hybride operasjoner» eller «gråsone operasjoner» viser til bruken av andre midler enn de tradisjonelle konvensjonelle militærstyrkene (Bērziņš, 2020). Konvensjonell krig bruker uniformerte soldater og åpenlyse operasjoner for å vinne terreng, mens denne typen krigføring vil utnytte usikkerheter i samfunnet for å bygge en historie som passer russiske planer og ønsker for videre handlingsrom. Et virkemiddel som passer godt inn i et slikt scenario er elektronisk krigføring. Det er viktig for styrkene å bygge oppunder en slik operasjon gradvis og gjøres troverdig.

Her legges det til grunn at det allerede har vært gjennomført operasjoner for undergraving og påvirkning av det sivile samfunnet hvor operasjonen skal gjennomføres. Dette kan gjøres gjennom påvirkning av media med falske historier eller leserinnlegg som påpeker skjevheter i samfunnet og undertrykkingen av grupper fra styresmaktenes side. EK kan benyttes som en viktig brikke i et slikt scenario så vel som

i stridssituasjoner. Russerne har utnyttet EK i Ukraina på en måte som også kan være vanskelig for vestlige nasjoner. De bruker EK for jamming og spoofing av diverse systemer. Gjennom å jamme sambandssystemer vil styrkene svekke tilliten til myndighetenes evne til å forvalte folkets behov for kommunikasjon. Dette kan være GSM-nettverk for befolkningens private kommunikasjon eller det kan være andre former for privatpersoners sambandstrafikk. Som et eksempel vil det være viktig for sikkerheten på sjøen at fartøyer kan kalle på hverandre eller varsle i tilfelle nød. En jamming av slike systemer vil senke tilliten til egen sikkerhet og myndighetenes evne til å sørge for befolkningens trygghet. Norge har mange kystsamfunn som er avhengig av ferjer. Gjennom å ramme disse med feilnavigering eller annen form for manglende situasjonsbilde så kan dette rammes og mediebildet formes deretter. Alle slike saker som undergraver myndighetens tillit er med på å bygge Russlands narrativ.

Det vil være vanskelig å oppdage hybride angrep dersom det ikke spesifikt fokuseres på det. Det vil innebære dedikert personell og tverrsektorielt samarbeid. Ikke bare i statlig regi, men absolutt et samarbeid mellom sivile og statlige. Selv med en dedikert avdeling kan det være vanskelig med tanke på kystlinjen og alle hendelser som skjer i et værutsatt land, som Norge er.

5.4 Oppsummering

Russland kan gjennom bruk av sine EK-kapasiteter og hybride krigføring utnytte norskekystens tilkomst for innsetting av materiell og personell ved behov. De kan utnytte sivile fartøy med påmontert materiell for innsamling av etterretninger på signalmiljøer og infrastruktur. Dette kan de så benytte på et senere tidspunkt for å påføre Norge problemer innen navigasjon langs kysten eller de kan sørge for at samband blir jammet. Det kan være situasjoner der det vil være ønskelig for Russland å benytte slike virkemidler for å skape usikkerhet langs kysten. Slike tiltak kombinert med skjulte tiltak mot infrastruktur på land kan gi Russland en fordel for å kunne gjennomføre skjulte oppdrag som flytter medias fokus vekk fra andre aktuelle tema Russland ikke ønsker på dagsorden. Innpass for slikt utstyr til kysten kan være gjennom russiske fartøy, med kapteiner som har farledsbevis.

Generelt vil det være nyttig for Russland å kunne påvirke Norge og troverdigheten til norske ressurser langs kysten. Gjennom å skape en usikkerhet om sikker navigasjon eller om det er mobilnett-dekning i områder gjør at mennesker må bruke tid og ressurser på å sikre seg og sine bedrifter. Russland vil kunne benytte sjansen til å skape mediebildet i Norge om en stat som ikke sørger for småsamfunnene langs kysten, og deretter utnytte dette for skjulte operasjoner.

6 EK fremover

Kunstig intelligens

En viktig utvikling innen elektronisk krigføring er bruken av kunstig intelligens (KI). Målet med kunstig intelligens er å utvikle en datamaskin som kan etterligne en menneskehjernes evne til problemløsning og kognitiv læring. Dette skal innebære selvstendig vurderingsevne og tilpasning til miljøer, som igjen vil gi muligheter for faktisk selvstyrende autonome kampsystemer (Andås, 2020, s. 32). For EK vil KI kunne bidra til avansert prosessering av stemmegjenkjenning og «forfalskning» på motstanderens samband for å simulere egne og fiendtlige sambandsmeldinger. Kanskje den viktigste bruken av KI innen EK kan bli evnen til å utmanøvrere motstanderens bruk av EMS og forhindre dennes bruk gjennom infiltrering og forstyrrelse av signalgangen. Det vil ikke nødvendigvis gjøres gjennom frekvensnektelse, men heller gjennom planting av falske data eller «forstyrrende» innhold som degraderer kommunikasjonen. Dette kan ta tid å etterforske hos motstanderen eller kunne forvirre lenge nok til at egen organisasjon kommer på innsiden av motstanderens OODA[4]-loop og utmanøvrerer motstanderen gjennom informasjonsoverlegenhet og handlingsrom. En Kunstig intelligens innen EK vil øke forståelsen av EMS-bruk og signalgang, til tross for kompleksiteten, på en måte som gjør at systemet vil utføre jobben uten en nødvendig «man-in-the-loop». Tidsbruken på beslutningsprosessen for hvordan ramme fienden vil kunne kuttes betraktelig (Andås, 2020, s. 32-33).

Kunstig intelligens vil øke evnen til å sammenstille frekvensbruk og signalgang på en måte som kan vanskeliggjøre overlegenhet i bruk av EMS (Bendett et al., 2021, s. 67-68). EK-systemer vil mulig bli helautomatiserte systemer som rammer fienden når det er mulig, eller det kan bli en semi-automatisert løsning der systemet legger til rette for beste løsning og mennesker kan trykke på knappen for «utfør». Uavhengig av hvilken løsning som blir valgt vil KI innen EK bli en «game-changer» for bruken av EMS-baserte K2-systemer i krigføring.

Svermeteknologi

Svermeteknologi er under stor utvikling. Teknologien er allerede i bruk i flere sammenhenger, men av den helt enkle sorten. Svermeteknologien vil kunne benyttes i flere sammenhenger i en stridssituasjon. For EK vil en svermeteknologi kunne spille inn et svært vanskelig scenario der et system skal kunne håndtere opptil flere hundre droner som kommer inn samtidig. Slik det er i dag vil slike droner være styrt sentralt fra motstanderen eller de er forhåndsprogrammerte med et oppdrag. Derimot vil det etter hvert komme kunstig intelligens som vil kunne desentraliseres ned til dronene selv og de kan gjennomføre angrep med en lokal adaptering til situasjonen, utført av dronene. Slike angrep vil kunne by på store utfordringer for et forsvarende EK-system. Derimot kan slike systemer også benyttes i en

[4] OODA-loop: Observe, Orient, Decide, Act. En mye brukt beslutningsmodell i Forsvaret

aktiv EK sammenheng der EK-systemet utnytter dronene til å gjennomføre sitt forsvar eller angrep mot en motstander ved hjelp av dronenes om bord-systemer. Slike systemer vil kunne gi drone-eieren et enormt situasjonsforståelses-fortrinn i en reell stridssituasjon der de kan sende ut hundrevis av droner som forer sanntidsdata til stridslederen (Andås, 2020, s. 57).

Kvante-datamaskiner

Behandlingen av informasjonen som er mulig å plukke opp gjennom eteren er enorm. Problemet vil ikke bare bestå i å systematisere den slik som KI nyttes til, men også å tolke dataene som ligger i utsendelsen. Informasjonen kan være kryptert eller på annen måte gjort «uleselig» for andre. Det er her kvante-datamaskiner kommer inn med en uovertruffen kapasitet og evne til prosessering. Disse maskinene kan ikke automatisk dekryptere all informasjon, men vil absolutt være et prosesseringsverktøy med, per i dag, ukjente egenskaper. Slike kvantemaskiner er ikke ferdig utviklet for praktisk bruk, men vil ved ferdigstillelse være et viktig bidrag for utnyttelse innen EK (Andås, 2020, s. 34). Kvantemaskiner vil ikke omtales videre i denne oppgaven, men dersom de får til en fungerende kvantemaskin-prosessor som kan utnyttes på mobile plattformer vil det kunne utgjøre en stor forskjell i evnen til prosessering av EMS og EK-tiltak i enhver situasjon.

7 Konklusjon

Russland har utviklet sin EK-kapasitet gjennom tiårene etter Berlin-murens fall. Russland har gjennom å se til USAs krigføring på 1990-tallet lagt listen for hva de må kunne av basisoppgaver for å stagge en motstander. Russland kan ikke bekjempe en motstander som NATO med antall soldater og materiell. Derfor satset de i stedet på utvikling av sine EK-kapasiteter for å evne å hemme motstanderens operasjonskonsept.

Gjennom sine operasjoner, i Ukraina etter 2014 og i Syria etter 2015, har de vist frem mange av sine kapasiteter og ikke minst taktikken i bruken av disse. De har gjennomført operasjoner i begge land med samme materiell, men de har utnyttet materiellet forskjellig. Gjennom operasjonen i Ukraina har de testet evner i det skjulte, da de har nektet for egne soldater i området. Gjennom aktive operasjoner med EK som middel har russiske styrker høstet mange erfaringer på materiellets faktiske egenskaper. Syria har på den annen side vært mer åpenlyst. I Syria har de foruten EK testet våpenmateriell i store mengder. EK-styrkene har hatt en mer passiv rolle og har blitt brukt mer for sikring av baser enn angreps kapasitet.

Russland har med sine EK-operasjoner i Ukraina vist hvordan et målrettet angrep på mobilnett kan fungere. Gjennom bruk av droner har de kontrollert mobilnettverk i store områder. De har utnyttet falske basestasjoner og droner til gjennomføring av påvirkningsaksjoner med «elektroniske flyveblader» og regelrett hacking av telefoner for maksimal effekt mot personellet. Russland har vist at påvirkningsaksjoner fungerer gjennom å adressere mennesker direkte gjennom mobiltelefonen. Mobiltelefonen er kanskje det viktigste kommunikasjonsmiddelet for svært store grupper, og den er som regel alltid med. Gjennom slik propagandataktikk direkte i lomma på menneskene i stridsområder, øker sjansen for at noen til slutt tror på budskapet. Slike angrep på mobilnett har vært mer utbredt i Ukraina enn i Syria. I Syria har målet primært vært mobiltelefoner i kjente terrornettverk for å stanse terroraksjoner mot det syriske regimet. For USA og NATO virker mobiltelefon-operasjonene, i Ukraina og Syria, som vindu mot hva de kan vente seg dersom en strid mellom Russland og NATO skulle oppstå. NATO har nå hatt mulighet til å følge russisk utvikling og bruk av EK gjennom flere år med operasjoner i et relativt statisk område. Det som er vanskelig å bedømme som passiv aktør på utsiden, er hvordan innsatsen faktisk påvirker. Rapportering om reell påvirkning ved slike angrep blir ofte holdt unna åpne kilder for å hindre at aggressoren får innblikk i hvordan aksjonen fungerer, eller ikke fungerer.

Russland så hvordan USAs presisjonsvåpen på 90-tallet ble styrt med GPS. Skulle Russland forsvare seg mot noe slikt måtte de ha kapasitet til å nekte slike våpen deres posisjonsnøyaktighet. Som vist i operasjoner i hele sitt nærområde, og internt i eget land, har Russland en velutviklet evne til

gjennomføring av GNSS-jamming og enda viktigere GNSS-spoofing. Ved jamming vil det raskt bli detektert hos «offeret» at de mister signalene, men gjennom spoofing kan de sørge for at «offeret» først må finne ut at de er på blindspor før de retter seg inn igjen. Denne evnen benyttes i mange situasjoner både som villedning av innkommende GNSS-styrte våpen eller droner, eller for å sørge for forvirring og kaos i områder. I Ukraina benytter de påvirkning av GNSS som metode for å hindre droner i overvåking i russiskkontrollerte områder. Samtidig som dronene mister posisjonssignaler jammer russerne også kommando-linken til droneføreren. USA og Russland er ikke i konflikt, men gjennom begges aktiviteter i Syria rapporteres det fra amerikanske styrker hvordan Russland stadig beviser sin evne til jamming av deres kommando og kontroll signaler på satcom. Som uttalt målsetting for russiske styrker er evnen til å yte desorganisering av motstanderens kommando og kontroll. Russland viser ved flere operasjoner at de forsøker stanse motstanderens tilgang på kommunikasjon og evne til situasjonsforståelse. De mest brukte, og observerbare, kapasitetene i dette ar nettopp påvirkning av GSM/samband, GNSS og satellitt-samband. NATO er avhengig av satellittkommunikasjon for de fleste av sine K2-systemer og må følge nøye med på hvilke midler russiske styrker benytter for å evne å motvirke deres forsøk på påvirkning.

Gjennom skjulte innsettinger av EK-midler i Norge kan Russland forberede områder før en eventuell strid starter. Norge er et langt land og Russland kan med enkle midler benytte russiskregistrerte fartøyer som seiler i norsk farvann for innsettelse av nødvendig utstyr for å gjennomføre en slik påvirkning. Ved å periodevis jamme mobilnett og spoofe GNSS kan de skape farlige situasjoner og usikkerhet, og undergrave tilliten til norske myndigheters prioritering av kyststrøkene. Russland vil utnytte muligheten til å kartlegge viktig infrastruktur og signalmiljøet langs norskekysten for å være klar med sine jammekapasiteter ved en eventuell situasjon mellom Norge og Russland. Ved hjelp av falske basestasjoner vil det være mulig for russiske EK-styrker å kartlegge personell og mobiler for senere å benytte dette i krisesituasjoner. Russland vil ikke bruke slike virkemidler mot Norge uten god planlegging og forberedelser. Problemet for Norge vil være å detektere de anomaliene som skiller slike angrep fra hverdagshendelser. Russland er godt forberedt for slike operasjoner og har godt trent personell med mye erfaring fra operasjoner i diverse miljøer etter flere år med krig. Norge har sannsynlig vært av interesse for Russland helt siden den kalde krigen og deres fokus på russiske sjømenn med farledsbevis bygger oppunder dette. Etter Russlands siste angrep på Ukraina er det iverksatt flere begrensende faktorer for russisk skipstrafikk langs norskekysten. Det er

usikkert hvor lenge et slikt forbud vil vare, men et slikt forbud vil ikke stanse en eventuell russisk interesse for operasjoner mot Norge. Det er slike operasjoner som sørger for at Russland er beredt dersom en konflikt skulle oppstå med Norge.

Russland har målrettet bygd opp EK-kapasitetene gjennom siste tiårene. Dette for å sørge for å kunne berede stridsområder for egne styrker. Gjennom å rette innsatsen mot hverdagshjelpemidler som mobiltelefoner og navigasjonsmidler så sørger de for å lamme områdene for menneskene som holder til der. For å ta siste stikk mot militæravdelinger sørger de for å jamme styrkenes tilgang på kommunikasjon med overordnede og dermed forsinke deres kommando og kontroll. Når kommando og kontroll ikke fungerer tidsriktig blir også situasjonsforståelsen ødelagt hos overliggende kommandoledd. Dette er med på å gi russiske styrker overtak i situasjonen og de kan angripe situasjonen som de ønsker.

Russland har gjennom sitt engasjement i Ukraina og Syria vist frem hvilke evner de besitter innen elektronisk krigføring. De har ikke rettet sine kapasiteter mot militære mål, men alle tilgjengelige mål som befinner seg i stridsområdet. De benytter sine evner innen elektronisk krigføring mot sivile for rettede informasjonskampanjer for svekking av kampmoral, samtidig som de benytter samme kapasitet til å ramme militære mål gjennom samme taktikk. Elektronisk krigføring er noe annet enn det som ofte blir diskutert innunder betegnelsen EK. Jamming av radar og radio er viktige midler, men som sett i Ukraina er det kontroll over signalmiljøet generelt og spesielt det som kan ramme menneskene i området som gir mest uttelling i slike miljøer.

Russland har bevist at de mestrer det elektromagnetiske spektrum. De har overbevist de fleste i vesten om at deres systemer er like gode som NATO sitt materiell, om ikke bedre. Gjennom deres operasjoner i Ukraina og Syria kan vi anta hvordan de kan benytte samme type kapasiteter i en fordekt operasjon mot Norge. Det vil bli en operasjon innunder begrepet hybrid krigføring og det vil kunne foregå over lang tid. Det er ikke et operasjonsmønster som tas på sparket og slike operasjoner er planlagt for å oppnå de rette målene. Problemet vil for Norge være å evne å fastslå at en slik operasjon er i gang gjennom analyse av rapporterte hendelser. Russland har gjennom flere år opparbeidet seg flere russiske sjømenn med farledsbevis i Norge. Dette er en kapasitet som vil kunne bidra i eventuelle operasjoner Russland ønsker gjennomført i Norge med landsetting av materiell eller personell for påvirkningsaksjoner. Disse kan ha med seg

koffertløsninger for EK-materiell som skal bidra til en undergravende funksjon av norske myndigheter. Gjennom påvirkning av mobilnett, navigasjonssikkerhet og signalmiljøer i Norge vil Russland bygge usikkerhet og sette dagsorden for politikere som må svare for samfunnssikkerheten i rurale områder. Dette for å unngå fokus i media på eksterne trusler fra Russland og deres handlinger.

«**starting a war without controlling the electromagnetic spectrum is tantamount to defeat**»

Sitat av Oberst Anatoly Tsyganok (medlem av Russian Center for Political-Military Studies) i sin artikkel fra 2021 (McCrory, 2021)

Forkortelser

AIS	Automatic Identification System
BeiDou	Kinesisk satellittsystem for navigasjon
EA	Elektronisk Angrep
EK	Elektronisk Krigføring
ELINT	Electronic Intelligence
EMS	ElektroMagnetiske Spektrum
EOB	Electronic Order of Battle (oversikt over identifiserte emittere i gitt område)
ESM	Elektronisk StøtteMiddel
Galileo	Europeisk satellittsystem for navigasjon
GLONASS	GLObal NAvigation Satellite System
GNSS	Global Navigation Satellite System
GPS	Global Positioning System
GSM	Global System for Mobile communications
HF	Høyfrekvens
IW	Information Warfare / også kjent som IO – Information Operations
K2	Kommando og Kontroll
K2D	Kommando og Kontroll Desorganisering
KI	Kunstig intelligens
LPI	Langtrekkende Presisjons Ild
PSYOPS	Psychological Operations
RF	Radio frekvens
SIGINT	Signal Intelligence

Litteraturliste

Adamsky, D. (2020). Russian campaign in Syria–change and continuity in strategic culture. *Journal of Strategic Studies*, *43*(1), 104-125.

Andås, H. E. (2020). *Emerging technology trends for defence and security* (20/01050). Forsvarets forskningsinstitutt. FFI. http://18.195.19.6/bitstream/handle/20.500.12242/2704/20-01050.pdf?sequence=1&isAllowed=y

Assymmetric Warfare Group. (2016). *Russian New Generation Warfare Handbook*. U. A. F. Meade. https://info.publicintelligence.net/AWG-RussianNewWarfareHandbook.pdf

BBC. (2019). *Study maps 'extensive Russian GPS spoofing'*. BBC. Hentet 31.08.2021 fra https://www.bbc.com/news/technology-47786248

Beale, J. (2017, 15.12.2017). Russia a 'risk' to undersea cables, defence chief warns. *BBC*. https://www.bbc.com/news/uk-42362500

Beale, J. (2022, 19.03.2022). Ukraine: What have been Russia's military mistakes? *British Broadcasting*. https://www.bbc.com/news/world-60798352

Bendett, S., Boulègue, M., Richard Connolly, Konaev, M., Podvig, P. & Zysk, K. (2021). Advanced military technology in Russia - Capabilities and implications. *Chatham House Russia and Eurasia Programme*. https://www.chathamhouse.org/2021/09/advanced-military-technology-russia

Bērziņš, J. (2020). The theory and practice of new generation warfare: The case of Ukraine and Syria. *The Journal of Slavic Military Studies*, *33*(3), 355-380.

Borden, A. (1999). *What is information warfare*. United States Air Force. Hentet 26.10.2021 fra https://www.airuniversity.af.edu/Portals/10/ASPJ/journals/Chronicles/borden.pdf

Brimelow, B. (2018, 26.04.2018). Syria Is Now The Most Aggressive Electronic Warfare Environment On The Planet - SOCOM Says. *Task Purpose*. https://taskandpurpose.com/military-tech/syria-aircraft-disabled-electronic-warfare/

Brown, D. (2017, 24.05.2017). Russia is using Syria as a testing ground for some of its most advanced weapons. *Business Insider*. https://www.businessinsider.com/russia-is-using-syria-testing-ground-some-advanced-weapons-2017-5?r=US&IR=T

C4ADS. (2019). *Above us only stars: Exposing GPS spoofing in Russia and Syria*. https://www.c4reports.org/aboveusonlystars

Clapper, J. R. (2016). *Worldwide threat assessment of the US intelligence community* (Statement for the record 2016). Director of National Intelligence. https://www.dni.gov/files/documents/SASC_Unclassified_2016_ATA_SFR_FINAL.pdf

Clark, M. (2021). *The Russian Military's Lessons Learned in Syria*. Institute for the Study of War. https://www.cfc.forces.gc.ca/259/290/308/305/carl.pdf

Collins, L. (2018). Russia Gives Lessons in Electronic Warfare. *Association of the United States Army*, *26*. https://www.ausa.org/articles/russia-gives-lessons-electronic-warfare

Connoly, R. & Boulegue, M. (2018). *Russia's New State Armament Programme Implications for the Russian Armed Forces and Military Capabilities to 2027*. C. House. https://www.chathamhouse.org/sites/default/files/publications/research/2018-05-10-russia-state-armament-programme-connolly-boulegue-final.pdf

Cozzens, T. (2019, 09.08.2019). *Iran jams GPS on ships in Strait of Hormuz*. GPS World. https://www.gpsworld.com/iran-jams-gps-on-ships-in-strait-of-hormuz/

Cunningham, C. (2020, 12.11.2020). *A Russian Federation Information Warfare Primer*. Universtity of Washington. https://jsis.washington.edu/news/a-russian-federation-information-warfare-primer/
DFRLab. (2017). Electronic warfare by drone and sms. *Medium.com*. https://medium.com/dfrlab/electronic-warfare-by-drone-and-sms-7fec6aa7d696
DFRLab. (2018). New Russian Electronic Warfare Systems in Eastern Ukraine. *#MinskMonitor*. https://medium.com/dfrlab/minskmonitor-new-russian-electronic-warfare-systems-in-eastern-ukraine-5b913afbb455
Doksheim, T. (2015, 28.02.2015). PST er varslet: Hevder Putin samler detaljkunnskap om norskekysten. *Dagbladet.no*. https://www.dagbladet.no/nyheter/pst-er-varslet-hevder-putin-samler-detaljkunnskap-om-norskekysten/60849245
Eversden, A. & Gill, J. (2022, 28.03.2022). *Why hasn't Russia used its 'full scope' of electronic warfare?* Breaking Media. https://breakingdefense.com/2022/03/why-hasnt-russia-used-its-full-scope-of-electronic-warfare/
Forsvaret. (2019a). *FFOD - Forsvarets fellesoperative doktrine*. Forsvarsstaben.
Forsvaret. (2019b). *Forsvarssjefens fagmilitære råd -Et styrket forsvar* (Forsvarssjefens fagmilitære råd 2019). Forsvarsdepartementet. https://www.forsvaret.no/aktuelt-og-presse/publikasjoner/fagmilitaert-rad
Forsvarets Forskningsinstitutt. *Elektronisk krigføring*. FFI. https://www.ffi.no/forskning/prosjekter/elektronisk-krigforing
Forsvarets Forskningsinstitutt. (2019, 29.05.2019). *Stordata kan brukes til å avsløre spionskip*. Forsvarets Forskningsinstitutt. https://www.ffi.no/aktuelt/nyheter/stordata-kan-brukes-til-a-avslore-spionskip
Galeotti, M. (2014). The 'Gerasimov Doctrine' and Russian Non Linear War. https://inmoscowsshadows.wordpress.com/2014/07/06/the-gerasimov-doctrine-and-russian-non-linear-war/
Giles, K. (2016a). *Handbook of Russian information warfare* (Fellowship Monograph 9). NATO Defense College. https://bdex.eb.mil.br/jspui/bitstream/123456789/4262/1/2016_Handbook,%20Russian%20Information%20Warfare.pdf
Giles, K. (2016b). Russia's 'new'tools for confronting the West: Continuity and innovation in Moscow's exercise of power. *Chatham House Russia and Eurasia Programme*. https://www.chathamhouse.org/sites/default/files/publications/2016-03-russia-new-tools-giles.pdf
Giles, K. (2017). *Assessing Russia's Reorganized and Rearmed Military* (Bd. 3). Carnegie Endowment for International Peace Washington DC:.
Glomsvoll, Ø. (2014). *Jamming of GPS & GLONASS signals-a study of GPS performance in maritime environments under jamming conditions, and benefits of applying GLONASS in Northern areas under such conditions* [Masteroppgave, The University of Nottingham]. https://fhs.brage.unit.no/fhs-xmlui/handle/11250/23896
Gordon, D. E. (1981). *Electronic warfare: element of strategy and multiplier of combat power*. Elsevier. https://www.sciencedirect.com/topics/engineering/electronic-warfare
Goward, D. (2019). Jammers at dachas add to Russia's ability to silence GPS - GPS World. Hentet 31.08.2021, fra https://www.gpsworld.com/jammers-at-dachas-add-to-russias-ability-to-silence-gps/
Grau, L. W. & Bartles, C. K. (2016). The russian way of war: force structures, tactics, and modernization of the russian ground forces. https://www.armyupress.army.mil/portals/7/hot%20spots/documents/russia/2017-07-the-russian-way-of-war-grau-bartles.pdf

Gross, J. A. (2019, 28.06.2019). *GPS jamming affecting Israel comes from Russian base in Syria*. The Times of Israel. https://www.timesofisrael.com/gps-jamming-affecting-israel-comes-from-russian-base-in-syria-us-researcher/

Halvorsen, T. (2022, 22.03.2022). Intensiverer jakten på falske basestasjoner. *Dagbladet*. https://www.dagbladet.no/nyheter/intensiverer-jakten-pa-mobil-tappere/75667354

Hambling, D. (2017). *Ships fooled in GPS spoofing attack suggest Russian cyberweapon*. New Scientist Ltd. Hentet 04.11.2021 fra https://www.newscientist.com/article/2143499-ships-fooled-in-gps-spoofing-attack-suggest-russian-cyberweapon/

Hoehn, J. R. (2019). *Ground Electronic Warfare: Background and Issues for Congress*. C. R. Service. Congressional Research Service. https://crsreports.congress.gov/product/pdf/R/R45919

Jaber, R. (2021, 16.07.2021). *Russian Defense Minister: Moscow Tested over 320 Developed Weapons in Syria*. H H Saudi Research and Marketing LTD. https://english.aawsat.com/home/article/3083256/russian-defense-minister-moscow-tested-over-320-developed-weapons-syria

Jacobsen, D. I. (2015). *Hvordan gjennomføre undersøkelser? : innføring i samfunnsvitenskapelig metode* (3. utg. utg.). Cappelen Damm akademisk.

Keller, J. (2019). *After experiencing Russian jamming up close in Syria, the Pentagon is scrambling to catch up*. Insider Inc. https://www.insider.com/pentagon-focus-on-electronic-warfare-after-russian-jamming-in-syria-2019-6

Kibar, O. (2021, 22.10.2021). OPERASJON LAZAREV: Slår alarm om kartlegging av Norges kritiske infrastruktur. *Dagens Næringsliv*. https://www.dn.no/magasinet/teknologi/spionasje/russland/etterretningstjenesten/operasjon-lazarev-slar-alarm-om-kartlegging-av-norges-kritiske-infrastruktur/2-1-1085420

Kjellén, J. (2018). Russian Electronic Warfare. The role of Electronic Warfare in the Russian Armed Forces. *Swedish Defence Research Agency FOI: Kista, Sweden*, 105. https://foi.se/rapportsammanfattning?reportNo=FOI-R--4625--SE

Kofman, M. & Rojansky, M. (2018). What kind of victory for Russia in Syria? *Military Review*, *24*(2), 6-23. https://www.armyupress.army.mil/Portals/7/military-review/Archives/English/Rojansky-Victory-for-Russia-1.pdf

McCrory, D. (2021). Russian Electronic Warfare, Cyber and Information Operations in Ukraine: Implications for NATO and Security in the Baltic States. *The RUSI Journal*, *165*(7), 34-44. https://www.tandfonline.com/doi/full/10.1080/03071847.2021.1888654

McDermott, R. N. (2017). *Russia's Electronic Warfare Capabilities to 2025: Challenging NATO in the Electromagnetic Spectrum*. International Centre for Defence and Security.

McDermott, R. N. (2021a, 31.08.2021). Russia’s Electronic Warfare Capabilities as a Threat to GPS. *Eurasia daily monitor*. https://jamestown.org/program/russias-electronic-warfare-capabilities-as-a-threat-to-gps/

McDermott, R. N. (2021b). Russia’s Military Boosts Electromagnetic Spectrum Capability. *Eurasia daily monitor*, *18*(144). https://jamestown.org/program/russias-military-boosts-electromagnetic-spectrum-capability/

McLeary, P. (2015, 21.10.2015). Russia’s Winning the Electronic War. *Foreign Policy*. https://foreignpolicy.com/2015/10/21/russia-winning-the-electronic-war/

Metrick, A. & Hicks, K. H. (2018). *Contested seas: Maritime domain awareness in northern Europe*. Rowman & Littlefield. https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/180328_MetrickHicks_ContestedSeas_Web.pdf?AaSGbCYstp_dV

Michaels, J. & Stanglin, D. (2015, 08.10.2015). Four Russian missiles fired at Syrian targets crash in Iran. https://eu.usatoday.com/story/news/world/2015/10/08/report-iran-pushed-russia-intervene-syria-iraq/73565592/
Monaghan, A. (2015). The'war'in Russia's' hybrid warfare'. *The US Army War College Quarterly: Parameters*, *45*(4), 8.
NATO. *NATO Terminology*. https://nso.nato.int/natoterm/Web.mvc
NATO. (2014, 05.09.2014). *Wales Summit Declaration - 2014* https://www.nato.int/cps/en/natohq/official_texts_112964.htm
NATO. (2019). *AJP-5 Allied Joint Doctrine for Planning of Operations*. NATO Standardization office (NSO).
NATO. (2020). *AAP-06 NATO Glossary of Terms and Definitions (English and French)*. NATO Standardization Office (NSO).
Navy Recognition. (2018, 07.08.2018). *Russian Navy Karakurt-class Corvettes Fitted with Orlan-10 UAVs*. Navy Recognition. https://www.navyrecognition.com/index.php/naval-news/naval-news-archive/2018/august-2018-navy-naval-defense-news/6387-russian-navy-karakurt-class-corvettes-fitted-with-orlan-10-uavs.html
Nikiforov, S. (2020, 04.06.2020). *Named the three most important technologies of the Russian Armed Forces in recent years*. politexpert.net. https://politexpert.net/199331-nazvany-tri-samye-vazhnye-tekhnologii-vs-rossii-poslednikh-let
Nilsen, T. (2017, 14.12.2017). Norway well prepared to meet Russian jamming. *The Barents Observer*. https://thebarentsobserver.com/ru/node/3327
Nilsen, T. (2019, 04.03.2019). Russian military officials arrive in Oslo as Norway puts GPS jamming facts on the table. *The Barents Observer*. https://thebarentsobserver.com/en/security/2019/03/russian-military-officials-arrive-oslo-norway-provides-facts-gps-jamming
Nimmo, B., Aleksejeva, N. & Barojan, D. (2017). Russia's Fake "Electronic Bomb". How a fake based on a parody spread to the western mainstream. *DFRLab*. https://medium.com/dfrlab/russias-fake-electronic-bomb-4ce9dbbc57f8
NKOM. (2021, 03.05.2021). *Prioritetsabonnement i mobilnett*. Nasjonal Kommunikasjonsmyndighet. https://www.nkom.no/sikkerhet-og-beredskap/prioritetsabonnementer-i-mobilnett
Osborn, A. (2018). Putin, before vote, unveils 'invincible' nuclear weapons to counter West. *Reuters*. https://www.reuters.com/article/us-russia-putin-nuclear-idUSKCN1GD514
Osborn, K. (2022, 06.03.2022). *How Ukrainian Forces are Defeating Russian Electronic Warfare*. The National Interest. https://nationalinterest.org/blog/buzz/how-ukrainian-forces-are-defeating-russian-electronic-warfare-200998
OSCE. (2021). *SMM long-range unmanned aerial vehicle lost due to dual GPS signal interference assessed as jamming near government controlled Stepanivka* https://www.osce.org/special-monitoring-mission-to-ukraine/491383
OSCE SMM. (2021). *News and press releases*. Organisation for Security and co-operation in Europe Special mission. Hentet 02.05.2022 fra https://www.osce.org/press-releases/GPS%20jamming?filters=+im_taxonomy_vid_1:(896)&solrsort=score%20desc&rows=10&category=News
Osflaten, A. (2021). Russian Strategic Culture after the Cold War: The Primacy of Conventional Force. *Journal of Military and Strategic Studies*, *20*(2), 110-132. https://jmss.org/article/view/67865/54680
Outlook web desk. (2022, 23.04.2022). *Explained: How Starlink Of Elon Musk Prevented Russian Electromagnetic Attack In Ukraine*. Outlook.

https://www.outlookindia.com/international/spacex-countered-russia-s-electromagnetic-warfare-in-ukraine-faster-than-us-military-pentagon-news-192868
Petkova, M. (2020). What has Russia gained from five years of fighting in Syria? Hentet 04.10.2021, fra https://www.aljazeera.com/features/2020/10/1/what-has-russia-gained-from-five-years-of-fighting-in-syria
Pomerleau, M. (2022, 08.03.2022). *Russia's lack of electronic warfare in Ukraine puzzling to experts*. Scoop News Group. https://www.fedscoop.com/russias-lack-of-electronic-warfare-in-ukraine-puzzling-to-experts/
Prop. 14 S (2020). *Evne til forsvar – vilje til beredskap Langtidsplan for forsvarssektoren*. Forsvarsdepartementet. https://www.regjeringen.no/no/dokumenter/prop.-14-s-20202021/id2770783/
Qiblawi, T., Hodge, N., Lister, T. & Kottasova, I. (2022, 22.02.2022). Why Donbas is at the heart of the Ukraine crisis. *Cable News Network*. https://edition.cnn.com/2022/02/19/europe/donbas-ukraine-russia-intl-cmd/index.html
Regjeringen. (2019). *Rapport fra arbeidsgruppen GNSS-GPS-forstyrrelser innen luftfart*. Regjeringen. Regjeringen. https://www.regjeringen.no/contentassets/ea62b7ef5071439a99390c77a54f2bc4/forstyrrelser-innen-luftfart.pdf
Reuters. (2017). Russian submarine fires cruise missiles at jihadi targets in Syria. Hentet 04.10-2021, fra https://www.reuters.com/article/us-mideast-crisis-syria-russia-idUSKCN1BX170
Richards, C. (2020). Boyd's OODA loop. *NECESSE*, *5*(1). https://fhs.brage.unit.no/fhs-xmlui/handle/11250/2683228
Schnelle, S. (2018). *Kartlegging av maritime hybride trusler - Kan bruk av stordata og sosial nettverksanalyse bidra til økt maritim situasjonsbevissthet?* [Master-oppgave, Forsvarets Høgskole]. https://fhs.brage.unit.no/fhs-xmlui/handle/11250/2583966
Smith, P. (2020). Russian Electronic Warfare: A Growing Tthreat to U.S. Battlefield Supremacy. *American Security Project*, 3. https://www.jstor.org/stable/resrep24679
Smura, T. (2016). Russian Anti-Access Area Denial (A2AD) Capabilities: Implications for NATO. https://pulaski.pl/wp-content/uploads/2015/02/Pulaski_Policy_Paper_No_29_16_EN.pdf
Sukhankin, S. (2020). Russia Unveils New Arctic Development Strategy: Focal Points and Key Priorities. *Eurasia daily monitor*, *17*(158). https://jamestown.org/program/russia-unveils-new-arctic-development-strategy-focal-points-and-key-priorities/
Tandberg, E. & Jarslett, Y. (2020, 05.11.2020). Drone. I Y. Jarslett (Red.), *Store Norske Leksikon*. https://snl.no/drone
TASS. (2021, 28.10.2021). *Ukraine obstructs flights of OSCE drones near Staromaryevka, DPR says* https://tass.com/world/1355407
The Moscow Times. (2018, 20.02.2018). Russian Military in Syria Ordered to Jam Phone Signals to Block Drones. *The Moscow Times*. https://www.themoscowtimes.com/2018/02/20/russian-military-syria-ordered-jam-phone-signals-block-drones-a60570
Thomas, T. (2020a). Russian Lessons Learned in Syria: An Assessment. *MITRE Center for Technology and National Security, June, June 2020*. https://www.mitre.org/sites/default/files/publications/pr-19-3483-russian-lessons-learned-in-syria.pdf
Thomas, T. (2020b). *Russias Electronic Warfare Force: Blending Concepts with Capabilities*. MITRE CORP MCLEAN VA.

https://www.mitre.org/sites/default/files/publications/pr-19-2714-russias-electronic-warfare-force-blending-concepts-with-capabilities.pdf
Thomas, T. L. (2019). *Russian Military Thought: Concepts and Elements*. MITRE CORP MCLEAN VA. https://www.mitre.org/sites/default/files/publications/pr-19-1004-russian-military-thought-concepts-elements.pdf
Trevithick, J. (2019, 30.10.2019). *Ukrainian officer details russian electronic warfare tactics including radio virus*. The War Zone. https://www.thedrive.com/the-war-zone/30741/ukrainian-officer-details-russian-electronic-warfare-tactics-including-radio-virus
Universitetet i Bergen. (2020, 07.09.2020). *Det elektromagnetiske spekteret*. Universitetet i Bergen. https://www.uib.no/hms-portalen/74856/det-elektromagnetiske-spekteret
Ure, K. (2021). *Russiske sjømenn i nærskipsflåten* [Masteroppgave, Forsvarets Høgskole, Forsvarets Høgskole]. https://fhs.brage.unit.no/fhs-xmlui/handle/11250/2835227
Varfolomeeva, A. (2018, 01.05.2018). *Signaling strength: Russia's real Syria success is electronic warfare against the US*. The Defense Post. https://www.thedefensepost.com/2018/05/01/russia-syria-electronic-warfare/
Von Hayek, F. (1974). *The pretence of knowledge*. The Nobel Prize. https://www.nobelprize.org/prizes/economic-sciences/1974/hayek/lecture/
Østensen, Å. G. (2020, 07.06.2020). *Russiske private militære selskap til sjøs – en trussel for Norge?* Stratagem. https://www.stratagem.no/russiske-private-militaere-selskap-til-sjos-en-trussel-for-norge/