FFI Forsvarets forskningsinstitutt

23/00868

FFI-RAPPORT

Cyberoperasjoner i et statsperspektiv

– utfordringer og analytiske verktøy for militær kontekst

Aasmund Thuv
Geir Enemo
Torbjørn Kveberg

Cyberoperasjoner i et statsperspektiv – utfordringer og analytiske verktøy for militær kontekst

Aasmund Thuv
Geir Enemo
Torbjørn Kveberg

Forsvarets forskningsinstitutt (FFI) 30. juni 2023

Emneord
Cyberoperasjoner
Analyse
Metoder
Verktøy

FFI-rapport
23/00868

Prosjektnummer
1501

Elektronisk ISBN
978-82-464-3480-3

Engelsk tittel
Cyber operations in a nation state perspective – challenges and analytical tools for military context.

Godkjennere
Ronny Windvik, *forskningssjef*
Espen Skjelland, *forskningsdirektør*

Dokumentet er elektronisk godkjent og har derfor ikke håndskreven signatur.

Sammendrag

FFI-prosjekt «Forsvarets bruk av det elektromagnetiske og digitale rom» har blant annet som formål å gjøre forsvarssektoren bedre i stand til å gjøre helhetlige vurderinger og forbedringer av cyberoperasjoner. Det gjelder både i forsvarsplanlegging, og i planlegging og gjennomføring av militære operasjoner. Prosjektet har utviklet et grunnlag for bedre å kunne analysere og forstå cyberoperasjoner. Grunnlaget kommer hovedsakelig i form av analytiske støtteverktøy som fageksperter og andre interessenter kan ta i bruk.

I om lag fire tiår har stater utviklet evner for å tilegne seg uautorisert tilgang til datasystemer for å fremme egne interesser overfor omverdenen. Hoveddriveren har vært etterretning og spionasje. Tilgangen har også vært brukt til for eksempel sabotasje og subversjon. Også kriminelle aktører er og har vært aktive, med ulike grader av organisering og profesjonalitet. Flere av disse trusselaktørene bruker også uautorisert tilgang som teknikk.

Stater og andre aktørers bruk av uautoriserte tilganger har skapt to vesentlige behov: Å forebygge dem, og også å håndtere dem når de skjer. Hovedansvaret for dette tilfaller ofte den som eier og drifter systemene. I senere tid ser vi også at det opprettes ulike strukturer i staten for bedre å kunne møte truslene. For eksempel kan stater ta ulike roller i håndtering gjennom nasjonale responsmiljøer, eller cybersikkerhetssentre. I militær sammenheng ser vi etableringen av enheter som har som oppgave å opprettholde militære organisasjoners handlefrihet i cyberdomenet og operativ evne. Vi ser også utviklingen av konsepter for å møte og håndtere cybertrusler både før, under og etter at hendelser inntreffer.

Det finnes ingen åpenbart riktige løsninger. Staters evne til selv å benytte seg av eller håndtere andres bruk av uautorisert tilgang blir institusjonalisert på ulikt vis fra stat til stat. Det endrer seg også over tid. Begrepsapparatet knyttet til cyberoperasjoner varierer, og er i utvikling. Det gjenspeiler en vekselvirkning mellom fag og politikk, både innad i land og mellom land.

Verktøyene som nevnes i denne rapporten gjør det mulig å argumentere på en konsistent og sporbar måte. De setter en felles kontekst for analyser og diskusjoner av viktige forhold. Det omfatter cyberoperasjoners egenskaper, nytte, risiko, mulighetsrom, begrensninger og dilemmaer. I rapporten oppsummeres tilnærmingen som er fulgt, identifiserte utfordringer, utviklede verktøy og anbefalinger for veien videre.

Summary

For about four decades, nation states have developed capabilities to gain unauthorized access to computer networks and systems in line with their own foreign policy interests. The main driver has been intelligence and espionage. Throughout this period, there have also been incidences where unauthorized access has been used to trigger technical effects, and through this conduct sabotage or subversion. Other threat actors than nation states, including criminals, have also been and are active, with different degrees of organization and professionalism. Many of these threat actors also use unauthorized access as a technique.

The use of unauthorized access by nation states and other actors has created a considerable need for capabilities to not only guard against such techniques, but also manage them when such use occurs. The main responsibility for this often lies with those who own or manage the systems, but in later times we also see the creation of different structures in the nation state to better meet those threats. For instance, state can take on different roles in incident management through national response teams or cyber security centres. In military context, we see the establishment of organizational elements tasked with preserving friendly freedom of movement in cyberspace and operational capabilities, and the development of concepts to meet and manage cyber threats before, during and after incidents occur.

In the absence of obvious solutions, the ability to utilize unauthorized access in line with state interests, or manage other nation states' use of the same, have been institutionalized differently across states and over time. The vocabulary of cyber operations is shaped accordingly. It reflects the confluence of politics and the given understanding of cyber operations at a certain point in time, either internal to a nation state or between nation states.

One of the objectives of FFI project "Armed Forces' use of the electromagnetic spectrum and cyber space" is to improve the ability of the Norwegian Defence Sector to assess and improve cyber operations in defence planning and in the conduct of military operations. The project has developed a foundation for improving the analysis and understanding of cyber operations. This foundation mostly consists of analytical tools that subject matter experts and other stakeholders may use.

The tools make it possible to create lines of reasoning that are consistent and traceable, and that sets a common context for analysis and discussions of important considerations like characteristics, utility, risk, space of options, constraints and dilemmas. This report summarizes the approach that has been used, identified challenges, the analytical tools that have been developed and recommendations for future work.

Innhold

1 Innledning

Stater har i om lag fire tiår utviklet evner for å tilegne seg uautoriserte tilganger[1] til datasystemer for å fremme egne interesser overfor omverdenen.[2] Slike evner er i dag profesjonalisert først og fremst til uoppdaget å samle inn data som er av interesse, typisk knyttet til etterretning og spionasje. Denne type aktiviteter kan sies å ha vært den viktigste driveren i utviklingen så langt, hvor stater setter inn tyngre innsats for å erverve informasjon i cyberdomenet og bevisst ser ut til å unngå skape skade i de tekniske systemene de bryter seg inn i. Innsatsen kan foregå over lengre tid uten at de som rammes er klar over at deres systemer har blitt kompromittert og at informasjon er hentet ut.[3]

Gjennom perioden er det også tilfeller hvor uautorisert tilgang anvendes med mål om å påføre datasystemer teknisk effekt. Slik utføres for eksempel sabotasje eller subversjon.[4] Det finnes også eksempler på at den offensive part kjemper for å beholde tilgang når de er oppdaget, eller er destruktive når de trekker seg ut.[5] Andre trusselaktører enn stater, deriblant kriminelle, har også vært – og er – aktive, med ulike grader av organisering og profesjonalitet.[6] Flere av disse trusselaktørene bruker også uautorisert tilgang som teknikk.

Stater og andre aktørers bruk av uautoriserte tilganger har skapt et vesentlig behov for evner til både å forebygge dem, og til å håndtere[7] dem når de skjer. Hovedansvaret for dette tilfaller ofte

[1] Ulike aktører bruker forskjellige begreper om dette fenomenet, herunder «dataangrep», «datainnbrudd», «*computer intrusion*» med mer. Begrepsapparatet i denne rapporten omtales mer inngående i kapittel 1.3 og vedlegg A.
[2] For mer om arbeidet Markus Hess utførte på oppdrag av sovjetisk etterretning rundt midten av 1980-tallet, se Stoll, C. (2005). *The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage*. Pocket Books.
[3] Se f.eks. Higgins, K. J. (2016, 7. september). OPM Breach: Two Waves Of Attacks Likely Connected, Congressional Probe Concludes. *Dark Reading*. https://www.darkreading.com/endpoint/opm-breach-two-waves-of-attacks-likely-connected-congressional-probe-concludes; Levi, M., Dahan, A., Serper, A. (2019, 25. juni). Operation Soft Cell: A Worldwide Campaign Against Telecommunications Provider. *Cybereason*. https://www.cybereason.com/blog/operation-soft-cell-a-worldwide-campaign-against-telecommunications-providers; Stubbs, J., Menn, J., Bing, C. (2019). Inside the West's failed fight against China's 'Cloud Hopper' hackers. *Reuters*. https://www.reuters.com/investigates/special-report/china-cyber-cloudhopper/; Greenberg, A. (2021, 20. mai). The Full Story of the Stunning RSA Hack Can Finally Be Told. *Wired*. https://www.wired.com/story/the-full-story-of-the-stunning-rsa-hack-can-finally-be-told/.
[4] For mer om dette, se for eksempel Rid, T. (2013). *Cyber War Will Not Take Place.* Oxford University Press; Rid, T. (2020). *Active Measures: The Secret History of Disinformation and Political Warfare.* Farrar, Straus and Giroux; Buchanan, B. (2020). *The hacker and the state: Cyber attacks and the new normal of geopolitics.* Harvard University Press.
[5] For en trusselaktør som kjemper for å beholde tilgang, se f.eks. Hodgson, Q. E., Shokh, Y., Balk, J. (2022, s. 28). *Many Hands in the Cookie Jar: Case Studies in Response Options to Cyber Incidents Affecting U.S. Government Networks and Implications for Future Response.* RAND Corporation, RR-A1190-1. https://www.rand.org/content/dam/rand/pubs/research_reports/RRA1100/RRA1190-1/RAND_RRA1190-1.pdf; for en destruktiv aktør med finansielle motiver, se FireEye (2018). *APT38: Un-usual suspects*. Special report. https://content.fireeye.com/apt/rpt-apt38.
[6] Se f.eks. omtale av trusselbildet og trusselaktører i Telenor (2022). *Digital sikkerhet 2022. Nye perspektiver.* https://www.telenor.no/binaries/om/digital-sikkerhet/2022/Digital_sikkerhet_2022.pdf; Microsoft (2021). *Microsoft Digital Defence Report 2021*. https://go.microsoft.com/fwlink/p/?LinkID=2173952&clcid=0x409&culture=en-us&country=us.
[7] Håndtere må her forstås på to måter: 1) å reagere når noe inntreffer, det vil si at noen benytter seg av uautorisert tilgang og at dette oppdages; 2) å møte en trussel i et bredere perspektiv, herunder å forberede seg på at ervervelse av uautorisert tilgang kan forekomme i fremtiden, og ved å handle proaktivt når forsøk på dette antas å være nært forestående. Disse nyansene reflekteres i begrepsapparatet vi bruker i rapporten, se kapittel 1.3 og vedlegg A.

den som eier og drifter systemene, men i senere tid ser vi også at det opprettes ulike strukturer i staten for bedre å kunne møte truslene. Stater kan for eksempel ta ulike roller i håndtering gjennom nasjonale responsmiljøer eller cybersikkerhetssentre.

I fravær av åpenbart riktige løsninger blir staters evne til å tilegne seg og utnytte uautorisert tilgang, og å håndtere andres bruk av dette, institusjonalisert på ulikt vis fra stat til stat og over tid. De offensive evnene befinner seg gjerne i én eller flere hemmelige tjenester, sammen med staters øvrige evner til fordekt innsamling. Blant vestlige land sorterer de under det som kalles cyberoperasjoner, hvor ervervelse og utnyttelse av uautorisert tilgang utgjør de offensive operasjonene og håndteringen utgjør de defensive operasjonene.[8] Enkelte land velger også å plassere uautorisert tilgang i andre kategorier enn cyberoperasjoner, som Russland med sitt begrepsapparat orientert rundt informasjonskrig. Der er det å bruke uautoriserte tilganger forstått som en form for informasjonstekniske tiltak,[9] og dette munner ut i en annen forståelse for verdien av tiltakene i understøttelsen av statens egne interesser.

Fra et analytisk ståsted er det dermed mulig å skille mellom utviklingslinjer i bruken og håndteringen av uautoriserte tilganger på den ene siden, og staters forståelse og konseptualisering på den andre – selv om det naturlig nok er sammenhenger mellom disse. Definisjoner og begrepsapparat knyttet til cyberoperasjoner gjenspeiler en vekselvirkning mellom fag og politikk funnet i interne prosesser på et punkt i tid, enten det er innad i land eller mellom land. Her kan for eksempel den eksisterende organiseringen i en stat og innenrikspolitiske hensyn virke fra innsiden, og impulser fra allierte virke fra utsiden.[10] Det er ikke mange år siden Nato anerkjente cyberdomenet som et krigføringsdomene på linje med land, luft, sjø og rom.[11] Det arbeides kontinuerlig i Nato med å forstå implikasjonene av dette og hvordan cyberdomenet best kan operasjonaliseres.[12] I dette bildet er det viktig å utvikle den faglige forståelsen som trekkes inn i prosessen uten å være kunstig påvirket av det som kommer ut av den.

---

[8] Sammenlign for eksempel definisjoner og beskrivelser i Forsvaret (2014). Forsvarets fellesoperative doktrine. Forsvarsstaben. http://brage.bibsys.no/xmlui/handle/11250/224031; Forsvaret (2019). Forsvarets fellesoperative doktrine. Forsvarsstaben. https://fhs.brage.unit.no/fhs-xmlui/bitstream/handle/11250/2631948/FFOD%202019%20.pdf; NATO (2020). *AJP-3.20 Allied Joint Doctrine for Cyberspace Operations*. Edition A Version 1. Allied Joint Publication. NATO Standardization Agency. Andre teknikker enn uautoriserte tilganger kan også omfattes av cyberoperasjoner i slike dokumenter.

[9] Giles, K. (2021). Russian information warfare. I T. Clack & R. Johnson (Red.), *The World Information War* (1. utg., s. 139–161). Routledge. https://doi.org/10.4324/9781003046905-12

[10] For Norges del har begrepsapparatet lenge vært tuftet på amerikanske tanker fra 1990-tallet, men skiftes nå ut med et nytt begrepsapparat mer på linje med alliansens første doktrine for cyberspaceoperasjoner (CO). Se for eksempel Cyberforsvaret (2022, 1. juli). *Konsept for defensive cyberoperasjoner.*.

[11] NATO (2016, 9. Juli, para 70). *Warsaw Summit Communiqué.* Press Release. https://www.nato.int/cps/en/natohq/official_texts_133169.htm. Selv om land, luft, sjø og rom her omtales som domener, omtales de i NATOs doktriner som omgivelser (*environments*). Det er således kun cyberdomenet som formelt sett er definert som et domene. For enkelthets skyld bruker vi likevel begrepet domener, i tråd med NATOs doktrine for cyberoperasjoner. Se NATO (2020, s.5 fotnote 3). *AJP-3.20 Allied Joint Doctrine for Cyberspace Operations.* Edition A Version 1. Allied Joint Publication. NATO Standardization Agency. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/899678/doctrine_nato_cyberspace_operations_ajp_3_20_1_.pdf.

[12] Se f.eks. Brent, L. (2019). NATO's Role in Cyberspace. *NATO Review*. https://www.nato.int/docu/review/articles/2019/02/12/natos-role-in-cyberspace/index.html; Davis, S. (2019). *NATO in the Cyber Age: Strengthening Security & Defence, Stabilising Deterrence*. Science and technology committee (STC), NATO Parliamentary Assembly. General report. https://www.nato-pa.int/download-

For de som er interessert i den militære dimensjonen er det lite empiri og åpne erfaringer å finne om cyberoperasjoner relatert til det å bruke uautoriserte tilganger i militære operasjoner. I dag brukes konflikten i Ukraina av flere eksperter som utgangspunkt for diskusjoner om dette, med blant annet dokumenterte eksempler på bruk av destruktiv skadevare. I hvor stor grad utførelsen har vært koordinert med, eller integrert i, den militære planleggingen er imidlertid usikkert, og de faktiske konsekvensene for krigføringen er også i liten grad belyst. I tillegg er det også uenighet om bruken av offensive cyberoperasjoner i denne konflikten er representativ og hvilke erfaringer en faktisk kan trekke.[13] For defensive cyberoperasjoner i militær kontekst omtales noen eksempler, men hva som omfattes av begrepet varierer og koblingen til en egen militær operasjon kan være svak.[14] Mer generelt kan vi finne beskrivelser av ulike former for cybersikkerhet og hendelseshåndtering i sivile, stats- og forsvarsrelaterte rammede systemer og nettverk. Beslutningsunderlaget og vurderingene til de som gjør hendelseshåndtering er imidlertid som regel mangelfullt gjengitt, og det kan være uenigheter internt om hva som faktisk skjedde og ble gjort.[15]

FFI-prosjekt 1501 «Forsvarets bruk av det elektromagnetiske og digitale rom» plasserer seg midt i denne tematikken, hvor staters anvendelse og håndtering av cyberoperasjoner i dag og i fremtiden søkes belyst og videreutviklet fra et militært ståsted. Prosjektet har blant annet som formål å gjøre FFI, Forsvaret og FD bedre i stand til å gjøre helhetlige vurderinger og forbedringer av cyberoperasjoner i forsvarsplanlegging og i planlegging og gjennomføring av

file?filename=/sites/default/files/2019-10/REPORT%20148%20STC%2019%20E%20rev.%201%20fin%20%20-%20NATO%20IN%20THE%20CYBER%20AGE.pdf; NATO (2022, 14. juni, para 32); *Brussels Summit Communiqué.* Press Release https://www.nato.int/cps/en/natohq/news_185000.htm.

[13] Se f.eks. Microsoft (2022a). *Special Report: Ukraine. An overview of Russia's cyberattack activity in Ukraine.* https://aka.ms/ukrainespecialreport; Microsoft (2022b). *Defending Ukraine: Early Lessons from the Cyber War.* https://aka.ms/June22SpecialReport ; Smalley, S. (2022, 1. juli). Cybersecurity experts question Microsoft's Ukraine report. *Cyberscoop*. https://www.cyberscoop.com/cybersecurity-experts-question-microsofts-ukraine-report/; Kaminska M., Shires, J., Smeets, M. (2022); *Cyber Operations during the 2022 Russian invasion of Ukraine: Lessons Learned (so far).* Tallinn Workshop Report. The European Cyber Conflict Research Initiative (ECCRI). https://eccri.eu/wp-content/uploads/2022/07/ECCRI_WorkshopReport_Version-Online.pdf. Også påstander om offensive cyberoperasjoner som styrkemultiplikator er omdiskutert; se for eksempel Smeets, M. (2018). The Strategic Promise of Offensive Cyber Operations. *Strategic Studies Quarterly*, *12*(3), 90-113. For et motstridende syn, se Maschmeyer, L. (2022b, 12. juli). Infiltrate, Exploit, Manipulate: Why the Subversive Nature of Cyber Conflict Explains Both Its Strategic Promise and Its Limitations. *Lawfareblog.* https://www.lawfareblog.com/infiltrate-exploit-manipulate-why-subversive-nature-cyber-conflict-explains-both-its-strategic.

[14] Se f.eks. omtalen av defensive cyberoperasjoner i Corera, G. (2022, 30. oktober) Inside a US military cyber team's defence of Ukraine. *BBC News*. https://www.bbc.com/news/uk-63328398; U.S. Cyber Command (2022, 17. oktober 2022). *CYBERCOM executed global cyberspace defensive operation*. https://www.cybercom.mil/Media/News/Article/3190716/cybercom-executed-global-cyberspace-defensive-operation/.

[15] For eksempler på hendelseshåndtering, se Telenor (2020). *Operasjon Bivrost*. https://www.telenor.no/om/digital-sikkerhet/2020/artikler/operasjon-bivrost.jsp; Bruvoll, J., Thuv, Aa., Enemo, G. (2022). *Håndtering av IKT-sikkerhetshendelsene i Helse Sør-Øst og fylkesmannsembetene - en vurdering*. FFI-rapport 20/01560. https://www.ffi.no/publikasjoner/arkiv/handtering-av-ikt-sikkerhetshendelsene-i-helse-sor-ost-og-fylkesmannsembetene-en-vurdering; US Congress (2016). *The OPM Data Breach: How the Government Jeopardized Our National Security for More than a Generation.* Majority Staff Report Committee on Oversight and Government Reform U.S. House of Representatives 114th Congress. https://republicans-oversight.house.gov/wp-content/uploads/2016/09/The-OPM-Data-Breach-How-the-Government-Jeopardized-Our-National-Security-for-More-than-a-Generation.pdf. For et motsvar til enkelte konklusjoner i US Congress (2016), se U.S. Congress (2016b). *Memorandum*. Committee on Oversight and Government Reform U.S. House of Representatives 114th Congress. https://oversight.house.gov/sites/democrats.oversight.house.gov/files/documents/2016-09-06.Democratic%20Memo%20on%20OPM%20Data%20Breach%20Investigation.pdf.

militære operasjoner. Dette er en oppgave som krever innsikt i empiri knyttet til staters bruk og håndtering av cyberoperasjoner i tillegg til etablering av en konsistent konseptuell forståelse av fenomenet. I vårt arbeid har vi i stor grad satt likhetstegn mellom cyberoperasjoner og uautorisert tilgang for å avgrense fenomenet på en tydelig måte. Uautorisert tilgang er da en teknikk som benyttes for å understøtte et mål. I en militær kontekst kan dette for eksempel være etterretning eller negativt å påvirke en motparts kapabiliteter og operative evne. Den defensive hensikten kan være å beskytte militære organisasjoners handlefrihet i cyberdomenet, og å møte og håndtere cybertrusler både før, under og etter fiendtlige cyberaktiviteter inntreffer og detekteres.

Prosjektet har arbeidet med å utvikle et grunnlag for bedre å kunne analysere og forstå cyberoperasjoner. Grunnlaget kommer hovedsakelig i form av analytiske støtteverktøy som fageksperter og andre interessenter kan ta i bruk. Verktøyene gjør det mulig å argumentere på en konsistent og sporbar måte. Ved å løfte frem sentrale faktorer settes en felles kontekst for analyser og diskusjoner av viktige forhold som cyberoperasjoners egenskaper, nytte, risiko, mulighetsrom, begrensninger og dilemmaer. Dette utgjør en betydelig utvikling innen faglig støtte for helhetlige vurderinger og forbedringer av den typen flere aktører i sektoren ønsker å gjøre.

Denne rapporten oppsummerer prosjektets arbeid med cyberoperasjoner. Dette inkluderer vår tilnærming, utfordringer vi har identifisert, verktøyene vi har utviklet og anbefalinger for veien videre.

1.1 Målsettinger med arbeidet

Den overordnede målsettingen for alle aktivitetene beskrevet i denne rapporten har vært å utvikle et grunnlag for bedre å kunne analysere og forstå cyberoperasjoner i forsvarsplanlegging og i planlegging og gjennomføring av militære operasjoner på en konsistent måte.

Mer detaljerte målsettinger har blitt utformet underveis i arbeidet etter hvert som vår forståelse har økt. Disse inkluderer:

- M1: Å etablere et konseptuelt grunnlag som hjelp til å identifisere og adressere sentrale problemstillinger knyttet til staters bruk av cyberoperasjoner.
- M2: Å bidra til økt innsikt i hvordan nytte, risiko, og mulighetsrom ved cyberoperasjoner i militære operasjoner kan utforskes, og hvordan cyberoperasjoner kan nyttiggjøres.
- M3: Å bidra til økt innsikt i anvendelsen av scenario- og kapabilitetsbasert metodikk for langtidsplanlegging som ramme for forsvarsplanlegging for cyberoperasjoner.[16]

Arbeidet har vært rettet mot skjæringspunktet mellom tekniske, operative og politiske forhold.

[16] Langtidsplanlegging i forsvarssektoren ledes av FD og støttes blant annet av FFIs prosjektserie *Støtte til FDs langtidsplanlegging* (SIMFOR). SIMFOR benytter en scenario- og kapabilitetsbasert metode, ofte omtalt som SIMFOR-metoden. Se kapittel 3.2.

1.2 Modenhetsnivå

Cyberoperasjoner er et fagområde i rivende utvikling. Den konseptuelle forståelsen i feltet anser vi som umoden, noe som setter sitt preg på verktøyene vi har utviklet. Ny kunnskap kan medføre behov for endringer i verktøyene, som derfor må sees på som preliminære og fremdeles under utvikling. Vi mener likevel at verktøyene, som de er nå, er til god hjelp med å utvikle vår forståelse av cyberoperasjoner.

1.3 Sentrale begreper

Som første setning i innledningen antyder har prosjektet tatt utgangspunkt i én sentral bit: staters bruk av uautorisert tilgang for å fremme egne interesser overfor omverdenen. Avgrensningen tillater oss en sporbar konseptuell utforsking av fenomenet, som også inkluderer den defensive siden.[17] Uautoriserte tilganger er en meningsfull avgrensning både teknisk sett og for staten, og fanger en større del av problemkomplekset med operasjoner som kan medføre store positive og negative konsekvenser for brukeren.[18]

Med denne forståelsen av cyberoperasjoner skilles det videre mellom to typer:[19]

- *Offensive cyberoperasjoner med bruk av uautoriserte tilganger* omfatter kategoriene cyberoperasjoner for etterretning og cyberoperasjoner for effekt.[20] Ved etterretning er målet å hente ut informasjon. Ved effekt er målet å skape tekniske effekter i systemet, med bestemte følgeeffekter av interesse for staten.[21]

- *Defensive cyberoperasjoner for håndtering av uautoriserte tilganger* omfatter kategoriene forberedelser og beredskap, proaktiv tilpasning på kort sikt, reaktiv hendelseshåndtering og proaktiv strategisk initiativtaking og posisjonering. Disse kategoriene er inspirert av ulike aktiviteter som er omtalt i tilknytning til defensive cyberoperasjoner og hendelseshåndtering.[22]

[17] Som for eksempel rammeverket omtalt i kapittel 4.1.
[18] Alternativet «dataangrep» er problematisk da ordet «angrep» kan leses til kun å omfatte staters villede angrep, utover etterretning og vanlig kriminalitet. Ordet «datainnbrudd» (engelske *computer intrusion*) er mer presist, men kan på norsk leses til kun å omfatte kriminell aktivitet. Vi bruker derfor «uautorisert tilgang».
[19] Mer utfyllende beskrivelser av offensive og defensive cyberoperasjoner som definert på denne måten, finnes i vedlegg A.
[20] Denne inndelingen gjenspeiler to ulike, sentrale mål for offensive cyberoperasjoner. Se for eksempel Poznansky, M. (2021, 23. mars). Covert action, espionage, and the intelligence contest in cyberspace. *War on the Rocks.* https://warontherocks.com/2021/03/covert-action-espionage-and-the-intelligence-contest-in-cyberspace/; Forsvaret (2019, s. 125). *Forsvarets fellesoperative doktrine (FFOD).* Forsvarsstaben. http://hdl.handle.net/11250/2631948. Det er mulig å definere flere kategorier, se for eksempel fransk doktrine for offensive cyberoperasjoner som har villedning som en tredje kategori. Delerue, F., Desforges, A., Géry, A. (2019, 23. april). A close look at France's new military cyber strategy. *War on the Rocks.* https://warontherocks.com/2019/04/a-close-look-at-frances-new-military-cyber-strategy/
[21] Legg merke til at påvirkning uten uautoriserte tilganger faller utenom denne kategorien. Et eksempel på dette er falske nyheter spredd via «boter» på sosiale medier.
[22] Kilder til inspirasjon for dette er blant annet ulike tankesett innen defensive cyberoperasjoner, *incident management* og beredskap og krisehåndtering. Se for eksempel NCSC (u.å.) *Incident Management.* https://www.ncsc.gov.uk/collection/incident-management; U.S. Cyber Command (2022, 25. oktober). *CYBER 101 –*

Vi mener denne definisjonen ikke bryter nevneverdig med formelle norske definisjoner for Forsvaret, men presiserer noe hvilket fenomen vi studerer.[23]

Øvrige sentrale begreper i rapporten er:

- *Forsvarsplanlegging* er en prosess som søker å sikre at en stat har et forsvar som klarer å utføre sine oppgaver og oppnå sine mål for hele spekteret av dets virksomhet.[24]

- *Langtidsplanlegging* er en planleggingsdisiplin for forsvarsplanlegging som fokuserer på en lengre tidshorisont, typisk 10–30 år.[25]

- *Strukturelement* er en klart avgrenset del av en organisasjon bestående av personell, prosesser og systemer.[26]

Defend forward and Persistent Engagement. https://www.cybercom.mil/Media/News/Article/3198878/cyber-101-defend-forward-and-persistent-engagement/; Laudrain, A. P. B. (2019, 26. februar). France's New Offensive Cyber Doctrine. *Lawfareblog.* https://www.lawfareblog.com/frances-new-offensive-cyber-doctrine; Vašíčková, V. (2020). Crisis Management Process - A Literature Review and a Conceptual Integration. *Acta Oeconomica Pragensia 27*(3-4):61-77. https://doi.org/10.18267/j.aop.628; Myndigheten for samhällsskydd och beredskap (2022, 19. september). *Nytt beredskapssystem träder i kraft den 1 oktober*. https://www.msb.se/sv/aktuellt/nyheter/2022/september/nytt-beredskapssystem-trader-i-kraft-den-1-oktober/. For norske kilder, se for eksempel NSM (2017, 7. desember). *Rammeverk for håndtering av IKT-sikkerhetshendelser.* https://nsm.no/regelverk-og-hjelp/andre-publikasjoner/rammeverk-for-handtering-av-ikt-hendelser/; Samfunnssikkerhetsinstruksen (2017). *Instruks for departementenes arbeid med samfunnssikkerhet.* FOR-2017-09-01-1349. https://lovdata.no/dokument/LTI/forskrift/2017-09-01-1349; Cyberforsvaret (2022, 1. juli). *Konsept for defensive cyberoperasjoner.*

[23] Cyberoperasjoner er i Forsvarets fellesoperative doktrine definert som «[…] handlinger i eller igjennom cyberdomenet for å sikre egen handlefrihet, og/eller skape effekter for å oppnå militær sjefs målsettinger. Overordnet deles cyberoperasjoner i offensive og defensive cyberoperasjoner. Cyberoperasjoner omfatter ikke CIS-støtte eller tiltak utenfor cyberdomenet for å påvirke dette.»
Videre er *offensive cyberoperasjoner* «[h]andlinger i eller gjennom cyberdomenet som projiserer makt for å skape effekter som bidrar til militær sjef sine målsettinger. I norsk sammenheng innebærer dette operasjoner i eller ved bruk av cyberdomenet med anvendelse av aktive metoder, i den hensikt å innhente og analysere informasjon med etterretningsformål eller skade, manipulere, forstyrre eller påvirke personell, materiell, informasjon eller aktivitet, for å skape en effekt hos motstanderen.»;
Defensive cyberoperasjoner er «[d]efensive handlinger i eller gjennom cyberdomenet, utført i den hensikt å bevare egen handlefrihet i cyberdomenet. I norsk sammenheng innebærer dette militær operativ hendelseshåndtering i cyberdomenet og er tiltak og aktiviteter som utøves i den hensikt å sikre og forsvare en militær sjefs operative evne gjennom beskyttelse av kritiske verdier. Tiltakene utøves for å hindre eller stoppe cyberangrep, redusere skade og håndtere konsekvensene av et angrep.» Se Forsvaret (2019, s. 125, 229–230, 242). *Forsvarets fellesoperative doktrine (FFOD).* Forsvarsstaben. http://hdl.handle.net/11250/2631948

[24] Fritt formulert etter (Stojkovic og Dahl, 2007 s. 7): «*Defence planning seeks to ensure that a nation has the necessary forces, assets, facilities and capabilities to fulfil its tasks throughout the full spectrum of its missions*». Stojkovic, D., Dahl, B. R. (2007). *Methodology for long term defence planning.* FFI-rapport 2007/00600. https://www.ffi.no/publikasjoner/arkiv/methodology-for-long-term-defence-planning

[25] Fritt formulert etter (Stojkovic og Dahl, 2007, s.7–10): «*Long term defence planning is a specific planning discipline that is related to the relatively distant future…*" (s. 7) "*… assumed to have a time horizon of 10 years or more*» (s. 10). Ibid.

[26] FMA (u.å) *Terminologi*. https://www.fma.no/prinsix/maler/terminologi. Videre: «Strukturelementet utfører en identifiserbar del av verdikjeden (etterretning, kampstyrke, ildstøtte, logistikk) og kan brytes ned i et hierarki og bestå av underordnede strukturelementer. I realiteten snakker vi da om byggeklosser av organisasjonselementer (artilleri-enhet, luftvernenhet, fregatt, kampflyenhet) …». I FFIs metode for langtidsplanlegging er det en forskjell mellom generiske enheter (f.eks. mekanisert infanteribataljon, FN-fregatt, kampfly) og faktiske strukturelementer (KNM Otto Sverdrup, Telemarkbataljonen). Se Hennum, A. C., Glærum, S. (2007, s. 20). *Metode for langtidsplanlegging – støtte*

1.4 Øvrige avgrensninger

I denne rapporten ser vi på cyberoperasjoner som et generelt fenomen som stater må forholde seg til. Utfordringene og verktøyene som beskrives er generiske og ikke tilpasset en gitt stat. Det er ikke gjort noen vurderinger av hvordan Norge anvender cyberoperasjoner eller av valgene Norge har tatt for sin cybervirksomhet. Likevel har vi størst fokus på småstater som er liberale demokratier.

Av offensive cyberoperasjoner ser vi primært på cyberoperasjoner for effekt, men inkluderer cyberoperasjoner for etterretning der det virker naturlig å se disse i sammenheng. Den tette koblingen mellom etterretningsoperasjoner og effektoperasjoner gjør det nødvendig å se offensive cyberoperasjoner i en noe bredere sikkerhetspolitisk ramme, selv når målet er å diskutere dem i militære operasjoner.

For defensive cyberoperasjoner ser vi primært på reaktiv hendelseshåndtering. Selv om også en defensiv cyberoperasjon i en militær operasjon kan påvirke og bli påvirket av hendelseshåndtering utenfor Forsvaret og forsvarssektoren, var det ikke behov for å ta høyde for dette i denne rapportens analyser. Vi avgrenser dermed defensive cyberoperasjoner til de som utføres i forbindelse med fiendtlige offensive cyberoperasjoner mot Forsvarets systemer. Dette er systemer som direkte understøtter Forsvarets operative evne og som Forsvaret selv har ansvar for å forsvare. Det er imidlertid mulig å gå bredere til verks i fremtidige studier, og inkludere for eksempel sivile tjenester av betydning for operativ evne eller håndtering av andres tilegnelse og anvendelse av uautoriserte tilganger i andre sektorer.

1.5 Rapportens innhold

Rapporten er delt inn i seks kapitler:

- I kapittel 2 beskrives fremgangsmåten som er benyttet i arbeidet.
- I kapittel 3 omtales utfordringer ved analyse og utvikling av analytiske verktøy.
- I kapittel 4 beskrives de analytiske verktøyene som er utarbeidet.
- I kapittel 5 gis en kort vurdering og anbefaling om veien videre.
- I kapittel 6 er rapportens konklusjon.

I tillegg konkretiseres begrepene offensive og defensive cyberoperasjoner som benyttet i denne rapporten, i vedlegg A.

til FS 07. FFI-rapport 2007/02174. https://www.ffi.no/publikasjoner/arkiv/metode-for-langtidsplanlegging-stotte-til-fs-07

2 Fremgangsmåte

Arbeidet har i stort vært preget av iterative prosesser. Over tid har vi forsøkt å inkludere mer og mer relevant tematikk knyttet til cyberoperasjoner på en konsistent måte i det totale konseptuelle grunnlaget vi utvikler. Analytiske verktøy vokste gradvis frem som en mulig teknikk for å hjelpe både oss selv og andre med å etablere konsistente, sporbare argumentasjonskjeder. For et umodent felt under rask utvikling vurderte vi at slike verktøy er hensiktsmessige for å komme videre, fremfor å begi oss ut i spekulasjoner preget av høy usikkerhet og kort gyldighetstid.

I dette kapitlet beskriver vi først den grunnleggende tilnærmingen i prosjektets arbeid med cyberoperasjoner. Deretter omtaler vi et fundamentalt veivalg vi har stått overfor i vårt arbeid. Til sist gis en beskrivelse av utviklingen av verktøyene.

2.1 Grunnleggende tilnærming

Prosjektet jobbet innledningsvis etter en tilnærming som var sterkt knyttet til FFIs metode for støtte til langtidsplanlegging. Med utgangspunkt i studier av trender innen teknologiutvikling og elektromagnetiske og digitale trusler, skulle scenarioer bli brukt for å belyse hvordan cyberoperasjoner, IKT og elektronisk krigføring (EK) kunne påvirke fremtidens operasjoner. I prosjektets første år ble det således gjort et innledende arbeid med å spenne ut mulige scenarioer og utvikle en detaljert taktisk vignett tilhørende et valgt krisescenario. Anvendelsen av cyberoperasjoner ble så studert i den taktiske vignetten basert på informasjon om cyberoperasjoner fra åpne kilder og tidligere opparbeidet kunnskap om temaet.

Imidlertid ble det klart at denne tilnærmingen alene var utilstrekkelig for å belyse cyberoperasjoner på en god måte. Dette skyldes blant annet uklarheter ved implikasjonene av å anvende og forberede ulike typer cyberoperasjoner, og at vi ikke hadde tilstrekkelig innsikt i hvilke faktorer som burde inkluderes i analysene. Informasjonsgrunnlaget for cyberoperasjoner ble derfor vurdert som utilstrekkelig, og vi begynte å lete etter alternative tilnærminger som kunne hjelpe oss med å etablere dette.

Prosjektet iverksatte flere aktiviteter i denne sammenheng. Disse ga grunnlaget for og brakte frem de analytiske verktøyene. Vi forsøkte først å utforske cyberoperasjoner forholdsvis fritt, slik at vi kunne etablere et felles utgangspunkt for videre diskusjoner. Selv om friheten her var stor, så vi at både tekniske, operative og politiske forhold måtte ivaretas for ikke å utelate sentrale deler av problemkomplekset. Etter at dette arbeidet var godt i gang, startet vi med metodeutvikling for å kunne utforske utvalgte forhold rundt forsvarsplanlegging med cyberoperasjoner. Dette var delvis utledet fra og inspirert av metodikk for langtidsplanlegging.

Disse to arbeidene ble på mange måter kjernen i prosjektets aktiviteter for cyberoperasjoner. De ga prosjektet økt forståelse for hvilke forhold en stat må ta innover seg i utviklingen av innrettingen for sin cybervirksomhet. Samtidig forsterket arbeidet prosjektets inntrykk av at modenhetsnivået til cyberoperasjoner som fagfelt var langt unna modenhetsnivået til IKT som fagfelt.

Der hvor IKT-arbeidet til prosjektet hadde et reelt fagfelt å lene seg på, med modeller og kunnskap bygd opp over tid, startet cyberoperasjonsarbeidet i mye større grad på bar bakke.

Vurderingen av modenhetsnivået førte til en bevisstgjøring om at en klassisk stegvis flyt i arbeidet, hvor leveranser produseres sekvensielt, ville føre til markant lavere kvalitet. Risikoen for å måtte gjøre arbeid på nytt ville vært stor. Prosjektet valgte å følge en annen flyt, hvor flere produkter ble utviklet i parallell. Dette gjorde det mulig i større grad å skape konsistens på tvers i arbeidene. Tilbakemeldinger på arbeidene ble innhentet gjennom dialog med interessenter og prosjektrådsmøter underveis i prosjektet.

Etter hvert ble deler av disse to arbeidene videreutviklet på ulike måter. Blant annet ble arbeidene tatt med inn i den internasjonale forskningsgruppen Nato STO SAS-167 *Assessing the value of cyber operations in military operations*.[27] Gruppen ledes av FFI, og arbeidet med cyberoperasjoner i prosjektet har vekselvirket med arbeidet i forskningsgruppen. Mot slutten av prosjektet gikk vi tilbake til metodikk for langtidsplanlegging og studerte denne på ny i lys av ny kunnskap. Blant annet trakk vi på erfaringer fra tilsvarende arbeid i prosjektet innen IKT.[28] Til sist brukte vi den oppsamlede erfaringen til å utvikle en liste over problemstillinger for staten.

2.2 Et fundamentalt veivalg

Underveis i arbeidet ble det klart at vi stod foran et veivalg. Valget gikk ut på om vi skulle søke tilgang til høygradert nasjonal informasjon og å etablere de analytiske verktøyene i lys av dette, eller kun ta utgangspunkt i lavgradert og ugradert informasjon. Begge alternativene hadde sine styrker og svakheter.

Da vi forsøkte å trekke en parallell til andre områder som er inkludert i forsvarsplanlegging, fremstod det som tydelig for oss at det er behov for mye kunnskap, erfaringer og informasjon for å gjøre gode analyser. Eksempelvis vil dypere vurderinger av kapabiliteter og ytelse til et strukturelement trekke på informasjon om oppbygging, utrustning, operasjonsmåter og andre sentrale karakteristikker. For mange områder, som for eksempel en mekanisert brigade, har det bygd seg opp en stabil kunnskapsbase over lengre tid som også er lavgradert eller ugradert. For en cyberenhet – et slags «cyberstrukturelement» – vil dette omfatte en kunnskapsbase med detaljert og inngående informasjon om trusselaktørers og egne cyberenheters organisering, prosesser, aktiviteter, leveranser og kapasiteter. Dette er informasjon som de fleste nasjoner har gradert høyt med sterke restriksjoner på deling.

Vårt utgangspunkt var og er at slik informasjon vil være svært nyttig i arbeidet med analytiske verktøy. Vi antar at resultatet vil være økt kvalitet på enkelte områder og en bedre tilpasning til nasjonale forhold. Samtidig medfører anvendelsen av slik informasjon andre ulemper. For

[27] En forskningsgruppe under Nato Science and Technology Organization (STO).
[28] Farsund, B., Thuv, Aa., Hansen, B. J. (2022). *Hvordan håndtere IKT i Forsvarets langtidsplanlegging.* FFI-rapport 22/01569. https://ffi-publikasjoner.archive.knowledgearc.net/bitstream/handle/20.500.12242/3082/22-01569.pdf.

eksempel er det sterke restriksjoner på hvordan informasjonen kan behandles og deles. Samarbeid med andre forskere internasjonalt og enkelte komponenter i verktøyene vil også kunne bli graderte. Dette kan medføre en annen form for kvalitetstap da andre fageksperter ikke kan inkluderes i arbeidet.

I praksis ble denne beslutningen tatt for oss gjennom de begrensningene som pandemien ga i perioden 2020–2022. Den eneste farbare veien under store deler av prosjektets levetid var å basere seg på ugradert informasjon. Dette muliggjorde distribuert arbeid på ugraderte samhandlingsløsninger og internasjonalt samarbeid. Dette kan imidlertid ha resultert i mer komplekse og abstrakte verktøy, som krever mer innsats ved bruk.

Hvordan verktøyene hadde blitt dersom prosjektet hadde gått i den andre retningen, er vanskelig å slå fast. Det kan tenkes at vi hadde havnet på samme spor som nå, eller at vi hadde funnet andre tilnærminger. Uansett er vår vurdering at dersom sensitiv informasjon om cyberenheter senere blir tilgjengelig, kan verktøyene videreutvikles og løftes til et nytt nivå. Dette kan også gjelde mindre sensitiv og potensielt åpent publisert informasjon om cyberenheter, dersom denne informasjonen blir analysert og strukturert på riktig måte.

2.3 Utvikling av verktøyene

I alt fire verktøy har blitt utviklet i prosjektet.

1. Rammeverk for analyse av cyberoperasjoner. Dette er et første forsøk på å samle grunnleggende kunnskap om cyberoperasjoner på en strukturert måte. Arbeidet gikk i hovedsak ut på å identifisere sentrale faktorer som burde vurderes, om ikke hensyntas, i diskusjoner og analyser av cyberoperasjoner som et statlig virkemiddel med flere bruksområder. Identifikasjon av faktorene var basert på tidligere arbeider, interne diskusjoner og dialog med eksterne fageksperter. Etter hvert som dette arbeidet tok form ble det skilt ut en egen seksjon i rammeverket for fundamentale premisser. Disse premissene skulle fungere som et felles utgangspunkt som videre argumentasjon kunne bygge på. Faktorene ble samtidig forsøkt satt i et strukturert hierarkisk system.

2. Metode for å utforske mulige anvendelser av cyberoperasjoner i en gitt situasjon. Målet med metoden er å belyse noen av de samme forholdene som forsvarsplanlegging gjør, selv om detaljert informasjon om motpartens kapabiliteter og operasjoner i cyberdomenet mangler. I utviklingsarbeidet gikk vi inn i rollen som både angripende og forsvarende part, for å identifisere hvilke steg partene må gjennom for å planlegge hensiktsmessig bruk av cyberoperasjoner i en gitt situasjon. Metoden trekker brukerne gjennom en serie diskusjoner knyttet til disse stegene i en ordnet rekkefølge. Verktøyet er logisk koblet sammen med det første verktøyet ved at flere faktorer i rammeverket er referert til i metoden.

Med utgangspunkt i disse to sentrale verktøyene er verktøy tre og fire utviklet. Arbeidet med disse verktøyene er utført i Nato STO-forskningsgruppen SAS-167.[29]

3. Et sett matriser som spenner ut mulige situasjoner som cyberoperasjoner kan bli brukt i. Matrisene kompletterer metoden som allerede var utviklet. Innholdet i matrisene er utviklet fra betraktninger rundt aktør, mål, metode og middel, og offensiv og defensiv virkemiddelbruk. Arbeidet er utviklet med Nato som en av aktørene og krever derfor noe tilpasning til nasjonal kontekst.

4. En stegvis prosessbeskrivelse for inkludering av cyberoperasjoner i planlegging og gjennomføring av militære operasjoner. Dette er en direkte videreutvikling og tilpasning av metoden i verktøy 2, som i større grad tar hensyn til arbeidsflyten i militære planprosesser. I arbeidet tok vi utgangspunkt i vår kjennskap til militære planprosesser for å tilpasse metodens steg til dette.

Et kompletterende arbeid ble utført i tillegg til verktøyene.[30] Dette inkluderer en vurdering av egnetheten til scenario- og kapabilitetsbasert metodikk for langtidsplanlegging for cyberoperasjoner, og en detaljering av problemstillinger en stat må adressere. Denne listen over problemstillinger ble til slutt tatt videre til en litt bredere og mer generisk liste også utover forsvarsplanlegging.

[29] Begge verktøyene er i skrivende stund fortsatt under utvikling i gruppen.
[30] Dette arbeidet er også dokumentert i denne rapporten, se kapittel 4.5.

3 Utfordringer ved analyse og utvikling av verktøy

Ved analyse av cyberoperasjoner og utvikling av analytiske verktøy møter vi en rekke utfordringer. Hvilke utfordringer vi møter, og hvor vanskelige disse er å håndtere, beror naturligvis på hva slags analyser vi ønsker å gjøre og typen verktøy vi søker å utvikle. Gitt en ambisjon om gjøre mer helhetlige vurderinger av cyberoperasjoner i forsvarsplanlegging og i planlegging og gjennomføring av militære operasjoner, er vi først nødt til å forstå cyber-operasjoner som et statlig virkemiddel. Dette skyldes at mange premisser og forutsetninger knyttet til anvendelsen av cyberoperasjoner i militær konktest er knyttet til statens anvendelser i andre kontekster. Grunnleggende utfordringer ved analyse av cyberoperasjoner som statlig virkemiddel vil dermed ha implikasjoner for videre analyser.

I dette kapitlet ser vi nærmere på utfordringene vi har identifisert. Vi ser først på utfordringer ved analyser av cyberoperasjoner som et statlig virkemiddel. Med dette som bakteppe ser vi mer spesifikt på hvorfor det er utfordrende å inkludere cyberoperasjoner i langtidsplanlegging, og i planlegging og gjennomføring av militære operasjoner.[31]

I sum har vi identifisert tolv overordnede utfordringer, se figur 3.1.

Utfordringer
Analyse av cyberoperasjoner som et statlig virkemiddel 1. Det er mangel på relevant empiri og teori 2. En stat har konkurrerende interesser og står i dilemmaer 3. Virkemidlet har særegne egenskaper
Inkludere cyberoperasjoner i langtidsplanlegging 4. Å utforske mulige cyberrelaterte trusler grundig er vanskelig 5. Hvordan krav bør utledes er ikke kjent 6. Det er store informasjonsmangler knyttet til referanseenhetene 7. Ytelsen til referanseenhetene er ustabil og usikker av natur 8. Scenarioene ilegges betydning utover den tiltenkte
Inkludere cyberoperasjoner i planlegging og gjennomføring av militære operasjoner 9. Meget høy grad av hemmelighold ved offensive cyberoperasjoner 10. Ulike planleggings- og gjennomføringsrytmer 11. Kommunikasjonsutfordringer mellom fageksperter og annet militært personell 12. Manglende kunnskap om egen avhengighet av IKT

Figur 3.1 Oversikt over identifiserte utfordringer.

[31] Utfordringene kan deles inn på ulike måter, og det er sammenhenger mellom dem. Vi diskuterer de mer grunnleggende utfordringene i kapittel 3.1, før mer spesifikke utfordringer omtales i kapittel 3.2 og 3.3.

De identifiserte utfordringene er i hovedsak basert på egne erfaringer som analytikere. Vi har likevel forsøkt å knytte utfordringene til åpne kilder der vi ser at liknende vurderinger og erfaringer er gjort.

3.1 Analyse av cyberoperasjoner som et statlig virkemiddel

Mange stater bruker cyberoperasjoner som virkemiddel for å fremme egne interesser overfor omverdenen. De brukes i fred, krise og væpnet konflikt, og anvendelsen går fra taktisk og kortsiktig til strategisk og langsiktig. Det er mange uklare sammenhenger mellom tekniske, operative og strategiske forhold, og mellom årsak-virkning generelt. Dette gjør det vanskelig å vurdere sentrale sider ved cyberoperasjoner på samme måte som kinetiske virkemidler. Særlig tre utfordringer utpeker seg:

- Det er mangel på relevant empiri og teori (kapittel 3.1.1).
- En stat har konkurrerende interesser og står i dilemmaer (kapittel 3.1.2).
- Virkemidlet har særegne egenskaper (kapittel 3.1.3).

Disse utfordringene sprer seg også videre inn i analyser knyttet til langtidsplanlegging og planlegging og gjennomføring av militære operasjoner.

3.1.1 Det mangler relevant empiri og teori

Empiri

Å hevde at det er mangel på relevant empiri for cyberoperasjoner kan virke overraskende på mange. Medier og andre åpne kilder rapporterer relativt hyppig om ulike former for ondsinnede aktiviteter i cyberdomenet. Det er etter hvert ganske mange aktører som bidrar til åpne data om cyberoperasjoner eller som på andre måter forsøker å belyse ulike sider ved dette temaet. I tillegg til nyhetsmedier er det en rekke uavhengige fageksperter, analytikere, statlige virksomheter og kommersielle selskaper som bidrar åpent med sine kommentarer og analyser.

Den store majoriteten av rapporterte hendelser skjer på eller via internett, og dekker et bredt spekter av aktiviteter. Dette inkluderer kriminelle aktiviteter som løsepengevirus (*ransomware*) og hacktivisme, etterretningsoperasjoner som blir oppdaget og ulike former for påvirkningsoperasjoner.[32] Begrepsbruken varierer noe – cyberoperasjoner, cyberangrep, «*data hack*» – men det tegnes et bilde av et stort omfang av oppdagede aktiviteter og et omfattende empirisk grunnlag.

[32] Se for eksempel *BBC News*-artikler sortert under *cyber-security.* https://www.bbc.com/news/topics/cz4pr2gd85qt. «Påvirkningsoperasjoner» omfatter i denne sammenheng ofte aktiviteter uten bruk av uautoriserte tilganger, som spredning av falske nyheter på sosiale medier.

Kvaliteten og dybden i datamaterialet er imidlertid meget varierende, og også mengden av tilgjengelige data varierer stort avhengig av hva som er i fokus. Noen ganger kan det også diskuteres hvor skillelinjene går mellom empiri og kvalifiserte vurderinger. Svært ofte er det for eksempel kun et begrenset antall aktører eller individer som sitter nærme faktiske hendelsesforløp eller observerer direkte hva trusselaktører gjør, mens andre ser bruddstykker gjennom flere ledd med beskrivelser, vurderinger og aggregeringer. Hvordan det empiriske grunnlaget kan benyttes på en analytisk forsvarlig måte er derfor utfordrende.

Rent tematisk er det mange sider ved cyberoperasjoner som omtales i åpne kilder. Blant annet finnes data om:

- trusselaktører som er aktive
- skadevare som benyttes
- spesifikke hendelser som inntreffer
- hendelseshåndteringen til rammede aktører
- staters tilnærminger[33]
- cyberoperasjoner i militær kontekst

Trusselaktører som er aktive. En rekke sikkerhetsmiljøer publiserer sine analyser og vurderinger av infrastrukturen, operasjonsmåtene, skadevaren og målsettingene til trusselaktører. Dette inkluderer både trusselaktører som anses å være rene kriminelle organisasjoner og de som trolig er tilknyttet en stat. Enkelte miljøer leter kontinuerlig etter slike aktører og følger aktivt med på dem over lengre tid. Noen av vurderingene gjøres basert på åpne kilder, mens andre beror på tilgang til mer lukket informasjon. Her er det ofte naturlige begrensninger på hvor mye informasjon et miljø kan få tak i om trusselaktørenes interne organisering, prosesser og vurderinger. Enkelte miljøer, som typisk er aktører i sikkerhetsbransjen, klarer likevel å oppnå god innsikt i ulike trusselaktører.[34]

Skadevare som benyttes. Det empiriske tilfanget av ren skadevare er stort. En av de største kommersielle aktørene, VirusTotal, tilbyr tilgang til en database med flere milliarder eksemplarer av potensielt skadelige filer, og de produserer flere millioner nye automatiske filanalyser per dag.[35] Standardiserte datasett til forskningsformål finnes også. For eksempel inneholder data-

[33] Dette inkluderer både hva statene selv sier, og hva andre attribuerer av aktiviteter til dem.
[34] Se for eksempel analyse av målsettinger og modus operandi for trusselaktøren DarkSide i Gallager, S., Loman, M. Mackenzie, P., Polat, Y. (2021, 11. mai). *A defender's view inside a DarkSide ransomware attack.* Sophos. https://news.sophos.com/en-us/2021/05/11/a-defenders-view-inside-a-darkside-ransomware-attack/; analysen av aktøren APT 1 i Mandiant (2013). *APT1 Exposing One of China's Cyber Espionage Units*. https://www.mandiant.com/sites/default/files/2021-09/mandiant-apt1-report.pdf.
[35] Tall hentet fra Virustotal (2023, 7. mars). *Intelligence Overview*. https://www.virustotal.com/gui/intelligence-overview.

settet SoReL-20M fra Sophos og Reversing Labs 20 millioner eksemplarer av bekreftede skadevarefiler.[36] Slike databaser sier i utgangspunktet lite om trusselaktøren og trusselaktørens intensjon. Empirien her består i stor grad av enkeltstående rapporter fra sikkerhetsselskap som manuelt analyserer skadevare i en gitt kontekst, typisk i forbindelse med konkrete hendelser.

Spesifikke hendelser som inntreffer. Mange aktører analyserer og diskuterer spesifikke hendelser. Særlig større hendelser blir ofte diskutert og kommentert over tid av journalister og eksperter. Blant annet diskuteres forhold som tekniske hendelsesforløp, tidslinjer, aktører, konsekvenser og reaksjoner. Her viser imidlertid en svakhet i det empiriske grunnlaget seg, da det som regel er store informasjonsmangler om hva som faktisk har skjedd selv ved velkjente hendelser. Eksempelvis er det ofte stor usikkerhet om både tekniske og taktiske forhold, og en klar konsensus blir ikke etablert blant ekspertene. Avhengig av hvem en velger å tro på er det mulig å trekke motstridende konklusjoner. Dette gjelder både hvem som står bak, detaljer i hendelsesforløpet og eventuelle operative konsekvenser.[37]

Hendelseshåndteringen til rammede aktører. Når en hendelse rammer en aktør vil aktøren typisk gjøre vurderinger og iverksette tiltak som en del av sin hendelseshåndtering. Rammede aktører går imidlertid sjelden ut med detaljert informasjon om hendelsene og håndteringen. Media omtaler ofte hendelser når de inntreffer eller blir oppdaget, men de interne analysene og vurderingene til aktørene blir sjelden offentliggjort. Dette bidrar til at konsensus om hendelsene er vanskelig å etablere. Det hender dog at enkelte detaljer blir delt av aktørene eller på andre måter kommer ut i offentligheten.[38]

Staters tilnærminger. Empiri om staters aktiviteter i cyberdomenet kan i visse tilfeller sies å være det samme som empiri om trusselaktører. Disse trusselaktørene har da blitt vurdert til å ha en klar tilknytning til en stat. I visse tilfeller kan man ut ifra aktivitetenes innretting gjøre noen antakelser om hvorfor staten handler som den gjør, for eksempel i lys av annen politikk som staten fører. Har man ikke slik trusselaktørempiri, kan man likevel få en form for empiri gjennom staters publiserte doktriner, strategier og policyer om cybersikkerhet og cyberoperasjoner

[36] Sophos, Reversing Labs (2023, 7. mars). *Sophos-ReversingLabs 20 million sample dataset*. https://github.com/sophos/SOREL-20M.

[37] Se for eksempel motstridende meninger i Blessing, J. (2022, 2. september). *Revisiting the Russain Viasat Hack: Four Lessons About Cyber on the Battlefield*. American Enterprise Institute. https://www.aei.org/foreign-and-defense-policy/revisiting-the-russian-viasat-hack-four-lessons-about-cyber-on-the-battlefield/; og Zetter, K. (2022, 26. september). *Viasat Hack «Did Not» Have Huge Impact on Ukrainian Military Communications, Official Says.* https://zetter.substack.com/p/viasat-hack-did-not-have-huge-impact.

[38] Se for eksempel beskrivelse av hendelsesforløp og enkelte tiltak og vurderinger i US Congress (2016). *The OPM Data Breach: How the Government Jeopardized Our National Security for More than a Generation.* Majority Staff Report Committee on Oversight and Government Reform U.S. House of Representatives 114th Congress. https://republicans-oversight.house.gov/wp-content/uploads/2016/09/The-OPM-Data-Breach-How-the-Government-Jeopardized-Our-National-Security-for-More-than-a-Generation.pdf;
Greenberg, A. (2018, 22. august). The Untold Story of NotPetya, the Most Devastating Cyberattack in History. *Wired.* https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/; Van Hees, M. (2020). *The 2017 MAERSK Cyber Incident. Learning from and applying the Lessons of a Major Cyber Incident* https://fhi.nl/app/uploads/sites/75/2020/10/201029-FHI_Maersk.pdf; Ashton, G. (2020) *Maersk, me & Notpetya.* https://gvnshtn.com/posts/maersk-me-notpetya/.

dersom det eksisterer.[39] Disse dokumentene går imidlertid svært sjeldent inn i hvordan staten har kommet frem til de posisjoner som er stadfestet og hvilke vurderinger og avveiinger som er gjort underveis. Det samme blir heller ikke automatisk belyst ved å lese omtaler av eller observere enkelte av aktivitetene som en stat utfører. Det er derfor lite tilgjengelig empiri som sier noe om statenes egne vurderinger av cyberoperasjoner som et statlig virkemiddel.

Militær kontekst. Det siste året har vi sett et økt fokus på cybertematikk i militær kontekst, i stor grad grunnet krigen i Ukraina. En rekke aktører har blant annet begynt å føre oversikter over cyberrelaterte hendelser knyttet til denne krigen.[40] Enkelte andre aktører, med egne informasjonskilder, beskriver også et mer nyansert bilde av cyberoperasjoner globalt. For eksempel blir målrettet bruk av løsepengevirus og andre destruktive teknikker tillagt stater som er i konflikt med hverandre.[41] Deler av dette datamaterialet er imidlertid svært aggregert, og det er vanskelig å få innsikt i de reelle datapunktene som foreligger. Statene selv er som regel meget tilbakeholdne med hva de faktisk gjennomfører av cyberoperasjoner i militære operasjoner. Det åpne empiriske grunnlaget for cyberoperasjoner i militær kontekst ser derfor fremdeles ut til å være meget tynt.[42]

Teori

Den teoretiske forståelsen for cyberoperasjoner som et statlig virkemiddel er fremdeles på et tidlig stadium, og svakhetene i det empiriske grunnlaget bidrar til at utviklingen av teori går sakte.[43] Det teoretiske grunnlaget varierer noe ut i fra hvilket grunnperspektiv en ønsker å tolke

[39] Se for eksempel Laudrain, A. P. B. (2019, 26. februar). France's New Offensive Cyber Doctrine. *Lawfareblog.* *https://www.lawfareblog.com/frances-new-offensive-cyber-doctrine*; Public Safety Canada (2020, 31. juli). *Cyber Security in the Canadian Federal Government*. https://www.publicsafety.gc.ca/cnt/ntnl-scrt/cbr-scrt/fdrl-gvrnmnt-en.aspx; U. S. The White House (2023). *National Cybersecurity Strategy*. https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf.

[40] Se for eksempel National Security Archive (2022). *Cyber Vault Project – The Ukraine Project.* https://nsarchive.gwu.edu/project/ukraine-cyber-project; The Cyber Peace Institute (2022). *Cyber Attacks in Times of Conflict Platform #Ukraine* https://cyberconflicts.cyberpeaceinstitute.org/.

[41] Se for eksempel Microsofts vurderinger av krigen i Ukraina og spenningene mellom Iran og Israel i Microsoft (2022c, s. 35, s. 38). *Digital Defence Report 2022*. https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE5bUvv?culture=en-us&country=us.

[42] Dette gjelder både offensive og defensive cyberoperasjoner i militær kontekst. Det er veldig lite åpen empiri som entydig belyser operativ nytte av cyberoperasjoner for effekt, inklusive cyberoperasjoner som styrkemultiplikator. For defensive cyberoperasjoner er det empiriske grunnlaget om mulig enda tynnere, med lite informasjon om operasjonene i seg selv og tilhørende operative konsekvenser. Ofte er koblingen til en spesifikk militær operasjon svak. Se f.eks. omtalen av defensive cyberoperasjoner i Corera, G. (2022, 30. oktober) Inside a US military cyber team's defence of Ukraine. *BBC News*. https://www.bbc.com/news/uk-63328398; U.S. Cyber Command (2022, 17. oktober 2022). *CYBERCOM executed global cyberspace defensive operation*. https://www.cybercom.mil/Media/News/Article/3190716/cybercom-executed-global-cyberspace-defensive-operation/. For påstander om nytte av offensive cyberoperasjoner som styrkemultiplikator, se for eksempel Smeets, M. (2018). The Strategic Promise of Offensive Cyber Operations. *Strategic Studies Quarterly*, *12*(3), 90-113. For et motstridende syn, se Maschmeyer, L. (2022b, 12. juli). Infiltrate, Exploit, Manipulate: Why the Subversive Nature of Cyber Conflict Explains Both Its Strategic Promise and Its Limitations. *Lawfareblog.* https://www.lawfareblog.com/infiltrate-exploit-manipulate-why-subversive-nature-cyber-conflict-explains-both-its-strategic.

[43] For eksempler på teori, se Maschmeyer, L. (2022a). Subversion, cyber operations, and reverse structural power in world politics. *European Journal of International Relations*, 13540661221117052. https://doi.org/10.1177/13540661221117051; Maschmeyer, L. (2021). The Subversive Trilemma: Why Cyber Operations Fall Short of Expectations. *International Security*, *46*(2), 51–90.https://doi.org/10.1162/isec_a_00418.;

empirien ut ifra. For eksempel kan cyberoperasjoner for etterretning tolkes inn i en etterretningsramme. Eksisterende erfaringer, tradisjoner og kutymer innen etterretning kan være et bakteppe for å vurdere alvorlighetsgrad og hensiktsmessig respons ved hendelser. Videre kan en slik ramme være med på å forme egne cyberoperasjoner for etterretning. Denne rammen er imidlertid i mindre grad egnet for å forstå mulige operative og strategiske implikasjoner av cyberoperasjoner for effekt i militære operasjoner, utover implikasjoner for etterretningsvirksomheten.

For modeller og teorier for cyberoperasjoner for effekt er etterretningsperspektivet alene utilstrekkelig. Slike modeller og teorier bør omfatte cyberoperasjoner for effekt fra et statsperspektiv, både sivilt og militært, og dekke tekniske, operative og politiske forhold. De bør også kunne relateres til den empirien som finnes. For den militære konteksten spesielt mangler muligheten til å analysere og simulere anvendelsen av cyberoperasjoner som et militært virkemiddel slik en gjør med andre strukturelementer.

Defensive cyberoperasjoner kan også forstås på ulike måter. Dette påvirker hvilken kunnskap det er behov for. Forstått som et teknisk virkemiddel anvendt i egne nettverk og systemer for å beskytte militære operasjoner, er det kunnskap om de tekniske systemene, de militære operasjonene og avhengigheten mellom disse som står sentralt. Forstått i tillegg som et virkemiddel som påvirker oppførselen til trusselaktører, både i og utenfor cyberdomenet, kommer det inn en ytterligere operativ og politisk dimensjon. Dette gjelder både når defensive cyberoperasjoner er avgrenset til egne nett, og når de utføres utenfor dem. Dersom en stat ser på virkemidlet som et aktivt statlig virkemiddel, forsterkes den politiske dimensjonen ytterligere.

Dersom tolkningen begrenses til at defensive cyberoperasjoner kun er et teknisk virkemiddel, reduseres kunnskapsbehovet til teknisk-operative forhold. Dersom en bredere tolkning legges til grunn, er det behov for kunnskap om ytterligere operative og potensielt politiske forhold.[44] Hvordan analyser av defensive cyberoperasjoner med en slik bred tolkning bør gjøres, er imidlertid uklart.

3.1.2 En stat har konkurrerende interesser og står i dilemmaer

Når en stat skal anvende eller planlegge for anvendelsen av cyberoperasjoner, vil staten kunne ha motstridende eller konkurrerende interesser som trekker i ulike retninger. Hva som er den mest hensiktsmessige bruken av cyberoperasjoner for en stat kan derfor være uklart. Dette medfører at staten må gjør en rekke avveiinger og løse dilemmaer som oppstår. Enkelte

Harknett, R. J., & Smeets, M. (2022). Cyber campaigns and strategic outcomes. *Journal of Strategic Studies*, 45:4, 534-567, DOI: https://doi.org/10.1080/01402390.2020.1732354; Smeets, M. (2018). The Strategic Promise of Offensive Cyber Operations. *Strategic Studies Quarterly*, *12*(3), 90–113; Egloff, F. J., & Maschmeyer, L. (2021). Shaping not Signaling: Understanding Cyber Operations as a Means of Espionage, Attack, and Destabilization. *International Studies Review*, *23*(3), 997–998. https://doi.org/10.1093/isr/viaa086; Fischerkeller, M. P., & Harknett, R. J. (2020). *Cyber Persistence Theory, Intelligence Contests and Strategic Competition* (s. 534–567). https://www.tandfonline.com/doi/full/10.1080/01402390.2020.1732354; Libicki, M., & Tkacheva, O. (2020). Cyberspace Escalation: Ladders or Lattices? *Cyber Threats and NATO 2030: Horizon Scanning and Analysis.* https://ccdcoe.org/uploads/2020/12/Cyber-Threats-and-NATO-2030_Horizon-Scanning-and-Analysis.pdf

[44] Som et eksempel ser Forsvarets konsept for defensive cyberoperasjoner ut til å legge en slik bredere tolkning til grunn. Se Cyberforsvaret (2022, 1. juli). *Konsept for defensive cyberoperasjoner.*

dilemmaer må vurderes fra sak til sak, mens andre er mer grunnleggende og påvirker innrettingen av statens virksomhet generelt. Dette gjelder for både offensive og defensive cyberoperasjoner.

En type dilemma som oppstår for offensive cyberoperasjoner er knyttet til graden av hemmelighold og deling av informasjon. Rotårsaken er at offensive cyberoperasjoner i stor grad må tilpasses målsystemet som en bryter seg inn i og potensielt ønsker å utløse effekt i, og dette krever mye innsats. Det er ikke mye informasjon om potensielle målsystemer eller likende som trenger å komme ut før det er stor risiko for at motparten kan oppdage og spolere operasjonene. Gjennom dette kan også motparten oppnå innsikt i statens prioriteringer og kapabiliteter. Derfor legger mange stater opp til meget strengt hemmelighold. Ulempen er at mange statlige aktører som kunne ha dratt nytte av mer informasjon for å løse sine oppgaver ikke får denne, og dermed får utfordringer i sitt eget arbeid. I tillegg kan ulike diskurser om cyberoperasjoner både i offentligheten og i mer lukkede miljøer bli mindre opplyst. Hva en hensiktsmessig balanse for hemmelighold og informasjonsdeling vil være for en gitt stat må trolig utvikles over tid.

Et annet velkjent dilemma er om cyberoperasjoner skal brukes til etterretning eller for å oppnå effekt. Årsaken til dette dilemmaet er at tilganger til eksterne nettverk og systemer som er etablert i forbindelse med cyberoperasjoner for etterretning, ofte er utgangspunktet for cyberoperasjoner for effekt. Dersom tilgangene brukes til effektoperasjoner, må tilgangene som regel anses som tapt for videre etterretningsformål.[45] Dette dilemmaet er særlig aktuelt når det kommer et ønske om å bruke cyberoperasjoner for effekt i militære operasjoner, som da potensielt vil føre til tap av etterretningstilganger som er av stor betydning i fred. Bruken av cyberoperasjoner i militær kontekst er dermed tett knyttet til, og påvirkes gjensidig av, anvendelsen i andre sammenhenger.

Et relatert dilemma er i hvilken grad negative konsekvenser for fredstidsvirksomheten skal godtas for å forberede mulige fremtidige effektoperasjoner som kanskje aldri vil bli benyttet. Dette dilemmaet oppstår blant annet fordi forberedelser til de ønskede effektoperasjonene ofte må gjøres i fred. Dette er ikke nødvendigvis i seg selv problematisk eller uvanlig for militære virkemidler, men det kan fremtvinge harde prioriteringer som kan gå ut over ressursene til fredstidsvirksomheten for øvrig. Dessuten kan det fremtidige mulighetsrommet for fredstidsvirksomheten også bli negativt påvirket dersom effektoperasjonene faktisk blir gjennomført. Dette skyldes at teknikker og metoder blir identifisert, og dermed ikke kan brukes lenger. I tillegg kan pågående og tidligere etterretningsoperasjoner som bruker eller har brukt de samme teknikkene også bli oppdaget og attribuert. Dette gjelder statens egne operasjoner og potensielt operasjonene til allierte.

[45] Se for eksempel US Joint Chiefs of Staff (2018, s. IV-7). *Joint Publication 3-12 Cyberspace Operations*. https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf: "[A] planning concern is that maneuver and fires in red and gray cyberspace could potentially compromise intelligence collection activities sources and methods. To the maximum extent practicable, an IGL [intelligence gain/loss] assessment is required prior to executing such actions." En parallell finnes også hos kommersielle aktører, når de vurderer hvor mye informasjon de skal gå ut med om trusselaktører som de følger med på. Se for eksempel Mandiant (2013, s. 6). *APT1 Exposing One of China's Cyber Espionage Units*. https://www.mandiant.com/sites/default/files/2021-09/mandiant-apt1-report.pdf

Et annet relatert dilemma er om risikoen ved å jobbe aktivt mot et militært mål i fredstid skal godtas for å øke evnen til å gjennomføre mulige fremtidige effektoperasjoner. Dersom målsystemet kompromitteres og systemet ikke har noen særlig etterretningsverdi i fredstid, faller etterretningsoperasjoner vekk som mulig forklaring dersom aktiviteten blir oppdaget. Aktiviteten kan bli ansett å være mer aggressiv enn «normal» etterretning, og potensielt forberedelser på en destruktiv operasjon. Hvordan den rammede staten vil reagere på dette er heftet med stor usikkerhet. Den utøvende staten kan også få et forklaringsproblem overfor andre stater, med mindre slike operasjoner allerede er en kjent del av statens virkemiddelbruk. Ikke minst kan det være juridiske og etiske forhold som begrenser mulighetene for slike aktiviteter.

I statens relasjoner til allierte kan det også oppstå et dilemma om en ønsket cyberoperasjon skal gjennomføres på tross av ulempen den kan påføre allierte stater. Ethvert målsystem som en stat ønsker å rette en cyberoperasjon mot, kan allerede være et mål for cyberoperasjoner fra en alliert stat. Uten koordinering mellom allierte stater vil disse cyberoperasjonene kunne gå i bena på hverandre.[46] I tillegg til at selve cyberoperasjonene ikke oppnår sine målsettinger, kan dette ha negative konsekvenser for relasjonen til den allierte staten. Staten må dermed bestemme seg for om nytten av cyberoperasjonene vil være verdt et slikt utfall. I hvilken grad potensialet for slike utilsiktede konsekvenser vil være retningsstyrende vil trolig variere fra stat til stat. En kan se for seg at mindre stater vil være mer lydhøre for ønskene til større allierte stater enn motsatt, selv om dette er avhengig av den sikkerhetspolitiske konteksten.

Ved anvendelsen av defensive cyberoperasjoner kan det også oppstå dilemmaer mellom å øke antatt effektivitet på den ene siden, og å etterleve etablerte prinsipper og jus på den andre siden. Særlig vil stater som er liberale demokratier kunne oppleve motstridende interesser. Dette er noe uavhengig av den doktrinelle innpakningen av defensive cyberoperasjoner. Særlig kan det oppstå dilemmaer i skillet mellom den militære og den sivile sfære, og det offentlige og private. Folkerett og prinsipielle ansvarsfordelinger på samfunnsnivå kan, med gode grunner, her forhindre full utnyttelse av teknologiske muligheter og blokkere samarbeid mellom aktører. Et eksempel på dette kan være i hvilken grad Forsvaret eller andre statlige entiteter skal få tilgang

[46] For et eksempel hvor to kriminelle aktører går i bena på hverandre, se Palmer, D. (2022, 1. mars). This is what happens when two ransomware gangs hack the same target - at the same time. *Zdnet.* https://www.zdnet.com/article/two-ransomware-gangs-hacked-the-same-target-at-the-same-time-heres-what-happened-next/. Det finnes også eksempler på at statlige aktører kompromitterer og utnytter tilgangene til andre statlige aktører. Se for eksempel NCSC (2019, 21. oktober) *Advisory: Turla group exploits Iranian APT to expand coverage of victims.* https://www.ncsc.gov.uk/news/turla-group-exploits-iran-apt-to-expand-coverage-of-victims; Corera, G. (2019, 21. oktober) Russian hackers cloak attacks using Iranian group. *BBC News.* https://www.bbc.com/news/technology-50103378; Applebaum, J., Gibson, A., Guarnieri C., Müeller-Maughn, A., Poitras, L., Rosenbach, M., Ryge, L., Schmundt, H., Sontheimer, M. (2015, 17. januar) NSA Preps America for Future Battle. *Der Spiegel.* https://www.spiegel.de/international/world/new-snowden-docs-indicate-scope-of-nsa-preparations-for-cyber-battle-a-1013409.html. Enkelte publiserte, offisielle dokumenter ser også ut til å peke behovet for koordinering mellom stater. Se UK MOD (2022 s. 57) *Cyber primer (3rd)*: "The span of military, multi-agency and multinational partners conducting cyber activities means simple supported/supporting relationships are more complex in reality. Instead, the commander and specialist staff must understand and manage multiple relationships, each of which is governed by particular freedoms and constraints. Government and industry must adopt a cautious but trusted partnered approach to cyber activity, orchestrated across strategic to tactical levels of command. This also applies to allies and coalition partners." https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1108280/Cyber_Primer_Edtion_3.pdf.

til kommersielle eller andre aktørers nettverk og systemer for å gjennomføre overvåking og håndtering.[47] Et annet eksempel er hvilken folkerettslige status personellet som ender opp med å ha en rolle i understøttelsen av militær operativ evne skal ha.[48]

Staten vil også møte et dilemma der valget står mellom å styrke cybersikkerhetsnivået til staten eller å opprettholde et mulighetsrom for offensive operasjoner. Når staten blir klar over en ukjent sårbarhet i egne systemer som også er tilstede i motparts systemer, må staten bestemme seg for hva som skal gjøres med sårbarheten. En mulighet er at sårbarheten kan tettes for å øke egen sikkerhet, men da kan en motpart potensielt se hva som er gjort og tette sine egne systemer. Da fjernes en potensiell angrepsvektor fra statens offensive mulighetsrom. Alternativt kan sårbarheten være forbeholdt offensiv bruk. Da risikerer staten at sårbarheten, som da blir værende i egne systemer (offentlige og private), også blir funnet og utnyttet av trusselaktører.[49] Et relatert dilemma er om staten bevisst skal bygge sårbarheter eller «bakdører» inn i programvare, algoritmer og protokoller som den kan utnytte ved behov, eller lage løsninger som er så sikre som mulig. Dette kan både skje åpent og skjult.[50] Slike bakdører kan imidlertid også bli overtatt av trusselaktører.[51]

Innad i en stat vil en også finne interessenter og aktører med ulike roller og ansvar. Disse kan, grunnet sine individuelle mandater, ha forskjellige interesser. Dette kan resultere i at aktørene

[47] Se for eksempel diskusjonen om hvor mye tilgang NSM skal ha til systemer hos rammede virksomheter for å bistå i hendelseshåndtering. Bruvoll, J., Thuv, Aa., Enemo, G. (2022, s. 34, 53–54). Håndtering av IKT-sikkerhetshendelsene i Helse Sør-Øst og fylkesmannsembetene - en vurdering. FFI-rapport 20/01560. https://www.ffi.no/publikasjoner/arkiv/handtering-av-ikt-sikkerhetshendelsene-i-helse-sor-ost-og-fylkesmannsembetene-en-vurdering. Et annet tilfelle er lagring og analyse av data som passerer landegrenser. Se for eksempel FAD (2008, 8. desember) *Rapporter om den svenske FRA-loven.* Pressemelding. https://www.regjeringen.no/no/dokumentarkiv/stoltenberg-ii/sd/Nyheter-og-pressemeldinger/pressemeldinger/2008/rapporter-om-den-svenske-fra-loven-/id538690/; FD (2018, 12. november) *Ny lov om Etterretningstjenesten på høring*. Pressemelding. https://www.regjeringen.no/no/dokumentarkiv/regjeringen-solberg/aktuelt-regjeringen-solberg/fd/pressemeldinger/2018/ny-lov-om-etterretningstjenesten-pa-horing/id2618704/.

[48] Se for eksempel Riksrevisjonens kommentarer om uklare folkerettslige konsekvenser ved strategisk samarbeid. Riksrevisjonen (2022, s. 19). *Riksrevisjonens undersøkelse av Forsvarets informasjonssystemer for kommunikasjon og informasjonsutveksling i operasjoner*. Ugradert versjon av Dokument 3:3 (2022−2023). https://www.riksrevisjonen.no/rapporter-mappe/no-2022-2023/undersokelse-av-forsvarets-informasjonssystemer-informasjonssystemer-til-bruk-i-operasjoner/.

[49] Enkelte land har innført prosesser for å avklare hvordan dette dilemmaet skal håndteres fra sak til sak. Se for eksempel U.S. The White House (2017, 15. november). *Vulnerabilities Equities Policy and Process for the United States Government.* https://trumpwhitehouse.archives.gov/sites/whitehouse.gov/files/images/External%20-%20Unclassified%20VEP%20Charter%20FINAL.PDF; Thompson, A. W. (2021, 13. januar). Assessing the Vulnerabilities Equities Process, Three Years After the VEP Charter. *Lawfareblog.* https://www.lawfareblog.com/assessing-vulnerabilities-equities-process-three-years-after-vep-charter.

[50] Dette gjelder både sårbarheter som stater selv bygger inn, dersom de har tilgang og mulighet til det, og forsøk på å instruere kommersielle virksomheter til å bygge inn sårbarheter i deres produkter. Se for eksempel Gallagher, S. (2015, 14. desember). What the government should've learned about backdoors from the Clipper Chip. *Ars Technica.* https://arstechnica.com/information-technology/2015/12/what-the-government-shouldve-learned-about-backdoors-from-the-clipper-chip/; Ball, J., Borger, J., Greenwald, G. (2013, 6. september). Revealed: How US and UK spy agencies defeat internet privacy and security. *The Guardian.* https://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security; Newman, L. H. (2020, 16. januar). This Apple-FBI Fight Is Different From the Last One. *Wired.* https://www.wired.com/story/apple-fbi-iphone-encryption-pensacola/

[51] For et eksempel hvor dette sannsynligvis har skjedd, se Green, M. (2015, 22. desember) *On the Juniper backdoor*. A Few Thoughts on Cryptographic Engineering. https://blog.cryptographyengineering.com/2015/12/22/on-juniper-backdoor; Robertson, J. (2021, 2. september). Juniper Breach Mystery Starts to Clear With New Details on Hackers and U.S. Role. *Bloomberg.* https://finance.yahoo.com/news/juniper-breach-mystery-starts-clear-130016591.html.

kan komme med motstridende anbefalinger om hva staten bør prioritere og gjøre, både generelt og i gitte situasjoner. Staten kan dermed ende opp i dilemmaer der den må velge hvilke synspunkter som skal tillegges størst vekt. Dette kan omfatte innrettingen av både offensive og defensive cyberoperasjoner, og prioriteringer mellom dem.

3.1.3 Virkemidlet har særegne egenskaper

Cyberoperasjoner skiller seg på flere områder fra operasjoner som utføres på land, i luft og til sjøs.[52] Tilsvarende skiller «cyberstrukturelementene» (cyberenhetene) seg fra mer regulære strukturelementer. Dette skyldes i stor grad at cyberdomenet er et relativt nytt menneskeskapt domene med særegne karakteristikker, og at selve domenet er i kontinuerlig utvikling. Spesielt følgende egenskaper utpeker seg:

- rask utvikling
- begrenset nytte av eksisterende historikk og empiri
- ustabilitet og usikkerhet om forventet ytelse og suksessrater
- store kompetansekrav
- ulike referanserammer og vokabular

Rask utvikling. Dagens cyberoperasjoner og kapabilitetene som er utviklet og anvendes nå, er ikke identiske med de som fantes for noen år siden. Dette skyldes blant annet at operasjonsmiljøet er blitt mer utfordrende (mer komplekse systemer, nye sikkerhetsmekanismer og hyppigere oppdateringer av programvare), og at måten trusselaktører og forsvarere arbeider på stadig utvikles og profesjonaliseres.[53] Kappløpet mellom forsvarere og angripere foregår kontinuerlig og raskt. Utviklingen går så fort, og er av en slik grunnleggende karakter, at analyseapparatet henger etter.[54] Analyseobjektet blir et kontinuerlig bevegelig mål (*moving target*).

[52] Se for eksempel NATO (2020, s. 13–16). *AJP-3.20 Allied Joint Doctrine for Cyberspace Operations.* Edition A Version 1. Allied Joint Publication. NATO Standardization Agency. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/899678/doctrine_nato_cyberspace_operations_ajp_3_20_1_.pdf.

[53] For et eksempel som viser kontrasten mellom eldre og nyere måter for en angriper å jobbe på, se Guerrero-Sade, J. A., Raiu, C., Moore, D., Rid, T. (2017, «Pseudo-Automation») *Penquin's Moonlit Maze. The Dawn of Nation-State Digital Espionage*. Kaspersky Lab og King's College London. https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/07180251/Penquins_Moonlit_Maze_PDF_eng.pdf.

[54] Se for eksempel Atlantic Council (u.å.). *Transcript: Lessons from Our Cyber Past – The First Military Cyber Units.* March 5, 2012 Cyber Statecraft Initiative event. https://www.atlanticcouncil.org/commentary/transcript/transcript-lessons-from-our-cyber-past-the-first-military-cyber-units/: "The threat is constantly changing. The technology is changing so fast that it's difficult to even have a current threat assessment based on the technical threat that you're facing, so you have to be tremendously agile." En av årsakene til manglende metrikker for å måle nytteverdien av ulike utviklingsprogrammer innen cyberoperasjoner, er også knyttet til nye taktikker og kontinuerlige endringer i cyberoppdraget (*the cyber mission*). Se GAO (2022,

Begrenset nytte av eksisterende historikk og empiri. Historikken og empirien som per i dag er åpent tilgjengelig for analyse, er begrenset og potensielt ensidig.[55] Den må derfor brukes med varsomhet, og det stilles store krav til analytikernes kompetanse. Det er uklart hvor representativ empirien er for all aktivitet i cyberdomenet, og den raske utviklingen gjør at empiri utdateres og at bruken av den kan lede til feilslutninger. Dette vil høyst sannsynlig vedvare fremover. Empirien som faktisk finnes har dermed begrenset levetid dersom den brukes til å spå fremtiden.[56] Dette gjør også at utviklingen av teori blir vanskelig. Det er høyst usikkert i hvilken grad en har vært igjennom alle revolusjonene som leder til en stabil forståelse av cyberoperasjoner som fenomen.[57]

Ustabilitet og usikkerhet om forventet ytelse og suksessrater. En grunnleggende egenskap ved særlig offensive cyberoperasjoner er at usikkerheten knyttet til om operasjonen vil bli vellykket ikke lett lar seg redusere eller estimere. Dette gjelder selv om innsatsen økes. Innsikt i parametere som styres av utførende aktør, som antall personell, kompetanse, utstyr, programvare, informasjon og tidsbruk er ikke tilstrekkelig til å estimere sannsynligheten for suksess. Årsaken er at suksess er betinget av en rekke forhold i målsystemet som kan være svært dynamiske, og som det er vanskelig å forutse eller kompensere for i forkant. Mye av arbeidet med offensive cyberoperasjoner er av en svært kreativ art. Det er høy usikkerhet rundt hvor mye arbeid som må gjennomføres for å lykkes. For ervervelse og opprettholdelse av tilgang til systemer kan suksess ansees å være enten-eller (0 eller 100 prosent), i den forstand at en delvis suksess gjør at nødvendig tilgang for utnyttelse ikke er oppnådd. For tekniske effekter og følgekonsekvenser videre i og ut av cyberdomenet som utløses når nødvendig tilganger er tilstede, kan suksess være mer nyansert. Blant annet kan motpartens oppfattelse av hendelsen spille inn.

Defensive cyberoperasjoner har også usikkerhet ved seg. Et grunnleggende forhold er at det er en generell usikkerhet knyttet til hvor god sikkerhet en har i egne systemer og nettverk. Å kvantifisere og måle IKT-sikkerhet er meget vanskelig. Dette gjelder både det reelle sikkerhetsnivået i systemer og nettverk, og hvor god evnen til å møte trusler og håndtere hendelser er. Det er for eksempel vanskelig å vite om en synkende deteksjonsrate skyldes forbedringer i sikkerheten, eller dårligere deteksjonsevne som følge av at angriper har forbedret seg. Mengden ondsinnede handlinger en trusselaktør kan rette mot systemer og nettverk er også meget stor, noe som gjør det vanskelig å vite hva en bør sikre seg mot hvis ikke spesifikk trusselinformasjon foreligger. En blir da redusert til å følge *best practice* og å stadig forbedre tekniske

s. 17). *Defense Acquisition. Cyber Command Needs to Develop Metrics to Assess Warfighting Capabilities.* GAO-22-104695. https://www.gao.gov/assets/gao-22-104695.pdf.

[55] Se kapittel 3.1.1 for en beskrivelse av hva den åpne empirien består av.

[56] Dette betyr ikke at det ikke kan være verdifullt å samle og analysere empiri, men en må være varsom med å spå for langt inn i fremtiden og være klar over potensielle mørketall.

[57] Se for eksempel Rid, T., Buchanan, B. (2015, s. 25–26). Attributing Cyber Attacks, Journal of Strategic Studies, 38:1-2, 4-37, DOI: 10.1080/01402390.2014.977382: "Cyber operations are so new that 'firsts' are not uncommon. Analysing these precedents and trying to uncover what they portend for the future is not easy: a new method may either be a one-off, or the beginning of a trend. Some may reveal new possibilities […] Others may be noteworthy but less significant […] [for instance] a new technical step, but not one of wider strategic importance."

kapabiliteter innenfor de rammer en opererer innenfor. Dette inkluderer både reaktiv deteksjon og ulike former for proaktive undersøkelser av egne systemer og logger.[58]

Ved deteksjon og respons står man ofte i en paradoksal situasjon. Mengden informasjon om egne systemer og nettverk som er tilgjengelig for analyse er ofte for omfattende til at dette kan gjøres manuelt, samtidig som dekningsgraden ofte er for lav sammenliknet med hva den potensielt kan og bør være. Dette skyldes blant annet praktiske hensyn, som høye kostnader, en manglende evne til å håndtere et stort antall sensorer og alarmer og uvisshet om hva sensorene burde dekke. Teknikker som kryptering gjør også at tradisjonelle nettverkssensorer i økende grad blir blinde. Ulike måter å håndtere dette på kan ha andre ulemper, som for eksempel utfordringer knyttet til personvern dersom mer inngripende analyser gjøres. I tillegg er det stor usikkerhet knyttet til hva som vil være den mest hensiktsmessige måten å agere på (hvilke defensive teknikker som bør iverksettes, og når) ved deteksjon av en fiendtlig cyberoperasjon. Her vil forståelse for pågående og fremtidige militære operasjoner og avhengigheten av IKT være sentral.

Store kompetansekrav. Cyberoperasjoner skjer i et menneskeskapt domene som er grunnleggende teknisk i sin natur, og de utøves med et avansert teknisk håndverk. For å kunne forstå de tekniske sidene ved hvordan domenet virker, hvilke operasjoner som er mulige, hvilke effekter som kan og vil oppnås, og hvilken vei utviklingen går, er det nødvendig med dyp kompetanse som det tar tid å etablere på individuell og institusjonell basis. Samtidig har cyberoperasjoner klare operative og politiske implikasjoner, som medfører at en god forståelse av fenomenet krever innsikt i både tekniske, operative og politiske aspekter. Dette setter høye krav til både utøvende personell, ledere og beslutningstakere som sammen skal gjøre cyberoperasjoner til et velfungerende virkemiddel.

Ulike referanserammer og vokabular. I en stats diskusjoner om cyberoperasjoner vil både teknisk kyndig personell, militært operativt personell, byråkrater og politikere delta. Å skape en felles forståelse av muligheter, begrensninger og hva som er hensiktsmessige prioriteringer er en stor utfordring. Dette skyldes ikke nødvendigvis at de involverte personene er dypt uenige, men deres ulike kompetanseprofiler og at de ikke har en felles referanseramme og vokabular. Dette gjør at de ikke oppnår en felles forståelse, og dermed tilsynelatende kan havne i konflikt.

3.2 Inkludere cyberoperasjoner i langtidsplanlegging

Langtidsplanlegging er en disiplin innen forsvarsplanlegging som fokuserer på en lang tidshorisont. Det overordnede målet er å sikre at staten har et forsvar som klarer å utføre sine oppgaver og oppnå sine mål for hele bredden av dets virksomhet, over et tidsperspektiv på 10–30 år.[59] Dette gjøres typisk ved å finne en balanse mellom oppgavene som militære styrker

[58] Herunder såkalt *threat hunting.*
[59] Stojkovic, D., Dahl, B. R. (2007). *Methodology for long term defence planning.* FFI-rapport 2007/00600. https://www.ffi.no/publikasjoner/arkiv/methodology-for-long-term-defence-planning.

skal løse, sammensetningen til de militære styrkene og kostnadene ved å ha slike militære styrker som kan operere på et gitt ambisjonsnivå.

Som prosess kan langtidsplanlegging inkludere mange ulike aktiviteter. I Norge og Nato brukes blant annet en scenario- og kapabilitetsbasert metode. Metoden består i essens av tre deler.[60] Den ene delen omfatter en identifisering av mulige trusler, vurdering av ulike ambisjonsnivåer og utledning av krav til Forsvaret fra disse. Den andre delen omfatter en kapabilitetsanalyse av styrkestrukturen for å få en oversikt over hva strukturen yter. Den tredje delen omfatter en gap-analyse mellom krav og hva strukturen kan levere. Hver del av metoden består av flere steg og en rekke ulike analytiske teknikker benyttes underveis. Blant annet brukes morfologisk analyse for å utforske mulige trusler, og scenarioer og vignetter for å beskrive partenes militære styrker og hvordan de møter hverandre i taktiske stridssituasjoner.

Med et ønske om at langtidsplanleggingen skal ha en felles metodisk tilnærming for mest mulig av Forsvarets kapabiliteter og styrker, er det ikke urimelig å forsøke å inkludere cyberoperasjoner i slik metodikk. En møter imidlertid flere utfordringer når en forsøker på dette:

- Å utforske mulige cyberrelaterte trusler grundig er vanskelig.
- Hvordan krav bør utledes er ikke kjent.
- Det er store informasjonsmangler knyttet til referanseenhetene.
- Ytelsen til referanseenhetene er av natur ustabil og usikker.
- Scenarioene ilegges betydning utover den tiltenkte.

I dette kapitlet går vi videre inn i disse fem utfordringene.

3.2.1 Å utforske mulige cyberrelaterte trusler grundig er vanskelig

For å utforske mulige trusler benytter den scenario- og kapabilitetsbaserte metoden morfologisk analyse. På overordnet nivå lages en matrise som søker å spenne ut de sentrale parameterne i mulighetsrommet over potensielle trusler. Typisk vil parameterne dekke forhold som aktørtype, mål, middel og fremgangsmåte. Deretter lages scenarioklasser basert på gyldige kombinasjoner av parameterverdiene. Med dette som utgangspunkt utvikles et sett med scenarioer innenfor de ulike klassene, som så er utgangspunktet for analyse med fageksperter.[61] Ofte vil et scenario være detaljert med vignetter som beskriver taktiske stridssituasjoner.

Dersom valg av parametere og verdier og gjennomgangen av kombinasjoner er gjort grundig, kan en med en viss grad av sikkerhet si at store deler av det teoretiske mulighetsrommet er

[60] Vatne, D. F., Køber, P. K., Guttelvik, M. S., Arnfinnsson, B., Rise, Ø. R. (2020). *Norwegian long-term defence analysis – a scenario- and capability-based approach.* FFI-rapport 20/02367. https://www.ffi.no/publikasjoner/arkiv/norwegian-long-term-defence-analysis-a-scenario-and-capability-based-approach.
[61] Ibid.

utforsket på overordnet nivå. Scenarioene som utvikles kan sees på som et utvalg av mange mulige instansieringer i hver scenarioklasse som eksemplifiserer og konkretiserer hva en trussel kan omfatte i mer detalj. Et sett med scenarioer omtales noen ganger som en scenarioporteføljе, og blir et referansepunkt for mer konkrete trusler og situasjoner som kan oppstå.

For cyberoperasjoner er det imidlertid vanskelig å vite for en analytiker om truslene har blitt tilstrekkelig utforsket og konkretisert på ulike nivåer i analysen. Dette gjelder både om de mest signifikante trusselhandlingene er valgt, og om realismen er ivaretatt:

- *I morfologisk matrise og opprettelsen av scenarioklasser.* Er cyberoperasjoner i tilstrekkelig grad inkludert i den morfologiske matrisen og tatt hensyn til i opprettelsen av scenarioklasser?

- *I scenarioporteføljen.* Bør nye scenarioer utvikles og legges til scenarioporteføljen, fordi mulige fiendtlige cyberoperasjoner leder til noen signifikant nye situasjoner som kan oppstå?

- *I vignetter.* Viser de detaljerte vignettene i et gitt scenario, eller på tvers av flere scenarioer, de mest signifikante trusselhandlingene som kan brukes i en taktisk stridssituasjon?

Hovedutfordringen er å bedømme hva som er *tilstrekkelig* eller *signifikant* på de ulike nivåene, og om det som er *mulig* er godt nok utforsket. På teknisk nivå finnes en meget stor mengde ulike teknikker og operasjonsmåter. Det er vanskelig å vurdere hvilke av disse som bør eksemplifiseres i vignetter, om de viktigste operative konsekvensene av mulige trusselhandlinger er funnet og om de mest instruktive taktiske stridssituasjonene er plukket ut.

Potensielt står vi overfor nye situasjoner som bør inn i scenarioporteføljen. For eksempel kan det tenkes at om motparten er en stat som er geografisk plassert i en annen del av verden og har særskilte statlige interesser, kan dette lede til hendelsesforløp vi ikke har analysert tidligere. Videre er det et åpent spørsmål om vi har nok innsikt til å vite hvordan cyberoperasjoner best kan representeres i den morfologiske matrisen på toppnivå, eller om vi må tenke grunnleggende nytt.[62]

3.2.2 Hvordan krav bør utledes er ikke kjent

I det fysiske domenet møter og kjemper militære styrker med hverandre på land, i lufta og til sjøs. Det eksisterer mye historikk og erfaring med de ulike strukturelementtypene, som gjør det mulig å vite hvilke styrkesammensetninger som kan passe for å møte motstanderens militære styrker i et gitt scenario. Basert på hva motstanderen stiller med av styrker samt hvilke målsettinger og handlemåter motstanderen har, er det i stor grad mulig å utlede krav til egne styrker. Avhengig av bestemt ambisjonsnivå vil både egne defensive og offensive kapabiliteter kunne

[62] For et eksempel på hvordan cyberoperasjoner kan representeres i en slik matrise, se revisjonen av matrisen som er grunnlaget for scenarioklassene i FFIs scenarioporteføljе. Johansen, I. (2022). *Scenarioklasser for forsvarsplanlegging – revisjon av FFIs scenariogrunnlag.* FFI-rapport 21/01788. https://www.ffi.no/publikasjoner/arkiv/scenarioklasser-for-forsvarsplanlegging-revisjon-av-ffis-scenariogrunnlag.

kravsettes. For eksempel kan fiendtlige luftstyrker og deres anvendelse være utgangspunktet for å diskutere behovet for luftvern og egne fly. I tillegg til empiriske data har vi også simuleringsmodeller og -data som kan belyse forløpet i en strid mellom tradisjonelle strukturelementer. Det er nærliggende å overføre dette tankesettet til cyberdomenet.

Dessverre har vi ikke tilsvarende kunnskap om hvordan en strid i cyberdomenet bør modelleres og cyberkapabiliteter kravsettes i en taktisk stridssituasjon. For det første er det stor usikkerhet knyttet til hvordan fiendtlige offensive cyberkapabiliteter og cyberoperasjoner bør beskrives. Dernest er det usikkert hvordan krav til egne styrker kan utledes av dette. For eksempel har vi ingen klar logikk for hvordan fiendtlige offensive cyberoperasjoner kan resultere i krav til egne defensive cyberkapabiliteter og cyberoperasjoner, utover en formening om at jo bedre offensive kapabiliteter motparten har, jo bedre defensive evner bør vi selv ha.

Tilsvarende vet vi ikke hvordan krav til egne offensive cyberkapabiliteter og cyberoperasjoner kan utledes av en taktisk stridssituasjon. Det er ikke urimelig å forvente at kravene bør være knyttet til IKT-avhengigheten som motparten har i sine strukturelementer, dersom utgangspunktet er at en skal utløse effekter i cyberdomenet som påvirker disse strukturelementene.[63] Motpartens defensive cyberkapabiliter og cyberoperasjoner bør da også være et element i utledning av kravene. Det er imidlertid ukjent hvordan en «cyber» Order of Battle og cyberoperasjoner bør beskrives slik at en kan begynne å etablere argumentasjonskjeder for slike krav.

En skal heller ikke utelukke at det er behov for å tenke annerledes om hvordan offensive cyberkapabiliteter og cyberoperasjoner blir anvendt i en strid. For eksempel kan en se for seg at egne offensive cyberoperasjoner for effekt i mindre grad er rettet mot fiendtlige regulære strukturelementer, og kun moderat synkronisert med det taktiske hendelsesforløp i fysisk domene. I stedet kan dette virkemidlet benyttes som et mer generelt påtrykk mot fiendtlig IKT-infrastruktur og -systemer med løsere koordinering i tid og rom. Dette inkluderer både direkte å motvirke og potensielt angripe fiendtlige offensive cyberkapabiliteter, inklusive etablerte angrepsinfrastrukturer, og å angripe andre typer IKT-systemer for å skape stress og forvirring og å binde ressurser.

Mulig bruk av offensive cyberoperasjoner for effekt må imidlertid veies opp mot kinetiske alternativer som har høyere sannsynlighet for suksess og er heftet med mindre usikkerhet. Kreative forslag til mulige anvendelser av cyberoperasjoner for effekt er det forholdsvis lett å komme opp med, men de kan være urealistiske både med tanke på ønsket effekt og nødvendige ressurser (for eksempel «ta kontrollen over fiendtlige missiler»). En må også vurdere nytten av å gjennomføre etterretningsoperasjoner med de samme ressursene. I sum er det stor usikkerhet rundt hvordan krav til både defensive og offensive cyberoperasjoner kan utledes av en taktisk stridssituasjon.

[63] For å kunne inkludere IKT i langtidsplanlegging har prosjekt 1501 utviklet en metode for å knytte IKT-avhengighet til strukturelementers kapasiteter. Metoden kan i prinsippet også anvendes på en motpart. Se Farsund, B., Thuv, Aa., Hansen, B. J. (2022). *Hvordan håndtere IKT i Forsvarets langtidsplanlegging.* FFI-rapport 22/01569. https://www.ffi.no/publikasjoner/arkiv/hvordan-handtere-ikt-i-forsvarets-langtidsplanlegging.

3.2.3 Det er store informasjonsmangler knyttet til referanseenhetene

I den scenario- og kapabilitetsbaserte metoden har hvert strukturelement blitt tilordnet et sett med kapabiliteter. Det er kapabilitetene som beskriver hva strukturelementet kan gjøre. For hver kapabilitet er det definert en referanseenhet, som gjør det mulig å beskrive og sammenlikne hvor mye kapasitet strukturelementene har av sine kapabiliteter.[64] Referanseenheten er typisk et valgt strukturelement. En måte å inkludere cyberoperasjoner i metoden på, er å definere kapabiliteter for henholdsvis defensive og offensive cyberoperasjoner med tilhørende referanseenheter. For å kunne gjøre dette er det sentralt å avklare:

- Hva er et «cyberstrukturelement»?
- Hvilke kapabiliteter har «cyberstrukturelementer»?
- Hva er referanseenhetene for de ulike kapabilitetene?

For land, luft og sjø er mange strukturelementer som brukes taktisk konkrete og håndgripelige. For eksempel en bataljon, et kompani, et fly eller et fartøy. For cyberoperasjoner har vi i dag ingen klart definerte militære strukturelementer, utover at en gruppe mennesker arbeider sammen mot et felles mål. Ofte finner vi disse i en felles administrativ enhet, og vi kan definere dette til å være en cyberenhet – vårt cyberstrukturelement. Selv om organisering kan variere stort fra stat til stat, er det ikke urimelig å forsøke seg med en defensiv og en offensiv cyberenhet da det ofte er ulike grupper som jobber med dette.

Hvordan man kan beskrive en cyberenhet med kapabiliteter og kapasitet som passer i langtidsplanlegging, er ikke klart. Hvilke nivå kapabiliteter bør beskrives på og hva de bør omfatte er uvisst. Men dersom ambisjonen er å behandle cyberoperasjoner som et taktisk virkemiddel som kan kravsettes, bør kapabiliteter og kapasiteter på et eller annet nivå være knyttet til meningsbærende størrelser. Om dette oppnås vil avhenge av hva vi velger som referanseenheter og hva som ligger i disse.

På overordnet nivå er referanseenheter liknende «offensiv cyberenhet» og «defensiv cyberenhet» ikke unaturlig. Utfordringen er at vi ikke vet hva dette betyr i praksis. Dersom vi har en Nansen-fregatt, en F-16 eller en standardisert bataljon som referanseenhet, så vet vi hva dette impliserer fordi vi har mye kunnskap om hva disse kan yte. Blant annet har vi kjennskap til oppbygging, utrustning, operasjonsmåter og andre sentrale karakteristikker. Selv om slik informasjon behandles aggregert og abstrahert og ikke eksplisitt detaljeres i mer overordnede analyser, er denne kunnskapen tilgjengelig og indirekte trukket på når referanseenhetene benyttes og forstås. Dette gjelder selv om deler av informasjonen er høyt gradert.

[64] Vatne, D. F., Køber, P. K., Guttelvik, M. S., Arnfinnsson, B., Rise, Ø. R. (2020). *Norwegian long-term defence analysis – a scenario- and capability-based approach.* FFI-rapport 20/02367. https://www.ffi.no/publikasjoner/arkiv/norwegian-long-term-defence-analysis-a-scenario-and-capability-based-approach.

For cyberenheter har vi per nå ikke nok tilsvarende kunnskap. For å etablere denne kunnskapen mener vi det er nødvendig med detaljert og inngående informasjon om organisering, prosesser, aktiviteter, leveranser og kapasiteter. Primært trenger vi denne kunnskapen om egne cyberenheter for å forstå hvordan vi kan lage gode – også ugraderte – abstraksjoner som gir mening og som kan brukes i analyser. Herunder beskrivelser av referanseenhetene og hva de kan yte. Ideelt sett skulle en hatt noe liknende kunnskap om motparts cyberenheter, i alle fall tilstrekkelig informasjon til å forstå eventuelle forskjeller i kapabiliteter og kapasitet.

3.2.4 Ytelsen til referanseenhetene er ustabil og usikker av natur

Selv om vi skulle få all informasjon vi ønsker oss om ulike cyberenheter, er det en generell utfordring at ytelse knyttet til offensive og defensive cyberoperasjoner ofte er ustabil og usikker av natur.[65] Dette skyldes blant annet en rekke komplekse sammenhenger knyttet til iboende egenskaper ved teknologien som brukes, interaksjonen mellom brukere og rammede systemer, følgekonsekvensene i og ut av cyberdomenet og oppfattelsen som motpart og egne har av situasjonen. Konsekvensen er at referanseenhetene ikke vil fungere som stabile størrelser, men ha potensielt store ytelsessvingninger selv under relativt like forutsetninger.

Denne svingningen gjør det vanskelig å etablere og argumentere for et gitt ytelsesnivå i for eksempel en konkret taktisk stridssituasjon. Risikoen er stor for at en i så fall «definerer» seg selv til suksess. Med dette menes at en legger til grunn en uforholdsmessig lang liste av antakelser for å få det utfallet en ønsker. Antakelsene vil typisk være både implisitte og til dels ukjente. En motvekt til dette kan være å inkludere den usikkerheten som cyberenheter kjemper med underveis i sine aktiviteter i vignettbeskrivelsene. Dette bør gjøres løpende, slik at endringer i usikkerhet og forståelsen av usikkerhet tas med. Utover dette er det vanskelig å vite hvordan slike svingninger i ytelse best bør håndteres.

3.2.5 Scenarioene ilegges betydning utover den tiltenkte

Fra analytikerens ståsted brukes scenarioer i den scenario- og kapabilitetsbaserte metoden for å eksemplifisere og konkretisere hva en fremtidig trussel kan omfatte og hvordan den kan møtes. I prinsippet legger ikke et scenario noen føringer på byråkratiske eller politiske beslutninger. Scenarioet beskriver en tenkt situasjon – ut av mange mulige tenkte situasjoner – og det har en konkret rolle i metodikken for langtidsplanlegging. De er i utgangspunktet ikke tiltenkt å spille inn i andre typer vurderinger. For å oppfylle deres rolle tilstrebes det at scenarioene er nøytrale, objektive beskrivelser av konkretiserte situasjoner med korrekt informasjon og realistisk detaljering, og med tydelige antakelser der de gjøres.

En vil imidlertid kunne oppleve at scenarioenes mulige implikasjoner blir lest og tolket utover den tiltenkte bruken. Eksempelvis kan det hende at enkeltscenarioene blir gitt for mye tyngde i en investeringsdiskusjon, og at strukturelementer som ikke har fått demonstrert sin nytteverdi feilaktig blir nedprioritert. Da brukes scenarioene i strid med den opprinnelige intensjonen, og

[65] Se kapittel 3.1.3.

det er ikke nødvendigvis noe feilaktig eller misvisende med scenarioene av den grunn. Slike utfordringer må til en viss grad forventes, uten at dette betyr at scenarioene bør endres.

Samtidig mener vi det er en ekstra dimensjon knyttet til cyberoperasjoner i denne sammenheng. Dette skyldes at cyberoperasjoner som statlig virkemiddel har sentrale bruksområder på utsiden av militær kontekst. Den tette koblingen mellom ulike anvendelser – eksempelvis at effekt-operasjoner kan ødelegge for etterretningsoperasjoner både i fortid og fremtid, som diskutert i kapittel 3.1.2 – gjør at den samlede vurderingen av nytteverdien til cyberoperasjoner for effekt blir mangelfull og misvisende dersom disse implikasjonene ikke blir tatt med. Således kan en si at en stat er mer sårbar for feilaktig bruk av scenarioer med cyberoperasjoner, fordi de i mindre grad gir et godt helhetlig bilde sammenliknet med det de gir for andre militære strukturelementer. Dette gjelder også om en hel militær scenarioportefølje sees under ett. For å unngå dette må vurderinger av implikasjonene for annen statlig virkemiddelbruk enten tas med i scenarioene, eller håndteres i et eget løp på utsiden.

3.3 Inkludere cyberoperasjoner i planlegging og gjennomføring av militære operasjoner

Mange av utfordringene ved analyse av cyberoperasjoner som et statlig virkemiddel og inkludering i langtidsplanlegging, er gjeldende også for inkludering i planlegging og gjennomføring av militære operasjoner. Mangelen på relevant empiri og teori, konkurrerende interesser og dilemmaer samt de særegne egenskapene ved virkemidlet er like utslagsgivende når cyber-operasjoner skal settes inn en operativ planleggings- og gjennomføringsramme. Det samme gjelder usikkerheten rundt krav og behov, og hvordan cyberoperasjoner best kan bidra inn i en militær operasjon. Samtidig er det enkelte andre forhold som slår ekstra sterkt ut. Dette inkluderer:

- meget høy grad av hemmelighold ved offensive cyberoperasjoner
- ulike planleggings- og gjennomføringsrytmer
- kommunikasjonsutfordringer mellom fageksperter og annet militært personell
- manglende kunnskap om egen avhengighet av IKT

I dette kapitlet går vi videre inn i disse fire utfordringene.

3.3.1 Meget høy grad av hemmelighold ved offensive cyberoperasjoner

Offensive cyberoperasjoner er meget spesialiserte og innebærer en stor grad av tilpasning til målsystemet som en bryter seg inn i og potensielt ønsker å utløse effekt i. Denne spesialiseringen kan resultere i en meget høy grad av hemmelighold rundt hvilke systemer en stat har brutt eller ønsker å bryte seg inn i hos en motpart. Dette skyldes i hovedsak at dersom motparten får en mistanke om at et spesifikt system er kompromittert, vil sannsynligheten for å bli oppdaget

gå markant opp. Skulle tilstedeværelsen bli oppdaget og tilgangene til systemene bli fjernet, kan reetablering ta meget lang tid eller vise seg umulig. Resultatet av dette er en form for skjørhet, som gjør at informasjon om hvilke systemer en stat har kompromittert eller har planer om å kompromittere i overskuelig fremtid, holdes tilbake. Særlig når cyberoperasjoner er knyttet til etterretningsvirksomhet, praktiseres strengt hemmelighold for å forhindre at detaljer om reelle og mulige målsystemer lekker ut.

I denne sammenheng kan også regulære planleggingsfora internt i en militær organisasjon bli sett på som for åpne til at detaljer om offensive cyberoperasjoner blir delt. Dette vil typisk inkludere informasjon om hvilke målsystemer cyberoperasjoner rettes mot og hvor langt en har kommet. Her vil et positivt tilsagn om at tekniske effekter vil kunne utløses i et spesifikt system innen rimelig tid være tilstrekkelig for andre til å forstå at systemet trolig er kompromittert allerede.

Samtidig er det nettopp denne typen detaljer militært personell kan trenge for å forstå og utnytte mulighetsrommet som ligger i offensive cyberoperasjoner. Ved planlegging og gjennomføring av militære operasjoner er det et relativt sett stort stabsapparat som settes i sving. Dersom informasjon om offensive cyberoperasjoner ikke kommer inn i de regulære mekanismene i dette apparatet, vil en operativ sjef kunne få en mangelfull forståelse for muligheter og begrensninger ved virkemidlet. Sjefen med sin stab får dermed ikke vurdert potensialet eller risikoen knyttet til inkludering av cyberoperasjoner i den militære operasjonen med dennes operasjonsdesign og taktiske handlemåter.

Det er nødvendig å finne løsninger som balanserer disse to ulike interessene. Operativ sjef og hans stab må ha tilstrekkelig innsikt til å kunne utnytte cyberoperasjoner og gjøre de nødvendige vurderinger til rett tid og med tilstrekkelig dybde, samtidig som det rettmessige behovet for skjerming av informasjon knyttet til cyberoperasjoner blir ivaretatt. Samme utfordring er tilstede ved forsvarsplanlegging, men der er mulighetene større til å autorisere en mindre gruppe mennesker som kan gjøre analyser i isolasjon. Det er imidlertid usikkert hvor og hvordan denne balansen mellom skjerming og informasjonsdeling best kan oppnås i en operativ setting.

3.3.2 Ulike planleggings- og gjennomføringsrytmer

Behovet for forberedelser før et virkemiddel kan benyttes er ikke ukjent i militær kontekst. Alle virkemidler må i prinsippet trenes, øves, utrustes og gjøres klar til strid. Enkelte kjente virkemidler som elektromagnetisk krigføring[66] har også behov for klargjørings- og oppdateringsfaser hvor rett informasjon jevnlig må samles, vurderes og omsettes til handling. Samtidig fremstår offensive cyberoperasjoner som noe unike, på grunn av et stort behov for kontinuerlig oppdatert informasjon og justeringer på teknisk nivå som er vanskelige å forutse. Dette skaper stor

[66] Tidligere kalt elektronisk krigføring. Se for eksempel «Note on the Terms 'electronic' vs 'electromagnetic'» i amerikansk luftdoktrine. U.S. Air Force (2019, s. 2). *Air Force Doctrine Publication (AFDP) 3-51. Electromagnetic warfare and electromagnetic spectrum operations*. https://www.doctrine.af.mil/Doctrine-Publications/AFDP-3-51-EW-and-EMS-Ops/

usikkerhet selv ved vanlig virke. I denne sammenheng er det også vanskelig å løfte de fleste cyberkapabiliteter ut av en gitt kontekst for å sette dem inn i en annen på kort varsel.

Lang forberedelsestid, stor usikkerhet og treghet ved omstilling gir offensive cyberoperasjoner en planleggings- og gjennomføringsrytme som det er utfordrende å samkjøre med militære planprosesser. Fleksibiliteten som andre virkemidler viser ved kortere planleggingshorisonter, ved at de kan brukes på ulike måter eller til ulike formål på kort varsel, er i stor grad fraværende. For at cyberkapabiliteter skal kunne benyttes til et gitt formål må beslutningen ofte være tatt lenge før den militære planprosessen legger opp til at beslutningen skal tas. Dette gjør at mulige anvendelser av cyberoperasjoner i militære operasjoner må utforskes, vurderes og til en viss grad besluttes i forkant av de militære operasjonene. I praksis velges da et fåtalls målsystemer, før en vet sikkert om den neste militære operasjonen vil dra nytte av dette. Denne spenningen mellom ulike rytmer i planlegging og gjennomføring er vanskelig å unngå.

3.3.3 Kommunikasjonsutfordringer mellom fageksperter og annet militært personell

Offensive og defensive cyberoperasjoner er særdeles kompetansekrevende disipliner, hvor små tekniske detaljer kan ha store implikasjoner operativt og politisk. For fageksperter kan det være vanskelig å kommunisere hva de mener er sentrale sider ved en situasjon, uten at språket blir for teknisk for personer med en annen faglig bakgrunn. Tilsvarende kan det være utfordrende for fageksperter å forstå operasjonelle forhold ved en militære operasjon, på tross av at fagekspertene også kan være militære. Dette gjør det utfordrende å forstå hvordan tekniske og operative forhold påvirker hverandre i en gitt situasjon, og derigjennom å håndtere risiko og gripe muligheter. Enkelte stater har sett på løsninger med en egen «*cyber advisor*» som skal bidra til å bygge bro over dette gapet.[67]

3.3.4 Manglende kunnskap om egen avhengighet av IKT

Dagens militære styrker er som oftest store brukere av ulike former for IKT. Hvordan styrkene er avhengige av IKT er det likevel meget vanskelig å få oversikt over.[68] Det kreves mye ressurser for å analysere og vurdere IKT-avhengighet i en så stor og kompleks virksomhet som et nasjonalt forsvar. Det er behov for bedre metoder for dette, særlig når operasjonelle implikasjoner av avhengigheten skal vurderes.[69]

Hvordan avhengigheten spiller inn i nytte og risiko er relevant ved planlegging og gjennomføring av militære operasjoner. I en konkret militær operasjon vil både motparts og egne styrker

[67] Se for eksempel Johnson, D. B. (2023, 26. april). Sifting through the top cyber myths in the military service branches. *SC Media*. https://www.scmagazine.com/analysis/careers/top-cyber-myths-military-service-branches.
[68] For eksempel har Forsvaret i dag ikke god nok oversikt over hvilke informasjonssystemer som Forsvaret selv bruker. Se Riksrevisjonen (2022, s. 12). *Riksrevisjonens undersøkelse av Forsvarets informasjonssystemer for kommunikasjon og informasjonsutveksling i operasjoner*. Ugradert versjon av Dokument 3:3 (2022−2023). https://www.riksrevisjonen.no/rapporter-mappe/no-2022-2023/undersokelse-av-forsvarets-informasjonssystemer-informasjonssystemer-til-bruk-i-operasjoner/
[69] Prosjektets arbeid med denne problemstillingen, gjort i forbindelse med forsvarsplanlegging, kan være relevant også her. Se Farsund, B., Thuv, Aa., Hansen, B. J. (2022). *Hvordan håndtere IKT i Forsvarets langtidsplanlegging*. FFI-rapport 22/01569. https://www.ffi.no/publikasjoner/arkiv/hvordan-handtere-ikt-i-forsvarets-langtidsplanlegging.

kunne velge mellom handlemåter som har ulik avhengighet av IKT. Avhengighet bør være en faktor ved valg av egen handlemåte og stå sentralt i hvordan beskyttelsestiltak og defensive cyberoperasjoner tilpasses den militære operasjonen. Hvordan operative prosesser bør forløpe med analyser og vurderinger knyttet til disse problemstillingene, er imidlertid uklart.

4 Analytiske verktøy

De analytiske verktøyene er etablert for å kunne skape konsistente argumentasjonskjeder på en sporbar måte. De skal hjelpe brukere med å heve kvaliteten på analyser og vurderinger knyttet til cyberoperasjoner. Målet med verktøyene er således ikke å finne frem til allmenne sannheter, men å tvinge brukerne til å etablere tydelige resonnementer som så kan diskuteres og kritiseres. På sikt vil dette kunne fasilitere økt felles forståelse blant ulike aktører med en aksje i cyber-operasjoner og blant individer med ulik fagbakgrunn.

Verktøy (V1-V4)	Hovedmål
V1. Rammeverk for analyse av cyberoperasjoner	M1
V2. Metode for å utforske mulig bruk av cyberoperasjoner i en gitt situasjon	M2
V3. Matriser for utspenning av mulige situasjoner	M2
V4. Sentrale steg for integrasjon av cyberoperasjoner i planlegging og gjennomføring av militære operasjoner	M2
(T1. Tillegg – vurdering av scenario- og kapabilitetsbasert metodikk)	M3

M1: Etablering av et konseptuelt grunnlag	M2: Økt innsikt i utforsking av nytte, risiko, mulighetsrom, og nyttiggjøring av CO	M3: Økt innsikt i anvendelsen av scenario- og kapabilitetsbasert metodikk som ramme for forsvarsplanlegging av CO

Tabell 4.1 Oversikt over analytiske verktøy og hovedmål.

Tabell 4.1 viser verktøyene og de respektive hovedmålene som disse støtter opp om. Flere av verktøyene bidrar til flere mål samtidig, selv om dette ikke er markert. De to første verktøyene kan ansees som de mest utviklede. I tillegg er arbeidet som var grunnlaget for vurderingene av utfordringene i kapittel 3 også listet opp i tabellen og omtalt i dette kapitlet.

I sum vil disse verktøyene kunne brukes i en rekke ulike analysesituasjoner, blant annet:

- forsvarsplanlegging/langtidsplanlegging
- strategiarbeid, planarbeid og operative planprosesser
- planlegging og gjennomføring av øvelser
- frittstående analyser av staters tilnærminger til cyberoperasjoner

I dette kapitlet går vi igjennom hvert av verktøyene, før vi avslutter med en oversikt over hvilke utfordringer de ulike verktøy forsøker å møte.

4.1 Verktøy 1 – Rammeverk for analyse av cyberoperasjoner

Rammeverk for analyse av cyberoperasjoner er en strukturert sammenstilling av grunnleggende kunnskap om cyberoperasjoner. Hensikten er å bidra til å skape en bedre forståelse av hvilke dilemmaer og valg stater står i, og beslutningene de har tatt eller skal ta knyttet til innrettingen av sin cybervirksomhet. Fremfor å binde oss til en gitt stats forståelse av cyberoperasjoner som uttrykt gjennom direktiver, doktriner og organisatoriske løsninger, har vi forsøkt å studere cyberoperasjoner som et fenomen som de fleste, om ikke alle, stater møter.

Et sentralt hensyn ved utviklingen av rammeverket har vært å inkludere flere faglige perspektiver på en integrert måte. Slik kan personer med ulik bakgrunn få en felles referanseramme. Dette inkluderer for eksempel operative, politiske, byråkratiske og teknologiske perspektiver. Anvendelse av rammeverket kan fasilitere målrettede diskusjoner og analyser for grupper med en sammensatt kompetanseprofil. Det er imidlertid nødvendig å tilpasse anvendelsen av rammeverket til deltakerne og de spesifikke problemstillingene som ønskes belyst.

Rammeverket består i skrivende stund av fem premisser, og et trettitalls faktorer plassert i et hierarki. Premissene er formulert som korte utsagn med en tilhørende tekstlig virkelighetsbeskrivelse, som konkretiserer det vi mener er et statsperspektiv for cyberoperasjoner. De fem premissene er:

1. Cyberoperasjoner skjer i en kontekst
2. Staten er den sentrale aktøren
3. Cyberenheten er statens operative element
4. Privat industri har sentrale roller
5. Cyberkriminalitet er et eget økosystem

1. Cyberoperasjoner skjer i en kontekst. Cyberoperasjoner er ikke en teknisk aktivitet som kun utføres for å oppnå tekniske effekter i cyberdomenet. Både statlige aktører og ikke-statlige aktører prioriterer, planlegger og utfører cyberoperasjoner i en bred kontekst hvor andre elementer eksisterer og andre aktiviteter foregår. Det er denne konteksten som former hva slags cyberoperasjoner som er hensiktsmessig og hva som faktisk blir utført. Dette gjelder offensivt som defensivt.[70]

2. Staten er den sentrale aktøren i denne konteksten. Det er et bredt spekter av aktører som former cyberdomenet og aktivitetene i det. Dette inkluderer individer, grupper, firmaer, stater og

[70] Dette omfatter valg av hva som skal angripes (offensivt) eller forsvares (defensivt), valg av taktikker og valg av teknikker.

internasjonale organisasjoner og allianser som NATO, FN og EU. Staten fremstår som den viktigste aktøren som former rivalisering og konflikt i cyberdomenet.

3. Cyberenheten er statens operative element. Cyberenheten planlegger og gjennomfører cyber-operasjoner på vegne av staten. En slik enhet kan være en formell del av staten, en proxy eller en mer selvstendig ikke-statlig aktør. Det er denne enheten som faktisk anvender verktøy i cyberdomenet. Avhengig av en gitt stats organisering, vil elementer som for eksempel taktisk ledelse og strategisk styring kunne ligge hos cyberenheten selv eller i et organisasjonselement på lavere, sideordnet eller høyere nivå. En stat kan i praksis ha flere cyberenheter, og disse kan analyseres hver for seg eller som én aggregert enhet.[71]

4. Privat industri har sentrale roller. Privat industri er blant annet motoren i forskning og utvikling av teknologi og hovedleverandøren av infrastruktur, tjenester og sikkerhet i cyber-domenet. Mange stater bruker privat industri i utviklingen av egne cyberkapabiliteter, enkelte også for de offensive.[72] Industrien er ofte tungt involvert i hendelseshåndtering i cyberdomenet som eiere av infrastruktur og leverandører av tjenester.[73] Enkelte private aktører er så store at de ser på seg selv som viktige aktører i politikken tilknyttet konflikter i cyberdomenet.[74]

5. Cyberkriminalitet er et eget økosystem. Det er over tid vokst frem avansert organisert kriminalitet i cyberdomenet, med kriminelle aktører som kjøper og selger tjenester seg imellom (CaaS[75]). Også enkelte stater deltar i dette markedet, hvor det blant annet tilbys tilgang til kompromitterte identiteter, kompromitterte systemer,[76] villedende domener og administrerte

[71] En cyberenhet i vårt arbeid er en abstraksjon som representerer de som er involvert i cyberoperasjoner på vegne av staten. Det er ikke påkrevet å inkludere i en analyse hvordan staten har fordelt ansvar, roller og myndighet, med mindre dette er hensiktsmessig gitt målsettingen med analysen. En reell cyberenhet kan derfor bli analysert som flere konseptuelle cyberenheter, og en konseptuell cyberenhet kan i praksis omfatte flere reelle cyberenheter.

[72] Se for eksempel Mahoney, C. W. (2021). Corporate Hackers: Outsourcing US Cyber Capabilities. *Strategic Studies Quarterly, 15*(1), 61-89. https://www.airuniversity.af.edu/Portals/10/SSQ/documents/Volume-15_Issue-1/Mahoney.pdf ; DeSombre, W., Campobasso, M., Allodi, L., Shires, J., Work, J. D., Morgus, R., O'Neill, P. H., Herr, T. (2021, 1. mars). A primer on the proliferation of offensive cyber capabilities. *Atlantic Council*. https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/a-primer-on-the-proliferation-of-offensive-cyber-capabilities/.

[73] Se for eksempel Beecroft, N. (2022, 3. november). Evaluating the International Support to Ukrainian Cyber Defence. *Carnegie Endowment for International Peace.* https://carnegieendowment.org/2022/11/03/evaluating-international-support-to-ukrainian-cyber-defense-pub-88322

[74] Burt, T. (2020, 21. desember). Cyber mercenaries don't deserve immunity. *Microsoft.* https://blogs.microsoft.com/on-the-issues/2020/12/21/cyber-immunity-nso/; Smith, B. (2020, 17. desember). A moment of reckoning: the need for a strong and global cybersecurity response. *Microsoft*. https://blogs.microsoft.com/on-the-issues/2020/12/17/cyberattacks-cybersecurity-solarwinds-fireeye/

[75] Cybercrime as a Service.

[76] For kriminelle aktører som selger systemtilgang til andre kriminelle aktører, se for eksempel Tatar, S. (2022, 19. september). *What Are Initial Access Brokers?* Arcticwolf. https://arcticwolf.com/resources/blog/initial-access-brokers/; Intel471 (2022, 2. juni). *The relationship between access brokers and ransomware crews is growing.* https://intel471.com/blog/access-brokers-ransomware-relationship-growing.

tjenester. Sistnevnte kan omfatte tjenestenekt, phishing og andre typer angrep i form av abonnementstjenester.[77] Den totale omsetningen i cyberkriminalitet er blitt meget stor.[78]

Til disse premissene er det knyttet et hierarki av faktorer. Faktorene er sentrale sider ved cyberoperasjoner som det potensielt bør tas hensyn til i analyser og diskusjoner. Premissenes virkelighetsbeskrivelse fungerer som en forankring for det øverste nivået av hierarkiet, med sporbarhet mellom innholdet i premissbeskrivelsene og toppnivåfaktorene.

Faktorene dekker forhold som:

- Nasjonale ambisjoner, prioriteter og ressurser
- Organisatorisk struktur
- Konseptualisering og avgrensing av cyberoperasjoner
- Strategiske og operative kontekster
- Føringer og beskrankninger på cyberoperasjoner
- Bidrag og effekter i operasjoner
- Operative prosesser og mekanismer
- Teknologiske systemer
- Argumentasjonskjeder
- Risikotyper og risikoaksept

Alle toppnivåfaktorene er konkretisert etter et bestemt format. Faktorene har et nummer og et navn. Med hver sin setning angis hva faktoren omfatter, og hvorfor faktoren er relevant. Deretter følger et fritekstfelt som gir en beskrivelse av faktoren i mer detalj. Dersom faktoren har underfaktorer knyttet til seg, blir disse beskrevet med et undernummer, et navn og mulige verdier. Underfaktorene har således mer begrensede beskrivelser enn toppnivåfaktorene, og brukes for å spenne ut relevante parametere. Underfaktorene kan selv ha flere underfaktorer. Se figur 4.1.

[77] Microsoft (2022c, s. 18–19). *Digital Defence Report 2022*. https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE5bUvv?culture=en-us&country=us

[78] I 2018 ble det estimert at den samlede omsetningen innen cyberkriminalitet var over 1,5 billioner amerikanske dollar ($1{,}5 * 10^{12}$). Dette var fordelt på illegale markeder (860 milliarder dollar), tyveri av forretningshemmeligheter og IP (500 milliarder dollar), salg av stjålne data som kredittkort og bankinformasjon (160 milliarder dollar), CaaS (1.6 milliarder dollar) og betalt ransomware (1 milliard dollar). Se McGuire, M. (2018). *Into the Web of Profit. Understanding the Growth of the Cybercrime Economy.* Bromium. https://www.bromium.com/wp-content/uploads/2018/05/Into-the-Web-of-Profit_Bromium.pdf

- **F14. Contribution to the broader context**
- **What:** What the cyber operation contributes to in the broader context
- **Why:** The contribution is the rationale for conducting the cyber operation
- **Description**
  A cyber operation is always conducted because it supports something greater than itself. This might for instance be the support of a strategic objective in peacetime, or an operational objective or decisive condition in a military operation.

  The contribution of a cyber operation is defined from the perspective of the broader context in which the cyber operations is conducted. The contribution makes sense as seen and understood by the higher levels tasking the cyber unit, from a non-technical perspective.
- **Structure**
  The contribution is broken down into two main factors:
  - **F14A. Contribution significance.** The significance of the contribution to the higher purpose. The significance has four levels: DECISIVE, SUBSTANTIAL, LIMITED and MARGINAL. The greater the significance of the contribution, the more likely that the higher purpose will not be fulfilled if the cyber operation fails.
  - **F14B. Contribution level.** The level of operation where the contribution primarily have an effect. The level has four options: STRATEGIC, OPERATIONAL, TACTICAL and SUB-TACTICAL.

Figur 4.1 Eksempel på en faktor – bidrag til større kontekst. Hentet fra Framework for analysis of cyber operations (FFI-notat under arbeid).

Ved bruk av rammeverket for en gitt analyse eller diskusjon, er det nødvendig med et forarbeid. I dette forarbeidet må det vurderes hvilke deler av rammeverket som er relevant for problem-stillingene som skal belyses. Deretter må en hensiktsmessig anvendelse planlegges. Dette kan medføre at rammeverket må tilpasses eller utvides, for eksempel med metodiske betraktninger eller steg.

Eksempler på forhold som påvirker utvalg og anvendelse av rammeverket er blant annet hvilken problemstilling en søker å belyse, hvor mye tid som er til rådighet, hvilke krav som settes til grundighet og dybde og hvilken kompetanse deltakerne har. Rammeverket er ikke en *silver bullet* som gir svar ut av intet; det forutsettes at det blir gitt tilstrekkelig med informasjon inn i prosessen hvor rammeverket benyttes. Personer med kunnskap og kompetanse må bidra med faglige vurderinger, da rammeverket i seg selv ikke gir noen avveiinger eller prioriteringer.

Der ulike typer personell skal møtes til diskusjon, anbefales det at det brukes en fasilitator som leder gruppen gjennom et spesialtilpasset opplegg. Dersom det er vanskelige problemstillinger som skal belyses, kan det være nødvendig med flere sesjoner for gradvis å bygge en felles forståelse av hva som er reelle uenigheter og hva som er språklige misforståelser.

4.2 Verktøy 2 – Metode for å utforske mulig bruk av cyberoperasjoner i en gitt situasjon

MECOGS[79] er en metode i syv steg for å utforske hvilke cyberoperasjoner som kan være hensiktsmessige i en gitt situasjon. Med situasjon menes en klart definert kontekst, for eksempel en militær operasjon med både motparts (røde) og egne (blå) målsettinger og handlemåter definert. Både offensive og defensive cyberoperasjoner omfattes av metoden.

[79] MEtode for å utforske mulig bruk av CyberOperasjoner i en Gitt Situasjon.

Metoden trekker på en blanding av ekspertvurderinger, faktorer fra rammeverket og forhåndsdefinerte maler for å fasilitere en serie diskusjoner i en ordnet rekkefølge. Brukerne veksler på å være den angripende og forsvarende part. Behovet for å definere gode cyberkapabiliteter unngås ved å knytte cyberoperasjoner til ambisjoner på utsiden av cyberdomenet gjennom identifiseringen av viktige systemer.

Metoden kan brukes for ulike formål. Dette inkluderer blant annet støtte til langtidsplanlegging, utvikling av scenarioer og vignetter ved øvelsesplanlegging, og analysestøtte for deltakere i øvelser og spill. Selve gjennomføringen kan utføres som table-tops, workshoper eller ulike former for strukturerte diskusjoner. For mange av disse formålene vil metoden anvendes på fiktive aktører, med en intensjon om å beskrive realistiske, men ikke reelle situasjoner, kapabiliteter og operasjoner. Således er det ikke nødvendig med høyt gradert informasjon for å få nytte av metoden. Samtidig er kvaliteten på resultatene direkte knyttet til kvaliteten på informasjonen som er tilgjengelig, uavhengig om denne er reell eller fiktiv.

De syv stegene i metoden er:

1. Velg situasjon
2. Sett motpartens ambisjoner for sine cyberoperasjoner
3. Identifiser mulige målsystemer og effekter som vil realisere motpartens ambisjoner
4. Sett sammen en leveranse for motparten
5. Vurder motpartens ressursbruk
6. Bestem defensivt operasjonskonsept
7. Vurder egen ressursbruk

1. Velg situasjon. Vi starter med å velge situasjonen som skal analyseres. Her brukes ordet *situasjon* fremfor det mer vanlige *scenario.* Hensikten med dette ordvalget er å unngå å bli unødig påvirket av hva som allerede er konkretisert av eksisterende scenarioer eller scenarioklasser. Det kan også være bevisste eller ubevisste begrensninger ved hvordan scenarioer vanligvis blir valgt og utviklet, som vi ikke ønsker å være bundet av. Situasjonen setter konteksten som videre bruk av cyberoperasjoner skal forstås inn i og vurderes opp imot.

2. Sett motpartens ambisjoner for sine cyberoperasjoner. Vi legger til grunn at motparten er den aktøren som har initiativet og som starter med offensive handlinger. Brukerne av metoden går inn i rollen som rød aktør og konkretiserer rammene for dennes bruk av offensive cyberoperasjoner. Dette inkluderer eventuelle føringer («*do's and dont's*»). Her er det tre understeg:

a. Definer hvilke type teknologiske systemer som potensielt kan være et mål. Her settes også mulige begrensninger, som for eksempel at kritisk infrastruktur eller operative teknologier (OT) ikke skal rammes.

b. Definer akseptable målsettinger i cyberdomenet. Dette kan for eksempel være uthenting av informasjon, tjenestenekt, destruktive effekter eller mer tilpasset manipulasjon av informasjon.

c. Beskriv hvordan motstanderens ambisjon i cyberdomenet bidrar inn i den større konteksten.[80]

3. Identifiser mulige målsystemer og effekter i disse som vil realisere motpartens ambisjon i cyberdomenet. På dette stadiet kjenner vi motpartens ambisjoner fra forrige steg. Nå går vi inn i rollen som blå aktør. Med kunnskap om egne systemer skal vi identifisere mulige målsystemer og effekter. To momenter bør vurderes:

a. Hvilke systemer er viktige for blå aktør, og hvorfor[81]

b. Hva er gode kandidater av målsystem- og effektkombinasjoner for å oppnå motparts ambisjon

Høyst sannsynlig er det en sammenheng mellom hvilke systemer som er viktige for blå, og hvilke systemer som rød kan angripe for å realisere sin ambisjon. Det skal likevel ikke utelukkes at systemer som er mindre viktige for blå kan angripes, dersom målsettingene til rød og blå ikke er direkte motstridende.

4. Sett sammen en leveranse for motparten. Her spesifiseres motpartens mulige cyberoperasjoner i mer detalj. Vi går derfor tilbake til rollen som rød aktør. For hvert alternativ vi ønsker å utforske setter vi sammen en *leveranse*[82] for motparten, som beskriver en rekke egenskaper ved en offensiv cyberoperasjon:

a. Valgt (teknisk) effekt

b. Valgt målsystem

c. Krav til egenskaper som presisjon, nøyaktighet og omfang (*precision*, *accuracy* og *magnitude*)

5. Vurder motpartens ressursbruk. Hva mener vi er nødvendig innsats for å kunne lage og levere en gitt leveranse? For å ha en formening om hvor mye innsats som er nødvendig for ulike leveranser, kreves det et forarbeid med å kalibrere ulike nivåer av innsats opp mot ulike målsystemer og vanskelighetsgraden i det en forsøker å få til. Vi foreslår at dette gjøres ved å

[80] Her brukes rammeverket for å gi struktur til beskrivelsen, ved hjelp av faktoren *F14. Contribution to the broader context*. Se figur 4.1 hvor denne faktoren er omtalt.
[81] Dersom militære systemer er mulige mål, kan deler av prosjektets metode for å inkludere IKT i langtidsplanlegging benyttes for å identifisere systemer som er viktige for realiseringen av militær evne. Dette vil imidlertid kreve en del forarbeid. Se Farsund, B., Thuv, Aa., Hansen, B. J. (2022). *Hvordan håndtere IKT i Forsvarets langtidsplanlegging.* FFI-rapport 22/01569. https://www.ffi.no/publikasjoner/arkiv/hvordan-handtere-ikt-i-forsvarets-langtidsplanlegging.
[82] *Leveranse* er en oversettelse av begrepet *deliverable*, som her peker på at faktor *F15. Deliverable* i rammeverket skal konkretiseres. Denne faktoren beskriver en teknisk effekt i et teknisk system samt en rekke egenskaper.

utarbeide og fylle inn et sett med maler som kobler ulike angrep og egenskaper ved disse til ulike innsatsnivåer. I skrivende stund er forslag til parametere i malene utarbeidet. Gitt en slik tilnærming foreslås følgende understeg:

a. Velg en passende mal eller utarbeid en ny hvis ingen ferdigutfylte maler passer.

b. Verifiser eller utfør kalibreringen av innsats.

c. Utfør en realitetssjekk – er det realistisk å oppnå den valgte effekten med dennes karakteristikker, å sette av den nødvendige innsatsen? Mener vi denne løsningen er hensiktsmessig gitt motpartens plan i og på utsiden av cyberdomenet?

Realitetssjekken vil også kunne utføres opp mot eventuelle krav til eller rammebetingelser for den utøvende cyberenheten. For eksempel vil to ulike cyberenheter kunne ha ulik risikoappetitt som medfører at den ene vil utføre operasjoner som den andre ikke vil gjøre. Det samme gjelder stater. Realitetssjekken kan også gjøres mot dilemmaer som stater står i, for å unngå at det utføres cyberoperasjoner som er i strid med statens valgte innretting.[83]

6. Bestem defensivt operasjonskonsept. Vi går da tilbake til å være blå aktør. Dersom målsettingen med en blå defensiv cyberoperasjon er å kunne avverge, stå imot, håndtere eller mitigere den spesifikke røde offensive cyberoperasjonen, hva slags defensivt operasjonskonsept vil være passende i den gitte situasjonen?[84] Ulike defensive operasjonskonsepter bør her utvikles, enten i forkant eller som en del av anvendelsen av metoden.

7. Vurder egen ressursbruk, og eventuelt andre krav som blir identifisert.[85] I prinsippet speiler dette steget steg nummer fem, ved at ulike former for innsats knyttes til ulike blå defensive cyberoperasjoner. Igjen er det et behov for å utvikle maler med spesifiserte og kalibrerte innsatsnivåer.

Beskrivelsen av metoden har lagt til grunn at motparten er den offensive part. Dermed er én eller flere offensive cyberoperasjoner av motpart og én eller flere defensive cyberoperasjoner av oss som forsvarende part gjennomgått. Det er imidlertid ingen hindringer mot å snu hvem som er den offensive og defensive part. Dette beror på hvem som er *initiativtaker.* Dersom det er ønskelig å utforske muligheter for egne offensive cyberoperasjoner og motparts defensive cyberoperasjoner, velger vi oss selv som rød aktør og motpart som blå. Med et slikt utgangspunkt vil for eksempel bruk av egne cyberoperasjoner for etterretning og effekt kunne utforskes, inklusive rammer for juridisk og etisk forsvarlig bruk.

[83] Se kapittel 3.1.2.
[84] I dette steget har vi valgt å knytte den defensive cyberoperasjonen direkte til motparts offensive cyberoperasjon. Dersom en gjør dette vil hva som er et passende defensivt operasjonskonsept være styrt av den gitte situasjonen (som blant annet inkluderer motparts offensive cyberoperasjon, vår egen militære operasjon, og statens prioriteringer). Det er imidlertid ikke gitt at å koble de defensive cyberoperasjonene til motparts offensive cyberoperasjoner på denne måten alltid er hensiktsmessig.
[85] Andre krav kan for eksempel være hvilke støtteverktøy eller egenskaper informasjonsinfrastrukturen må ha for å kunne understøtte valgte defensive konsepter.

4.3 Verktøy 3 – Matriser for å spenne ut mulige situasjoner

Matriser for å spenne ut mulige situasjoner er et hjelpemiddel for bedre å forstå hva slags situasjoner det kan være relevant for staten å bruke cyberoperasjoner i. Matrisene dekker dermed ikke cyberoperasjoner som sådan, men ulike strategiske kontekster hvor cyber-operasjoner kan tas i bruk. Ved utforsking av tenkte situasjoner er verktøyet ment å være en hjelp i første steg av verktøy 2 – metode for å utforske mulig bruk av cyberoperasjoner i en gitt situasjon.

En matrise i denne sammenheng er et sett kolonner med verdier. Kolonnene dekker viktige parametere som definer en situasjon, mens cellene dekker mulige verdier. Et eksempel er kolonnen for geografisk aktivitetsområde, som har verdiene *eget territorium*, *NATO-medlems-land*, *naboland til NATO-medlemsland* og *stat som ikke grenser til NATO.* Matrisene er første steg i morfologiske analyse, uten at vi har gått videre inn i slike analyser.[86]

Det er utviklet fire ulike matriser for røde og blå aktører, som dekker:

- Rød offensiv matrise
- Rød defensiv matrise
- Blå offensiv matrise
- Blå defensiv matrise

Matrisene er utviklet i den internasjonale forskningsgruppen SAS-167, og har derfor NATO som blå aktør. Gradering gjør at selve matrisene ikke kan inkluderes i denne rapporten.

4.4 Verktøy 4 – Sentrale steg for integrasjon av cyberoperasjoner i planlegging og gjennomføring av militære operasjoner

Sentrale steg for integrasjon av cyberoperasjoner er en tilpasning av syv-stegs-metoden MECOGS til en bestiller-leverandør-modell for cyberoperasjoner. Den grunnleggende idéen er at eieren av en kontekst, som sjefen for en militær operasjon, og aktørene som står for cyber-operasjoner må finne frem til offensive cyberoperasjoner som er hensiktsmessige for alle parter. I denne bestiller-leverandør-modellen setter eieren noen grunnleggende krav, leverandørene vurderer sine muligheter og legger disse frem på en måte som ikke bryter med nødvendig hemmelighold.

Avhengig av hvordan ansvar, roller og myndighet er fordelt i en gitt nasjon, kan ulike entiteter påta seg rollen som bestiller og leverandør. Eksempelvis kan én entitet la ulike interne enheter innta hver sin rolle og gjennomføre alle stegene internt. I Nato-sammenheng vil rammene for

[86] For en introduksjon til morfologisk analyse, se Johansen, I. (2018). Scenario modelling with morphological analysis. *Technological Forecasting and Social Change, 126*(January 2018), 116–125. https://doi.org/10.1016/j.techfore.2017.05.016

bestiller-leverandør kunne være SCEPVA[87], selv om nåværende ansvarsfordeling trolig vil føre til at begge roller ivaretas av medlemslandene.

4.5 Tillegg – vurdering av scenario- og kapabilitetsbasert metodikk for inkludering av cyberoperasjoner

For å bidra til økt innsikt i forsvarsplanlegging av cyberoperasjoner har vi gjort vurderinger av scenario- og kapabilitetsbasert metodikk for langtidsplanlegging og dennes egnethet. Arbeidet er grunnlaget for kapittel 3.2.

Problemstillinger	Verktøy
Etablere grunnforståelse av cyberoperasjoner i en større kontekst	
1. Hva er cyberoperasjoner og hvilke typer finnes?	-
2. Hva er sentrale forhold og rammefaktorer for en stat?	V1
3. Hva er sentrale faktorer å ta hensyn til i analyser og diskusjoner?	V1
Utforske mulig bruk av cyberoperasjoner for en liberal demokratisk småstat	
4. Hvilke typer CO bør studeres?	-
5. Hva er staters ambisjoner som kan støttes med CO?	V1
6. Hvilke muligheter og begrensninger ligger i virkemidlet?	V1, V2
7. I hvilke situasjoner er det potensielt relevant å benytte CO?	V3
8. Gitt en situasjon, hva er mulig kost, nytte og risiko ved bruk av CO?	V2
9. Hvordan kan stater balansere sin CO-innsats mellom effekt, etterretning og påvirkning (off. og def.)?	V1
10. Hvordan vekter vi mellom ulike alternativer?	V1
Inkludere cyberoperasjoner i forsvarsplanlegging	
11. Hvordan passer CO i eksisterende metodikk for forsvars- og langtidsplanlegging?	T1
12: Hvilke utfordringer må løses ved inkludering?	T1
13. Hvilke andre metodikker kan være egnet for inkludering av cyberoperasjoner?	-
14. Hvordan kan vi integrere CO i disse?	-
15. Hvordan kan vi sammenstille og vurdere resultater fra disse?	-
Integrere cyberoperasjoner i planlegging og gjennomføring av militære operasjoner	
16. Hvordan kan planlegging og utførelse av CO integreres i en planprosess	V4
17. Hvordan kan kommunikasjonsutfordringer mellom fageksperter og annet militært personell løses?	V4, V1
18. Hvordan kan manglende kunnskap om egen avhengighet om IKT opparbeides?	*

Tabell 4.2 Sentrale problemstillinger for en stat, knyttet til analytiske verktøy.[88]

Som en del av dette arbeidet ble det også utviklet en innledende liste over sentrale spørsmål som en stat vil ønske å besvare knyttet til forsvarsplanlegging. Denne listen ble senere utviklet til en første versjon av en mer generell liste over sentrale problemstillinger ved cyberoperasjoner for en stat, dog med noe bias i retning langtidsplanlegging. (Se tabell 4.2).

[87] «Sovereign Cyber Effects Provided Voluntarily by Allies», Natos mekanisme for å integrere cyberoperasjoner levert av medlemsland i Natos operasjoner. Se f.eks. Brent, L. (2019). NATO's Role in Cyberspace. *NATO Review*. https://www.nato.int/docu/review/articles/2019/02/12/natos-role-in-cyberspace/index.html

[88] I tabellen angir en bindestrek at ingen av verktøyene adresserer den gitte problemstillingen i nevneverdig grad. En stjerne angir at andre arbeider i prosjektet møter problemstillingen, i dette tilfellet prosjektets arbeid med en metode for å håndtere IKT i langtidsplanlegging. Se Farsund, B., Thuv, Aa., Hansen, B. J. (2022). *Hvordan håndtere IKT i Forsvarets langtidsplanlegging*. FFI-rapport 22/01569. https://www.ffi.no/publikasjoner/arkiv/hvordan-handtere-ikt-i-forsvarets-langtidsplanlegging.

For mange av spørsmålene finnes det i utgangspunktet ingen unike, korrekte svar. En dialog må føres mellom ulike interessenter for å utforske, vurdere og etter hvert bestemme hva statens nasjonale tilnærming til cyberoperasjoner skal være. Her er identifisering av avveiinger og dilemmaer sentralt. Listen av problemstillinger kan også være et utgangspunkt for å bestemme hva en skal forsøke å jobbe mer målrettet mot og hva fokuset til nye verktøy skal være.

4.6 Oversikt over utfordringer og verktøy

Verktøyene omtalt i dette kapitlet kan bidra til å håndtere utfordringene som ble identifisert i kapittel 3. Se tabell 4.3 for en samlet oversikt.

Utfordringer	Verktøy
Analyse av cyberoperasjoner som et statlig virkemiddel	
1. Det er mangel på empiri og teori	V1
2. En stat har konkurrerende interesser og står i dilemmaer	V1
3. Virkemidlet har særegne egenskaper	V1
Inkludere cyberoperasjoner i langtidsplanlegging	
4. Å utforske mulige cyberrelaterte trusler grundig er vanskelig	V2, V3
5. Hvordan krav bør utledes er ikke kjent	V2
6. Det er store informasjonsmangler knyttet til referanseenhetene	V2
7. Ytelsen til referanseenhetene er av natur ustabil og usikker	-
8. Scenarioene ilegges betydning utover den tiltenkte	-
Inkludere cyberoperasjoner i planlegging og gjennomføring av militære operasjoner	
9. Meget høy grad av hemmelighold ved offensive cyberoperasjoner	V4
10. Ulike planleggings- og gjennomføringsrytmer	V4
11. Kommunikasjonsutfordringer mellom fageksperter og annet militært personell	V1
12. Manglende kunnskap om egen avhengighet av IKT	*

Tabell 4.3 Utfordringene og relevante verktøy.[89]

I hovedsak kan rammeverket (V1) bidra til å håndtere utfordringene knyttet til analyse av cyberoperasjoner som et statlig virkemiddel, samt utfordringene ved kommunikasjon mellom fageksperter og annet militært personell. MECOGS (V2) kan bidra i håndteringen av flere av utfordringene knyttet til inkludering av cyberoperasjoner i langtidsplanlegging. Her kan også matrisene (V3) bidra til en bedre utforsking av trusler. Bestiller-leverandør-modellen (V4) kan bidra i planlegging og gjennomføring av militære operasjoner. Denne fremstillingen er imidlertid en forenkling og en må vurdere de konkrete målene med et gitt arbeid for å se hvordan de ulike verktøyene best kan brukes.

[89] Tegnsettingen i tabell 4.3 er lik tegnsettingen i tabell 4.2, men tabell 4.3 viser utfordringer fremfor problem-stillinger. Se fotnote 87.

5 Vurdering og anbefaling om veien videre

Stater står overfor en rekke spørsmål knyttet til cyberoperasjoner. Dette inkluderer blant annet hva slags cyberoperasjoner en stat kan gjennomføre, hva hensiktsmessige ambisjoner er for disse, hvilken risiko staten står overfor og hvilke konsept de involverte enheter kan operere etter. I dette ligger det også vurderinger om hva slags aktør staten ønsker å fremstå som, og hvilke forventninger staten ønsker å innfri fra andre stater og allianser. Slike spørsmål må besvares på veien til å finne ut av hvordan staten bør innrette sine cyberoperasjoner, hva staten skal sette av midler til, og hvordan allokerte penger skal benyttes.

Vår tilnærming til å begynne å finne svar på slike spørsmål, har vært å bygge analytiske verktøy. Gitt behovet for økt sporbarhet og tydelighet i argumenter når kunnskapsgrunnlaget er tynt, er vårt fokus på å etablere metoder og struktur fremfor å spekulere oss raskest mulig frem til svar. Dette mener vi vil tydeliggjøre avveiinger og dilemmaer, og gjøre det enklere å se forutsetninger, antakelser og vurderinger.

Utviklingen av verktøy har bidratt til å avdekke sammenhenger og underliggende problemstillinger. Vi mener at det er mer å hente langs dette sporet og at verktøyutvikling derfor bør fortsette. Å jobbe på lav gradering har gjort det mulig å involvere internasjonale fagmiljøer, og dette bør opprettholdes. Samtidig er det nødvendig å teste verktøyene i reelle analysesituasjoner, for kvalitetskontroll og for å utvikle verktøyene. Med reell analysesituasjon menes her en situasjon der faktiske interessenter har et analysebehov og hvor verktøyene forsøkes anvendt for å støtte interessentene.

Dersom den norske konteksten skal belyses, vil det være nødvendig å samarbeide tett med relevante aktører nasjonalt for å få mer informasjon om særnorske forhold og valg som er tatt. Dette inkluderer også detaljert informasjon om Norges cyberenheter og deres operasjoner. Slik informasjon kan være starten på et eget analyseløp som i større grad tar utgangspunkt i Norges situasjon.[90] Gitt sensitiviteten på temaet vil dette være en meget lukket prosess. Innsikt fra dette analyseløpet vil likevel være til nytte for å forbedre de utviklede verktøyene. En utfordring vil i så måte være å unngå at sensitiv informasjon kan leses ut av verktøyene, samtidig som den lave graderingen blir opprettholdt.

En tilnærming som går mer inn i de ulike nasjonale aktørenes behov er meget aktuell. For eksempel kan departementer og andre aktører bli intervjuet for å kartlegge i større detalj hvilke beslutninger de skal ta knyttet til cyberoperasjoner og hva slags beslutningsgrunnlag de har behov for. Dette kan gi mer målrettede verktøy og analyser som direkte understøtter aktørenes behov. Et slikt arbeid kan være et godt utgangspunkt for å lage en forankret oversikt over hvilke problemstillinger Norge som stat må arbeide med.

[90] Dette kan sees på som den andre retningen i veivalget vi stod overfor tidligere i prosjektet, som omtalt i kapittel 2.2.

Her kan også samarbeid med andre stater være nyttig, for å få innsikt i hvilke sentrale problemstillinger statene har identifisert og hvilke løsninger de har vurdert. Det er imidlertid ikke rett frem å overføre lærdommer fra andre stater, selv om statene gjør liknende avgrensninger, står i de samme dilemmaene og er like på andre områder. En gitt stats sikkerhetspolitiske interesser, historie, kultur, lovverk med mer påvirker hva som er akseptabelt og hensiktsmessig og kan avvike fra hva en annen ellers liknende stat vil legge til grunn. Hvilke lærdommer som eventuelt er overførbare til norsk kontekst, må derfor vurderes grundig.

6 Oppsummering

Utviklingen av trusselbildet i de senere år medfører at de fleste, om ikke alle stater må ta stilling til hvordan de skal forholde seg til cyberoperasjoner. Dette inkluderer håndtering av fiendtlige cyberoperasjoner, ved å gjennomføre egne defensive cyberoperasjoner. Det inkluderer selv å utnytte det offensive mulighetsrommet, gjennom egne offensive cyberoperasjoner. For en stat som ønsker å bruke cyberoperasjoner som et militært virkemiddel, er forsvarsplanlegging og gjennomføring og planlegging av militære operasjoner to sentrale områder hvor det er viktig å få cyberoperasjoner inkludert på en god måte.

Inkludering av cyberoperasjoner i disse to områdene er imidlertid ikke enkelt. Det eksisterer en rekke utfordringer, omtalt i kapittel 3, som gjør det vanskelig å analysere og behandle cyber-operasjoner som tradisjonelle militære virkemidler. Dette gjør det vanskelig å bruke etablerte metoder for langtidsplanlegging, og kompliserer inkluderingen i militære operative prosesser.

I vårt arbeid har vi forsøkt å skape analytiske verktøy for å møte utfordringene. Disse skal hjelpe analytikere og andre brukere med å skape konsistente argumentasjonskjeder på en sporbar måte. Verktøyene gir ikke endelige svar, men bidrar til å sette en felles kontekst, løfte frem sentrale faktorer og å lede brukerne fremover ved analyser og diskusjoner. Det vil imidlertid alltid være en viss usikkerhet knyttet til resultatene fra slike verktøy.

Gjennom utvikling av verktøyene har vi gjort oss mange erfaringer, og vi har vurdert mange sider ved analyse av cyberoperasjoner. En sentral konklusjon er at cyberoperasjoner må ses på som et statlig virkemiddel, ikke kun et militært virkemiddel. Statsperspektivet er grunnleggende for å gjøre gode vurderinger. Umodenheten i fagfeltet gjør at det er behov for etablering og videreutvikling av et konsistent konseptuelt grunnlag som understøtter dette. Det inkluderer å ivareta tekniske, operative og politiske forhold, å tydeliggjøre avgrensninger og å understøtte ulike konseptuelle valg. Stater har ulike interesser, ambisjoner og prioriteringer, og dette må grunnlaget – inklusive verktøyene – kunne ta hensyn til.

Det er imidlertid ikke opplagt hvordan relevant kunnskap best kan utvikles. Veien videre bør derfor gå langs flere spor. Dette kan inkludere å lære av andre stater, så lenge en er bevisst på at hva som passer for stat A ikke nødvendigvis passer for stat B. Her må det gjøres grundige vur-deringer. Verktøyene kan utvikles videre, med videreføring av internasjonalt samarbeid eller i dialog med nasjonale aktører. Til sist kan verktøyene, med de rette forberedelser, nå anvendes for å belyse spesifikke problemstillinger.

Arbeidet har i stort vært generisk, i den forstand at vi ikke har bundet oss stramt til Norges eller andre staters eksisterende tolkninger og tilnærminger til cyberoperasjoner. Dette har vært bevisst og nødvendig for å unngå kunstige begrensninger i analyser og vurderinger. Men veien fremover bør derfor også bestå av en bevisstgjøring, en konkretisering, en *instansiering* av det generelle til norske forhold eller til andre stater som vi ønsker økt innsikt i.

Vedlegg

A Konkretisering av begrepene offensive og defensive cyberoperasjoner

Valg av definisjoner og konkretisering av disse kan være en utfordrende eksersis. I vårt arbeid har vi behov for et begrepsapparat som lar oss avgrense fenomenet vi ønsker å studere på en fornuftig måte, samtidig som begrepene hjelper oss med å forstå andre stater i tillegg til vår egen.

Som nevnt i kapittel 1, er autoritative begreper også under utvikling og gjenspeiler en vekselvirkning mellom fag og politikk. Valg av bestemte enkeltord og begreper, grenseoppganger mellom dem, hvordan de sammenstilles og settes i rekkefølge samt andre nyanser kan ha stor betydning for hvordan innholdet skal forstås og hva innholdet impliserer. Dette skyldes ikke bare det språklige eller fenomenale, men også forhold som fordeling av ansvar, roller og myndighet, juridiske forhold, allokering av finansielle ressurser.

Hva en stat velger å inkludere i dens definisjoner bidrar dermed til å forme hva staten gjør og mengden innsats den legger ned. Med en avgrensning av offensive cyberoperasjoner til tilegnelse og anvendelse av uautoriserte tilganger, vil offensive operasjoner typisk fremstå som mye mer marginale for en stat i omfang sammenliknet med innsatsen for å håndtere uautorisert tilgang. Offensive cyberoperasjoner blir en smal disiplin, ofte planlagt og teknisk gjennomført av mennesker med høy spesialkompetanse. Avhengig av statens organisering, vil elementer som for eksempel taktisk ledelse og strategisk styring også inngå i organisasjonsstrukturen.

På den defensive siden vil en bred tolkning omfatte alle som er involvert i arbeidet med å sikre, overvåke og håndtere hendelser med uautoriserte tilganger i systemer og infrastrukturer som befinner seg i en stat, offentlig som privat. Proaktivt arbeid i forkant av en hendelse vil også kunne inkluderes. Samtidig vil en smal tolkning av defensive cyberoperasjoner kunne innebære en tilsvarende eller mindre innsats enn den offensive innsatsen. For eksempel om defensive cyberoperasjoner defineres til kun å omfatte arbeidet til en mindre militær enhet, som opererer i militær infrastruktur og som ikke har ansvar for grunnsikring, drift og vedlikehold eller regulær sikkerhetsovervåking. En stat vil kunne velge å fokusere sin innsats innen defensive cyberoperasjoner mot utvalgte deler av det en tolkning gir rom for, basert på egne vurderinger og prioriteringer.

I vår rapport tar vi utgangspunkt i staters bruk av uautoriserte tilganger for å fremme egne interesser overfor omverdenen, og motstykket – den defensive siden – staters håndtering av andres bruk av uautoriserte tilganger.

Alternativet «dataangrep» er problematisk da ordet angrep kan leses til kun å omfatte staters villede angrep, utover etterretning og vanlig kriminalitet. Ordet «datainnbrudd» (*computer intrusion*) er mer presist, men kan på norsk leses til å kun omfatte kriminell aktivitet. Vi bruker derfor «uautorisert tilgang».

Offensive cyberoperasjoner

Offensive cyberoperasjoner med bruk av uautoriserte tilganger fremstår som en egen type operasjoner som kan lede til potensielt store positive og negative konsekvenser for stater som bruker dem, både operativt og politisk. Det tekniske håndverket er en egen disiplin, og den taktiske dynamikken mellom forsvarer og angriper er særegen.[91] Vi deler inn i to typer offensive cyberoperasjoner som benytter uautoriserte tilganger:[92]

1. *Cyberoperasjoner for etterretning* omfatter uautoriserte tilganger hvor målet er å hente ut informasjon. Innbruddet og videre aktiviteter holdes typisk skjult, slik at tilstedeværelsen ikke blir oppdaget og uthentingen forhindret.

2. *Cyberoperasjoner for effekt* omfatter uautoriserte tilganger hvor de oppnådde tilgangene brukes til å iverksette en teknisk effekt. Den tekniske effekten er bare starten på en lengre årsakskjede som på en eller annen måte skal ha ønskede konsekvenser på utsiden av cyber-domenet. Ofte benytter cyberoperasjoner for effekt tilganger som er ervervet gjennom cyberoperasjoner for etterretning. Det finnes dog mer opportunistiske operasjonsmåter som ikke legger egne, tidligere etablerte tilganger til grunn for cyberoperasjonene.

Bruk av systemer og infrastruktur som ikke krever uautoriserte tilganger, definerer vi til ikke å være cyberoperasjoner. Det betyr at for eksempel bruk av falske kontoer på sosiale medier som formidler feilaktig informasjon, ikke ansees som en cyberoperasjon. Likevel kan flere opera-sjonstyper settes sammen i en kampanje, og derigjennom spille sammen. For eksempel kan en cyberoperasjon for etterretning hente ut informasjon, og en påvirkningsoperasjon kan legge informasjonen ut på internett. Til sammen blir dette *hack-and-leak*. Påvirkningsoperasjonen omfatter i dette tilfellet ikke en cyberoperasjon, med mindre uautoriserte tilganger brukes å lekke informasjonen via et bestemt system.

Det finnes også andre måter å kategorisere og karakterisere offensiver cyberoperasjoner på. For eksempel ved hjelp av nivået operasjonen gjennomføres eller søker effekt på (strategisk, operasjonelt, taktisk), om effektene er logiske effekter i IT-systemer eller fysiske utslag i OT[93]-

[91] Dette gjelder særlig uautorisert tilgang der sikkerhetsmekanismer i operativsystem og programvare er brutt på teknisk nivå.
[92] Denne inndelingen gjenspeiler to ulike, sentrale mål for offensive cyberoperasjoner. Se for eksempel Poznansky, M. (2021, 23. mars). Covert action, espionage, and the intelligence contest in cyberspace. *War on the Rocks.* https://warontherocks.com/2021/03/covert-action-espionage-and-the-intelligence-contest-in-cyberspace/; Forsvaret (2019, s. 125). *Forsvarets fellesoperative doktrine (FFOD).* Forsvarsstaben. http://hdl.handle.net/11250/2631948. Det er mulig å definere flere kategorier, se for eksempel fransk doktrine for offensive cyberoperasjoner som har villedning som en tredje kategori. Delerue, F., Desforges, A., Géry, A. (2019, 23. april). A close look at France's new military cyber strategy. *War on the Rocks.* https://warontherocks.com/2019/04/a-close-look-at-frances-new-military-cyber-strategy/
[93] Operative teknologier.

systemer og aktuatorer (åpne en dam, ødelegge en sentrifuge). Videre diskusjon om dette er utenfor denne rapporten.

Defensive cyberoperasjoner

Defensive cyberoperasjoner for håndtering av uautoriserte tilganger gjør det mulig å analysere offensive og defensive cyberoperasjoner med en tydeligere sammenheng mellom dem. For å ha mulighet til å fange opp den fulle bredden av hva håndtering av uautoriserte tilganger kan omfatte, legger vi til grunn fire ulike aktivitetskategorier som spenner over det tekniske, operative og politiske:[94]

1. Forberedelser og beredskap
2. Proaktiv tilpasning på kort sikt
3. Reaktiv hendelseshåndtering
4. Proaktiv strategisk initiativtaking og posisjonering

Kategori 1 – forberedelser og beredskap innebærer å etablere en velfungerende evne til rettidig utøvelse av defensive cyberoperasjoner, med blant annet alt som trengs av planarbeid, utvikling av konsepter, og implementering av prosesser.

Kategori 2 – proaktiv tilpasning på kort sikt omfatter å gjøre de nødvendige endringer for å være best mulig stilt i lys av en overhengende identifisert trussel. Dette kan for eksempel være tekniske endringer i infrastrukturen og prosessuelle endringer i organisasjonen (f.eks., opprettelsen av en arbeidsgruppe) som gjøres ved mottak av etterretningsinformasjon om at fiendtlige offensive cyberoperasjoner er nært forestående eller øker i innsats. En god forståelse for pågående og planlagte operasjoner, inkludert operasjonsdesign, mulige handlemåter og avhengigheten til infrastrukturen som benyttes, er nødvendig.

Kategori 3 – reaktiv hendelseshåndtering omhandler hendelseshåndtering ved deteksjon av en fiendtlig offensiv cyberoperasjon. Hendelseshåndtering tolkes her bredt og inkluderer evne til

[94] Kilder til inspirasjon for disse kategoriene er blant annet ulike tankesett innen defensive cyberoperasjoner, *incident management* og beredskap og krisehåndtering. Se for eksempel NCSC (u.å.) *Incident Management*. https://www.ncsc.gov.uk/collection/incident-management; U.S. Cyber Command (2022, 25. oktober). *CYBER 101 – Defend forward and Persistent Engagement*. https://www.cybercom.mil/Media/News/Article/3198878/cyber-101-defend-forward-and-persistent-engagement/; Laudrain, A. P. B. (2019, 26. februar). France's New Offensive Cyber Doctrine. *Lawfareblog.* https://www.lawfareblog.com/frances-new-offensive-cyber-doctrine; Vašíčková, V. (2020). Crisis Management Process - A Literature Review and a Conceptual Integration. *Acta Oeconomica Pragensia 27*(3-4):61-77. https://doi.org/10.18267/j.aop.628; Myndigheten for samhällsskydd och beredskap (2022, 19. september). *Nytt beredskapssystem träder i kraft den 1 oktober*. https://www.msb.se/sv/aktuellt/nyheter/2022/september/nytt-beredskapssystem-trader-i-kraft-den-1-oktober/. For norske kilder, se for eksempel NSM (2017, 7. desember). *Rammeverk for håndtering av IKT-sikkerhetshendelser.* https://nsm.no/regelverk-og-hjelp/andre-publikasjoner/rammeverk-for-handtering-av-ikt-hendelser/; Samfunnssikkerhetsinstruksen (2017). *Instruks for departementenes arbeid med samfunnssikkerhet.* FOR-2017-09-01-1349. https://lovdata.no/dokument/LTI/forskrift/2017-09-01-1349; Cyberforsvaret (2022, 1. juli). *Konsept for defensive cyberoperasjoner.*

deteksjon og alle tiltak og vurderinger som gjøres som reaksjon på den detekterte cyberoperasjonen. Selv om fokuset i hovedsak er vendt innover på egen infrastruktur, kan dette også inkludere iverksettelsen av en offensiv cyberoperasjon og politiske reaksjoner som respons.

Med hendelseshåndtering må det ikke forstås en implementering av en helpdesk eller en tradisjonell IT-organisasjon i tråd med ISO-standarder eller rammeverk som ITIL. Vi legger til grunn at i en militær kontekst vil hendelseshåndtering bli implementert på en måte som er forenelig med andre operative prosesser, og at vurderingene som gjøres i håndteringen er farget av militære prioriteringer og operative forhold i lys av pågående og planlagte militære operasjoner.

Kategori 4 – proaktiv strategisk initiativtaking og posisjonering omhandler strategisk posisjonering på lengre sikt. Dette omfatter for eksempel iverksettingen av konsepter som *defend forward*, hvor kompromittering og nøytralisering av fiendtlig cyberinfrastruktur gjøres før angrep inntreffer, og *hunt forward* hvor egne cyberressurser som personell og utstyr flyttes ut til en samarbeidspartner og hvor disse sitter sammen for å gjøre undersøkelser og hendelseshåndtering i partneres nett. Samarbeidspartneren kan være en annen stat.

Alle kategoriene reflekterer et tankesett om at vi er i en konflikt med én eller flere trusselaktører som benytter uautoriserte tilganger som teknikk. Grunnsikring og drift og vedlikehold av en infrastruktur, som er en sentral del av å være godt forberedt på fiendtlige offensive cyberoperasjoner, definerer vi i utgangspunktet til å håndteres som en del av løpende, kontinuerlig cybersikkerhetsarbeid på utsiden av defensive cyberoperasjoner.

Denne måten å definere defensive cyberoperasjoner har også sine ulemper. Den tar i mindre grad hensyn til eksisterende grenseoppganger mellom begreper som cybersikkerhet, hendelseshåndtering og defensive cyberoperasjoner. Det er således fullt mulig å være uenig i denne oppdelingen. Dette er imidlertid ikke nødvendigvis et problem for å kunne nyttiggjøre seg av resultater fra analyser som bruker denne tilnærmingen.

Referanser

Applebaum, J., Gibson, A., Guarnieri C., Müeller-Maughn, A., Poitras, L., Rosenbach, M., Ryge, L., Schmundt, H., Sontheimer, M. (2015, 17. januar). NSA Preps America for Future Battle. *Der Spiegel.* https://www.spiegel.de/international/world/new-snowden-docs-indicate-scope-of-nsa-preparations-for-cyber-battle-a-1013409.html [sist besøkt 27. november 2022].

Ashton, G. (2020) *Maersk, me & Notpetya.* https://gvnshtn.com/posts/maersk-me-notpetya/ [sist besøkt 22. november 2022].

Atlantic Council (u.å.). *Transcript: Lessons from Our Cyber Past – The First Military Cyber Units.* March 5, 2012 Cyber Statecraft Initiative event. https://www.atlanticcouncil.org/commentary/transcript/transcript-lessons-from-our-cyber-past-the-first-military-cyber-units/ [sist besøkt 28. november 2022].

Ball, J., Borger, J., Greenwald, G. (2013, 6. september). Revealed: How US and UK spy agencies defeat internet privacy and security. *The Guardian.* https://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security [sist besøkt 20. mars 2023].

Beecroft, N. (2022, 3. november). Evaluating the International Support to Ukrainian Cyber Defence. *Carnegie Endowment for International Peace.* https://carnegieendowment.org/2022/11/03/evaluating-international-support-to-ukrainian-cyber-defense-pub-88322 [sist besøkt 16. mars 2023].

Blessing, J. (2022, 2. september). *Revisiting the Russain Viasat Hack: Four Lessons About Cyber on the Battlefield*. American Enterprise Institute. https://www.aei.org/foreign-and-defense-policy/revisiting-the-russian-viasat-hack-four-lessons-about-cyber-on-the-battlefield/ [sist besøkt 25. november 2022].

Brent, L. (2019). NATO's Role in Cyberspace. *NATO Review*. https://www.nato.int/docu/review/articles/2019/02/12/natos-role-in-cyberspace/index.html [sist besøkt 31. oktober 2022].

Bruvoll, J., Thuv, Aa., Enemo, G. (2022). *Håndtering av IKT-sikkerhetshendelsene i Helse Sør-Øst og fylkesmannsembetene - en vurdering*. FFI-rapport 20/01560. https://www.ffi.no/publikasjoner/arkiv/handtering-av-ikt-sikkerhetshendelsene-i-helse-sor-ost-og-fylkesmannsembetene-en-vurdering

Buchanan, B. (2020). *The hacker and the state: Cyber attacks and the new normal of geopolitics.* Harvard University Press.

Burt, T. (2020, 21. desember). Cyber mercenaries don't deserve immunity. *Microsoft.* https://blogs.microsoft.com/on-the-issues/2020/12/21/cyber-immunity-nso/ [sist besøkt 16. mars 2023].

Corera, G. (2019, 21. oktober) Russian hackers cloak attacks using Iranian group. *BBC News.* https://www.bbc.com/news/technology-50103378 [sist besøkt 7. mars 2023].

Corera, G. (2022, 30. oktober). Inside a US military cyber team's defence of Ukraine. *BBC News.* https://www.bbc.com/news/uk-63328398 [sist besøkt 31.oktober 2022].

Cyberforsvaret (2022, 1. juli). *Konsept for defensive cyberoperasjoner.*

The Cyber Peace Institute (2022). *Cyber Attacks in Times of Conflict Platform #Ukraine* https://cyberconflicts.cyberpeaceinstitute.org/ [sist besøkt 28. november 2022].

Davis, S. (2019). *NATO in the Cyber Age: Strengthening Security & Defence, Stabilising Deterrence*. Science and technology committee (STC), NATO Parliamentary Assembly. General report. https://www.nato-pa.int/download-file?filename=/sites/default/files/2019-10/REPORT%20148%20STC%2019%20E%20rev.%201%20fin%20%20-%20NATO%20IN%20THE%20CYBER%20AGE.pdf [sist besøkt 31. oktober 2022].

Delerue, F., Desforges, A., Géry, A. (2019, 23. april). A close look at France's new military cyber strategy. *War on the Rocks.* https://warontherocks.com/2019/04/a-close-look-at-frances-new-military-cyber-strategy/ [sist besøkt 23. mars 2023].

DeSombre, W., Campobasso, M., Allodi, L., Shires, J., Work, J. D., Morgus, R., O'Neill, P. H., Herr, T. (2021, 1. mars). A primer on the proliferation of offensive cyber capabilities. *Atlantic Council*. https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/a-primer-on-the-proliferation-of-offensive-cyber-capabilities/ [sist besøkt 16. mars 2023].

Egloff, F. J., & Maschmeyer, L. (2021). Shaping not Signaling: Understanding Cyber Operations as a Means of Espionage, Attack, and Destabilization. *International Studies Review*, *23*(3), 997–998. https://doi.org/10.1093/isr/viaa086.

Fischerkeller, M. P., & Harknett, R. J. (2020). *Cyber Persistence Theory, Intelligence Contests and Strategic Competition* (s. 534–567). https://www.tandfonline.com/doi/full/10.1080/01402390.2020.1732354.

FAD (2008, 8. desember). *Rapporter om den svenske FRA-loven.* Pressemelding. https://www.regjeringen.no/no/dokumentarkiv/stoltenberg-ii/sd/Nyheter-og-pressemeldinger/pressemeldinger/2008/rapporter-om-den-svenske-fra-loven-/id538690/ [sist besøkt 27. november 2022].

Farsund, B., Thuv, Aa., Hansen, B. J. (2022). *Hvordan håndtere IKT i Forsvarets langtids-planlegging.* FFI-rapport 22/01569. https://www.ffi.no/publikasjoner/arkiv/hvordan-handtere-ikt-i-forsvarets-langtidsplanlegging.

FD (2018, 12. november) *Ny lov om Etterretningstjenesten på høring*. Pressemelding. https://www.regjeringen.no/no/dokumentarkiv/regjeringen-solberg/aktuelt-regjeringen-solberg/fd/pressemeldinger/2018/ny-lov-om-etterretningstjenesten-pa-horing/id2618704/ [sist besøkt 27. november 2022].

FireEye (2018). *APT38: Un-usual suspects*. Special report. https://content.fireeye.com/apt/rpt-apt38 [sist besøkt 30. oktober 2022].

FMA (u.å). *Terminologi*. https://www.fma.no/prinsix/maler/terminologi [sist besøkt oktober 2022].

Forsvaret (2014). Forsvarets fellesoperative doktrine. Forsvarsstaben. http://brage.bibsys.no/xmlui/handle/11250/224031.

Forsvaret (2019). *Forsvarets fellesoperative doktrine (FFOD).* Forsvarsstaben. http://hdl.handle.net/11250/2631948.

Gallagher, S. (2015, 14. desember). What the government should've learned about backdoors from the Clipper Chip. *Ars Technica.* https://arstechnica.com/information-technology/2015/12/what-the-government-shouldve-learned-about-backdoors-from-the-clipper-chip/ [sist besøkt 20. mars 2023].

Gallager, S., Loman, M. Mackenzie, P., Polat, Y. (2021, 11. mai). *A defender's view inside a DarkSide ransomware attack*. Sophos. https://news.sophos.com/en-us/2021/05/11/a-defenders-view-inside-a-darkside-ransomware-attack/ [sist besøkt 20. mars 2023].

GAO (2022, s. 17). *Defense Acquisition. Cyber Command Needs to Develop Metrics to Assess Warfighting Capabilities.* GAO-22-104695. https://www.gao.gov/assets/gao-22-104695.pdf [sist besøkt 28. november 2022].

Giles, K. (2021). Russian information warfare. I T. Clack & R. Johnson (Red.), *The World Information War* (1. utg., s. 139–161). Routledge. https://doi.org/10.4324/9781003046905-12

Green, M. (2015, 22. desember) *On the Juniper backdoor*. A Few Thoughts on Cryptographic Engineering. https://blog.cryptographyengineering.com/2015/12/22/on-juniper-backdoor [sist besøkt 27. november 2022].

Greenberg, A. (2018, 22. august). The Untold Story of NotPetya, the Most Devastating Cyberattack in History. *Wired.* https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/ [sist besøkt 28. februar 2023].

Greenberg, A. (2021, 20. mai). The Full Story of the Stunning RSA Hack Can Finally Be Told. *Wired*. https://www.wired.com/story/the-full-story-of-the-stunning-rsa-hack-can-finally-be-told/ [sist besøkt 25. oktober 2022].

Guerrero-Sade, J. A., Raiu, C., Moore, D., Rid, T. (2017). *Penquin's Moonlit Maze. The Dawn of Nation-State Digital Espionage*. Kaspersky Lab og King's College London. https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/07180251/Penquins_Moonlit_Maze_PDF_eng.pdf [sist besøkt 28. november 2022].

Harknett, R. J., & Smeets, M. (2022). Cyber campaigns and strategic outcomes. *Journal of Strategic Studies*, 45:4, 534-567, DOI: https://doi.org/10.1080/01402390.2020.1732354. Først publisert på internett mars 2020.

Hennum, A. C., Glærum, S. (2007, s. 20). *Metode for langtidsplanlegging – støtte til FS 07*. FFI-rapport 2007/02174. https://www.ffi.no/publikasjoner/arkiv/metode-for-langtidsplanlegging-stotte-til-fs-07

Higgins, K. J. (2016, 7. september). OPM Breach: Two Waves Of Attacks Likely Connected, Congressional Probe Concludes. *Dark Reading*. https://www.darkreading.com/endpoint/opm-breach-two-waves-of-attacks-likely-connected-congressional-probe-concludes [sist besøkt 28. oktober 2022].

Hodgson, Q. E., Shokh, Y., Balk, J. (2022). *Many Hands in the Cookie Jar: Case Studies in Response Options to Cyber Incidents Affecting U.S. Government Networks and Implications for Future Response.* RAND Corporation, RR-A1190-1. https://www.rand.org/content/dam/rand/pubs/research_reports/RRA1100/RRA1190-1/RAND_RRA1190-1.pdf [sist besøkt 30.oktober 2022].

Intel471 (2022, 2. juni). *The relationship between access brokers and ransomware crews is growing.* https://intel471.com/blog/access-brokers-ransomware-relationship-growing [sist besøkt 15. mars 2023].

Johansen, I. (2018). Scenario modelling with morphological analysis. *Technological Forecasting and Social Change, 126*(January 2018), 116–125. https://doi.org/10.1016/j.techfore.2017.05.016

Johansen, I. (2022). *Scenarioklasser for forsvarsplanlegging – revisjon av FFIs scenario-grunnlag.* FFI-rapport 21/01788. https://www.ffi.no/publikasjoner/arkiv/scenarioklasser-for-forsvarsplanlegging-revisjon-av-ffis-scenariogrunnlag

Johnson, D. B. (2023, 26. april). Sifting through the top cyber myths in the military service branches. *SC Media.* https://www.scmagazine.com/analysis/careers/top-cyber-myths-military-service-branches. [sist besøkt 28. april 2023].

Kaminska M., Shires, J., Smeets, M. (2022*); Cyber Operations during the 2022 Russian invasion of Ukraine: Lessons Learned (so far)*. Tallinn Workshop Report. The European Cyber Conflict Research Initiative (ECCRI). https://eccri.eu/wp-content/uploads/2022/07/ECCRI_WorkshopReport_Version-Online.pdf [sist besøkt 28.oktober 2022].

Laudrain, A. P. B. (2019, 26. februar). France's New Offensive Cyber Doctrine. *Lawfareblog. https://www.lawfareblog.com/frances-new-offensive-cyber-doctrine* [sist besøkt 16. mars 2023]

Levi, M., Dahan, A., Serper, A. (2019, 25. juni). Operation Soft Cell: A Worldwide Campaign Against Telecommunications Provider. *Cybereason*. https://www.cybereason.com/blog/operation-soft-cell-a-worldwide-campaign-against-telecommunications-providers [sist besøkt 27. oktober 2022].

Libicki, M., & Tkacheva, O. (2020). Cyberspace Escalation: Ladders or Lattices? *Cyber Threats and NATO 2030: Horizon Scanning and Analysis.* https://ccdcoe.org/uploads/2020/12/Cyber-Threats-and-NATO-2030_Horizon-Scanning-and-Analysis.pdf [sist besøkt 20. mars 2023].

Maschmeyer, L. (2021). The Subversive Trilemma: Why Cyber Operations Fall Short of Expectations. *International Security*, *46*(2), 51–90. https://doi.org/10.1162/isec_a_00418.

Maschmeyer, L. (2022a). Subversion, cyber operations, and reverse structural power in world politics. *European Journal of International Relations*, 13540661221117052. https://doi.org/10.1177/13540661221117051.

Maschmeyer, L. (2022b, 12. juli). Infiltrate, Exploit, Manipulate: Why the Subversive Nature of Cyber Conflict Explains Both Its Strategic Promise and Its Limitations. *Lawfareblog.* https://www.lawfareblog.com/infiltrate-exploit-manipulate-why-subversive-nature-cyber-conflict-explains-both-its-strategic [sist besøkt 23. mars 2023].

Mahoney, C. W. (2021). Corporate Hackers: Outsourcing US Cyber Capabilities. *Strategic Studies Quarterly, 15*(1), 61-89. https://www.airuniversity.af.edu/Portals/10/SSQ/documents/Volume-15_Issue-1/Mahoney.pdf [sist besøkt 16. mars 2023].

Mandiant (2013). *APT1 Exposing One of China's Cyber Espionage Units*. https://www.mandiant.com/sites/default/files/2021-09/mandiant-apt1-report.pdf [sist besøkt 28. februar 2023].

McGuire, M. (2018). *Into the Web of Profit. Understanding the Growth of the Cybercrime Economy.* Bromium. https://www.bromium.com/wp-content/uploads/2018/05/Into-the-Web-of-Profit_Bromium.pdf [sist besøkt 8. mars 2023].

Microsoft (2021). *Microsoft Digital Defence Report 2021*. https://go.microsoft.com/fwlink/p/?LinkID=2173952&clcid=0x409&culture=en-us&country=us [sist besøkt 28. oktober 2022].

Microsoft (2022a). *Special Report: Ukraine. An overview of Russia's cyberattack activity in Ukraine.* https://aka.ms/ukrainespecialreport [sist besøkt 25. oktober 2022].

Microsoft (2022b). *Defending Ukraine: Early Lessons from the Cyber War*. https://aka.ms/June22SpecialReport [sist besøkt 25. oktober 2022].

Microsoft (2022c). *Digital Defence Report 2022*. https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE5bUvv?culture=en-us&country=us [sist besøkt 23. november 2022].

Myndigheten for samhällsskydd och beredskap (2022, 19. september). *Nytt beredskapssystem träder i kraft den 1 oktober*. https://www.msb.se/sv/aktuellt/nyheter/2022/september/nytt-beredskapssystem-trader-i-kraft-den-1-oktober/ [sist besøkt 23. mars 2023].

National Security Archive (2022). *Cyber Vault Project – The Ukraine Project.* https://nsarchive.gwu.edu/project/ukraine-cyber-project [sist besøkt 28. november 2022].

NSM (2017, 7. desember). *Rammeverk for håndtering av IKT-sikkerhetshendelser.* https://nsm.no/regelverk-og-hjelp/andre-publikasjoner/rammeverk-for-handtering-av-ikt-hendelser/

NATO (2016, 9. juli). *Warsaw Summit Communiqué.* Press Release. https://www.nato.int/cps/en/natohq/official_texts_133169.htm [sist besøkt 25. oktober 2022].

NATO (2020). *AJP-3.20 Allied Joint Doctrine for Cyberspace Operations.* Edition A Version 1. Allied Joint Publication. NATO Standardization Agency. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/899678/doctrine_nato_cyberspace_operations_ajp_3_20_1_.pdf [sist besøkt 3. november 2022].

NATO (2022, 14. juni); *Brussels Summit Communiqué*. Press Release. https://www.nato.int/cps/en/natohq/news_185000.htm [sist besøkt 25. oktober 2022].

NATO STO (2020); *Assessing the Value of Cyber Operations in Military Operations.* https://www.sto.nato.int/Lists/STONewsArchive/displaynewsitem.aspx?ID=583 [sist besøkt 25. oktober 2022].

NCSC (2019, 21. oktober) *Advisory: Turla group exploits Iranian APT to expand coverage of victims.* https://www.ncsc.gov.uk/news/turla-group-exploits-iran-apt-to-expand-coverage-of-victims [sist besøkt 27. november 2022].

NCSC (u.å.) *Incident Management.* https://www.ncsc.gov.uk/collection/incident-management [sist besøkt 23. mars 2023].

Newman, L. H. (2020, 16. januar). This Apple-FBI Fight Is Different From the Last One. *Wired.* https://www.wired.com/story/apple-fbi-iphone-encryption-pensacola/ [sist besøkt 20. mars 2023].

Palmer, D. (2022, 1. mars). This is what happens when two ransomware gangs hack the same target - at the same time. *Zdnet.* https://www.zdnet.com/article/two-ransomware-gangs-hacked-the-same-target-at-the-same-time-heres-what-happened-next/ [sist besøkt 25. november 2022].

Poznansky, M. (2021, 23. mars). Covert action, espionage, and the intelligence contest in cyberspace. *War on the Rocks.* https://warontherocks.com/2021/03/covert-action-espionage-and-the-intelligence-contest-in-cyberspace/ [sist besøkt 23. mars 2023].

Public Safety Canada (2020, 31. juli). *Cyber Security in the Canadian Federal Government*. https://www.publicsafety.gc.ca/cnt/ntnl-scrt/cbr-scrt/fdrl-gvrnmnt-en.aspx [sist besøkt 16. mars 2023].

Rid, T. (2013). *Cyber War Will Not Take Place.* Oxford University Press.

Rid, T., Buchanan, B. (2015). Attributing Cyber Attacks, Journal of Strategic Studies, 38:1-2, 4-37, DOI: 10.1080/01402390.2014.977382.

Rid, T. (2020). *Active Measures: The Secret History of Disinformation and Political Warfare.* Farrar, Straus and Giroux.

Riksrevisjonen (2022). *Riksrevisjonens undersøkelse av Forsvarets informasjonssystemer for kommunikasjon og informasjonsutveksling i operasjoner*. Ugradert versjon av Dokument 3:3 (2022−2023). https://www.riksrevisjonen.no/rapporter-mappe/no-2022-2023/undersokelse-av-forsvarets-informasjonssystemer-informasjonssystemer-til-bruk-i-operasjoner/ [sist besøkt 27. november 2022].

Robertson, J. (2021, 2. september). Juniper Breach Mystery Starts to Clear With New Details on Hackers and U.S. Role. *Bloomberg.* https://finance.yahoo.com/news/juniper-breach-mystery-starts-clear-130016591.html [sist besøkt 27. november 2022].

Samfunnssikkerhetsinstruksen (2017). *Instruks for departementenes arbeid med samfunnssikkerhet.* FOR-2017-09-01-1349. https://lovdata.no/dokument/LTI/forskrift/2017-09-01-1349.

Smalley, S. (2022, 1. juli). Cybersecurity experts question Microsoft's Ukraine report. *Cyberscoop*. https://www.cyberscoop.com/cybersecurity-experts-question-microsofts-ukraine-report/ [sist besøkt 28. oktober 2022].

Smeets, M. (2018). The Strategic Promise of Offensive Cyber Operations. *Strategic Studies Quarterly*, *12*(3), 90–113.

Smith, B. (2020, 17. desember). A moment of reckoning: the need for a strong and global cybersecurity response. *Microsoft*. https://blogs.microsoft.com/on-the-issues/2020/12/17/cyberattacks-cybersecurity-solarwinds-fireeye/ [sist besøkt 16. mars 2023].

Sophos, Reversing Labs (2023, 7. mars). *Sophos-ReversingLabs 20 million sample dataset*. https://github.com/sophos/SOREL-20M [sist besøkt 7. mars 2023].

Stojkovic, D., Dahl, B. R. (2007). *Methodology for long term defence planning.* FFI-rapport 2007/00600. https://www.ffi.no/publikasjoner/arkiv/methodology-for-long-term-defence-planning [sist besøkt 7. mars 2023].

Stoll, C. (2005). *The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage*. Pocket Books.

Stubbs, J., Menn, J., Bing, C. (2019). Inside the West's failed fight against China's 'Cloud Hopper' hackers. *Reuters*. https://www.reuters.com/investigates/special-report/china-cyber-cloudhopper/ [sist besøkt 27.oktober 2022].

Tatar, S. (2022, 19. september). *What Are Initial Access Brokers?* Arcticwolf. https://arcticwolf.com/resources/blog/initial-access-brokers/ [sist besøkt 15. mars 2023].

Telenor (2020). *Operasjon Bivrost*. https://www.telenor.no/om/digital-sikkerhet/2020/artikler/operasjon-bivrost.jsp [sist besøkt 25. oktober 2022].

Telenor (2022). *Digital sikkerhet 2022. Nye perspektiver.* https://www.telenor.no/binaries/om/digital-sikkerhet/2022/Digital_sikkerhet_2022.pdf [sist besøkt 28. oktober 2022].

Thompson, A. W. (2021, 13. januar). Assessing the Vulnerabilities Equities Process, Three Years After the VEP Charter. *Lawfareblog.* https://www.lawfareblog.com/assessing-vulnerabilities-equities-process-three-years-after-vep-charter [sist besøkt 17. mars 2023].

UK MOD (2022) *Cyber primer (3rd).* https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1115061/Cyber_Primer_Edition_3.pdf [sist besøkt 27. november 2022].

U.S. Air Force (2019). *Air Force Doctrine Publication (AFDP) 3-51. Electromagnetic warfare and electromagnetic spectrum operations*. https://www.doctrine.af.mil/Doctrine-Publications/AFDP-3-51-EW-and-EMS-Ops/

U.S. Congress (2016). *The OPM Data Breach: How the Government Jeopardized Our National Security for More than a Generation.* Majority Staff Report. Committee on Oversight and

Government Reform U.S. House of Representatives 114th Congress. https://republicans-oversight.house.gov/wp-content/uploads/2016/09/The-OPM-Data-Breach-How-the-Government-Jeopardized-Our-National-Security-for-More-than-a-Generation.pdf [sist besøkt 25. oktober 2022].

U.S. Congress (2016b). *Memorandum*. Committee on Oversight and Government Reform U.S. House of Representatives 114th Congress. https://oversight.house.gov/sites/democrats.oversight.house.gov/files/documents/2016-09-06.Democratic%20Memo%20on%20OPM%20Data%20Breach%20Investigation.pdf [sist besøkt 31. oktober 2022].

U.S. Cyber Command (2022, 17. oktober 2022). *CYBERCOM executed global cyberspace defensive operation.* https://www.cybercom.mil/Media/News/Article/3190716/cybercom-executed-global-cyberspace-defensive-operation/ [sist besøkt 31. oktober 2022].

U.S. Cyber Command (2022, 25. oktober). *CYBER 101 – Defend forward and Persistent Engagement.* https://www.cybercom.mil/Media/News/Article/3198878/cyber-101-defend-forward-and-persistent-engagement/ [sist besøkt 23. mars 2023].

U.S. Joint Chiefs of Staff (2018). *Joint Publication 3-12 Cyberspace Operations*. https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf [sist besøkt 25. november 2022].

U. S. The White House (2023). *National Cybersecurity Strategy*. https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf [sist besøkt 16. mars 2023].

U.S. The White House (2017, 15. november). *Vulnerabilities Equities Policy and Process for the United States Government*. https://trumpwhitehouse.archives.gov/sites/whitehouse.gov/files/images/External%20-%20Unclassified%20VEP%20Charter%20FINAL.PDF [sist besøkt 17. mars 2023].

Van Hees, M. (2020). *The 2017 MAERSK Cyber Incident. Learning from and applying the Lessons of a Major Cyber Incident.* https://fhi.nl/app/uploads/sites/75/2020/10/201029-FHI_Maersk.pdf [sist besøkt 28. februar 2023].

Vašíčková, V. (2020). Crisis Management Process - A Literature Review and a Conceptual Integration. *Acta Oeconomica Pragensia 27*(3-4):61-77. https://doi.org/10.18267/j.aop.628 [sist besøkt 23. mars 2023].

Vatne, D. F., Køber, P. K., Guttelvik, M. S., Arnfinnsson, B., Rise, Ø. R. (2020). *Norwegian long-term defence analysis – a scenario- and capability-based approach.* FFI-rapport 20/02367. https://www.ffi.no/publikasjoner/arkiv/norwegian-long-term-defence-analysis-a-scenario-and-capability-based-approach.

VirusTotal (2023, 7. mars). *Intelligence Overview*. https://www.virustotal.com/gui/intelligence-overview [sist besøkt 7. mars 2023].

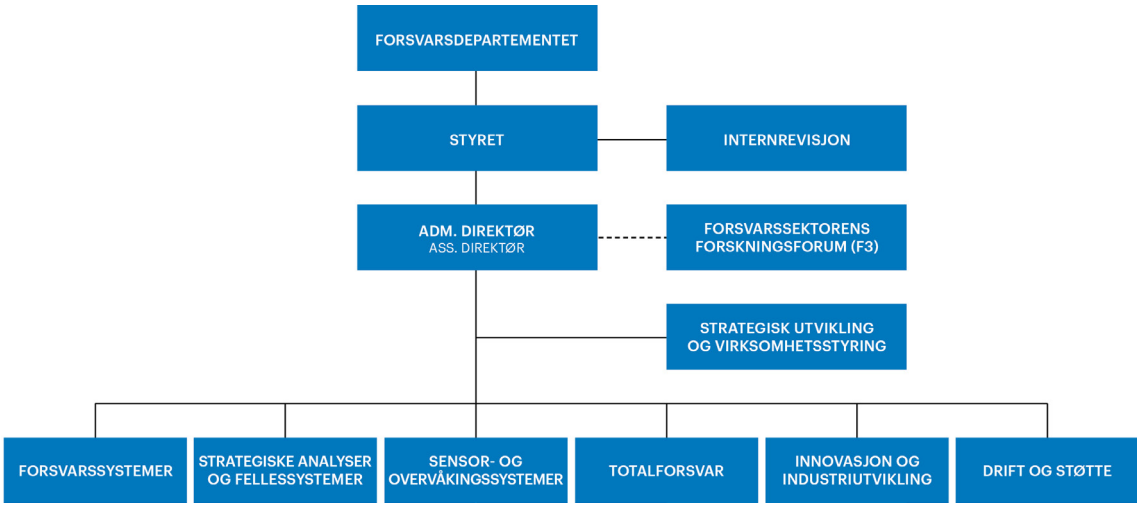
Zetter, K. (2022, 26. september). *Viasat Hack «Did Not» Have Huge Impact on Ukrainian Military Communications, Official Says.* https://zetter.substack.com/p/viasat-hack-did-not-have-huge-impact [sist besøkt 25. november 2022].

Om FFI
Forsvarets forskningsinstitutt ble etablert 11. april 1946. Instituttet er organisert som et forvaltningsorgan med særskilte fullmakter underlagt Forsvarsdepartementet.

FFIs formål
Forsvarets forskningsinstitutt er Forsvarets sentrale forskningsinstitusjon og har som formål å drive forskning og utvikling for Forsvarets behov. Videre er FFI rådgiver overfor Forsvarets strategiske ledelse. Spesielt skal instituttet følge opp trekk ved vitenskapelig og militærteknisk utvikling som kan påvirke forutsetningene for sikkerhetspolitikken eller forsvarsplanleggingen.

FFIs visjon
FFI gjør kunnskap og ideer til et effektivt forsvar.

FFIs verdier
Skapende, drivende, vidsynt og ansvarlig.



Forsvarets forskningsinstitutt (FFI)
Postboks 25
2027 Kjeller

Besøksadresse:
Kjeller: Instituttveien 20, Kjeller
Horten: Nedre vei 16, Karljohansvern, Horten

Telefon: 91 50 30 03
E-post: post@ffi.no
ffi.no

Norwegian Defence Research Establishment (FFI)
PO box 25
NO-2027 Kjeller
NORWAY

Visitor address:
Kjeller: Instituttveien 20, Kjeller
Horten: Nedre vei 16, Karljohansvern, Horten

Telephone: +47 91 50 30 03
E-mail: post@ffi.no
ffi.no/en