FORSVARET

Værnsfælles Doktrin for Militære Cyberspaceoperationer

1. Udgave version A

September 2019

FORSVARSAKADEMIET

København juli 2019
Forsvarsakademiet
Svanemøllens Kaserne
2100 København Ø
Tlf.: +45 728 17000
Layout: Forsvarsakademiet
ISBN: 978-87-7147-263-9

Forord

Cyberspace griber ind i alle aspekter af et moderne samfund. Aktiviteter i cyberspace kan derfor påvirke et samfund på samme måde som aktiviteter i de fysiske kamprum. Det betyder først og fremmest, at cyberspace skal beskyttes og forsvares. Men det betyder også, at cyberspace giver adgang til en række nye muligheder, når Forsvaret skal løse sine opgaver.

Værnsfælles Doktrin for Militære Cyberspaceoperationer (VDMCO) beskriver et cyberspace, der ikke kun er et netværk af computere, men som i realiteten udgør et ikke-fysisk rum, der gør det muligt at bevæge sig, positionere sig og opnå militære fordele. Cyberspaceoperationer kan skabe effekter, der også rækker ud over grænserne for cyberspace selv.

VDMCO bidrager til at normalisere begrebet "cyberspaceoperationer", og doktrinen definerer et fælles sprog og en fælles forståelse for området. Normaliseringen betyder, at cyberspace kan inddrages i strategiske, operative og taktiske overvejelser på samme måde som de fysiske kamprum. Normaliseringen af cyberspaceoperationer bidrager til, at Forsvaret også i fremtiden kan løse sine opgaver effektivt.

VDMCO er udarbejdet på Forsvarsakademiet i et tæt samarbejde med Forsvarets Computer Network Operationskapacitet (CNO-kapaciteten) og med bidrag fra myndigheder, værn og stabe i hele Forsvarsministeriets område. Doktrinen bygger desuden på tilgængelig forskning og erfaringer omkring cyberspaceoperationer og læner sig op af NATO's policy og doktrinudvikling på området. Doktrinen vil løbende blive revideret.

VDMCO er et væsentligt bidrag til Forsvarets bestræbelser på at opnå en effektiv kapabilitet til at operere defensivt såvel som offensivt i cyberspace.

Henrik Ryberg
Kontreadmiral
Chef for Forsvarsakademiet

Indholdsfortegnelse

Annex

1. Indledning

1.1. Formål

Værnsfælles Doktrin for Militære Cyberspaceoperationer (VDMCO) beskriver principperne for planlægning og gennemførelse af militære cyberspaceoperationer (CO) i en national ramme. VDMCO fastlægger en fælles forståelse for CO og anviser principper for anvendelse af disse. VDMCO danner grundlag for øvrige nationale doktriner, procedurer, uddannelse og træning, der er relateret eller henviser til CO.

1.2. Anvendelse

VDMCO er det primære grundlag for planlægning, gennemførelse og integration af CO.

VDMCO anvendes til at give førere og planlæggere på det taktiske niveau den viden og de redskaber, der gør dem i stand til effektivt at integrere CO med egne operationer og aktiviteter. VDMCO er ikke begrænsende i forhold til førernes opgaveløsning.

VDMCO fastsætter anvendt CO-relateret terminologi.

VDMCO tager udgangspunkt i doktriner og policy fra North Atlantic Treaty Organization (NATO). VDMCO er en fortolkning af disse tilpasset en dansk kontekst.

Forsvarets øvrige doktrinære grundlag, herunder NATO's Allied Joint Publications (AJP), er gældende for de områder, der ikke er dækket af VDMCO.[1]

I forbindelse med planlægning og gennemførelse af CO i rammen af NATO finder både gældende NATO-doktriner og VDMCO anvendelse.[2] Ved divergenser finder VDMCO anvendelse.

1.3. Afgrænsning

Doktrinen dækker offensive såvel som defensive militære operationer i cyberspace. Hvis ikke andet er beskrevet, anvendes begrebet cyberspaceoperationer samt forkortelsen CO om *militære* cyberspaceoperationer*,* hvilket defineres som: **militære aktiviteter i eller gennem cyberspace, der, afgrænset i tid og rum og gennem anvendelse af cyberspacekapaciteter, har til hensigt at opnå militære mål**. Denne afgrænsning er nærmere beskrevet i kapitel 4.

[1] For det operative niveau se Værnsfælles Forsvarskommando, *Bestemmelse for Behandling af NATO AJP Inden for Værnsfælles Forsvarskommandos Område* (ikke-klassificeret), dok.nr. VFKBST U.210-0, november 2011.

[2] Særlig opmærksomhed henledes på begrebet Sovereign Cyber Effects Provided Voluntarily by Allies (SCEPVA), der refererer tilbage til anvendelse af national doktrin, se annex A (TTJ).

Den kontinuerlige, daglige drift af informations- og kommunikationsteknologiske systemer (IKT), som i andre dokumenter og kilder kan ses betegnet som cyberspace-operationer, er ikke omfattet af denne doktrin.

Førere skal være opmærksomme på, at det er konteksten, altså den militære operation, og ikke typen af aktivitet, der bestemmer, om aktiviteten betegnes CO eller ej. Således kan den samme type aktivitet (fx en analyse af logfiler fra en server) indgå som en del af CO i én kontekst, mens den i en anden kontekst indgår som en del af den kontinuerlige varetagelse af it-sikkerheden, der finder sted som en almindelig del af driften af et IKT-system.

1.4. Baggrund

Den teknologiske udvikling, digitaliseringen og den øgede afhængighed af netværksbaserede systemer har ført til nye sårbarheder, men også nye muligheder for at opnå militære fordele gennem cyberspace.

Fjendtlige handlinger i cyberspace kan i stigende grad påvirke en stats sammenhængskraft, politiske beslutningstagning og forsvarsevne. Dermed udgør disse handlinger en risiko for statens sikkerhed.

CO skal kunne bidrage til at imødegå sådanne risici og samtidig udnytte cyberspaces potentiale til selvstændigt eller gennem støtte til andre operationer at opnå militære fordele.

1.5. Hvem gennemfører CO?

Offensive CO (OCO) samt den centraliserede del af de defensive CO (DCO) gennemføres i Danmark af CNO-kapaciteten. Center for Cybersikkerhed (CFCS) er udførende på sidstnævnte.

Gennemførelse af CO i sammenhæng med Forsvarets øvrige indsatser koordineres som udgangspunkt på det værnsfælles niveau. Det er dog vigtigt, at CO også indgår i planlægningen af operationer på taktisk niveau, da dette niveau direkte bidrager til DCO og, gennem integration med egne operationer, indirekte til OCO. Som eksempel vil en hærenhed altså ikke skulle indsætte egne hackere mod modstanderen, men vil i stedet kunne støtte eller blive støttet af OCO udført af CNO-kapaciteten.[3]

En effektiv integrering af CO med andre typer operationer, effekter og aktiviteter nødvendiggør, at de taktiske førere, uanset om deres enheder besidder evnen til at gennemføre CO, skal kende CO-doktrin.[4]

[3] For underopdeling af CO og uddybning af roller og ansvar se kapitel 4.
[4] Afsnit 5-5.3 beskriver CO-effekter, anvendelsen af krigsførelsens grundprincipper samt sammenhængen mellem CO og joint functions.

1.6. Beskyttelse af eget cyberspace

Beskyttelse af eget cyberspace består ikke kun af CO, men udgøres af flere dele, som understøtter hinanden og vanskeliggør et eventuelt fjendtligt angreb. CO udgør en væsentlig del af forsvaret, men kan ikke alene garantere fortrolighed, integritet og tilgængelighed eller etablere og fastholde bevægelses- og handlefrihed i cyberspace. Som eksempler på beskyttelsestiltag, som ikke er CO, kan nævnes:

- Fysisk sikkerhed (skalsikring, adgangskontrol, bevogtning mv.).
- Datasikkerhed (datasikring, backup, redundans mv.).
- Informationssikkerhed (fortrolighed, integritet og tilgængelighed).
- Kryptering.
- Netværksdesign (subnets, proxyservere mv.).
- Firewalls, antivirus, overvågning.
- IKT-styring (central styring af opdateringer, installation af applikationer, hardware m.v).
- Cybersikkerhedsstrategi.
- Samarbejde med myndigheder og virksomheder.
- Organisatorisk uddannelse og cyber awareness.[5]

1.7. Doktrinens opbygning

Doktrinens hovedtekst er opdelt i to dele:

Del I, som består af kapitel 2 og 3, forklarer og afgrænser cyberspace i en militær kontekst. Her beskrives, hvordan cyberspace anskues som et operationsmiljø på linje med land, luft og det maritime operationsmiljø.

Del II, som består af kapitel 4 og 5, angiver principper for, hvordan CO tænkes ind og integreres i militære operationer. Desuden skitseres de overordnede processer, der på operativt niveau tilvejebringer efterspurgte effekter i cyberspace. Del II henvender sig dermed både til førere og planlæggere på det værnsfælles, operative niveau samt til de førere, der på de underliggende niveauer skal integrere og synkronisere med CO.

Som supplement til doktrinens hovedtekst tilføjes seks uddybende annexer:

Annex A, som beskriver, hvorledes planlægning og gennemførelse af CO finder sted på operativt niveau. Dette annex er klassificeret TIL TJENESTEBRUG.

Annex B, som indeholder et resumé af doktrinens definitioner og overvejelser til anvendelse som reference i forbindelse med planlægning og gennemførelse af CO på operativt niveau.

[5] Cyber awareness er et udtryk for en organisations samlede forståelse for og opmærksomhed på trusler fra og i cyberspace. Cyber awareness er essentielt for cybersikkerhed (CS), da den menneskelige faktor ofte er en væsentlig del af sårbarheder i cyberspace.

Annex C, som indeholder et resumé af doktrinens definitioner og overvejelser til anvendelse som reference for styrkechefer, der skal koordinere egne aktiviteter med CO.

Annex D, som beskriver en kronologisk opdeling af doktrinens overvejelser i forbindelse med OCO.

Annex E, som beskriver en kronologisk opdeling af doktrinens overvejelser i forbindelse med DCO.

Annex F, som forklarer relationen til NATO-doktrin for CO, herunder forskelle i terminologi, definitioner og procedurer.

Doktrinen anvender engelske begreber, hvor disse begreber er defineret i gældende engelsksproget doktrin, fx AJP.

Del I: Cyberspace

2. Afgrænsning af cyberspace

Cyberspace defineres som: **den samlede globale mængde af entiteter, som behandler, lagrer og transmitterer digitale informationer og kode, hvad enten de er forbundne eller ej**. Ved entiteter forstås digitale IKT-systemer, øvrige elektroniske systemer og netværk – samt deres data.[6]

Cyberspace er dermed ikke kun internettet, men inkluderer også intranet og IKT-dele af fx kritisk infrastruktur og sensor- og våbensystemer samt kommando- og kontrolsystemer.

Cyberspace beskrives ved tre lag: et fysisk lag, et logisk lag og et cyberpersonalag.

Figur 1, De tre lag i cyberspace

Det fysiske lag består af hardware, infrastruktur og forbindelseselementer. Dette inkluderer netværksudstyr,[7] computere,[8] databærende medier,[9] kablede og trådløse forbindelser[10] mv.

Alle komponenter i det fysiske lag har en geografisk placering, er under ejerskab og underlagt national jurisdiktion.

[6] Begrebet data anvendes om informationer, der er lagret og/eller transporteres digitalt.
[7] Fx modemmer, hubs, routere og switche.
[8] Fx servere, tablets, mobiltelefoner og pc'er.
[9] Fx harddiske, bånd, hukommelse, cd-rommer og USB-nøgler.
[10] Fx datakabler, stik, access points og bærebølger.

Det er gennem det fysiske lag, at cyberspace er i direkte kontakt med de fysiske operationsmiljøer og det elektromagnetiske spektrum (EMS).

Det logiske lag er det informationsbærende og instruktionsgivende lag og består af data og kode. Dette inkluderer dokumenter, filer, firmware, operativsystemer, protokoller, programmer, scripts mv.

Det logiske lag kan ikke fungere uden det fysiske lag, idet det er det fysiske lag, hvorigennem digitale informationer og kommandoer flyttes og lagres.

Det er et særligt kendetegn ved cyberspace, at bevægelse og lagring af data og instruktioner ikke alene er underlagt fysikkens love, men også menneskeskabte regler og rutiner, som kan påvirkes.

Det logiske lag kan eksistere som bl.a. elektromagnetiske bølger, magnetiske tilstande, kvantetilstande og spændingsforskelle.

Cyberpersonalaget består af virtuelle repræsentationer af organisationer og identiteter. Disse inkluderer e-mailadresser, bruger-id, konti på de sociale medier, alias, IP- og MAC-adresser[11] mv.

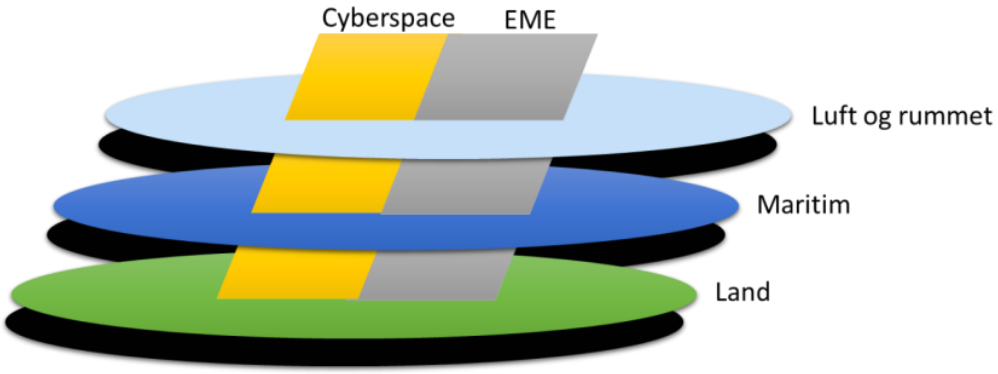
Virtuelle repræsentationer er ikke nødvendigvis en spejling af identiteter i den fysiske verden. En enkelt virtuel repræsentation (cyberpersona) kan anvendes af flere fysiske personer/organisationer. På samme måde kan en enkelt person/organisation have flere virtuelle repræsentationer (cyberpersonaer).

[11] IP-adresser er netværkstildelte adresser. MAC-adresser er unikke fysiske identifikationsnumre på udstyr, der kan tilgå netværk, fx netværkskort, mobiltelefoner, printere mv.

3. Cyberspace som operationsmiljø

Cyberspace udgør et operationsmiljø for militære operationer på linje med land, luft, det maritime og det elektromagnetiske operationsmiljø. Cyberspace er på samme måde som fx det elektromagnetiske miljø (EME)[12] beskrevet som et ikke-fysisk battlespace.[13] Cyberspace har dog også en fysisk komponent (fx i form af entiteter i det fysiske lag, computerkodes manifestering i elektroniske tilstande mv.). Cyberspace er derfor adskilt fra, men samtidig i berøring med de fysiske operationsmiljøer.

Cyberspace undergår konstant menneskeskabt udvikling og tilpasning. Cyberspace er derfor både et komplekst og uigennemsigtigt miljø, hvor det kan være udfordrende at forudsige sammenhænge og effekter af de aktiviteter, der gennemføres.



Figur 2, Cyberspace og de øvrige miljøer

3.1. Elementer i operationsmiljøet cyberspace

Operationsmiljøet cyberspace kan analyseres og beskrives ved hjælp af en række elementer, herunder forskellige aktører, som har indflydelse på planlægning og gennemførelse af CO:

- Fysisk udstrækning og fysiske forhold.
- EMS.
- Informationsmiljøet.
- Egne og allierede enheder og operationer.
- Fjendtlige aktører.
- Neutrale aktører.
- Indflydelse fra andre operationsmiljøer.

[12] Electromagnetic Environment.
[13] NATO, *Allied Joint Doctrine for the Conduct of Operations* (ikke-klassificeret), annex C, dok.nr. AJP-3(c), februar 2019.

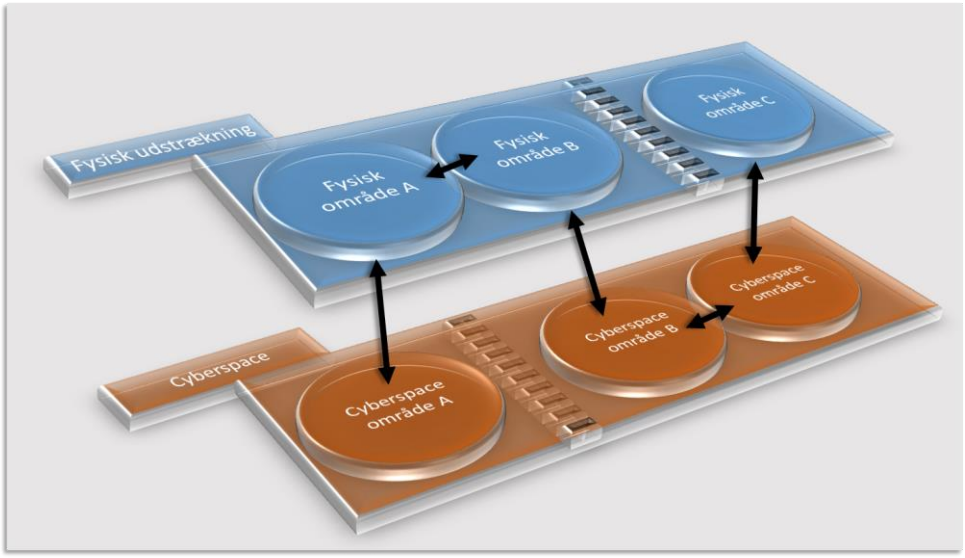
3.1.1. Fysisk udstrækning og fysiske forhold

Fysiske forhold såsom vejr, terræn og geografi, som har stor betydning for land, luft og det maritime operationsmiljø, er også relevante for operationsmiljøet cyberspace. Fx har rumvejr betydning for elektromagnetisk udbredelse af digitale informationer, og temperatur har betydning for funktionaliteten af elektronisk udstyr.

Alle komponenter i det fysiske lag er i en eller anden grad sårbare over for fysiske påvirkninger, herunder vejrlig.

Cyberspace er globalt dækkende, men anvendelsen er ikke lige udbredt i alle dele af verden. Cyberspace rummer desuden flaskehalse i forbindelserne mellem forskellige netværk og systemer. Disse udgøres bl.a. af internetserviceudbydere, undersøiske kabelforbindelser og jordstationer til satellitforbindelser. Påvirkning af sådanne flaskehalse kan berøre større dele af cyberspace.

Gennem cyberspace kan der skabes forbindelser til militære mål, herunder genstande og personer, som ikke umiddelbart kan nås fysisk. Omvendt kan man i den fysiske verden skabe forbindelse til dele af cyberspace, der ikke kan nås alene via cyberspace. Fx kan man anvende specialoperationsstyrker til at anbringe USB-nøgler med computervirus eller til at afdække information om eventuelle trådløse netværk og dermed skabe forbindelse mellem to adskilte dele af cyberspace.[14]



Figur 3, Forbindelser fysisk og i cyberspace

CO rettet mod entiteter i cyberspace kræver, at der skabes forbindelse til disse entiteter på det logiske lag, så digitale informationer og/eller kode kan overføres eller trækkes ud. Geografisk placering kan få betydning med hensyn til lovgrundlaget for at gennemføre CO, da målet kan befinde sig uden for operationsområdet eller tilhøre en

[14] Denne type operationer kaldes også Close Access Operations eller populært "sneakeroperationer", som henviser til, at man må "tage skoene på" for at nå sit mål i cyberspace.

neutral aktør. Anvendelse af cloudløsninger vanskeliggør i nogen grad geografisk lokalisering af entiteter og udvisker linjerne mellem civile og militære tjenester.[15]

Såfremt der ikke er netværksforbindelse til et system eller netværk, kan forbindelse etableres ved anvendelse af fx USB-stik, datakabler eller ved at tvinge systemet over på et trådløst netværk. Systemets eller netværkets geografiske placering og de fysiske adgangsforhold kan derfor have betydning for muligheden for at gennemføre CO.

3.1.2. EMS

Trådløs digital IKT supplerer og erstatter i stigende grad kablede forbindelser, om end langt den største del af datatrafikken i cyberspace foregår via kablede forbindelser. EMS er ikke som sådan en del af cyberspace, men data og kode kan residere i og transporteres gennem EMS. Bærebølger er i den sammenhæng at betragte som elektromagnetiske udgaver af datakabler. EMS inkluderer fx gammastråling, varmestråling mv., der hverken indeholder data eller kode.[16]

Selvom der er et vist sammenfald mellem CO og elektromagnetiske operationer (EMO) i forhold til brugen af EMS, kan de to operationstyper ikke sidestilles. Cyberspace og EMS er forskellige, men de griber ind i hinanden.

EMO kan skabe effekter i cyberspace, fx ved at jamme en trådløs dataforbindelse, men kan også skabe effekter uden for cyberspace, fx ved at jamme en analog VHF-kanal. På samme vis kan CO skabe effekter i EMS, fx ved at afbryde et trådløst access point, såvel som uden for EMS, fx ved at ændre data gemt på et USB-nøgle.

CO, der påvirker EMS, skal koordineres i forhold til spectrum management og EMO. Tilsvarende skal EMO, der berører ét eller flere lag i cyberspace, koordineres med CO. Denne koordination finder sted i operationsplanlægningen og løbende under operationens gennemførelse.

3.1.3. Informationsmiljøet

Informationer, der bliver gjort tilgængelige i cyberspace, kan tilgås globalt i næsten samme øjeblik. Cyberspace giver derfor gode muligheder for at dele og søge informationer.

---

[15] Cloudløsninger udgøres hovedsageligt af cloud computing og cloud storage, som er ydelser, der udbydes online til hhv. computerberegninger og digital lagerplads.

[16] EMS udgøres af den samlede fordeling af elektromagnetiske bølger i forhold til deres frekvens eller bølgelængde. Dette inkluderer radiobølger, mikrobølger, varmestråling, synligt lys, ultraviolet stråling, røntgenstråler, elektromagnetisk kosmisk stråling og gammastråling. Se NATO, *Allied Joint Doctrine for Electronic Warfare* (NATO RESTRICTED), udgave B version 1, dok.nr. AJP-3.6, juli 2012.

Cyberspace rummer en stor mængde informationer i form af data på åbne såvel som på lukkede netværk og systemer samt de metadata, der er knyttet til lagring og transport af data.[17]

Cyberspace er en del af det overordnede informationsmiljø, og CO kan anvendes i forbindelse med informationsaktiviteter (IA). Eksempelvis kan IA bestå i manipulation af informationer i cyberspace. CO kan således være et element i Information Warfare (IW).

Informationsmiljøet rummer flere lag, bl.a. det kognitive lag,[18] hvor mennesker træffer beslutninger på baggrund af deres forståelse af den aktuelle situation. Nogle aktører anvender cyberspace til målrettet at påvirke det globale informationsmiljø med henblik på at skabe og påvirke situationsforståelse, narrativer, meninger, politiske dagsordner mv. og dermed påvirke beslutninger.

3.1.4. Egne og allierede enheder og operationer

Aktiviteter i det logiske lag af cyberspace eller deres effekter er ikke nødvendigvis umiddelbart synlige. Der kan derfor opstå risiko for, at flere enheder opererer i samme del af cyberspace uden at kende til hinandens tilstedeværelse. Dette kan resultere i, at enhed A blokerer for enhed B's opgaveløsning, fx ved at enhed A slukker for den fjendtlige server, som enhed B er i færd med at kopiere data fra.

Koordination er derfor centralt, men kan, hvis flere allierede opererer sammen, være vanskeligt, fordi dette indebærer deling af følsomme informationer. Der skal derfor som en del af den tidlige operationsplanlægning træffes aftaler og fastlægges rammer for, om, hvordan og i hvilket omfang denne deling og koordination kan finde sted. De overvejelser, som indgår heri, er bl.a.:

- Afvejning af fordele og ulemper ved at afsløre eller give indikation på offensive såvel som defensive evner og muligheder.
- Afvejning af risici for at afsløre teknologier, hvis hemmeligholdelse er nødvendig for succesfuld gennemførelse af fremtidige CO.
- Omfanget af de planlagte aktiviteter, herunder den vurderede operative gevinst.
- Andre overvejelser af operationssikkerhedsmæssig karakter.

Det er forventeligt, at andre aktører, selv tætte samarbejdspartnere og allierede, vil være tilbageholdende med at dele informationer om igangværende, fortidige og fremtidige CO og den understøttende teknologi. Det skal derfor iagttages, at også alliereedes og samarbejdspartneres CO kan få negative konsekvenser for egne styrkers mulighed for at operere.

[17] Metadata er data om data, fx oplysninger om forfatteren til et Worddokument, gps-oplysninger tilknyttet et digitalt fotografi mv.
[18] NATO, *Allied Joint Doctrine for Information Operations* (NATO UNCLASSIFIED), udgave A version 1, dok.nr. AJP-3.10, december 2015.

Koordination mellem enheder optimeres af kendskab til hinandens CO, hvad angår:

- Information om anvendt teknologi, herunder information om erkendte/udnyttede sårbarheder, leveringsmåde mv.
- Information om anvendt effekt, herunder mål, tid, varighed, afledte effekter mv.

Koordination af OCO bidrager til at undgå, at aktiviteter i cyberspace har negative effekter på egne eller allieredes øvrige operationer. Koordination af DCO er vigtig fx i forbindelse med anvendelsen af delte eller sammensatte computernetværk eller ved anvendelse af samme programmer.

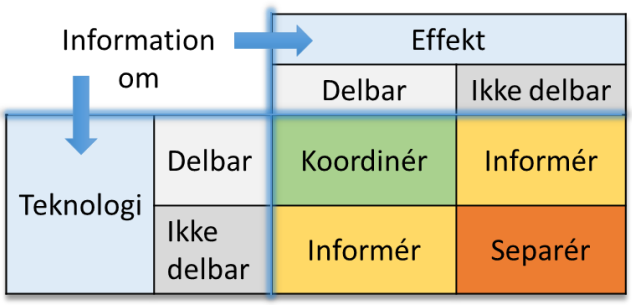
Fuld koordination af CO med egne og allieredes øvrige operationer kræver, at der deles information om den teknologi, som operationen anvender, samt om den effekt, der leveres.

Hvis det fx vurderes uhensigtsmæssigt at dele information omkring et cybervåbens anvendte teknologi, er det vigtigt, at der i videst muligt omfang informeres om den effekt, anvendelsen vil have, herunder hvor og hvornår. På den måde minimeres risikoen for, at de pågældende CO vil have unødvendig negativ indflydelse på de øvrige operationer.

Såfremt det vurderes uhensigtsmæssigt at dele information om både anvendt teknologi og den planlagte effekt, bør planlægningen af de pågældende CO tage alle tilgængelige hensyn for at skabe *egen separation* og derigennem reducere risikoen for utilsigtede sideeffekter.

Ved egen separation forstås, at man i videst muligt omfang planlægger og gennemfører CO, således at uønskede påvirkninger af andre kendte aktiviteter minimeres. Egen separation kan skabes i tid og/eller rum på baggrund af et opdateret situationsbillede over det fysiske operationsområde og cyberspace.

For CO, dvs. både for OCO og DCO, skal der på baggrund af omfanget af informationsdeling laves planer for: 1) direkte koordination, 2) begrænset informering eller 3) etablering af egen separation.



Figur 4, Koordination med allierede og samarbejdspartnere

3.1.5. Fjendtlige aktører

Militære enheders bevægelses- og handlefrihed i cyberspace er udsat for mange trusler. Den høje tilgængelighed til cyberspace, teknologisk viden og computer- og netværksudstyr har banet vej for aktører, som ellers ikke ville have haft mulighed for at gennemføre offensive operationer globalt. Ikke-statslige aktører har muligheder for at skabe effekter med selv relativt små investeringer i teknologi og tekniske kompetencer, selvom omfang, kvalitet og varighed af disse aktiviteter sjældent når niveauet for statslige aktører. Samtidig rummer cyberspace gode muligheder for at sløre den, der udfører eller står bag en skadelig aktivitet i cyberspace. Aktørlandskabet i cyberspace er derfor vanskeligt at overskue, og der er ikke nødvendigvis en direkte forbindelse mellem cyberpersonaer og identiteter i den fysiske verden.

Cyberspaces kompleksitet og uigennemsigtighed gør det muligt at sløre eller skjule de forbindelser, der måtte være. Det kan derfor være vanskeligt at udpege en specifik aktør bag en given aktivitet.

I de tilfælde, hvor det er muligt at kæde en fjendtlig aktivitet i cyberspace sammen med en fysisk identitet, kan det tilmed være vanskeligt at påvise et eventuelt kommandoforhold fx til en organisation eller stat alene ved hjælp af tekniske beviser. Det kan derfor være nødvendigt at foretage en dybere analyse af aktivitetens natur. Dette inkluderer bl.a. dybere teknisk analyse og adfærdsanalyse, der sigter mod at kortlægge den bagvedliggende kontekst. Der kan desuden være juridiske, politiske og militærstrategiske overvejelser forbundet med at udpege en aktør.[19]

Fjendtlige statslige aktører

Flere stater har udviklet evnen til at udnytte cyberspace til at skaffe sig adgang til systemer, netværk og beskyttede informationer med henblik på at opnå militære, politiske eller økonomiske fordele. Det er derfor forventeligt, at der i konflikter mellem stater, herunder krig, vil indgå fjendtlige aktiviteter i cyberspace. Disse aktiviteter kan være rettet mod alle søjler i samfundet og dermed også den militære søjle. Fjendtlige aktiviteter kan skabe effekter i alle lag af cyberspace såvel som afledte effekter uden for cyberspace.

En stats funktioner kan være mere eller mindre integreret med cyberspace. Jo større integration, jo større er konsekvensen for staten, såfremt noget i cyberspace holder op med at virke eller virker forkert. Effekter af aktiviteter og operationer i cyberspace kan have direkte eller indirekte indflydelse på staters sammenhængskraft samt staters evne og vilje til at modstå fjendtlige angreb i og uden for cyberspace. CO kan dermed ikke blot skabe taktiske og operative effekter, men også strategiske effekter som supplement eller alternativ til effekter af fysiske aktiviteter.

[19] De juridiske overvejelser kan fx være, om en aktørs handlinger kan tilskrives en part til konflikten.

Den effekt, CO kan skabe, er proportional med den angrebne aktørs afhængighed af cyberspace. Fordi stater kan have forskellige niveauer af sikkerhed i cyberspace, er der dog ikke nødvendigvis proportionalitet mellem denne afhængighed, og hvor let det er at skabe effekten. Det er dermed ikke nødvendigvis givet, at CO kan træde i stedet for enhver anden type af operation.

Statslige aktører har generelt flere ressourcer og redskaber til rådighed end ikke-statslige aktører. Førere skal dermed forudse, at de mest effektive fjendtlige aktiviteter i cyberspace vil udgå fra stater. Stater vil ofte have længere strategiske planlægningshorisonter; stater vil gennem lovgivning kunne udføre handlinger, der ville være ulovlige for almindelige borgere, og derfor handle mere frit; stater har ofte flere økonomiske ressourcer; og stater har ofte bedre mulighed for at påvirke, samarbejde med eller styre adgangsskabende virksomheder (fx internetudbydere). Dermed kan de gennemføre mere avancerede og komplekse CO.

Nogle stater anvender ikke-statslige aktører til at gennemføre CO fx for at kunne benægte deres indblanding i aktiviteterne. Rationalet for dette kan være at undgå militære, politiske eller økonomiske konsekvenser, fordi disse aktiviteter kan bryde nationale, juridiske, etiske, kulturelle eller diplomatiske regler og normer. Benægtelse kan også være et forsøg på at skjule statens egen evne til at operere i cyberspace.

Fjendtlige ikke-statslige aktører

Ikke-statslige aktører kan tilslutte sig en stats politik og gennemføre aktiviteter i cyberspace, som støtter denne. En sådan tilslutning kan være mere eller mindre åben, og de gennemførte aktiviteter kan støtte staten i større eller mindre grad.

Ikke-statslige aktører dækker yderligere over insidere, terrorister, hacktivister og kriminelle, der udgør en trussel mod bevægelses- og handlefriheden i cyberspace.

Begrebet hacktivist dækker over individer, der gennemfører aktivisme (politisk) gennem hacking.

Insidere dækker over personer med legitim adgang til IKT-systemer, der forsætligt, ved et uheld eller som resultat af manipulation eller vildledelse foretager aktiviteter, som udgør en trussel mod disse systemers fortrolighed, integritet eller tilgængelighed.

3.1.6. Neutrale aktører

Neutrale aktører er de aktører, der ikke er part i den konflikt, som operationen er en del af.

Neutrale aktører kan være til stede overalt i cyberspace. Og da ikke alle lag af cyberspace har en geografisk placering, kan det være svært at fastlægge, hvilke dele af cyberspace som anvendes eller tilhører neutrale og udenforstående aktører.

Det kan ikke altid kontrolleres, hvilken vej data bevæger sig gennem cyberspace. En aktør bevarer derfor sin neutralitet, selvom et angreb uden den neutrale aktørs kendskab rutes igennem dennes del af cyberspace.

Med den hastigt voksende udnyttelse af cyberspace, herunder fx internettet, må det forventes, at der vil være en lang række neutrale aktører i et operationsområde, herunder civile individer og organisationer.

3.1.7. Indflydelse fra andre operationsmiljøer

Operationsmiljøer kan påvirke hinanden. CO kan påvirke og påvirkes fra land, luft og det elektromagnetiske og det maritime operationsmiljø. Ofte vil mere end ét af disse miljøer udgøre det samlede operationsmiljø for en given operation, hvorfor CO sjældent vil stå alene.

Når operationsmiljøet i cyberspace analyseres, er det vigtigt, at føreren er opmærksom på, hvilke kontaktpunkter og afhængigheder der eksisterer mellem cyberspace og andre miljøer. Kontaktpunkter til det fysiske lag af cyberspace kan være generatorer, kølemateriel i serverrum mv. Kontaktpunkter til det logiske lag kan være procedurer for systemopdateringer, installation og distribution af anvendte programmer, brugeres adgang til at installere eller ændre software eller tilkoble eksternt udstyr (fx egen mobiltelefon) mv. Kontaktpunkter til cyberpersonalaget kan bestå af sammenkoblingen af en fysisk identitet og en cyberpersona. Det kan fx være en persons adgang til en mailkonto, brugerkonto eller social profil.

Ofte er det i disse kontaktpunkter, at svagheder og sårbarheder kommer til udtryk. En systemopdatering af en kritisk entitet i cyberspace, der bliver leveret på CD-rom med posten, vil fx udgøre en alvorlig sårbarhed, som kan udnyttes.

Føreren skal overveje:

- Hvilke kontaktpunkter og afhængigheder eksisterer der mellem eget cyberspace og andre operationsmiljøer?
- Hvilke kontaktpunkter og afhængigheder i modstanderens cyberspace kan udnyttes i forbindelse med OCO?

3.2. Fejl og systemnedbrud

Systemfejl kan opstå som resultat af misligholdelse, forkert brug, strømafbrydelser, fysiske forhold (fx overophedning), programmeringsfejl mv. Fejl kan true systemers fortrolighed, integritet og tilgængelighed.

Systemnedbrud kan blotlægge sårbarheder, og disse skal håndteres, så snart de erkendes, da de kan udnyttes af en fjendtlig aktør til fx at skabe adgang til systemet og tilsluttede systemer.

Ofte vil det være en driftsmyndigheds ansvar at genoprette systemets funktionalitet, og disse aktiviteter vil dermed ske uden for rammen af CO.

Føreren skal dog være opmærksom på, at hændelser, som umiddelbart ligner fejl og systemnedbrud, kan være resultatet af fjendtlige aktiviteter i cyberspace. Denne mulighed bør altid indgå i vurderingen af årsagen til hændelsen.

Del II: Principper for CO

4. CO

CO defineres som **militære aktiviteter i eller gennem cyberspace, der, afgrænset i tid og rum og gennem anvendelse af cyberspacekapaciteter, har til hensigt at opnå militære mål**.

Ved militære aktiviteter forstås aktiviteter gennemført under militær kommando.

Ved cyberspacekapacitet forstås en militær kapacitet, der er i stand til at operere i eller gennem cyberspace for at udføre CO.

CO involverer altid aktiviteter i det logiske lag ved hjælp af indsættelse af data og/eller kode i cyberspace. Militære aktiviteter, som påvirker cyberspace uden anvendelse af data eller kode, betragtes ikke som CO. Flyangreb på et datacenter er ikke CO, men et angreb på et fly via det logiske lag i cyberspace *er* CO.

Effekter af CO kan skabes på alle tre lag i cyberspace og ultimativt bidrage til at skabe effekter uden for cyberspace, herunder fx fysiske og kognitive effekter.

CO kan understøtte og indeholde alle kampformer, herunder forsvarskamp, angrebskamp og henholdende kamp, samt bidrage til efterretningsindhentning, overvågning og opklaring i forbindelse med operationer i cyberspace såvel som i andre operationsmiljøer.

CO opdeles i OCO og DCO. Det, der afgør, om CO er offensive eller defensive, er, hvorvidt der anvendes magt eller ej.

Med magtanvendelse i cyberspace forstås aktiviteter, der ændrer en modstanders cyberspace eller funktionaliteten af modstanderens entiteter i cyberspace.

DCO defineres som **CO, der uden at anvende magt har til hensigt at bevare eller genskabe egen bevægelses- og handlefrihed i cyberspace**.

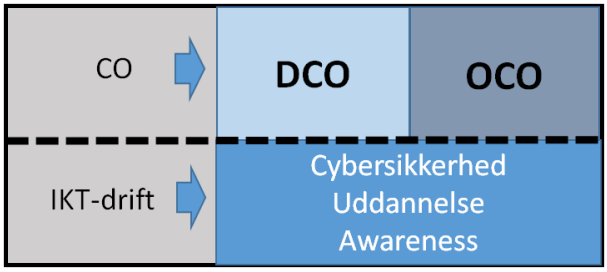
Ved bevægelses- og handlefrihed forstås evnen til at kontrollere og anvende de enkelte dele af cyberspaces tre lag. Egen bevægelses- og handlefrihed kan reduceres af fjendtlige aktiviteter eller andre trusler.

DCO omfatter aktiviteter til at imødegå en modstanders forsøg på at skabe offensive effekter.

DCO dækker ikke over almindelig cybersikkerhed (CS), der er en del af driften af IKT, og som på daglig basis varetages af de ansvarlige myndigheder enten centralt eller decentralt.

OCO defineres som **CO, der har til hensigt at anvende magt i eller gennem en modstanders del af cyberspace**.

CO kan ikke skabe effekter i en modstanders cyberspace uden magtanvendelse. CO, der medfører ændringer i modstanderens cyberspace, skal derfor henregnes som OCO. OCO omfatter dermed også CO, der anvender magt med et forsvarsmæssigt sigte.



Figur 5, Afgrænsning af CO

4.1. Roller og ansvar

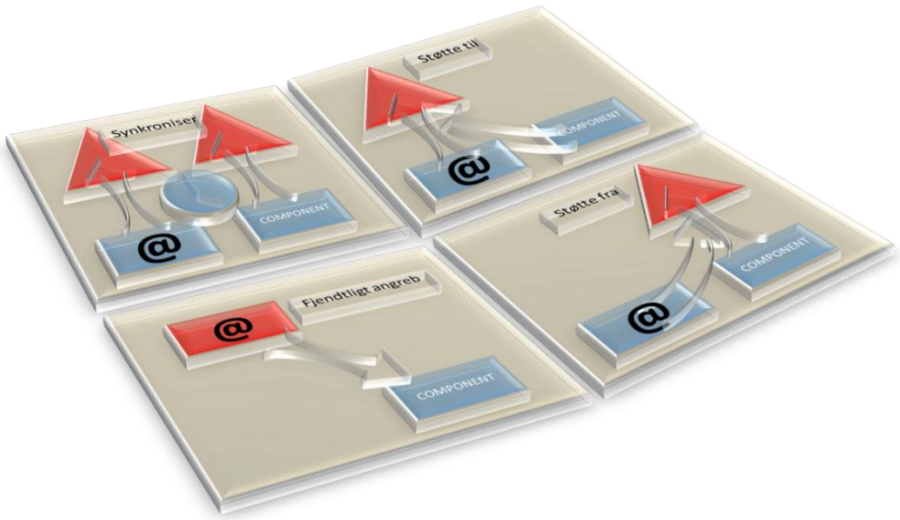
Planlægningen af CO foregår på operativt niveau gennem den proces, som er beskrevet i annex A.

4.1.1. Det taktiske niveaus rolle i CO

Operative stabe og enheder kan forvente at skulle støtte CO. De kan alle forvente at skulle planlægge og gennemføre kapacitetsudvikling, uddannelse og operative aktiviteter under hensyntagen til CO. De skal alle inddrage muligheden for støtte fra CO. Og de kan alle blive udsat for angreb og anden påvirkning fra fjendtlige CO. Det er derfor vigtigt, at man på det taktiske niveau er opmærksom på, hvilke effekter CO leverer, og hvordan CO understøtter og integreres i opgaveløsningen.

På det taktiske niveau er det vigtigt at overveje, hvordan den enkelte enhed eller våbenart bedst muligt kan integrere egne operationer med CO, herunder i form af støtte *til* og støtte *fra* CO. Nogle enheder, fx en EW-enhed eller en specialoperationsenhed, kan være særligt anvendelige til at skabe forbindelse til mål i cyberspace eller til at bidrage til relevant opklaring i forhold til enheder og aktiviteter i cyberspace. Andre enheder eller missioner vil have fordele af støtte fra egne CO, som skal identificeres.

Til at understøtte integration af CO med andre militære operationer kan der efter konkret vurdering placeres én eller flere Cyber Liaison Officers (CLO) i de taktiske stabe. CLO rådgiver styrkechefen og er kontaktpunkt til CNO-kapaciteten.



Figur 6, Det taktiske niveaus rolle i CO

Mission assurance

På taktisk niveau skal der etableres procedurer og koncepter, der sikrer, at enhederne kan operere under påvirkning af trusler fra cyberspace, hvad enten det drejer sig om fejl og systemnedbrud eller fjendtlige OCO. Disse procedurer og koncepter bidrager til at styrke enhedernes robusthed over for trusler fra cyberspace og skal tilpasses enhedernes udstyr, funktionalitet, beredskab og operationsmåde.

Det må forventes, at egne entiteter i cyberspace, selv under den bedst mulige beskyttelse, kan blive påvirket af hændelser, der ændrer eller begrænser deres funktionalitet helt eller delvist. Det er vigtigt, at enhederne har et overblik over, hvilke kontaktpunkter enheden har til cyberspace. Det vil oftest være i disse kontaktpunkter, at hændelser i cyberspace bliver til egentlige trusler mod systemet og dets anvendelse. Disse kontaktpunkter er fx udstyr, der udgør en entitet i det fysiske lag af cyberspace, men kan også være kontaktpunkter til det logiske lag (fx anvendelse af et computerprogram) eller cyberpersonalaget (fx en chefs e-mailkonto).

Hvis en enhed skal kunne fungere, selv under et højt trusselsniveau i cyberspace, skal den tage hensyn til to aspekter:

1. Opbygning af redundans.
2. Opbygning af robusthed.

Opbygning af redundans

Udnyttelse af cyberspace i opgaveløsningen og ikke mindst graden af afhængighed udgør en sårbarhed, og derfor skal balancen mellem anvendelse, afhængighed og sikkerhedsniveau løbende tilpasses. En enhed, hvis opgaveløsning i stort omfang afhænger af cyberspace, vil have behov for at opretholde en tilsvarende høj grad af sikker-

hed, hvilket kan være både omkostningstungt, bevægelseshæmmende og endda hæmmende for opgaveløsningen.

Selvom det kan betyde nedsættelse af operationshastighed og effektivitet, skal en enhed kunne fungere med begrænset eller ingen anvendelse af cyberspace. Der skal derfor opbygges redundans i opgaveløsningen, hvilket kan involvere at opbygge procedurer og metoder, der er uafhængige af adgang til cyberspace.

PACE:

Kritiske systemer kan ved hjælp af princippet PACE bygges op om fire dybder af redundans: 1: **P**rimary system, 2: **A**lternate system, 3: **C**ontingency system og 4: **E**mergency System. "System" kan her dække over fysisk materiel (fx et kommunikationssystem) såvel som procedurer.

Opbygning af robusthed

Robusthed i cyberspace kan skabes gennem anvendelse af de fem kernefunktioner: identify, protect, detect, respond, recover.[20]

1. Identify

Enhedens kritiske systemer med entiteter i eller afhængigheder af cyberspace. Klarlæg, hvordan angreb eller fejl på disse påvirker enhedens effektivitet i sin opgaveløsning.

2. Protect

Systemerne skal beskyttes bedst muligt under hensyntagen til balancen mellem anvendelse, afhængighed og sikkerhed. Indeholdt i overvejelsen omkring "sikkerhed" er også en vurdering af omkostninger i forhold til sikkerhedsniveau, idet omkostningerne ved at beskytte *alt mod alt* ofte vil mere meget høje. Overvejelserne omhandler fysisk sikkerhed såvel som sikkerhed i cyberspace. Selvom andre myndigheder kan være ansvarlige for dele af sikkerheden, kan der være lokale systemer eller praktiske forhold, der gør det nødvendigt at tage ekstra beskyttelsesmæssige tiltag.

3. Detect

Hændelser, herunder fjendtlige OCO, der nedsætter funktionaliteten af entiteter i cyberspace, er ikke nødvendigvis synlige. Fx kan en radarskærm vise et tomt luftrum, enten fordi luftrummet er tomt, eller fordi systemet ikke fungerer korrekt. For alle systemer skal det overvejes, hvordan hændelserne erkendes, og hvordan systemets funktionalitet kan verificeres.

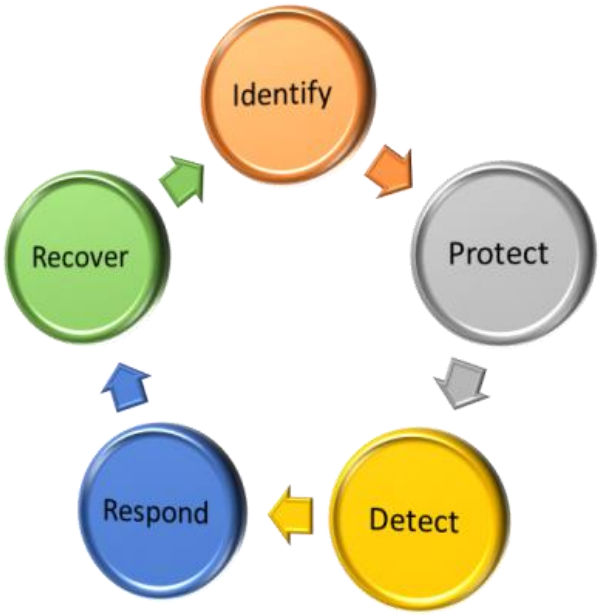
[20] Funktionerne baserer sig på US NIST Cybersecurity Framework: National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity,* version 1.1, 2018.

4. Respond

Procedurer for håndtering af hændelser skal være fastlagt, kendt og indøvet. Forberedte procedurer kan fx indeholde planer for Emission Control (EMCON), Information Control (INCON) og overgang til alternative systemer. Procedurerne skal tilpasses de lokale forhold. For nogle systemer og situationer vil en procedure kunne være at lukke systemet helt ned. Andre situationer vil tale for at fortsætte anvendelsen af systemet, fx med henblik på at observere fortsat fjendtlig aktivitet. Alt efter hændelsens karakter kan det være nødvendigt at koordinere reaktionen med CNO-kapaciteten, eventuelt med henblik på at gennemføre yderligere CO.

5. Recover

Genskabelse af systemet kan involvere geninstallering af systemet, opdatering, patching, udskiftning, ændring af systemvejledning og procedurer mv.



Figur 7, Kernefunktioner i opbygning af robusthed

5. Førerens overvejelser

Hvad enten føreren er den øverst ansvarlige for en værnsfælles militæroperation, den ansvarlige for indsættelsen af CNO-kapaciteten eller en fører uden for CNO-kapaciteten, fx en styrkechef, skal denne kende til forhold omkring anvendelse af CO, således at dette kan indgå i førerens overvejelser.

Førerens overvejelser kan deles op i overvejelser, der relaterer sig til:

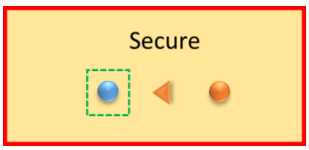
1. Effekter i cyberspace.
2. Joint functions.
3. Krigsførelsens grundprincipper.

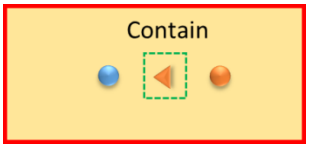
5.1. Effekter i cyberspace

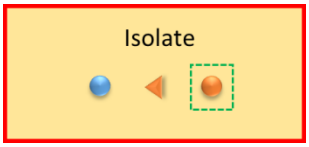
Ved planlægning af CO anvendes nedenstående effekttermer, der refererer til de effekter, som CO kan skabe i eller via cyberspace. Disse effekter bidrager til at skabe taktiske, operative og strategiske effekter, der leder til opnåelse af militære mål.

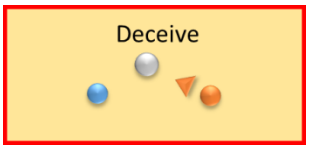
Når effekterne opnås gennem OCO, kan de være sammenlignelige med effekter af kinetiske angreb, uden at de nødvendigvis er permanent ødelæggende for målet, idet de kan være reversible.

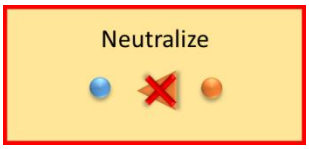
Secure	Sikring af fortrolighed, integritet og tilgængelighed i afgrænsede dele af cyberspace mod fjendtlige CO.
Contain	Standsning af fortsat spredning ved at inddæmme skadelige data eller kode.
Isolate	Isolation af modstanderen fra sin indsatte kode, så modstanderen forhindres i at interagere med koden og dermed også det påvirkede system eller netværk.
Deceive	Imødegåelse af mulige angreb ved at ændre på cyberspace med henblik på at lede angriberen uden om kritiske systemer og netværk.
Neutralize	Neutralisering af skadevoldende kode ved at gøre den ude af stand til at påvirke den del af cyberspace, som anvendes af egne styrker.
Manipulate	Effekten består af undergrupperne infiltrate og modify.
Infiltrate	Overførelse af data og kode til modstanderens systemer eller netværk.
Modify	Ændring af data eller kode på modstanderens systemer eller netværk.
Exfiltrate	Indhentning af informationer gennem kompromittering af modstanderens systemer og netværk.

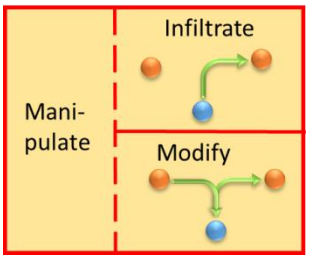


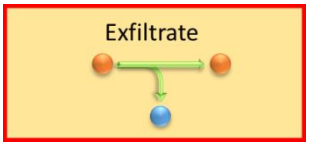




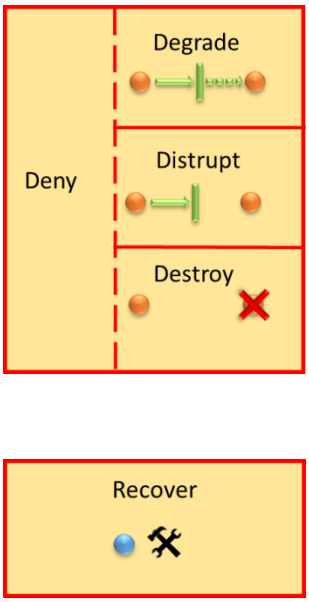








Deny	Effekten deny består af undergrupperne degrade, disrupt og destroy.
Degrade	Reducering af modstanderens mulighed for at anvende sine egne entiteter i cyberspace.
Disrupt	Forstyrrelse af modstanderens mulighed for at anvende sine egne entiteter i cyberspace inden for fastlagte tidsrum.
Destroy	Ødelæggelse af modstanderes entiteter i cyberspace fuldstændigt og permanent. Effekten er ikke reversibel.
Recover	Genoprettelse af funktionaliteten af påvirkede systemer og netværk, herunder at fjerne eller reducere effekterne af et fjendtligt angreb, fx ved genskabelse af data.



Figur 8, CO-effekter

5.2. Joint functions

Dette afsnit omhandler, hvordan joint functions skal forstås i relation til CO. Heri indgår også, hvordan CO understøtter joint functions og krigsførelsens grundprincipper på taktisk niveau. Formålet med afsnittene er at understøtte CNO-kapacitetens planlægning og gennemførelse af CO samt integrationen af CO på alle niveauer.

Joint functions er betegnelsen for værnsfælles principper, der beskriver de overordnede forhold, som skal tages i betragtning for at integrere, synkronisere og anvende CO.[21]

5.2.1. Fires

Et cybervåben defineres i denne doktrin som: **computerkode, der anvendes til at opnå den ønskede effekt på målet**. Våbenaflevering er det øjeblik, hvor koden deployeres mod modstanderens del af cyberspace. Effekten af et cybervåben kan være fysisk såvel som virtuel. Den tidsmæssige udstrækning af effekten kan være kortvarig, længerevarende eller varig, og cybervåbnet kan være designet med en forsinkelse, så effekten udmønter sig lang tid efter selve våbenafleveringen.

Aktiviteter i cyberspace kan påvirke selve operationsmiljøet og ikke kun de tilstedeværende entiteter og aktører. Det er med andre ord muligt at ændre på, hvordan dele af cyberspace opfører sig og ser ud. Det kunne være i form af påvirkning af måden,

[21] NATO, *Allied Joint Doctrine for Operational-Level Planning* (ikke-klassificeret), dok.nr. AJP-5, juni 2013.

hvorpå data fordeles på computernetværk, ændring af computeres fortolkning af data og instruktioner, degradering af et systems evne til at håndtere dataforespørgsler mv.

Et cybervåben designes på en sådan måde, at det i videst muligt omfang ikke kan kompromitteres eller kopieres efter anvendelse og ultimativt blive vendt mod egne enheder. Inden våbenaflevering skal det tilsikres, at egne og allierede operationer og enheder ikke bliver unødvendigt påvirket. CO skal derfor efter omstændighederne koordineres med øvrige operationer og aktiviteter, herunder aktiviteter i EME.

Cybervåben kan skabe strategiske effekter (fx påvirkning af kritisk infrastruktur), operative effekter (fx nedbrydning af modstanderens Command and Control (C2)) og taktiske effekter (fx ødelæggelse af våbensystemer). Formålet med fires i cyberspace er at påvirke modstanderens evne, vilje og forståelse.

Nogle effekter kan være sammenlignelige med effekter af konventionelle våben, og i nogle tilfælde vil CO derfor kunne erstatte eller støtte indsættelsen af fysiske våben.

Cybervåben med reversible effekter kan være særligt attraktive i forhold til en efterfølgende genopbygning.

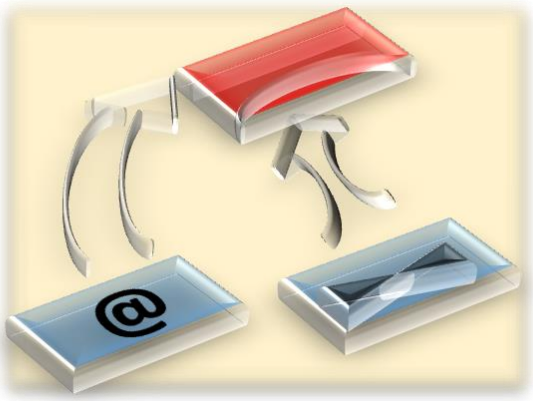
Cybervåben kan indsættes i forsvar, i angreb, støttet eller støttende. På grund af kompleksitet og uigennemsigtighed i cyberspace kræver udviklingen af cybervåben en grundig analyse af dets virkning og effekt i netop den del af cyberspace, som våbnet skal indsættes i. Risici for uønskede effekter skal minimeres, og der skal foretages Collateral Damage Estimate (CDE).

Effektive cybervåben er sjældent hyldevarer. Etablering af adgange og udvikling af cybervåben designet til at angribe et specifikt mål med en given effekt vil normalt være så kompliceret og ressourcekrævende, at det ikke kan foregå ved den enhed og på det tidspunkt, det skal indsættes. Våbenafleveringen vil derfor oftest ske fra CNO-kapaciteten via koordination med CLO. Styrkechefen skal være opmærksom på, at det kan tage måneder at etablere grundlaget for at udvikle og anvende cybervåben.

Forud for deployering af et styrkebidrag vil det i særlige tilfælde være muligt på forhånd at forberede specifikke effekter, som kan leveres i forbindelse med bidraget. Styrkechefen kan også få til opgave at synkronisere egne fires med aflevering af cybervåben.

5.2.2. Manoeuvre

Manøvrer anvendes til at opnå militære fordele i forhold til modstanderen og til at påvirke dennes forståelse af situationen, ødelægge dennes sammenhæng i kampen og underminere dennes vilje til at kæmpe. Manøvrer kan finde sted i alle lag af cyberspace. Manøvrer i cyberspace anvendes i koordination med indsættelsen af cybervåben.



Figur 9, Synkroniserede manøvrer

På det logiske lag i cyberspace kan man opnå en særlig høj grad af bevægelighed, fordi afstand og tid ikke er begrænsende på samme måde som i fysiske rum. Manøvrer kan gennemføres med længere rækkevidde og inden for kort tid. Manøvrer kan udnytte muligheden for anonymitet i cyberspace til at styrke fleksibilitet, agilitet, sløring og dækning. I nogle tilfælde er det dog nødvendigt at manøvrere i fysiske rum for at få adgang til ikke-forbundne områder af cyberspace.

Manøvrer i cyberspace kan ske uafhængigt af fysiske manøvrer, men kan også gennemføres parallelt med fysiske manøvrer, fx under et angreb, hvor et mål engageres både med kinetiske våben og med angreb gennem cyberspace. For nogle typer CO er det ikke muligt at indøve anvendelsen af et cybervåben og teste dets våbenvirkning forud for operationen, fx fordi operationen anvender teknologi eller teknikker, der enten kun virker mod det specifikke mål, eller hvis effekt vil svækkes, hvis cybervåbnet er kendt.

Defensive manøvrer i cyberspace omfatter manøvrer, der har til hensigt at:

- Skabe dækning (fx at opstille en firewall eller gennemføre fokuseret datatrafikanalyse).
- Skabe sløring (fx at indsætte proxyservere eller på anden måde skjule layoutet af eget cyberspace).
- Samt skabe afstand til modstanderen ved at afskære dennes mulighed for fysisk eller logisk at forbinde til dele af eget cyberspace (fx ved at afkoble eller adskille forbundne systemer).

5.2.3. C2

Effektiv C2 er nødvendig for at kunne planlægge, synkronisere og gennemføre CO. Da CO kan skabe operative effekter uden for cyberspace, skal CO koordineres og synkroniseres med øvrige aktiviteter og operationer.

Det er essentielt, at C2 på alle niveauer opbygges med en høj grad af modstandskraft og redundans i forhold til påvirkning fra cyberspace, idet der skal tages hensyn til fjendtlige aktørers offensive kapaciteter. C2-informationssystemer (C2IS) skal først og

fremmest beskyttes bag et robust forsvar, der kan afvise fjendtlige CO. Samtidig skal C2IS i videst muligt omfang kunne fortsætte med at understøtte C2 selv under fjendtlige angreb gennem cyberspace.

Fjendtlige CO kan ske uvarslet og skabe stor effekt selv mod et stærkt forsvaret netværk. Denyeffekter kan sætte et computernetværk ud af spil i en længere periode. Men også andre fjendtlige effekter kan betyde, at netværk eller dele af netværk er uanvendelige, fx som følge af sikkerhedslukning, opdateringer, geninstallation mv.

Styrkechefen skal i sin planlægning inddrage fjendtlige aktørers kapacitet til at skabe effekter i cyberspace, der begrænser anvendelsen af C2IS. Dette bør tage udgangspunkt i en risikovurdering.

De afledte konsekvenser af risikovurderingen kan indeholde tiltag, der sikrer, at C2 fungerer uden bevægelses- og handlefrihed i cyberspace. Dette kan ultimativt betyde, at styrkechefens C2 skal indeholde et tilstrækkeligt analogt alternativ til de C2IS, der er afhængige af cyberspace.

C2- og C2IS-robusthed samt evnen til at understøtte egne operationer, selv under fjendtlige offensive effekter, kan styrkes gennem øvelser og træning.

5.2.4. Intelligence

CO er afhængige af forudgående efterretningsindhentning både i og uden for cyberspace.

Nødvendigheden af forudgående efterretningsindhentning stiger med kompleksiteten af et cybervåben. Et cybervåben, som er udviklet til at engagere et specifikt mål, vil ofte skulle udvikles på baggrund af oplysninger om målet, der ikke er umiddelbart tilgængelige. Idet ikke alle dele af cyberspace er i forbindelse med hinanden, kan det være nødvendigt at inddrage efterretningsaktiviteter og/eller specialstyrkeoperationer for at kunne skabe forbindelse til et mål.

Efterretninger indhentet via cyberspace kan anvendes til støtte for CO såvel som andre operationer på alle niveauer. Forud for planlægning af militære operationer skal der altid foretages analyse af relevante dele af operationsmiljøet, herunder cyberspace.

Cyberspace kan understøtte indhentningsdiscipliner såsom SIGINT, IMINT, OSINT og HUMINT. Cyberspace kan give adgang til mål, der ellers vil være uden for rækkevidde.

Information omkring de dele af cyberspace, der er kontrolleret af en modstander, kan bidrage med vigtige informationer om modstanderen, herunder dennes organisation, C2, C2IS, planer, kapabilitet mv.

Aktiviteter i cyberspace kan understøtte Joint Intelligence Preparation of the Operational Environment (JIPOE).

5.2.5. Information

CO og IA skal koordineres og synkroniseres, så de ikke påvirker hinanden negativt. Ved planlægning af CO skal det overvejes, om operationen kan influere strategisk kommunikation (STRATCOM) negativt.

Aktiviteter i cyberspace kan, på samme måde som fysiske aktiviteter, påvirke informationsmiljøet og dermed vilje, forståelse og evne på strategisk såvel som på operativt og taktisk niveau. Styrkechefen skal sikre, at aktiviteter i cyberspace er analyseret for at belyse eventuelt ønskede eller uønskede sideeffekter i informationsmiljøet.

Styrkechefen skal desuden være opmærksom på, at egne styrker gennem cyberspace kan være under påvirkning af informationer og skadelige handlinger i informationsmiljøet, som ikke er umiddelbart synlige. Dette kan fx være en modstanders forsøg på at intimidere, provokere, forvirre eller på anden måde påvirke.

5.2.6. Sustainment

CO kan bidrage til at skabe og opretholde det nødvendige niveau af funktionalitet og sikkerhed i cyberspace. Evnen til sustainment i cyberspace bygger i høj grad på en effektiv IKT-drift og et veludbygget cyberforsvar.

Digitaliseringen af militære logistik-, vedligeholdelses-, personale- og sundhedssystemer mv. betyder, at disse systemer i høj grad er afhængige af bevægelses- og handlefrihed i cyberspace. Systemerne skal på samme måde som C2IS være modstandskraftige, redundante og i tilstrækkelig grad kunne fungere uden adgang til cyberspace.

5.2.7. Force Protection

CO kan anvendes til at sikre egen bevægelses- og handlefrihed i cyberspace samt til at opretholde egne styrkers effektivitet. Informationer indhentet gennem cyberspace, fx angående modstanderens intentioner, midler, metoder og bevægelser i og uden for cyberspace, kan bidrage til at styrke sikkerheden for egne enheder.

DCO kan indeholde særlige systemsårbarhedsanalyser, der bidrager til Force Protection (FP) i relation til militære installationer, faciliteter og materiel, herunder våbensystemer.

Beskyttelse af personel handler ikke alene om at skærme personellet fra direkte trusler såsom identitetstyveri, phishing mv. FP handler også om at beskytte servere og databaser, der gemmer oplysninger om personellet, så disse oplysninger ikke på sigt kan misbruges til fx at miskreditere, misinformere eller true personel, fx med henblik på at undergrave moralen.

5.2.8. Civil-Military Cooperation

En stor del af det fysiske lag i cyberspace er ejet eller drevet af civile aktører. Samarbejde med disse aktører understøtter CO. Kontakt til en lokal ISP kan fx give adgang til at tilgå eller påvirke ellers lukkede dele af cyberspace.

I forbindelse med Civil-Military Cooperation (CIMIC) kan CO anvendes til at styrke civile aktørers CS, hvilket kan bidrage til at opbygge gensidig tillid og styrke samarbejdet. Civile aktørers niveau af CS kan have betydning for militære aktiviteter både i og uden for cyberspace.

Det skal overvejes, hvorvidt det er nødvendigt eller formålstjenstligt at anvende DCO til at beskytte civile samarbejdspartneres cyberspace. Det kunne fx ske ved at etablere netværksovervågning eller vildledende foranstaltninger i samarbejdspartnerens systemer. Fx kan et velfungerende samarbejde mindske risikoen for insidertrusler og angreb via underleverandørers cyberspace.

5.3. Krigsførelsens grundprincipper

CO indgår, sammen med andre typer af militære aktiviteter, i den operative planlægning og gennemførelse af militære operationer. De overordnede principper, som gælder for militære aktiviteter, gør sig også gældende for CO.[22]

5.3.1. Kræfternes samspil

Kræfternes samspil dikterer, at alle militære aktiviteter skal pege mod opfyldelsen af de militær-strategiske mål.

CO er i den henseende en naturlig del af enhver operation og kan både blive støttet af og støtte andre militære aktiviteter. Specialoperationsstyrker kan fx støtte CO ved at installere teknisk udstyr i en modstanders netværk, og CO kan støtte en fremrykning ved at manipulere modstanderens C2IS.

CO er i nogle tilfælde et alternativ til andre typer af militære aktiviteter og kan anvendes til selvstændigt at opnå operative effekter, fx immobilisering af modstanderens kapaciteter og bekæmpelse af modstanderens vilje, evne og forståelse. Samspillet kan ske mellem de militære magtmidler samt mellem militære og statslige magtmidler uden for den militære søjle, herunder økonomiske og diplomatiske magtmidler.

Kræfternes samspil styrkes af entydige kommandoforhold og koordination af aktiviteter samt af en overordnet strategi og fælles doktriner, taktikker, teknikker og procedurer. Teknisk interoperabilitet samt et højt uddannelsesniveau har også betydning for kræfternes samspil.

[22] Grundprincipperne er generelt omtalt i NATO, *Allied Joint Doctrine*, udgave E version 1 (ikke-klassificeret), dok.nr. AJP-01(E), februar 2017, og Hæren, Feltreglement I (ikke-klassificeret), dok.nr. HRN 010-001, juni 2016.

Grundet hensyn til operationssikkerhed er det særligt vanskeligt for CO at give enheder uden for CNO-kapaciteten indsigt i planlægning og gennemførelse af de enkelte aktiviteter. Støttede enheder må derfor ofte henholde sig til de informationer, de kan få via CLO, herunder hvilke effekter der kan blive stillet til rådighed for styrkechefen. Den manglende indsigt herudover kan udgøre en begrænsning i forhold til at opnå et effektivt samspil mellem anvendelse af kræfter i henholdsvis cyberspace og de fysiske operationsmiljøer.

5.3.2. Tyngde

De militære midler, der er til rådighed for en fører, skal koncentreres i tid og rum. Tyngde kan skabes i cyberspace ved koncentration af kræfterne mod et enkelt mål. Et eksempel på dette er DDoS-angreb, hvor regnekraften fra mange angribende computere indsættes mod et enkelt mål, der dermed overbelastes.[23]

Et andet eksempel på tyngdedannelse er, at CO tildeles flere ressourcer, fx flere hackere, til at kunne gennemføre et angreb eller lade andre typer af operationer støtte CO.

Når der skabes tyngde i cyberspace gennem flere samtidige CO, skal det ske under detaljeret koordination. De enkelte CO's påvirkning af hinandens funktionalitet skal om muligt være afklaret og testet forud for iværksættelse.

Såfremt flere CO udnytter den samme sårbarhed i det angrebne system, er der risiko for, at modstanderen blokerer for udnyttelse af sårbarheden efter det første angreb. En sådan blokering, fx blokering af en netværksport, kan i nogle tilfælde ske automatisk og med maskinhastighed.[24]

Gennem koordination og synkronisering af CO med øvrige aktiviteter kan der skabes tyngde. CO kan udgøre en force multiplier, fx gennem manipulation af en modstanders luftforsvarssystemer, hvorved der kan leveres en højere effekt i målet.

5.3.3. Økonomi med kræfterne

De militære midler, en fører har til rådighed, skal anvendes, således at der opnås størst mulig operativ effekt med færrest mulige anstrengelser.

En fordel ved CO er, at de kan levere effekt, uden at større mængder af materiel skal transporteres til operationsområdet. Ved hjælp af CO kan ét angreb med maskinhastighed skabe effekt flere steder i cyberspace.

---

[23] Distributed Denial of Service (DDoS) er et angreb, hvor et netværk af fjernstyrede computere anvendes til at overvælde målet med datatrafik, således at målet ikke har nok hukommelse, regnekapacitet eller netværksbåndbredde til at behandle de data, det bliver belastet med.

[24] Maskinhastighed er den hastighed, hvormed computere arbejder, og data flyttes. Komplicerede beregninger kan tage længere tid, men de fleste informationsudvekslinger foregår med nær lysets hastighed.

OCO bliver ikke nødvendigvis detekteret af modstanderen med det samme. Angriberen kan således være til stede i modstanderens cyberspace i en længere periode og udnytte tilstedeværelsen til at skabe gentagne effekter med lille ressourceforbrug. Såfremt angrebet detekteres, kan det medføre stort ressourceforbrug for forsvareren at imødegå angrebet og fjerne angriberens adgang, genoprette den ønskede funktionalitet af det angrebne system eller netværk og mitigere langtidsvirkningerne af angrebet.

Udviklede taktikker, teknikker, procedurer og kode kan i princippet genanvendes helt eller delvist. Men de må dog forventes at have en begrænset levetid som følge af teknologisk udvikling, opdateringer og patching af software. Især må det forventes, at udnyttelse af en sårbarhed i en modstanders system eller netværk vil lede til blokering af sårbarheden, hvorved den ikke længere kan udnyttes mod samme modstander.

Det antages, at modstanderen tager ved lære af den valgte fremgangsmåde, herunder anvendt taktik, teknik, procedure eller kode. Desuden skal man være forberedt på modstanderens kopiering og modificering af anvendt kode og ultimativt risikoen for, at den bliver vendt imod én selv.

Forberedelse af CO kan kræve mange ressourcer og involvering af mange militære funktioner og våbenarter. Det kan være omkostnings- og tidskrævende at udvikle cybervåben, og det skal derfor nøje overvejes, om det er kræfterne værd, eller om der fx skal anvendes konventionelle våben.

Styrkechefen skal overveje, om CO kan træde i stedet for andre aktiviteter, fx for at nedbringe belastning eller frigøre kapaciteter til andre opgaver.

5.3.4. Handlefrihed

Anvendelse af CO er, som alle andre styrkeindsættelser, underlagt en række politiske, juridiske og militær-strategiske begrænsninger, så der tages fornødent hensyn til Danmarks politisk-strategiske interesser. Dette betyder, at danske enheders mulighed for at operere kan adskille sig fra udenlandske enheders, ligesom fjendtlige aktører kan have større handlefrihed end egne styrker. Dette forhold gælder også CO, hvorfor rettidig planlægning og tidlig afklaring af rammer og bindinger, herunder Rules of Engagement (ROE) og krav til operationssikkerhed, er væsentligt i forhold til at afklare den operative handlefrihed.

Frihed til at træffe de rette beslutninger og handle uden unødvendige restriktioner er en forudsætning for at kunne justere kampindsatsen hurtigt og effektivt i mødet med modstanderen.

Beslutningskompetencen til at iværksætte CO bør delegeres til det lavest mulige niveau, som operationens vilkår tilsiger, og som kravet om kontrol og opretholdelse af operationssikkerhed muliggør. Uddelegering af råderetten til at reagere på hændelser

styrker modstandskraften, men kræver særligt strenge krav om koordination og kommunikation.

Under alle CO skal der være tilstrækkeligt tilsyn med aktivitetens gennemførelse til at kunne reagere på eventuelle afvigelser fra det planlagte, herunder mulighed for at afslutte aktiviteten, når den ikke længere skal udføres.

Førere, der anmoder om støtte fra CNO-kapaciteten, bør angive den ønskede effekt og undlade at pålægge CNO-kapaciteten unødige restriktioner for, hvordan den givne effekt ønskes opnået.

5.3.5. Målet

CO skal, som andre operationer, have klart definerede og opnåelige mål, der ligger inden for det politiske mandat, de juridiske rammer og de opstillede ROE.

5.3.6. Fleksibilitet

Planer og procedurer for CO bør være fleksible nok til at tillade justeringer som følge af uventede forløb og hændelser og give maksimal handlefrihed til føreren.

Fleksibilitet øges ved formulering af ønskede effekter frem for løsningsmodeller, ved effektiv anvendelse af kommunikationsmidler, ved tillid mellem involverede enheder samt ved styrkelse af situationsforståelse, herunder udarbejdelse og vedligeholdelse af et opdateret situationsbillede både i og uden for cyberspace.

Princippet om fleksibilitet kan være udfordret i forbindelse med CO. Cybervåben, som er udviklet til at angribe specifikke mål, kan ikke nødvendigvis justeres i tid og rum eller rettes mod nye mål.

På samme måde kan defensive foranstaltninger ikke nødvendigvis beskytte mod nye trusler, idet disse nye trusler kan anvende ukendte angrebsvektorer og teknologi, hvilket kræver fornyet analyse af truslerne og fortsat udvikling af forsvaret.

5.3.7. Initiativ

Initiativ handler om at erkende muligheder, når de opstår, og handle på dem for at opnå militære fordele. En fører bør have tilstrækkelig frihed til at kunne udvise initiativ og bør motivere underordnede til at gøre det samme.

Initiativ handler også om at reagere på uventede hændelser og melde videre, såfremt det ikke ligger inden for egen myndighed eller kompetence at reagere på den observerede hændelse. Dette har særlig vigtighed i forhold til at erkende og reagere rettidigt på fjendtlige handlinger mod egne entiteter i cyberspace.

Initiativ i cyberspace styrkes aktivt ved anvendelse af CO og proaktivt gennem cyber awareness, uddannelse og træning.

CO kan bidrage til at vinde initiativet og fastholde presset på modstanderen, fx fordi CO kan:

- Indsættes i perioder, hvor fysiske styrker er under bevægelse eller genopbygger kampkraft.
- Anvendes mod mål, der kan være uden for rækkevidde af andre våbensystemer.
- Skabe træghed og ineffektivitet i modstanderens C2 og dermed fremme eget initiativ og operationstempo i forhold til modstanderens.
- Bidrage til at ændre modstanderens situationsforståelse og dermed medvirke til at modstanderen træffer mindre effektive beslutninger.
- Sløre egne operationer og bevægelser, så modstanderen fx bruger sit initiativ på falske eller ulønsomme mål.
- Uskadeliggøre fjendtlige kampmidler, der er afhængige af entiteter i eller adgang til cyberspace.

5.3.8. Offensiv

En proaktiv tankegang bør ligge bag CO, så initiativet fastholdes. En defensiv og reaktiv tilgang til CO vil ofte være utilstrækkelig på grund af hastigheden, hvormed fjendtlige OCO kan levere effekt, samt på grund af cyberspaces unikke karakter, der gør det muligt at skjule kommende eller igangværende angreb.

En proaktiv tankegang kræver forudseenhed og rettidig omhu, så der levnes fornøden tid til planlægning og forberedelse af CO.

Et højt operationstempo i relation til CO kræver rettidig involvering af CNO-kapaciteten og effektiv anvendelse af efterretningskapaciteter med henblik på at indhente nødvendige oplysninger for gennemførelse af CO.

Operationstempoet kan øges ved at anlægge en fremadskuende og proaktiv tilgang til identifikation af mulige effekter, indhentning mod mulige mål, planlægning af CO og indhentning af politisk autorisation.

Muligheder for at anvende CO til at støtte andre aktiviteter skal identificeres så tidligt som muligt, og styrkechefen skal, eventuelt ved hjælp af CLO, så præcist som muligt kortlægge og beskrive den effekt, der ønskes leveret.

5.3.9. Overraskelse

Et overraskende angreb rammer modstanderen på et tidspunkt, et sted eller en måde, som modstanderen ikke er forberedt på.

Det er meget vanskeligt at erkende fjendtlige OCO, før de iværksættes. Og det er vanskeligt at erkende avancerede angreb, selv efter de er iværksat.

Systemer og netværk indeholder kompleks software, hvilket gør det usandsynligt, at alle sårbarheder kan erkendes og blokeres. CO rummer derfor et stort potentiale for at kompromittere en modstanders systemer og netværk, men også risiko for modstanderens kompromittering af egne systemer og netværk.

Aktiviteter i cyberspace kan gennemføres med maskinhastighed og en høj grad af anonymitet, hvilket kan give angriberen en tidsmæssig fordel, idet modstanderen skal erkende angrebet og identificere angriberen forud for iværksættelse af et eventuelt modangreb.

CO kan gøre brug af vildledning, hvilket kan bidrage til at overraske modstanderen. Vildledning kan anvendes både offensivt, fx ved at gemme malware i en tilsyneladende harmløs applikation,[25] og defensivt, fx ved anvendelse af honeynet.[26]

5.3.10. Sikring

Sikring bidrager til at skabe bevægelses- og handlefrihed i cyberspace og minimerer en modstanders mulighed for at udnytte sårbarheder.

Sikring indebærer en afvejning mellem sikkerhed og bevægelsesfrihed. I cyberspace er det i høj grad vigtigt at balancere mellem sikkerhedsforanstaltninger og bevægelsesfrihed for ikke at risikere unødig nedslidning, begrænsning og ressourceforbrug.

Passiv sikring bygger både på en forudsætning om stærk CS, grundig forberedelse af aktiviteter i cyberspace samt tilstrækkelig overvågning af den del af cyberspace, hvori CO finder sted.

Det er nødvendigt at opretholde et højt niveau af operationssikkerhed omkring aktiviteterne for både at beskytte egne enheder og systemer og tilsikre fortsat effekt af sikkerhedsforanstaltninger og cybervåben.

Procedurer for håndtering af brud på CS bør, selv for ikke-klassificerede netværk og systemer, være klassificerede, idet en modstanders viden om hændelseshåndteringen kan styrke dennes mulighed for at kompromittere systemet eller netværket.

Sikring involverer at betragte de øvrige principper fra modstanderens synsvinkel med henblik på at erkende egne sårbarheder over for fjendtlige aktiviteter. Dette omfatter bl.a. følgende overvejelser:

- Forvent, at fysiske fjendtlige angreb kan blive støttet af cyberangreb.

[25] Et eksempel er en såkaldt trojansk hest, som er software, offeret har tillid til, men som indeholder skjult skadelig kode.
[26] Et honeynet er et falsk netværk, som skal tiltrække en eventuel angriber og lede opmærksomheden væk fra det sande netværk.

- Forvent, at cyberangreb kan sløre eller støtte andre aktiviteter – også i andre operationsmiljøer end cyberspace.
- Brug vildledning til at sløre eget cyberspace og egne offensive og defensive kapaciteter i cyberspace.
- Slør forbindelser til eget cyberspace, herunder fx eksistensen af cyberpersonaer, anvendte programmer og protokoller samt entiteter i cyberspace.
- Fasthold om muligt modstanderen i et ineffektivt angreb, eventuelt ved brug af vildledning, og udnyt muligheden for at forstå dennes cybervåben, teknik og taktik.
- Uddan, og træn personel i forhold vedrørende fjendtlige aktiviteter i cyberspace samt i generel cyber awareness.
- Opbyg så godt som muligt et dækkende situationsbillede over relevante dele af cyberspace, der dækker alle operationsmiljøets elementer.
- Forvent, at det umiddelbare situationsbillede kan være et resultat af modstanderens vildledelse.
- Opbyg særlig høj sikkerhed omkring C2 samt teknikker og funktioner til at verificere C2-fortrolighed og -integritet.
- Søg aktivt i eget cyberspace efter sårbarheder og fjendtlig udnyttelse af sårbarheder, også i tid og rum, hvor der ikke umiddelbart forventes angreb.
- Håndter fjendtlige CO ved at tænke i defensive effekter i stedet for metoder.

5.3.11. Enkelhed

Cyberspace er et komplekst og uigennemsigtigt operationsmiljø, hvor sammenhænge og forbindelser kan være vanskelige at gennemskue. Det vanskeliggør kontrol over effekten af de aktiviteter, der gennemføres. Der skal derfor lægges særlig vægt på at simplificere ordrer og planer, således at de ikke leder til misforståelser og forvirring.

5.3.12. Moral

Opretholdelse af moral blandt væbnede styrker kan inkludere opretholdelse af personellets adgang til at anvende IKT og internettet. Princippet om sikring bør så vidt muligt ikke unødvendigt begrænse egne og allierede styrkers adgang til fx at kommunikere med venner og familie. Dette indebærer naturligvis også at modstanderens kommunikationslinjer hjem til familie og venner, lønudbetalingssystemer mv. kan være lønsomme mål for egne og allierede styrker.

Moral styrkes ved, at der informeres om egne styrkers succesfulde CO og modstanderens fejlslagne CO, så egne styrker kan se, at deres indsats bærer frugt, og modstanderen får indtrykket af egen sårbarhed og spildte kræfter. Dette bør selvfølgelig ske under hensyntagen til operationssikkerhed (OPSEC), strategiske og politiske overvejelser mv.

Moral sikres tillige gennem efterlevelse af gældende lovgivning for CO og anvendelse af etiske principper, hvor lovgivningen enten ikke er klar eller fastsat.

Anvendte forkortelser

AJP	Allied Joint Publication
BDA	Battle Damage Assessment
C2	Command and Control
C2IS	Command and Control Information Systems
CDE	Collateral Damage Estimate
CFCS	Center for Cybersikkerhed
CHFE	Chefen for Forsvarets Efterretningstjeneste
CIMIC	Civil-Military Cooperation
CLO	Cyber Liaison Officer
CNO	Computer Network Operations
CO	Cyberspace Operations/cyberspaceoperationer
CS	Cyber Security/cybersikkerhed
CyOC	Cyber Operations Centre
DCO	Defensive Cyberspace Operations/defensive cyberspaceoperationer
DDoS	Distributed Denial of Service
EME	Electromagnetic Environment
EMO	Electromagnetic Operation/elektromagnetisk operation
EMS	Electromagnetic Spectrum/elektromagnetisk spektrum
FC	Forsvarschefen
FKO	Forsvarskommandoen
FP	Force Protection
HUMINT	Human Intelligence
IA	Information Activities/informationsaktiviteter
IW	Information Warfare
IKT	Informations- og kommunikationsteknologi
IMINT	Image Intelligence
ISP	Internet Service Provider
JIPOE	Joint Intelligence Preparation of the Operational Environment
LI	Lessons Identified
LL	Lessons Learned
OCO	Offensive Cyberspace Operations /offensive cyberspaceoperationer
OPG	Operational Planning Group /operativ planlægningsgruppe
OPLAN	Operationsplan
OPSEC	Operational Security
ORS	Operationel risikostyring
OSINT	Open Source Intelligence
PPP	Private-Public Partnership
RE-TOA	Return Transfer of Authority
ROE	Rules of Engagement
SCEPVA	Sovereign Cyber Effect Provided Voluntarily by Allies
SIGINT	Signal Intelligence
STRATCOM	Strategic Communication/strategisk kommunikation
TOA	Transfer of Authority
VDMCO	Værnsfælles Doktrin for Militære Cyberspaceoperationer

Doktrinens definitioner

Cyberspace: **den samlede globale mængde af entiteter, som behandler, lagrer og transmitterer digitale informationer og kode, hvad enten de er forbundne eller ej**.

- Cyberspace består af tre lag: det fysiske lag, det logiske lag og cyberpersonalaget.
- Cyberspace er et militært operationsmiljø på lige fod med land, sø og luft.

Cyberspaceoperationer (CO): **militære aktiviteter i eller gennem cyberspace, der, afgrænset i tid og rum og gennem anvendelse af cyberspacekapaciteter, har til hensigt at opnå militære mål**.

- Det afgørende skæringspunkt mellem definitionerne på offensive og defensive operationer er, om der indgår magtanvendelse i eller gennem modstanderens dele af cyberspace.

Offensive cyberspaceoperationer (OCO): **CO, der har til hensigt at anvende magt i eller gennem en modstanders del af cyberspace**.

Defensive cyberspaceoperationer (DCO): **CO, der uden at anvende magt har til hensigt at bevare eller genskabe egen bevægelses- og handlefrihed i cyberspace**.

Cybervåben: **computerkode, der anvendes til at opnå den ønskede effekt på målet**.

Bemærk at:

- OCO dækker over alle CO, der involverer ændringer på funktionaliteten af modstanderens dele af cyberspace. OCO omfatter dermed også denne type operationer, når de gennemføres med et forsvarsmæssigt sigte.
- Evnen til at gennemføre OCO ligger ved CNO-kapaciteten i FE.
- Koordination, herunder synkronisering og integrering af CO samt støtte til og fra CO sker hovedsageligt gennem anvendelse af CLO.

Liste over referencer

Feltreglement I (ikke-klassificeret), dok.nr. HRN 010-001, juni 2016.
Forsvarsministeriet og Værnsfælles Forsvarskommando, *Militærmanual om Folkeret for Danske Væbnede Styrker i Internationale Militære Operationer*, 2016.
NATO, *Allied Joint Doctrine for Electronic Warfare* (NATO RESTRICTED), udgave B version 1, dok.nr. AJP-3.6, juli 2012.
NATO, *Allied Joint Doctrine for Information Operations* (NATO UNCLASSIFIED), udgave A version 1, dok.nr. AJP-3.10, december 2015.
NATO, *Allied Joint Doctrine for Joint Targeting* (ikke-klassificeret), udgave A version 1, dok.nr. AJP-3.9, april 2016.
NATO, *Allied Joint Doctrine for Operational-Level Planning* (ikke-klassificeret), dok.nr. AJP-5, juni 2013.
NATO, *Allied Joint Doctrine for the Conduct of Operations* (ikke-klassificeret), dok.nr. AJP-3(c), februar 2019.
NATO, *Allied Joint Doctrine*, udgave E version 1 (ikke-klassificeret), dok.nr. AJP-01(e), februar 2017.
NATO, *Framework Mechanism for the Integration of Sovereign Cyber Effects Provided Voluntarily by Allies into Alliance Operations and Missions* (NATO RESTRICTED), dok.nr. MCM-0112-2018, maj 2018.
National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity*, version 1.1, 2018.
Værnsfælles Forsvarskommando, *Bestemmelse for Behandling af NATO AJP Inden for Værnsfælles Forsvarskommandos Område* (ikke-klassificeret), dok.nr. VFKBST U.210-0, november 2011.
Værnsfælles Forsvarskommando, *Standardiseret Operationsprocedure for den Operative Planlægningsgruppe*, Værnsfælles Forsvarskommando, 1. august 2017.

Figuroversigt

ANNEX B RESUMÉ AF OVERVEJELSER VEDRØRENDE DEN VÆRNSFÆLLES PLANLÆGNING OG GENNEMFØRELSE AF CO

Overvejelser relateret til joint functions

Funktion	Overvejelser
Fires	• Cybervåben skaber offensive effekter. • Cybervåben er sjældent hyldevarer. Nogle skal udvikles, hvilket, afhængigt af kompleksiteten af våbnet, kan tage fra uger til år. • Cybervåbnet kan designes, så effekter skabes lang tid efter indsættelsen. • Et cybervåben bør ikke kunne inddæmmes og analyseres af modstanderen. • Indsættelsen af cybervåben skal ske i koordination med øvrige aktiviteter, herunder eventuelt allierede eller samarbejdspartneres aktiviteter. • Cybervåben kan skabe strategiske, operative og taktiske effekter. • Cybervåben kan designes, så deres effekter er reversible, hvilket kan være attraktivt fx i forhold til en efterfølgende genopbygning. • Cybervåben kan indsættes i forsvar og angreb. • Cybervåben kan indsættes støttende eller støttet. • CNO-kapaciteten kan vælge at tilbyde enheder et katalog over mulige effekter, der kan opnås gennem CO.
Manouvre	• Manøvrer kan finde sted i alle lag af cyberspace. • Manøvrer i cyberspace kan ske uafhængigt af manøvrer i fysiske rum, men kan også synkroniseres med disse. • Manøvrer i cyberspace er ikke nødvendigvis begrænset af bevægelseshastighed og geografiske afstande. • Det kan være nødvendigt at manøvrere i fysiske rum i forbindelse med CO, fx for at nå ikke-forbundne dele af cyberspace. • Ild og bevægelse kan ske på kryds og tværs mellem fysiske rum og cyberspace.
C2	• C2 er nødvendigt for at kunne gennemføre effektive CO. • C2 kan indbygges i et cybervåben. • C2 og C2IS skal beskyttes mod fjendtlige CO. • De fleste C2IS er afhængige af cyberspace – og der kan være afhængigheder og dermed potentielle sårbarheder i alle lag. • C2 skal kunne fungere uden bevægelses- og handlefrihed i cyberspace – og ultimativt uden anvendelse af cyberspace. • Digitale C2IS skal have analoge alternativer.
Intelligence	• Efterretninger er forudsætningsskabende for effektive CO.

	• Nødvendigheden af efterretninger stiger med kompleksiteten af CO. • Efterretninger, der understøtter CO, kan indhentes i såvel som uden for cyberspace. • Efterretninger fra og om cyberspace kan understøtte planlægningen af aktiviteter uden for cyberspace. • Cyberspace kan give adgang til efterretningsindhentning på mål, der ikke er inden for geografisk rækkevidde. • Viden om strukturer og sammenhænge i modstanderens cyberspace kan give indikationer på, hvorledes modstanderen er organiseret, samt viden om modstanderens planlægning og kapabilitet. • Aktiviteter i cyberspace kan understøtte JIPOE.
Information	• Cyberspace er en delmængde af informationsmiljøet. • CO og IA skal koordineres og synkroniseres. • CO kan påvirke STRATCOM. • CO kan påvirke modstanderens vilje og situationsforståelse. • Effekten af CO skal analyseres grundigt for at klarlægge uønskede sideeffekter. • Modstanderen kan anvende cyberspace til at påvirke informationsmiljøet, herunder påvirke situationsforståelsen og provokere eller intimidere egne enheder.
Sustainment	• Cybersikkerhed, cyberforsvar og effektiv IKT-drift understøtter sustainment i cyberspace. • Sustainment i andre operationsmiljøer end cyberspace er ofte afhængig af handlefrihed i cyberspace, fx i forbindelse med logistik-, personel- og sundhedssystemer.
FP	• Informationer om aktiviteter i cyberspace kan styrke egen sikkerhed. • DCO, fx i form af sårbarhedsanalyser, bidrager til FP. • Fjendtlige CO kan true personel og operationer direkte, fx ved identitetstyveri, phishing mv. • Fjendtlige CO kan true personel og operationer indirekte, fx ved at modstanderen får kendskab til personfølsomme oplysninger.
CIMIC	• En stor del af cyberspace er ejet eller drevet af civile aktører. • Samarbejde med civile aktører (fx en ISP) kan styrke mulighederne for at skabe effekter ved hjælp af CO. • CO kan sikre civile dele af cyberspace, bl.a. med henblik på at sikre civile aktørers frie kommunikation eller mindske effekterne af fjendtlige IA i cyberspace.

Overvejelser relateret til krigsførelsens grundprincipper

Princip	Overvejelser
Kræfternes samspil	• Afklar mulighed for eller nødvendighed af, at CO bliver støttet af andre typer af operationer. • Identificer muligheder for, at CO kan støtte andre typer af operationer. • Afklar mulighed for at erstatte fysiske effekter med effekter fra CO. • Informer, under hensyntagen til bl.a. operationssikkerhed, om CO-muligheder og mulige effekter. • Styrk viden om doktrin for CO. • Styrk kommunikation mellem CNO-kapaciteten og andre enheder. • Synkroniser CO med operationer og aktiviteter i andre operationsmiljøer.
Tyngde	• Koncentrer indsatsen i tid og rum omkring et enkelt mål. • Opbyg slagkraft i det enkelte angreb. • Lad andre typer af operationer støtte CO. • Udnyt sårbarheder i modstanderens systemer på den tid og det sted, hvor der kan skabes størst effekt, idet sårbarheden måske lukkes, når modstanderen erkender angrebet. • Anvend støtte fra CO som force multiplier i forbindelse med operationer i de fysiske operationsmiljøer.
Økonomi med kræfterne	• Udnyt CO-mulighed for at levere effekt uden at skulle transportere materiel og personel til et operationsområde. • Udnyt CO-mulighed for at levere effekt og angribe flere mål med samme våben samtidig – uden at være begrænset af fysiske afstande. • Udnyt CO-mulighed for at aflaste enheder, der opererer i de fysiske operationsmiljøer. • Opbyg en tilstedeværelse i modstanderens dele af cyberspace med henblik på at skabe gentagne effekter med lille ressourceforbrug. • Undgå afsløring af metoder og udnyttede sårbarheder. • Overvej, om omkostninger og tid til udvikling af et kompliceret cybervåben står mål med fordelene i forhold til anvendelse af et konventionelt våben.
Handlefrihed	• Forstå de politiske, juridiske og militær-strategiske implikationer ved anvendelse af CO. • Forstå modstanderens tilgang til ovenstående. • Deleger indsættelsen af CO og cybervåben til lavest mulige niveau. • Sikr enhedernes fokus på og indøvelse af redundans og robusthed. • Indbyg kontrol og overvågningsfunktioner i CO, således at der kan justeres eller afbrydes.

	• Planlæg på effekter i stedet for metoder.
Målet	• Fastsæt klare mål for CO.
Fleksibilitet	• Planlæg CO med fleksibilitet for øje, da operationsmiljøet er dynamisk og uigennemsigtigt. • Vedligehold et opdateret situationsbillede. • Styrk kommunikationen mellem styrkechefer, CLO og CNO-kapaciteten. • Tag hensyn til, at cybervåben ofte designes til specifikke mål og dermed ikke nødvendigvis kan justeres i tid og rum.
Initiativ	• Opbyg, og træn eget beredskab over for fjendtlige aktiviteter i cyberspace. • Styrk egen cyber awareness. • Anvend CO til at nedbryde og skabe forsinkelser i modstanderens kommando- og kontrolstruktur. • Anvend CO til at påvirke modstanderens situationsforståelse. • Anvend CO til at uskadeliggøre fjendtlige kampmidler, der er afhængige af cyberspace. • Slør egne bevægelser og aktiviteter i cyberspace, så modstanderen har svært ved at erkende dem. • Udnyt, at CO kan indsættes i perioder, hvor der ellers genopbygges kampkraft. • Udnyt, at CO kan anvendes mod mål, der er uden for rækkevidden af andre våbenarter.
Offensiv	• Medtag CO så tidligt i planlægningen som muligt, så eventuelle effekter og cybervåben kan nå at blive forberedt. • På grund af udviklingstiden for effekter og cybervåben kan udviklingen af disse med fordel ske, inden øvrige operationer og aktiviteter planlægges.
Overraskelse	• Udnyt muligheden for at kunne levere effekt med maskinhastighed. • Udnyt muligheden for at kunne indsætte offensive kapaciteter i stor geografisk afstand fra målet. • Udnyt muligheden for at sløre egne aktiviteter i modstanderens del af cyberspace. • Udnyt fordelen af at kunne vælge tid og sted for et angreb. • Udnyt alle lag af cyberspace til at skabe vildledning og forvirring forud for anvendelsen af et cybervåben.
Sikring	• Oprethold et passende højt niveau af operations- og informationssikkerhed. • Oprethold et passende niveau af fysisk sikkerhed for egne entiteter i cyberspace. • Beskyt information om procedurer ved sikkerhedsbrud, systemfejl og fjendtlige CO.

	• Overvåg relevante dele af cyberspace. • Overvej, hvordan de dele af cyberspace, som er essentielle for egne operationer, men som opereres af civile aktører, kan sikres. • Se de øvrige grundprincipper fra modstanderens synsvinkel, og erkend egne sårbarheder i cyberspace over for fjendtlige CO såvel som aktiviteter i andre operationsmiljøer. o Forvent, at fysiske fjendtlige angreb kan blive støttet af cyberangreb. o Forvent, at cyberangreb kan sløre eller støtte andre aktiviteter – også i andre operationsmiljøer end cyberspace. o Brug vildledning til at sløre eget cyberspace og egne offensive og defensive kapaciteter i cyberspace. o Slør forbindelser til eget cyberspace, herunder fx eksistensen af cyberpersonaer, anvendte programmer og protokoller samt entiteter i cyberspace. o Fasthold om muligt modstanderen i et ineffektivt angreb, eventuelt ved brug af vildledning, og udnyt muligheden for at forstå dennes cybervåben, teknik og taktik. o Uddan, og træn personel i forhold vedrørende fjendtlige aktiviteter i cyberspace samt i generel cyber awareness. o Opbyg så godt som muligt et dækkende situationsbillede over relevante dele af cyberspace, der dækker alle operationsmiljøets elementer. o Forvent, at det umiddelbare situationsbillede kan være et resultat af modstanderens vildledelse. o Opbyg særlig høj sikkerhed omkring C2 samt teknikker og funktioner til at verificere C2-fortrolighed og -integritet. o Søg aktivt i eget cyberspace efter sårbarheder og fjendtlig udnyttelse af sårbarheder, også i tid og rum, hvor der ikke umiddelbart forventes et angreb. o Håndter fjendtlige CO ved at tænke i defensive effekter i stedet for metoder.
Enkelhed	• Tilstræb enkelhed i planlægningen, da små variationer i udførelsen, på grund af cyberspaces komplekse og uigennemsigtige karakter, kan lede til store forskelle i effekten af aktiviteterne.
Moral	• Tillad mest mulig tilgang og anvendelse af cyberspace for personel under hensyntagen til sikkerhed. • Udnyt muligheder for at demoralisere fjendtligt personel ved at påvirke deres adgang til cyberspace og fx funktionaliteten af modstanderens administrative systemer. • Informer, under hensyntagen til øvrige principper, om egne succeser i cyberspace. • Efterlev international lov og etik under gennemførelse af CO.

ANNEX C RESUMÉ AF STYRKECHEFENS OVERVEJELSER I FORBINDELSE MED INTEGRERING OG SYNKRONISERING AF EGNE OPERATIONER MED CO

Det taktiske niveaus rolle i CO

- Det taktiske niveau skal forudse at skulle integrere og synkronisere med CO.
- Det taktiske niveau kan støtte eller blive støttet af CO.
- Det taktiske niveau kommunikerer med CNO-kapaciteten hovedsageligt gennem CLO.
- Det taktiske niveau skal identificere kontaktpunkter til og afhængigheder af cyberspace for at klarlægge eventuelle sårbarheder.
- Det taktiske niveau skal gennemføre en risikovurdering i forhold til ovenstående.
- Det taktiske niveau skal udvikle egne planer og procedurer, der sikrer evnen til at operere under trusler og fjendtlige aktiviteter fra cyberspace. Dette indebærer at sikre:
  - Opbygning af redundans, eventuelt ved hjælp af "PACE".
  - Opbygning af robusthed, eventuelt ved hjælp af de fem kernefunktioner: identify, protect, detect, respond, recover.

Krigsførelsens grundprincipper i forbindelse med integrering og synkronisering med CO

Princip	**Overvejelser**
Kræfternes samspil	• Afklar mulighed for at støtte CO. • Afklar mulighed for at få støtte fra CO. • Afklar mulighed for at erstatte fysiske effekter med effekter fra CO. • Styrk egen viden om CO-muligheder og -effekter. • Styrk egen viden om doktrin for CO. • Sikr god kontakt til CNO-kapaciteten gennem CLO.
Tyngde	• Anvend støtte fra CO som force multiplier i forbindelse med operationer i de fysiske operationsmiljøer.
Økonomi med kræfterne	• Udnyt CO-mulighed for at levere effekt uden at skulle transportere materiel og personel til et operationsområde. • Udnyt CO-mulighed for at aflaste enheder, der opererer i de fysiske operationsmiljøer. • Forvent, at udvikling og anvendelse af et kompliceret cybervåben kan tage lang tid i forhold til at få leveret en effekt fra et konventionelt våben.
Handlefrihed	• Planlæg på effekter i stedet for metoder, således at CNO-kapaciteten har handlefrihed i forhold til, hvordan effekterne skabes.
Målet	• Ved rekvirering af CO-effekter skal det være tydeligt, hvad

	målet med effekten er.
Fleksibilitet	• Vedligehold et opdateret situationsbillede, herunder aktører og trusler i cyberspace. • Styrk kommunikationen mellem styrkechefer, CLO og CNO-kapaciteten. • Tag hensyn til, at cybervåben ofte designes til specifikke mål og dermed ikke nødvendigvis kan justeres i tid og rum.
Initiativ	• Opbyg, og træn eget beredskab over for fjendtlige aktiviteter i cyberspace. • Styrk egen cyber awareness. • Undersøg muligheden for at få støtte fra CO til at nedbryde og skabe forsinkelser i modstanderens kommando- og kontrolstruktur. • Undersøg muligheden for at få støtte fra CO til at påvirke modstanderens situationsforståelse. • Undersøg muligheden for at rekvirere CO til at uskadeliggøre fjendtlige kampmidler, der er afhængige af cyberspace. • Undersøg muligheden for at få støtte fra CO til at fastholde presset på modstanderen i perioder, hvor der genopbygges kampkraft. • Undersøg muligheden for at få støtte fra CO til at påvirke mål, der er uden for rækkevidde af egne våben. • Begræns modstanderens mulighed for at tilegne sig viden om anvendelse, kontaktpunkter og afhængigheder af cyberspace.
Offensiv	• Identificer på så tidligt et tidspunkt i planlægningen som muligt muligheden for at integrere egne operationer med CO, herunder eventuelt specifikke effekter fra CO, der kan støtte egne aktiviteter.
Overraskelse	• Undersøg muligheden for at få støtte fra CO til at skjule eller sløre egne aktiviteter i cyberspace såvel som i fysiske rum.
Sikring	• Oprethold et passende højt niveau af operations- og informationssikkerhed. • Oprethold et passende niveau af fysisk sikkerhed omkring egne entiteter i cyberspace. • Beskyt information om procedurer ved sikkerhedsbrud, systemfejl og fjendtlige CO. • Overvåg relevante dele af cyberspace. • Overvej, hvordan de dele af cyberspace, som er essentielle for egne operationer, men som opereres af civile aktører, kan sikres. • Se de øvrige grundprincipper fra modstanderens synsvinkel, og erkend egne sårbarheder i cyberspace over for fjendtlige

	CO såvel som aktiviteter i andre operationsmiljøer. ○ Forvent, at fysiske fjendtlige angreb kan blive støttet af cyberangreb, og identificer afhængigheder og kontaktpunkter til cyberspace. ○ Forvent, at cyberangreb kan sløre eller støtte modstanderens fysiske aktiviteter og operationer. ○ Slør kontaktpunkter og afhængigheder af cyberspace, herunder fx eksistensen af cyberpersonaer, anvendte programmer og protokoller samt entiteter i cyberspace. ○ Ved indikation på fjendtlige OCO skal der omgående koordineres med CNO-kapaciteten i forhold til reaktion. ○ Uddan, og træn personel i forhold vedrørende fjendtlige aktiviteter i cyberspace samt i generel cyber awareness. ○ Bidrag i muligt omfang til situationsbilledet over cyberspace ved brug af CLO. ○ Forvent, at det umiddelbare situationsbillede over cyberspace kan være et resultat af modstanderens vildledelse. ○ Opbyg særlig høj sikkerhed omkring C2 samt teknikker og funktioner til at verificere C2-fortrolighed og -integritet. ○ Søg aktivt i eget cyberspace efter sårbarheder og fjendtlig udnyttelse af sårbarheder, også i tid og rum, hvor der ikke umiddelbart forventes et angreb. ○ Håndter fjendtlige CO ved at tænke i defensive effekter i stedet for metoder.
Enkelhed	• Tilstræb enkelhed i planlægningen, da små variationer i udførelsen, på grund af cyberspaces komplekse og uigennemsigtige karakter, kan lede til store forskelle i effekten af aktiviteterne.
Moral	• Tillad mest mulig tilgang og anvendelse af cyberspace for personel under hensyntagen til sikkerhed. • Undersøg muligheden for at demoralisere fjendtligt personel ved at påvirke deres adgang til cyberspace og fx funktionaliteten af modstanderens administrative systemer. • Informer, under hensyntagen til øvrige principper, om egne succeser i cyberspace. • Anvend cyberspace til at dele information om succeser i øvrige operationsmiljøer.

ANNEX D FASEOPDELING AF OCO

OCO kan opdeles i fire overordnede faser:
4. Forberedelse.
5. Adgang.
6. Tilstedeværelse.
7. Effekt.

1. Forberedelse
Forberedelse involverer etablering af tilstrækkelig viden om målet til at kunne designe og udvikle et effektivt cybervåben samt identificere de sårbarheder, som skal give adgang til målet.

Viden om målet kan opnås gennem efterretningsindhentning, overvågning og opklaring og kan inkludere informationer fra åbne kilder såvel som lukkede. Forberedelsen bør, hvis det er muligt, indeholde taktisk og teknisk indøvelse, fx i form af en test på en kopi eller en simulation af det reelle mål.

2. Adgang
I nogle tilfælde vil man kunne anvende et bredt tilgængeligt eller tidligere udviklet cybervåben, der udnytter erkendte sårbarheder og giver adgang til målet. Ofte vil det dog være nødvendigt at tilpasse disse cybervåben eller udvikle helt nye for at kunne få adgang til det specifikke mål.

Adgang til mål og udnyttelse af sårbarheder kan kræve manøvrer i cyberspace såvel som i fysiske rum.

3. Tilstedeværelse
Når en sårbarhed er udnyttet til at få adgang til et mål i cyberspace, skal det tilsikres, at målet er tilgængeligt, som minimum indtil planlagte effekter er leveret.

I nogle tilfælde kan det være formålstjenligt at fastholde tilstedeværelsen, efter effekterne er leveret, fx med henblik på at holde målet åbent for fremtidige effekter eller for at kunne gennemføre BDA.

Opbygning af tilstedeværelse i et computersystem kan indebære at eskalere sine privilegier på systemet yderligere, fx ved at overtage andre legitime brugeres adgange til systemet. Eskalation og udvidelse af tilstedeværelsen i et mål skal kunne ske uden unødig risiko for at blive erkendt.

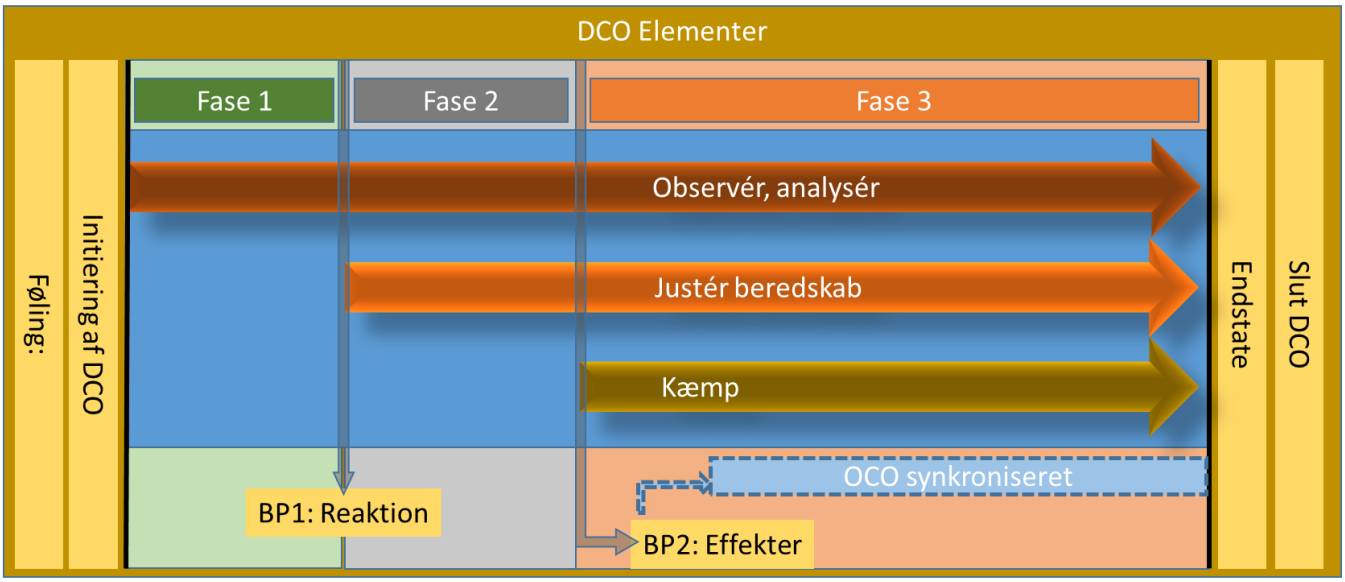
4. Effekt
Opnåelse af en specifik effekt kan kræve fortsat kommunikation med et afleveret cybervåben og dermed, at der etableres et virtuelt brohoved på det angrebne system og en sikker kommunikationskanal. Skabelsen af effekter kan styres i tid, fx ved indlæggelse af en tidsforsinkelse på et cybervåbens eksekvering af bestemte kommandoer eller ved at gennemføre den offensive operation i faser.

ANNEX E FASEOPDELING AF DCO

DCO iværksættes for at imødegå fjendtlige aktiviteter i cyberspace med henblik på at bevare eller genskabe egen bevægelses- og handlefrihed i cyberspace.

DCO kan overordnet deles op i tre faser med mellemliggende beslutningspunkter. Varigheden af faserne kan være sekunder til dage, afhængigt af karakteren af de fjendtlige aktiviteter. Det samlede forløb for DCO ser således ud:

1. Føling.
2. Initiering af DCO.
3. Fase 1: Observer og analyser.
4. Beslutningspunkt 1: Reaktion.
5. Fase 2: Observer, analyser, juster beredskab.
6. Beslutningspunkt 2: Effekter.
7. Fase 3: Observer, analyser, juster beredskab, kæmp.
8. Desired endstate.
9. Slut DCO.



1. Føling

En føling i cyberspace kan være en observation af fjendtlig (eller mulig fjendtlig) aktivitet i eget cyberspace (fx OCO) eller forsøg og forberedelser herpå. Følingen kan fx bestå af en indikation på fremmed tilstedeværelse i eget cyberspace, eller den kan bestå af erkendte fjendtlige effekter. I modsætning til de fleste kinetiske effekter kan visse effekter i cyberspace have eksisteret, længe inden de bliver opdaget.

2. Initiering af DCO
DCO initieres på baggrund af en føling. Initieringen består indledningsvist i at fastlægge ansvaret for den pågældende DCO. Såfremt der ikke er afvigelser i forhold til Standard Operating Procedures (SOP), består initieringen alene i en iværksættelsesordre.

3. Fase 1: Observer og analyser
Denne fase indeholder en fokusering af efterretningsindhentning, overvågning og opklaring. Der er ingen eller få aktiviteter i denne fase, der kan påvirke modstanderen og dennes aktiviteter. Fasen har til formål at:

- Verificere, at der er tale om fjendtlige aktiviteter og ikke andre typer af påvirkninger, angreb, fejl eller nedbrud.
- Mindske modstanderens mulighed for at gennemføre efterretningsindhentning, overvågning og opklaring.
- Tilvejebringe så mange informationer som muligt om den fjendtlige aktivitet, således at der skabes grundlag for beslutningspunkt 1, herunder:
  - Registrerede aktiviteter og effekter.
  - Den tidsmæssige udstrækning af aktiviteter og effekter.
  - Anvendt metode og teknik.
  - Aktivitetens angrebsvektor og eventuelt oprindelse.
  - Aktivitetens kompleksitet.
  - Udnyttede sårbarheder.
- Identificere eventuelt andre entiteter med samme sårbarheder, som derfor kan være under angreb eller i risiko for at komme under angreb.

4. Beslutningspunkt 1: Reaktion
Dette beslutningspunkt markerer overgangen fra fase 1 til fase 2 og indeholder en fremlæggelse af information fra fase 1 samt en beslutning om de aktiviteter, der skal indgå i fase 2. Den første og vigtigste beslutning er, i hvor høj grad man ændrer eller stopper anvendelsen af de entiteter, der er påvirket af den fjendtlige aktivitet, idet der i nogle tilfælde kan være fordele i at skjule for modstanderen, at angrebet er erkendt.

5. Fase 2: Observer, analyser, juster beredskab
Denne fase skal begrænse effekten af de fjendtlige aktiviteter. Den fokuserede efterretningsindhentning, overvågning og opklaring fortsættes, mens der nu gennemføres aktiviteter, der kan påvirke modstanderen og dennes aktiviteter. De tiltag, der iværksættes, har til formål i videst muligt omfang og under hensyntagen til beslutningspunkt 1 at begrænse risikoen for egne styrker ved at:

- Begrænse tilliden til påvirkede entiteter.
- Begrænse anvendelsen af påvirkede systemer.
- Samt begrænse modstanderens bevægelsesfrihed.

Begrænsningerne opnås ved en kombination af informering, systemnedlukning og iværksættelse af forberedte procedurer, fx iværksættelse af INCON-planer og overgang til redundante, alternative eller nødsystemer og procedurer.

6. Beslutningspunkt 2: Effekter

Dette beslutningspunkt markerer overgangen fra fase 2 til fase 3. På baggrund af observationer og effekten af beredskabsjusteringer udvælges og prioriteres de defensive effekter, der ønskes opnået. Desuden identificeres de ressourcer, herunder enheder og personel, der skal skabe effekten.

Succeskriteriet for DCO identificeres og opstilles som en desired endstate. Hvor effekterne er en beskrivelse af den påvirkning, man udsætter modstanderen for, er endstate formuleret som den ønskede situation, effekterne resulterer i.

Alt efter kompleksiteten af operationen kan dette beslutningspunkt indeholde planlægning for indsættelse og synkronisering af flere effekter, eventuelt i flere lines of effort.

I tilfælde af at en fjendtlig aktivitet besvares med OCO, sker dette ved hjælp af faseopdelingen for OCO, som synkroniseres og koordineres med de fortsatte aktiviteter i DCO fase 3.

7. Fase 3: Observer, analyser, juster beredskab, kæmp

Denne fase indeholder leveringen af de defensive effekter og afsluttes, når desired endstate er opnået. Fase 3 kan gennemføres synkroniseret med egne OCO.

Efterretningsindhentning, overvågning og opklaring fastholdes, mens selve kampen gennemføres som en kombination af levering af defensive effekter og fortsat beredskabsjustering. Kampen skal dermed ses som en kombination af ild og bevægelse, hvor ild er et udtryk for indsættelsen af defensive effekter, mens bevægelse er et udtryk for fortsatte beredskabsjusteringer. Disse justeringer kan forstås som defensive manøvrer og har under kampen til formål at sløre, skabe dækning og lægge afstand.

Sløre: Skjule egne bevægelser, handlinger og entiteter i alle tre lag af cyberspace, fx gennem INCON, anvendelse af proxyservere, ændring af netværksopsætninger mv.

Skabe dækning: Beskytte egne entiteter mod effekten af fjendtlige OCO, fx gennem patching af systemer, opsætning af firewalls mv.

Lægge afstand: Tilsikre, at sårbare entiteter i cyberspace ikke længere er inden for modstanderens rækkevidde, fx gennem afkobling af systemer og flytning af sårbare data og processer til ikke-angrebne systemer mv.

Bemærk, at ovenstående defensive manøvrer også kan bidrage til at skabe defensive effekter.

8. Desired endstate
Opnåelse af succeskriteriet for DCO, som blev defineret som en del af beslutnings-punkt 2, markerer afslutningen på DCO.

9. Slut DCO
Når desired endstate er opnået, afsluttes de pågældende DCO. Der gennemføres en debriefing, der har til hensigt at afklare konsekvenserne af den fjendtlige aktivitet samt at identificere Lessons Identified/Lesson Learned (LI/LL).

LI/LL overleveres efterfølgende til relevante enheder og myndigheder.

ANNEX F RELATIONER OG AFVIGELSER I FORHOLD TIL NATO-DOKTRIN FOR CO

Dette annex vil tilgå, efter NATO Allied Joint Publication 3.20 Doctrine for Cyberspace Operations er udgivet.