Kapittel 2: Operasjon Dempa Melodi – bruk av cyberåtak i ein luftoperasjon?

Mass Soldal Lund

Det israelske luftvåpenet (IAF) gjennomførte natt til 6. september 2007 eit bombetokt mot ein anonym bygning i ørkenen utanfor den syriske byen Deir ez-Zor. Utan å bli konfrontert av syriske styrkar kryssa åtte jagarfly store delar av syrisk luftrom og leverte 16 bombar på målet. Berre ein ruin stod igjen av det som før hadde vore ein atomreaktor. Det har blitt hevda at IAF unngjekk syrisk luftvern ved hjelp av eit cyberåtak, og operasjonen har difor blitt eit eksempel som går igjen i diskusjonar om militær bruk av cyberoperasjonar.[1] Ofte – diverre – vert hendinga referert til utan særleg med detaljar eller kjelder. I dette kapittelet er målet å gje ei meir detaljert framstilling av operasjonen, som går under namnet Operasjon Dempa Melodi.[2]

Som vi vil sjå, er det ikkje mogleg å gje eintydige svar om alle sider ved operasjonen. Før sjølve gjennomgangen er det difor verdt å gje eit lite innblikk i kjeldesituasjonen og bruk av kjeldene. Etter ein gjennomgang av bakgrunnen for og gjennomføringa av operasjonen vil kapittelet ta føre seg tre spørsmål. Det fyrste er i kva grad (det påståtte) cyberåtaket står fram som truverdig og sannsynleg slik det er skildra i kjeldene. Dersom operasjonen skal vere med å danne grunnlag for ei teoretisk forståing av cybermakt, synest ei slik vurdering å vere eit naturleg og naudsynt fyrstesteg. Det andre spørsmålet er om (det påståtte) cyberåtaket i det heile bør omtalast som eit cyberåtak, eller om det er riktigare å kalle det eit elektronisk åtak, slik nokre av kjeldene gjer. Dette er eit spørsmål av meir enn berre akademisk interesse; i vestleg militær tenking er det ein tendens til å sjå cyberkrigføring og elektronisk krigføring som to åtskilte domene. For eksempel er cyberoperasjonar i norsk doktrine definert som ein motsetnad til elektronisk krigføring, og det er ulike avdelingar og fagmiljø som har ansvaret for cyberoperasjonar og elektronisk krigføring.[3] Det tredje spørsmålet som kapittelet tek føre seg, er kva for effekt cyberåtaket hadde på operasjonen, og kva det har å seie for forståinga vår av bruk av cyberåtak i militære operasjonar. Operasjonen blir gang på gang framheva som eit eksempel på vellykka bruk av eit cyberåtak i ein militær operasjon. Då er det sjølvsagt interessant å sjå på kva som var suksessfaktorane i operasjonen. Men det er også relevant å spørje seg kvifor, gjeve suksessen, operasjonen meir enn 15 år seinare står fram som eit einestående eksempel.

---

[1] For eksempel på dette, sjå til dømes Clarke og Knake (2010, s. 1–8, 11), Cyber Law Toolkit (u.å.), Dipert (2013, s. 40–41), Healey (2013, s. 68), Liff (2012, s. 405), Moore (2022, s. 34–35), Pfleeger et al. (2015, s. 844), Richards (2014, s. 34), Rid (2012, s. 16–17, 2013, s. 11, 42–43), Schulze (2020, s. 189–190), Singer og Friedman (2014, s. 126–127), Smeets (2022, s. 41) og Tabansky og Ben-Israel (2015, s. 65–66).

[2] Operasjonen vert i engelske kjelder omtala som både «Operation Soft Melody» (Haren & Benn, 2018) og «Operation Silent Tone» (Giladi, 2018), som truleg er ulike omsetjingar av det hebraiske namnet på operasjonen. I tillegg er operasjonen også omtala som «Operation Orchard» (Bass, 2015, s. 45; Cyber Law Toolkit, u.å.; Smeets, 2022, s. 41) og «Operation Outside the Box» (Cyber Law Toolkit, u.å.; Melman & Raviv, 2018).

[3] Sjå til dømes *Forsvarets fellesoperative doktrine* (Forsvaret, 2019, s. 125, 146–148).

Referanse: Lund, M. S. (2024). Operasjon Dempa Melodi – bruk av cyberåtak i ein luftoperasjon? I V. R. Berrefjord & M. S. Lund (Red.), *Cybermakt – en tverrfaglig innføring* (s. 47–60). Universitetsforlaget.

Kjelder

Kapittelet er basert på engelskspråklege kjelder, som i hovudsak er journalistiske. Israelske myndigheiter anerkjente operasjonen opent fyrst i mars 2018 (Melman & Raviv, 2018). Kjeldene om operasjonen fell difor i to hovudkategoriar: For det fyrste rapportar basert på observasjonar i tida rett etter operasjonen i 2007. Fulghum, Wall og Barrie (2007) og Fulghum, Wall og Butler (2007) er dei viktigaste av desse. For det andre rapportar frå mars 2018 eller seinare, skrivne etter at israelske myndigheiter opna opp om operasjonen, særleg Harel og Benn (2018) og Katz (2019). Giladi (2018) gjev den offisielle versjonen frå det israelske luftvåpenet (IAF). Desse kjeldene skildrar operasjonen frå ein israelsk ståstad og kan ikkje seiast å vere spesielt kritiske, men har den fordelen at dei er baserte på intervju med aktørar involvert på israelsk side. Utover eit intervju gjort med ein tidlegare syrisk offiser i 2013 (Chulov, 2013) har det ikkje vore mogleg å finne engelskspråklege kjelder som viser den syriske oppfatninga av operasjonen. Bass (2015, s. 45–59) og Riedel (2013) presenterer det amerikanske synet på operasjonen basert på amerikanske kjelder.

Dei israelske kjeldene frå 2018 og utover har ingen detaljar om (det påståtte) cyberåtaket og omtaler det konsekvent som elektronisk krigføring. Framstillinga av (det påståtte) cyberåtaket er difor i hovudsak basert på ein systematisk gjennomgang av artiklar frå magasinet *Aviation Week & Space Technology*, inkludert Fulghum, Wall og Barrie (2007) og Fulghum, Wall og Butler (2007), men også tidlegare artiklar om (mistenkt) involvert teknologi. Data om seinare israelske luftåtak mot Syria er basert på ein systematisk gjennomgang av magasinet *Jane's Defence Weekly*, der særleg O'Connor (2014) har vore viktig for detaljar om syrisk luftvern.

Eit strategisk dilemma

Israel og Syria har vore i konflikt sidan opprettinga av Israel og den fyrste arabisk-israelske krigen i 1948. Bakgrunnen er ein grensekonflikt om Syrias tilgang til Jordanelva og Genesaretsjøen nord i Israel, og Syrias støtte til palestinarane i Israel–Palestina-konflikten. Under seksdagarskrigen i 1967 okkuperte Israel Golanhøgdene på den syriske sida av grensa. Oktoberkrigen («Jom kippur-krigen») i 1973, der Syria fyrst gjenerobra Golanhøgdene før Israel reokkuperte dei, gjorde det tydeleg at Syria ikkje kunne måle seg med Israel i konvensjonell krig. Tidleg på 1970-talet vart det òg klart at Israel hadde utvikla atomvåpen. I eit forsøk på å skape balanse starta Syria på 1980-talet utvikling av kjemiske våpen i tillegg til ei kraftig militær opprusting. Rundt årtusenskiftet hadde dei tilsynelatande også ein ambisjon om eit atomvåpenprogram. (Riedel, 2013; Slater, 2002)

Israelsk etterretning fatta seint i 2006 interesse for ein struktur i ørkenen utanfor Deir ez-Zor nord i Syria mot grensa til Irak (sjå kart i Figur 1) – ei kvadratisk bygning med grunnflate på 40 gongar 40 meter og 20 meter høg. Etter vidare etterretning kunne dei i mars 2007 slå fast at bygget skjulte ein atomreaktor som hadde vore under konstruksjon sidan starten av 2000-talet. Reaktoren var av nord-

koreansk design og av den typen som produserer plutonium til bruk i atomvåpen. Vurderinga var at det berre var få månadar igjen til reaktoren var klar til bruk. (Harel & Benn, 2018; Katz, 2019).

Figur 1: Israel og Syria

For israelsk politisk leiing var det openbert at dei ikkje ville tillate Syria å utvikle atomvåpen. Dette ville truge både Israels overlegenheit over Syria og det regionale atomvåpenmonopolet deira. Det vart raskt avgjort at reaktoren måtte øydeleggast (Katz, 2019; Riedel, 2013). Ifølgje Bass (2015) ville USA ikkje bidra, men nekta heller ikkje Israel å gjere noko (sjå også Riedel, 2013). Det israelske luftvåpenet (IAF) vart gjeve i oppdrag å planlegge eit luftåtak (Giladi, 2018; Katz, 2019). Samtidig stod den israelske leiinga i eit dilemma. Konflikten mellom Israel og Hizbollah sumaren 2006 («den andre Libanon-krigen») hadde vist at dei israelske militære styrkane (IDF) ikkje var klare for konvensjonell krig (Kober, 2008). Både den politiske leiinga og dei militære styrkane var prega av eksterne granskingar og sjølvransaking, og moralen var låg. Winograd-kommisjonen som var sett ned av israelske myndigheiter for å granske konflikten, leverte ein sterkt kritisk rapport i april 2007. Det var difor like openbert at Israel på det tidspunktet ikkje kunne risikere ein militær konfrontasjon med Syria. Men dei kunne heller ikkje vente for lenge; etterretninga tyda på at reaktoren kunne vere i drift mot slutten av september, og dei ville ikkje risikere miljøøydeleggingane som kunne resultere frå å bombe ein operativ atomreaktor (Harel & Benn, 2018; Katz, 2019).

Målet vart difor ein operasjon med så lite avtrykk som mogleg. Dei ville unngå konfrontasjon med syriske styrkar for å unngå eskalering – og gje den syriske leiaren Bashar al-Assad moglegheit til å nekte for at operasjonen hadde funne stad, og på den måten bevare andlet utan å måtte gjengjelde åtaket. Vidare måtte operasjonen vere overraskande og garantert øydeleggande – reaktoren var

tilsynelatande ubeskytta, og dei ville ikkje gje syrarane høve til å førebu eit forsvar (Harel & Benn, 2018; Katz, 2019).

Ein vellykka operasjon

5. september 2007, rundt 22:30 lokal tid, tok åtte fly av frå flybasen Hatzerim i Negevørkenen, fire av typen F-15I (Ra'am) og fire F-16I (Sufa). Formasjonane flaug i 100 meter høgd og entra syrisk luftrom frå Middelhavet. Dei flaug i radiostille og unngjekk syrisk luftvern ved hjelp av det éin rapport skildrar som «ampel use of electronic warfare as camouflage» (Harel & Benn, 2018), men som også har blitt omtala som eit cyberåtak (Tabansky & Ben-Israel 2015, s. 65–66). Effekten skal i følgje éin rapport ha vore at «[a]lmost immediately, the entire Syrian radar system went off the air for a period of time that included the raid» (Fulghum, Wall & Butler, 2007, s. 28).

Kl. 00:42 var formasjonane framme, og kvart av flya slapp to bombar på målet; fleire ulike typar ammunisjon vart nytta for å sikre garantert øydelegging. Kl. 00:45 vart det meldt tilbake at målet var øydelagt, og flya flaug tilbake til Middelhavet via den syrisk-tyrkiske grensa. Omtrent kl. 01:30 landa dei igjen på Hatzerim, utan å ha blitt oppdaga eller konfrontert av syrisk luftvern eller fly. Eitt av flya hadde dumpa ein ekstern drivstofftank som landa på tyrkisk territorium og vart identifisert som israelsk, men bortsett frå det var operasjonen ein suksess (Giladi, 2018; Harel & Benn, 2018; Katz, 2019).

Åtaket mot syrisk luftvern

Kva var denne bruken av elektronisk krigføring (EK) eller cyberåtak som gjorde at åtte israelske fly – som ikkje hadde stealth-teknologien som kunne gjort dei usynlege på radar – kunne gjennomføre bombetokt over Syria utan å verte oppdaga av syrisk luftvern? Det har blitt føreslått ulike måtar dette kan ha skjedd, inkludert leverandørkjedeåtak (med andre ord at luftvernsystemet hadde komponentar med innebygd «kill switch» eller «bakdør» som israelarane hadde tilgang til) og spesialoperasjonar der israelske operatørar har kome seg inn i systemet ved hjelp av fysisk tilgang til nettverkskablane til systemet (Adee, 2008, s. 35; Clarke & Knake, 2010, s. 6–8; Dipert, 2013, s. 40–41). Det finst ingen konkrete rapportar som bygg opp om desse forklaringane, og dei står fram som reine spekulasjonar. Den einaste forklaringa underbygd av konkrete (men riktig nok sprikande) rapportar peikar i retning av eit cyberåtak eller eit elektronisk åtak mot syrisk luftvern levert frå eit luftbore system (Fulghum & Barrie, 2007; Fulghum, Wall & Bulter, 2007). Dette er den einaste forklaringa presentert med tilstrekkeleg detaljar til å kunne gjere konkrete vurderingar. I fortsetjinga vil vi difor ha dette som utgangpunkt og vurdere ulike måte dette kan vere ein realitet.

Det amerikanske luftvåpenet (USAF) gjennomførte i fyrste halvdel av 2000-talet eksperiment med luftborne kapabilitetar for identifikasjon, manipulasjon og inntrenging i fiendtlege kommando- og kontrollsystem. Suter-systemet, utvikla av BAE Systems og L-3 Communication (no L3 Technology) for EK-flyet EC-130 Compass Call skal kunne både avlytte kommunikasjon, injisere datatrafikk og

overta kontrollen over kommando- og kontrollsystem – og skal ha ein eigen modul for åtak mot integrerte luftvernsystem. Med denne teknologien skal det vere mogleg å avlese fiendens radarbilete, injisere falske mål og ta over kontrollen av luftvernradarar (Fulghum, 2002, 2004a, 2004b, 2007; Fulghum et al., 2005). Det er difor ein teori om at Israel i 2007 hadde ein tilsvarande kapabilitet i sine Gulfstream G550 CAEW (Eitam)- eller F-16I (Sufa)-fly. (Fulghum, Wall & Barrie, 2007; Fulghum, Wall & Butler, 2007)

Det syriske luftvernet var godt utbygd – det mest omfattande i Midt-Austen – men i stor grad bygd på sovjetiske bakke-til-luft-rakettar og radarar, og difor relativt gamalt. Syria oppgraderte seinare med moderne russisk luftvern og kinesiske radarar, men dette var berre så vidt kome i gang i september 2007. Systemet var basert på sentralisert kommando og kontroll som nytta dedikerte radioliner (HF- og VHF-linkar) (Fulghum, Wall & Barrie, 2007; Fulghum, Wall & Butler, 2007; O'Connor, 2014).

Med dette som utgangspunkt er det mogleg å sjå føre seg ein måte åtaket kan ha skjedd: Eit fly med ein kapabilitet som skildra ovanfor sendte datapakker inn i det radioline-baserte syriske luftvern-nettverket ved å etterlikne ein av stasjonane eller knutepunkta i nettverket, det som i EK-litteraturen vert omtala som å spoofe datalinken (Adamy, 2015, s. 158; Lichtman et al., 2016, s. 50). Vidare vart desse datapakkane nytta til å gjere logisk skade på nettverket, for eksempel ved å skru av eller krasje systemet, eller ved å fløyme over nettverket med datatrafikk.

Samtidig finst ein rapport om at dei som opererte det syriske luftvernet, opplevde det som at radarane vart jamma, altså metta eller overbelasta av elektromagnetisk støy (Chulov, 2013). Utan meir detaljar er det sjølvsagt ikkje mogleg å utelukke formar for jamming som hindra radarane å sjå måla, men det er eit spørsmål om det ville vore tilstrekkeleg for å få heile det syrisk luftvernet til å gå ned, slik som sidan starten har vore ein del av forteljinga. Ein veikskap ved det syriske luftvernet skal ha vore at radarane hadde problem med å prosessere meir enn eitt mål av gongen. Ei alternativ forklaring kan difor vere bruk av avanserte eller «smarte» formar for jamming med komplekse bølgjeformer som skapte falske mål i radarane (Adamy, 2015, s. 320–323), og at luftvernsystemet vart «overwhelmed by a large number of targets» (O'Connor, 2014, s. 23).

Det finst òg ei fantasifull forklaring om eit cyberåtak levert gjennom avanserte elektromagnetiske signal til radarane. Men det verkar usannsynleg at ein kan ha så stor kontroll på signala ein sender inn i radaren at ein kan nytte det til å manipulere datapakkene generert av radaren, så denne forklaringa kan truleg avvisast. Det verkar meir sannsynleg at dette er ei misforstått samanblanding av dei føregåande forklaringane (Clarke & Knake, 2010, s. 6–7; Dipert, 2013, s. 40).

Cyberåtak eller elektronisk krigføring?

Hensikta her er å studere eit eksempel på militær bruk av cyberåtak. Eit spørsmål vi kan stille oss, er difor om åtaket (dersom åtaksvektoren i realiteten var luftvern-nettverket) er eit cyberåtak, eller om det kanskje er like riktig å rekne det for ei form for elektronisk krigføring. I eit elektronisk åtak vil ein

typisk nytte elektromagnetisk signal og effektar til å nekte fienden bruk av ein radar eller ein kommunikasjonslink (Adamy, 2015, s. 32–33). I motsetnad kan eit cyberåtak sjåast som utnytting av logiske sårbarheiter i eit datasystem (Lund, 2017, s. 30–32). Det finst openberre likskapar mellom elektroniske åtak og cyberåtak, til dømes at ein i båe typane åtak kan søkje former for tenestenekt (overbelasting av ein ressurs) eller spoofing (falske signal eller datapakker). Samtidig er det skilnadar. Ein skilnad, som antyda over, er metoden for å oppnå ein effekt: Eit elektronisk åtak sender elektromagnetiske signal i ei antenne, medan eit cyberåtak vil utnytte ein logisk tilgang, til dømes ein datalink, for å utføre eller påverke logiske instruksjonar (Adamy, 2015, s. 31–34; Lichtman et al., 2016, s. 47–48).

Åtaket som skildra ovanfor kan seiast å utnytte båe teknikkane, det sender elektromagnetiske signal i ei antenne for å få ein logisk tilgang til systemet via ein datalink. Lichtman et al. (2016, s. 50–51) definerer spoofing som «a signal transmission meant to look like a legitimate signal» og gjer eit skilje på kva nettverksprotokoll-lag signalet vert gjenkjent (godteke) på. Dersom signalet vert gjenkjent (og forstyrrar målsystemet) på det fysiske laget (der signala blir betrakta som radiobølgjer), men utan å verte gjenkjent av høgre protokoll-lag (der signala vert betrakta som logiske datapakker), vert det rekna som eit elektronisk åtak, meir spesifikt ei form for protokollmedviten jamming. Men dersom signalet også vert gjenkjent som ei gyldig datapakke på linklaget (og potensielt også nettverkslaget) vert det rekna som eit cyberåtak. Etter ein slik definisjon vil åtaket, dersom det vart utført ved å trenge inn i kommando- og kontrollnettverket til det syriske luftvernet og injisere logiske datapakker, vere eit cyberåtak. Dersom det var avansert jamming som skapte falske mål i radaren, var det «berre» eit elektronisk åtak.

Spørsmålet som naturleg følgjer, er om cyberåtaket slik det er skissert ovanfor er truverdig, om det er sannsynleg eller realistisk at det er på denne måten åtaket mot det syriske luftvernsystemet skjedde. Frå eit cybersikkerheitsperspektiv er det ikkje naudsynleg eit spesielt avansert åtak, gjeve at ein har tilgang til systemet. Erfaringar frå industrielle kontrollsystem og anna operasjonell teknologi er at dei sjeldan har cybersikkerheitsmekanismar implementert – spesielt om dei er gamle – og er sårbare for manipulasjon (Johnson, 2010; Lund et al., 2018). Vidare tyder rapportane på at det i dette tilfellet ikkje er snakk om avansert manipulasjon, men heller relativ enkel (logisk) sabotasje.

Det som talar imot er tidsaspektet. Sjølv med tilgang til nettverket ligg det i operasjonens natur at det vil vere minimalt med tid til logisk rekognosering av systemet. Det er vanleg å anta at «[e]vne til å skape effekt i cyberdomenet bygger på en forutgående etterretningsfase og er avhengig av integrasjon med sensitive etterretningskapabiliteter for å kunne utføres» (Forsvaret, 2019, s. 126), altså at målretta cyberåtak ikkje kan utførast utan god etterretning om systemet, og at åtakarane difor vil rekognosere eit system i lang tid før dei utfører handlingane som er målet med åtaket. Sagt med andre ord må ein føresetje at åtakaren ikkje kunne gjort seg nytte av informasjonsinnhenting under operasjonen, men må

ha hatt god kjennskap til det syriske luftvernsystemet på førehand. Samtidig er det ikkje urimeleg å anta at Israel har hatt ei langvarig interesse for syrisk luftvern, og det er difor ikkje umogleg at etterretnings-, overvakings- og rekognoseringsoperasjonar over tid kan ha akkumulert den naudsynte kunnskapen som ein del av utviklinga av kapabiliteten. Som vi har sett, skal USA ha utvikla og eksperimentert med denne typen cyberåtak sidan starten av 2000-talet og har erfaring med luftvern av sovjetisk design frå Jugoslavia og Irak (O'Connor, 2014, s. 23). Rapportar om at USA i 2011 vurderte bruk av cyberåtak mot libysk luftvern – som var bygd på mykje av den same teknologien som det syriske – er også ein indikasjon på at denne typen cyberåtak mot integrerte luftvernsystem er mogleg, sjølv om USA i 2011 valde å ikkje nytte seg av det (Nakashima, 2011; Schmitt & Shanker, 2011).

Effekten av åtaket for operasjonen

Det er ikkje mogleg å vite kva som var det faktiske hendingsforlaupet basert på opne kjelder. Det er heller ikkje mogleg å foreine dei ulike rapportane ein finn i desse kjeldene, som i stor grad er journalistiske og sprikar ein god del. Sjølv etter at israelske myndigheiter har byrja dele detaljar om operasjonen, er detaljane om kapabiliteten som lét dei unngå det syriske luftvernet framleis ein godt skjult løyndom. Likevel er effekten som dei ulike rapportane melder om den same: Dei åtte israelske flya kunne gjennomføre bombetokt djupt i syrisk territorium utan å verte konfrontert av syrisk luftvern. Kva dette tydde for operasjonen, kan vurderast uavhengig av korleis effekten vart oppnådd.

Med det som utgangspunkt kan vi sjå det som ei form for styrkevern som bidrog til å sikre handlefridom og kampkraft, i den forstand at IAF kunne gjennomføre bombetokta utan å verte forstyrra av syriske styrkar. Vi kan difor også seie at det fungerte som ein styrkemultiplikator som bidrog til det operasjonelle målet om total og garantert øydelegging av installasjonen på fyrste forsøk. Vidare var det sentralt for det strategiske målet om å gjennomføre operasjonen utan ein større konfrontasjon med Syria – både ved at det gav Assad ein utgang ved å nekte for at det hadde skjedd, og ved at det demonstrerte ein overlegenheit som kan ha fungert avskrekkande (Fulghum, Wall & Butler, 2007). Det verkar ikkje urimeleg å seie at åtaket på det syriske luftvernet var ein viktig faktor for suksessen til operasjonen, uavhengig av om det er å rekne for eit elektronisk åtak eller eit cyberåtak.

Operasjon Dempa Melodi demonstrerer at cyber- og elektroniske åtak kan inngå i militære operasjonar og fungere som styrkemultiplikatorar. Gjennomgangen viser også at det gjev meining å sjå militære cyberåtak og elektroniske åtak i samanheng. Den eine måten vi kan sjå det på er at spoofing av ein kommunikasjonslink (eit elektronisk åtak) kan nyttast som ein inngang til systemet for eit cyberåtak. Den andre måten er at vi i tilfelle som dette kan sjå på elektroniske åtak og cyberåtak som ulike metodar for å oppnå liknande effektar: blinding ved jamming av radar (elektronisk åtak) eller tenestenekt i kommunikasjonsnettverket (cyberåtak); villeiing ved falske mål i radar (elektronisk åtak) eller falske mål i kommunikasjonsnettverket (cyberåtak). Dette vert ytterlegare forsterka ved at vi

ikkje har tilstrekkeleg informasjon til å avgjere om det i denne konkrete operasjonen vart nytta eit elektronisk åtak eller eit cyberåtak.

Konklusjon: eit frampeik?

Operasjon Dempa Melodi er ofte framheva som ein vellykka operasjon, og ikkje minst eit eksempel på vellykka bruk av eit cyberåtak (eventuelt eit avansert elektronisk åtak, men med ein samanliknbar effekt) i ein militær operasjon. Moore (2022, s. 35) skildrar operasjonen som skuleeksempelet på samvirke mellom ein cyberkapabilitet og ein konvensjonell kapabilitet. For Richards (2015, s. 34) er det eit eksempel på eit cyberåtak som skapar ein taktisk situasjon som mogleggjer den militære operasjonen. I ein fellesoperativ tankegang – som er det grunnleggjande prinsippet for militære operasjonar i Noreg og andre vestlege land – vil det vere nettopp dette som er idealet: I ein fellesoperasjon vil ein søkje å kombinere effekt frå ulike taktiske styrkekomponentar for å nå operasjonelle og strategiske mål på ein mest mogleg effektiv måte. I Operasjon Dempa Melodi utretta kombinasjonen av cyberkomponenten og luftkomponenten noko som ingen av dei ville vore i stand til på eiga hand. Når den harde cybermakta skal finne plassen sin i norsk og vestleg militærdoktrine, er det gjerne på denne måten ein ser det føre seg (Forsvaret, 2019, s. 97–99, 129–131).

Viss Operasjon Dempa Melodi er skuleeksempelet på taktisk bruk av cyberåtak i samvirke med andre militære styrkekomponentar, er det naturleg å spørje om det finst andre døme som følgjer i kjølvatnet av operasjonen. Men det finst ingen andre konkrete rapportar om liknande bruk av cyberåtak mot eit luftvernsystem utført av Israel eller andre (med eit mogleg unntak referert nedanfor) gjennom dei fyrste 15 åra etter 2007. Israel gjennomførte ei serie lufttokt mot Syria i 2013, men O'Connor (2014, s. 26–28) meiner desse vart utførte med missil avfyrte utan at flya entra syrisk luftrom. Han ser dette som eit teikn på at Israel skal ha fått fornya respekt for syrisk luftvern etter at det gradvis vart modernisert etter 2007, og i 2013 ikkje lenger var i stand til å gjennomføre liknande operasjonar som Dempa Melodi. Samtidig er biletet noko meir komplisert. Det finst òg rapportar om at israelske jagarfly i det fyrste av åtaka i 2013 (30. januar mot eit militært forskingssenter i Jomrayah i utkanten av Damaskus) unngjekk syrisk luftvern (Binnie, 2013), og i følgje éin rapport at «[j]ust like at Deir Azzor six years [earlier], the Syrian air defences stayed silent» (Chulov, 2013). IAF har også seinare (i perioden 2016–2019) utført ei rekkje lufttokt i Syria, ofte i konfrontasjon med syrisk luftvern (sjå Lappin, 2016, 2017, 2018; Lappin & Binnie, 2018), men også djupt i syrisk luftrom (Binnie, 2018, 2019).

Mangelen på liknande eksempel kan indikere utfordringar med bruk av cyberåtak som taktisk verkemiddel. Det at Israel ikkje var i stand til å gjennomføre liknande operasjonar etter at Syria oppgraderte luftvernet, illustrerer i kva grad cyberkapabilitetar kan vere spesifikke for konkrete målsystem. Når svakheiter eller sårbarheiter som gjer eit spesifikt cyberåtak mogleg ikkje lenger er til stades etter ei oppgradering av målsystem, blir cyberåtaket ubrukeleg. Det å oppretthalde og

vedlikehalde ein cyberkapabilitet over tid vil difor i praksis tyde å vidareutvikle kapabiliteten ved å avdekke og lære seg å utnytte stadig nye sårbarheiter. Ikkje overraskande er dette ressurskrevjande (Smeets, 2022, s. 7–9). Det at teknologiske etterslep på det syrisk luftvernet synast å vere ein føresetnad for Operasjon Dempa Melodi kan òg gje eit hint om asymmetri som ein faktor – kanskje er teknologisk overlegenheit naudsynleg i utvikling av militære cyberkapabilitetar?

Meir generelt argumenterer Smeets (2022, s. 7–8) for at militær, taktisk bruk av cyberåtak er vanskeleg. Effekten må egne seg for å nå dei operasjonelle måla og vere presis, og timinga må vere riktig. Dei fleste vellykka cyberåtak har ein grad av opportunisme; dei leverer den effekten som er mogleg, på dei måla som er tilgjengelege, og på det tidspunktet åtakaren bestemmer. Ein slik fleksibilitet vil vere utfordrande i taktisk samvirke med andre styrkekomponentar. Som Smeets (2022, s. 41) påpeiker, hadde Operasjon Dempa Melodi sekvensielle avhengigheiter som gjorde at presis timing av cyberåtaket vart essensielt for operasjonen. Det kan vidare argumenterast for at effektar av cyberåtak ofte er indirekte og midlertidige; døme på cyberåtak med permanente og fysiske effektar er få (Rid, 2013). I Operasjon Dempa Melodi – der målet var å unngå luftvernet og halde avtrykket så lågt som mogleg – kan ein sjå dette som ein av fordelane ved å nytte eit cyberåtak. Ein kan dimed sjå det spesifikke i operasjonen som utslagsgjevande for suksessen: Den rette kapabiliteten var tilgjengeleg til rett tid for å nå dei konkrete operasjonelle og strategiske måla, og kunne leverast tilstrekkeleg presist.

USA skal ha vurdert, men avstått frå å nytte cyberkapabilitetar i etableringa av ei flyforbodssone i Libya i 2011. Grunnen skal ha vore både utfordringar med å førebu cyberåtaka i tide og behovet for meir permanent øydelegging av det libyske luftvernet. Det høyrer også med at operasjonane i Libya var langt meir kompliserte enn Dempa Melodi, med mange aktørar involvert, langt fleire mål og ikkje minst ein åtakar som var førebudd på åtak (Nygren, 2013). Sett i kontrast kan det ikkje verte utelukka at den relativt låge kompleksiteten i Operasjon Dempa Melodi også var ei faktor i den vellykka bruken av cyberåtak.

Sjølv om Operasjon Dempa Melodi står fram som skuleeksempelet på militær bruk av cyberkapabilitetar, er det ikkje mogleg å seie at operasjonen er representativ eller representerer noko form for mal for andre cyberoperasjonar. Gjeve at det faktisk var eit cyberåtak i ordets rette forstand, og med atterhald om at det er ei vurdering basert på opne kjelder, representerer Operasjon Dempa Melodi framleis eit einestående tilfelle. Operasjonen illustrerer korleis hard cybermakt kan inngå i ein fellesoperativ tankegang, men samtidig gjev mangelen på liknande eksempel indikasjonar om utfordringane som ligg i å integrere cyberkapabilitetar i militære operasjonar.

Referansar

Adamy, D. L. (2015). *EW 104: EW Against a New Generation of Threats*. Artech House.

Adee, S. (2008). The Hunt for the Kill Switch. *IEEE Spectrum*, *45*(5), 34–39.

Bass, W. (2015). *A Surprise Out of Zion? Case Studies in Israel's Decision on Whether to Alert the United States to Preemptive and Preventive Strikes, from Suez to the Syrian Nuclear Reactor.* RAND Corporation.

Binnie, J. (2013, 6. februar). Syria confirms Israeli strike. *Jane's Defence Weekly, 50*(6), 6.

Binnie, J. (2018, 25. juli). Israel accused of second airstrike deep inside Syria. *Jane's Defence Weekly, 55*(30), 20.

Binnie, J. (2019, 3. april). Syria reports deepest Israeli airstrike since S-300 transfer. *Jane's Defence Weekly, 56*(14), 16.

Chulov, M. (2013, 4. februar). Syrian rebel raids expose secrets of once-feared military. *The Guardian*, 2013. https://www.theguardian.com/world/2013/feb/04/syrian-rebel-raids-military-strongholds

Clarke, R. A. & Knake, R. K. (2010). *Cyber war. The next threat to national security and what to do about it*. HarperCollins Publishers.

Cyber Law Toolkit. (u.å.). *Operation Orchard/Outside the Box (2007)*. Henta 20. februar 2023 frå https://cyberlaw.ccdcoe.org/wiki/Operation_Orchard/Outside_the_Box_(2007).

Dipert, R. R. (2013). Other-Than-Internet (OTI) Cyberwarfare: Challenges for Ethics, Law, and Policy. *Journal of Military Ethics*, *12*(1), 34–53.

Forsvaret. (2019). *Forsvarets fellesoperative doktrine.* Forsvarets høgskole/Stabsskolen.

Fulghum, D. A. (2002, 4. november). Infowar To Invade Air Defense Networks. *Aviation Week & Space Technology*, *157*(19), 30.

Fulghum, D. A. (2004a, 28. juni). Sneak Attack. *Aviation Week & Space Technology*, *160*(26), 34.

Fulghum, D. A. (2004b, 16. august). Out of the Black. *Aviation Week & Space Technology*, *161*(7), 24–26.

Fulghum, D. A. (2007, 19. februar). Checking Pulses. *Aviation Week & Space Technology*, *166*(8), 31–32.

Fulghum, D. A. og Barrie, D. (2007, 5. oktober). Off the Radar. *Aviation Week & Space Technology*, *167*(14), 28–29.

Fulghum, D. A., Dornheim, M. A. & Scott, W. B. (2005, 14. februar). Black Surprises. *Aviation Week & Space Technology*, *162*(7), 68–69.

Fulghum, D. A., Wall, R. & Barrie, D. (2007, 5. november). All Arms Attack. *Aviation Week & Space Technology*, *167*(18), 32–33.

Fulghum, D. A., Wall, R. & Butler, A. (2007, 26. november). Cyber-combat's First Shot. *Aviation Week & Space Technology*, *167*(21), 28–31.

Giladi, T. (2018, 21. mars). *The Untold Story: IAF Attack of Syrian Nuclear Reactor*. Israeli Air Force. https://www.iaf.org.il/4471-50071-en/IAF.aspx

Harel, A. & Benn, A. (2018, 23. mars). No Longer a Secret: How Israel Destroyed Syria's Nuclear Reactor. *Haaretz*. https://www.haaretz.com/world-news/MAGAZINE-no-longer-a-secret-how-israel-destroyed-syria-s-nuclear-reactor-1.5914407

Healey. J. (2013). A Brief History of US Cyber Conflict. I J. Healey (red.), *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012* (s. 14–87). Cyber Conflict Studies Association.

Johnson, R. E., III. (2010). Survey of SCADA Security Challenges and Potential Attack Vectors. I *2010 International Conference for Internet Technology and Secured Transactions (ICITST 2010)*. IEEE.

Katz, Y. (2019). *Shadow strike. Inside Israel's secret mission to eliminate Syrian Nuclear Power*. St. Martin's Press.

Kober, A. (2008). The Israel Defense Forces in the Second Lebanon War: Why the Poor Performance. *Journal of Strategic Studies*, *31*(1), 3–40.

Lappin, Y. (2016, 21. september). Syria launches missiles at Israeli jets. *Jane's Defence Weekly*, *53*(38), 22.

Lappin, Y. (2017, 29. mars). Israel shoots down Syrian surface-to-air missile with Arrow 2 interceptor. *Jane's Defence Weekly*, *54*(13), 4.

Lappin, Y. (2018, 7. mars). Israeli investigation blames aircrew of downed F-16. *Jane's Defence Weekly*, *55*(10), 20.

Lappin, Y. og Binnie, J. (2018, 16. mai). Israel responds to rocket fire by striking Iranian targets in Syria. *Jane's Defence Weekly*, *55*(20), 4.

Lichtman, M., Poston, J. D., Amuru, S., Shahriar, C., Clancy, T. C., Buehrer, R. M. & Reed, J. H. (2016). A Communication Jamming Taxonomy. *IEEE Security & Privacy*, *14*(1), 47–54.

Liff, A. P. (2012). Cyberwar: A New 'Absolute Weapon'? The Proliferation of Cyberwarfare Capabilities and Interstate War. *Journal of Strategic Studies*, *35*(3), 401–428.

Lund, M. S. (2017). Cyber som operasjonsdomene. *Norsk Militært Tidsskrift*, *186*(1), 28–34.

Lund, M. S., Hareide, O. S. & Jøsok, Ø. (2018). An Attack on an Integrated Navigation System. *Necesse*, *3*(2), 149–163.

Melman, Y. & Raviv, D. (2018, 20. mars). Inside Israel's Secret Raid on Syria's Nuclear Reactor. *Politico Magazine*. https://www.politico.com/magazine/story/2018/03/20/inside-israels-secret-raid-on-syrias-nuclear-reactor-217663/

Moore, D. (2022). *Offensive Cyber Operations. Understanding Intangible Warfare*. Hurst.

Nakashima, E. (2011, 17. oktober). U.S. cyberweapons had been considered to disrupt Gaddafi's air defenses. *Washington Post*. https://www.washingtonpost.com/world/national-security/us-cyber-weapons-had-been-considered-to-disrupt-gaddafis-air-defenses/2011/10/17/gIQAETpssL_story.html

Nygren, A. (2013). Executing strategy from the air. I K. Engelbrekt, M. Mohlin & C. Wagnsson (red.), *The NATO Intervention in Libya. Lessons learned from the campaign* (s. 103–127). Routledge.

O'Connor, S. (2014, 9. april). Access denial. *Jane's Defence Weekly*, *51*(15), 22–28.

Pfleeger, C. P., Pfleeger, S. L. & Margulies, J. (2015). *Security in Computing* (5. utg.). Prentice Hall.

Richards, J. (2014). *Cyber-War. The Anatomy of the Global Security Threat.* Palgrave Macmillan.

Rid, T. (2012). Cyber War Will Note Take Place. *Journal of Strategic Studies*, *35*(1), 5–32.

Rid, T. (2013). *Cyber war will not take place.* Hurst & Company.

Riedel, B. (2013). Lessons of the Syrian Reactor. *The National Interest* (125), 39–46.

Schmitt, E. & Shanker, T. (2011, 17. oktober). U.S. Debated Cyberwarfare in Attack Plan on Libya. *New York Times*. https://www.nytimes.com/2011/10/18/world/africa/cyber-warfare-against-libya-was-debated-by-us.html

Schulze, M. (2020). Cyber in War: Assessing the Strategic, Tactical, and Operational Utility of Military Cyber Operations. I T. Jančárková, L. Lindström, M. Signoretti, I. Tolga & G. Visky (red.), *2020 12th International Conference on Cyber Conflict. 20/20 Vision: The Next Decade* (s. 183–197). NATO CCDCOE Publications.

Singer, P. W. & Friedman, A. (2014). *Cybersecurity and Cyberwar: What Everyone Needs to Know.* Oxford University Press.

Slater, J. (2002). Lost Opportunities for Peace in the Arab-Israeli Conflict. Israel and Syria, 1948–2001. *International Security*, *27*(1), 79–106.

Smeets, M. (2022). *No Shortcuts. Why States Struggle to Develop a Military Cyber-Force*. Hurst.

Tabansky, L. & Ben-Israel, I. (2015). *Cybersecurity in Israel*. Springer.