FORSVARSDEPARTEMENTET

Forsvarsdepartementets retningslinjer for informasjonssikkerhet og cyberoperasjoner i forsvarssektoren «FDs cyberretningslinjer»

FDs cyberretningslinjer fastsettes til bruk i Forsvarsdepartementet og underlagte etater.

Oslo, 1. mars 2014

Erik Lund-Isaksen
Departementsråd
Forsvarsdepartementet

Forsvarsdepartementets retningslinjer for informasjonssikkerhet og cyberoperasjoner i forsvarssektoren

Metadata

KORTTITTEL:	FDs cyberretningslinjer
SIKKERHETSGRADERING:	Ugradert
IKRAFTTREDELSE:	1. mars 2014
HJEMMEL:	Organisasjons- og instruksjonsmyndigheten
ANSVARLIG FAGMYNDIGHET:	Forsvarsdepartementet
GJELDER FOR:	Forsvarsdepartementet og underlagte etater
FORRIGE VERSJON:	

Innhold

1 Innledning 4

1.1 VIRKEOMRÅDE 4
1.2 FORMÅL 4
1.3 FORHOLDET TIL ANDRE RELEVANTE REGELVERK 4
1.4 SENTRALE BEGREPER 5
1.5 RESSURSER, ETATSSTYRING OG RAPPORTERING 6

2 Mål og ambisjonsnivå for forsvarssektorens arbeid i cyberdomenet 7

2.1 INFORMASJONSSIKKERHET I CYBERDOMENET 7
2.2 CYBEROPERASJONER 7

3 Fellesbestemmelser 9

3.1 SÆRLIGE KRAV TIL FORSVARSSEKTOREN I CYBERDOMENET 9
3.2 ETABLERING OG DRIFT AV EGNE SYSTEMER 9
3.3 INFORMASJONSSIKKERHET I CYBERDOMENET 9
3.4 VARSLING OG RAPPORTERING 10
3.5 HÅNDTERING AV CYBERHENDELSER 11
3.5.1 Strategisk kommunikasjon 11
3.6 SIVILT-MILITÆRT SAMARBEID 12
3.7 CYBEROPERASJONER 12
3.7.1 Generelt 12
3.7.2 Defensive cyberoperasjoner (CND) 12
3.7.3 Offensive cyberoperasjoner (CNE, CNA) 13
3.8 JURIDISKE RAMMER 13
3.8.1 Nasjonalt regelverk 13
3.8.2 Folkerettens regler for cyberangrep 13
3.8.2.1 Folkeretten og ansvar 13
3.8.2.2 Bruk av makt 14
3.8.2.3 Regler for digital krigføring 14
3.9 BEREDSKAP 14
3.10 KOMPETANSE, ØVING OG TRENING 14
3.11 INTERNASJONALT SAMARBEID 15
3.11.1 NATO og Norge 15
3.11.2 Forholdet til andre land 16
3.11.3 Særlig om nordisk samarbeid 16

4 Forsvarsdepartementet og underlagte etaters ansvar, oppgaver og myndighet 17

4.1 FORSVARSDEPARTEMENTET 17
4.2 FORSVARET 17
4.2.1 Forsvarssjefen 17
4.2.2 Særskilt om Etterretningstjenesten 18

4.3 NASJONAL SIKKERHETSMYNDIGHET 18
4.4 FORSVARETS FORSKNINGSINSTITUTT 19
4.5 FORSVARSBYGG 19
5 Sluttbestemmelser 20
Vedlegg 1: Definisjoner med relevans for informasjonssikkerhet og cyberoperasjoner 21
Vedlegg 2: Hjemmelsgrunnlag for sikring av systemer og hendelseshåndtering 24

1 Innledning

1.1 Virkeområde

Disse retningslinjene gjelder for informasjonssikkerhet i cyberdomenet[1] og cyberoperasjoner utført av forsvarssektoren i fredstid og under væpnet konflikt, i og utenfor Norge.

1.2 Formål

Formålet med cyberretningslinjene er å bidra til å sikre nødvendig handlefrihet i cyberdomenet, og å unngå eller redusere konsekvensene av alvorlige cyberangrep rettet mot egne systemer. Retningslinjene skal videre legge til rette for en bedre koordinering i sektoren. På et overordnet nivå skal retningslinjene bidra til dette gjennom å:

- definere forsvarssektorens arbeid med informasjonssikkerhet i cyberdomenet og cyberoperasjoner, samt fastsette fellesbestemmelser for ivaretakelse av dette arbeidet
- fastsette overordnede mål og ambisjonsnivå
- fastsette ansvar, oppgaver og myndighet.

1.3 Forholdet til andre relevante regelverk

Forsvarsdepartementets (FD) cyberretningslinjer gjelder med mindre annet følger av, eller besluttes ved, bestemmelser gitt i eller i medhold av lov og instruks.[2]

FD og underlagte etater kan utgi utfyllende regelverk til disse retningslinjene. FDs cyberretningslinjer er overordnet øvrige utfyllende regelverk på dette fagområdet, og vil ved motstrid gå foran.

Retningslinjene er i nødvendig grad tilpasset relevante NATO-regelverk.

---

[1] Fysiske og logiske sammenkoblinger av informasjonssystemer, herunder nettverksenheter, kommunikasjonsinfrastruktur, lagringsmedier og data.
Synonym: Det digitale rom

[2] Eksempelvis gjennom Beredskapssystem for forsvarssektoren (BFF) og Sivilt beredskapssystem (SBS).

1.4 Sentrale begreper

Forsvarssektoren
Samlebetegnelse på FD, Forsvaret, Forsvarets forskningsinstitutt (FFI), Forsvarsbygg (FB) og Nasjonal sikkerhetsmyndighet (NSM).

Informasjonssikkerhet[3]
Sikkerhetstiltak for i nødvendig grad å oppnå konfidensialitet, integritet, tilgjengelighet og autentisitet ved behandling av informasjon i alle situasjoner, uavhengig av verktøy og metoder. Cyberretningslinjene er innrettet mot håndtering av digital informasjon og informasjonssystemer.

Informasjonssikkerhet omfatter både etablering av barrierer, deteksjon av sikkerhetstruende hendelser og reaksjon på slike med tanke på gjenoppretting av sikker tilstand for informasjon og systemer. Defensive datanettverksoperasjoner omfattes av begrepet informasjonssikkerhet, men utføres i en operativ kontekst.

Cyber
Prefiks som viser at det ordet prefikset benyttes sammen med henviser til noe i cyberdomenet. F.eks. *cyberangrep* eller *cybertrussel.*

Cyberangrep
Handlinger i eller gjennom cyberdomenet med hensikt å skade eller påvirke personell, materiell eller konfidensialiteten, integriteten, tilgjengeligheten eller autentisiteten til et informasjonssystem.

Cyberdomenet
Fysiske og logiske sammenkoblinger av informasjonssystemer, herunder nettverksenheter, kommunikasjonsinfrastruktur, lagringsmedier og data.
Synonym: Det digitale rom

Cyberhendelse
Brukes i disse retningslinjene både om situasjoner der IKT-systemer blir utsatt for cyberangrep, og ved utilsiktet svikt forårsaket av ulykker eller uhell. Med alvorlige cyberhendelser menes cyberhendelser som rammer samfunnskritisk infrastruktur, samfunnskritisk informasjon eller samfunnskritiske funksjoner på en slik måte at det får betydning for samfunnets og befolkningens trygghet.

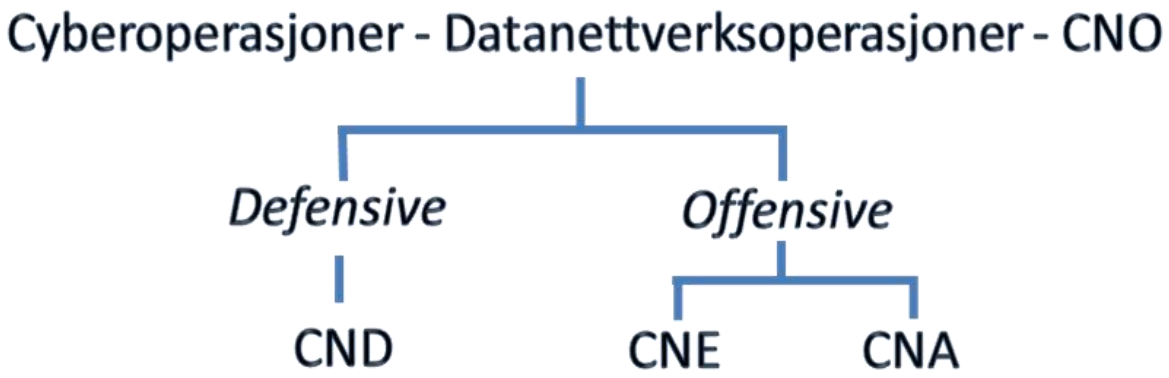
IKT-aktiviteter
Aktiviteter for å kunne utvikle og fasilitere et stabilt og sikkert cyberdomene. Dette inkluderer å utvikle, etablere, konfigurere, sikre, vedlikeholde, drifte og risikohåndtere cyberdomenet. IKT-aktiviteter omfatter daglig drift og støtte til operasjoner.
Synonym: CIS-aktiviteter

Cyberoperasjoner/Datanettverksoperasjoner
Datanettverksoperasjoner er et samlebegrep som tilsvarer det engelske begrepet Computer Network Operations (CNO). CNO er tiltak som gjennomføres i datanettverkene for å påvirke motstanders datanett og beskytte eget nett. Dette omfatter Computer Network Defence

[3] Se vedlegg for utfyllende beskrivelse

(CND), Computer Network Exploitation (CNE) og Computer Network Attack (CNA). CND er å anse som en defensiv aktivitet som skal sikre handlefrihet i egen informasjons-infrastruktur, til tross for offensive aktiviteter fra en motstander. CNE og CNA er å anse som offensive aktiviteter og gjennomføres normalt i en motstanders nettverk. CNE skal bidra til å søke etter, fange opp, identifisere og lokalisere aktiviteter og informasjon i cyberdomenet i den hensikt å oppnå situasjonsforståelse og for å kunne gjenkjenne trusler. CNA skal bidra til å redusere eller hindre en motstanders evne til å utnytte cyberdomenet til egne operasjoner. Informasjon fremskaffet gjennom CNE vil være av sentral betydning for både CNA- og CND-aktiviteter.

Cyberoperasjoner brukes i forsvarssektoren som et synonym til datanettverksoperasjoner. Cyberoperasjoner omfatter ikke IKT-aktiviteter. Cyberoperasjoner omfatter ikke tiltak utenfor datanettverkene for å påvirke disse, eksempelvis i form av kinetiske maktmidler og elektronisk krigføring. Cyberoperasjoner og operasjoner i det digitale rom kan benyttes som synonymer. I dette dokumentet benyttes begrepet cyberoperasjoner.



Figur 1. Cyberoperasjoner

1.5 Ressurser, etatsstyring og rapportering

Fastsettelse av FDs cyberretningslinjer utløser ikke særskilte ressurser.
Behov for ressurser, ressurstildeling og rutinemessig rapportering følger de ordinære styringslinjene. De til enhver tid gjeldende generelle prinsipper og prosesser for etatsstyring og utvikling skal også gjelde for fagområdet som er regulert i disse retningslinjene.

2 Mål og ambisjonsnivå for forsvarssektorens arbeid i cyberdomenet

Hovedmålsettingen for forsvarssektorens arbeid i cyberdomenet er at:

Forsvarssektoren skal ha nødvendig handlefrihet i cyberdomenet for å understøtte oppgaveløsing hjemme og ute.

For å realisere dette skal forsvarssektoren:

- sørge for effektiv ressursbruk, herunder hensiktsmessig fordeling av oppgaver, ansvar og myndighet innen arbeidet med informasjonssikkerhet og cyberoperasjoner
- ha sikre og forsvarbare, robuste og kostnadseffektive systemer og kommunikasjonsinfrastruktur
- bidra til at NATO har sikre systemer og er i stand til å bidra til medlemslandenes sikkerhet og forsvar i cyberdomenet
- bidra til å sikre et godt bi- og multilateralt samarbeid om informasjonssikkerhet i cyberdomenet og cyberoperasjoner der det er relevant
- være en vesentlig bidragsyter til teknologisk utvikling innen informasjonssikkerhet,
- sikre at beslutningstakere i forsvarssektoren og statsforvaltningen for øvrig har en god og oppdatert situasjonsforståelse innen cyberdomenet

2.1 Informasjonssikkerhet i cyberdomenet

Forsvarssektoren skal ha tilstrekkelig informasjonssikkerhet i cyberdomenet, og ivareta dette som en integrert del av sitt virke. Sektoren skal være forberedt på å håndtere alle former for hendelser som kan ramme egne IKT-systemer.

Forsvarssektoren skal til enhver tid forebygge, avdekke, vurdere og forsvare seg mot cyberangrep, samt ha evne til å gjenopprette normal funksjonalitet i tilfelle cyberangrep eller andre cyberhendelser.

NSM skal i tillegg til å sørge for egen informasjonssikkerhet også ivareta sin nasjonale sektorovergripende rolle innen informasjonssikkerhet

2.2 Cyberoperasjoner

Forsvarssektoren skal primært utøve beskyttelse av egen informasjonsinfrastruktur i den hensikt å opprettholde og bevare egen operativ evne.

Forsvarets evne til cyberoperasjoner skal være tilstrekkelig til å møte utfordringene i cyberdomenet og dette skal sikres gjennom regelmessig å trene prosedyrer og tiltak. Cyberoperasjoner skal rutinemessig innarbeides i øvelser på alle nivåer.

Forsvarets operative elementer skal gjennom sikre, robuste og redundante nettverk kunne samvirke effektivt nasjonalt og flernasjonalt for å kunne løse de militære oppdrag som er gitt.

Det skal foretas vurderinger av risikoen for cyberangrep, og tas nødvendig hensyn til denne risikoen i planlegging og gjennomføring av operasjonene.

Forsvaret skal ha interoperabilitet med NATO innenfor IKT-aktiviteter og defensive cyberoperasjoner der dette er hensiktsmessig.

3 Fellesbestemmelser

3.1 Særlige krav til forsvarssektoren i cyberdomenet

Selv om deler av forsvarssektorens virksomhet i cyberdomenet har likhetstrekk med tilsvarende virksomhet i det sivile samfunn, har forsvarssektoren et særskilt ansvar relatert til militære operasjoner, etterretning og håndtering av situasjoner som truer statssikkerheten. Dette stiller særlige krav til forsvarssektoren.

Sektoren må være forberedt på å håndtere situasjoner som ut fra sin natur ikke kan løses innenfor rammene av normal virksomhet. Dette kan være operasjoner med militært formål eller støtte til sivil krisehåndtering, basert på etablerte roller og ansvarsforhold. Det vil kunne være uklare skiller mellom normal virksomhet og kriseaktivitet, ettersom en situasjon vil kunne eskalere og kreve ulik håndtering i ulike deler av krisespennet.

3.2 Etablering og drift av egne systemer

Forsvarssektoren skal etablere kostnadseffektive systemer med en robusthet og redundans som er i henhold til gjeldende krav. Virksomhetene skal ha oversikt over avhengigheter mellom egne systemer og eksterne systemer. Der slik avhengighet berører kritiske funksjoner eller systemer, for Norge, NATO eller allierte, skal virksomheten iverksette tiltak som ivaretar leveransebehovet.

Forsvarssektoren skal stille krav til eksterne leverandører av IKT-systemer og -tjenester som sektoren er avhengig av, for å sikre at disse er robuste og pålitelige. Det skal også etableres en beredskap for å hindre at svikt i eksterne systemer får alvorlige, negative konsekvenser for forsvarssektoren. Etatene skal gjennom egne ressurser, og/eller gjennom avtaler med eksterne leverandører, ha evne til å gjenopprette egne IKT-systemer. Det skal foreligge lokale prosedyrer for hvordan etatene skal anmode om støtte til gjenoppretting av egne systemer.

Forsvarssektoren skal være i stand til å opprettholde drift av IKT-systemer som er kritiske for kjernevirksomheten, herunder ved kriser og væpnet konflikt. Enhetene som er ansvarlige for å drifte systemene skal, basert på oppdaterte risiko- og sårbarhetsanalyser, ha tilstrekkelig beredskap, bemanning og øvrig kapasitet til å kunne drifte IKT-systemene i henhold til gjeldende leveranseavtaler.

Når IKT-aktiviteter gjennomføres til støtte for operasjoner, skal IKT-aktivitetene underlegges de samme rammer og prioriteringer som operasjonen de støtter.

3.3 Informasjonssikkerhet i cyberdomenet

Sikring av IKT-systemer er kritisk for forsvarssektorens evne til å operere i cyberdomenet. Virksomhetene i sektoren er ansvarlige for å sikre sine egne IKT-systemer. Virksomhetenes internkontroll med sikkerhetsarbeidet skal være en integrert del av øvrig internkontrollarbeid. Virksomhetens leder har ansvaret for sikkerheten i systemene gjennom sin rolle som leder for sikkerhetsorganisasjonen. All delegering av myndighet skal gjøres skriftlig. Sikkerhetsorganisasjonen skal sammen med lokal informasjonsforvalter påse at virksomheten har nødvendig sikkerhetskompetanse og en tilstrekkelig god sikkerhetskultur.

Forsvarssektoren forvalter en rekke IKT-systemer med ulike beskyttelsesbehov. Virksomhetene skal, basert på regelverk og risiko- og sårbarhetsanalyser, etablere oversikt over hvilke beskyttelsesbehov de ulike systemene har, og beskytte systemene i henhold til

dette. Systemene skal beskyttes med tanke på sikring av informasjonens konfidensialitet, integritet, tilgjengelighet og autentisitet. Beskyttelse av egne systemer skal inngå som en integrert del av daglig systemdrift, og utføres både i normal virksomhet og i forbindelse med krise eller væpnet konflikt.

3.4 Varsling og rapportering

Informasjonsdeling, samordning og samhandling er avgjørende for å kunne møte cybertruslene på en effektiv måte. Forsvarssektoren skal bidra aktivt til en best mulig felles forståelse for de trusler og sårbarheter sektoren og nasjonen står overfor.

For å etablere et mest mulig komplett bilde av sikkerhetstilstanden i sektoren skal alle sikkerhetstruende hendelser rutinemessig rapporteres til intern sikkerhetsorganisasjon. Alvorlige cyberhendelser skal uten unødig opphold rapporteres til NSM, som på nasjonalt nivå koordinerer håndtering av alvorlige dataangrep rettet mot samfunnskritisk infrastruktur og informasjon.

Forsvarssektorens etater skal varsle alvorlige cyberhendelser parallelt til FD og NSM. NSM har et særskilt ansvar for å varsle Justis- og beredskapsdepartementet (JD), andre sektormyndigheter og relevante virksomheter. NSM skal ha prosedyrer for viderevarsling av relevante cyberhendelser fra NATO og andre internasjonale organisasjoner og stater til nasjonale aktører, og for varsling fra nasjonale aktører til NATO og andre internasjonale organisasjoner og stater, innen NSMs ansvarsområde. Forsvaret skal også ha prosedyrer for samtidig varsling til og fra NATO for cyberhendelser som berører militære operasjoner. NSMs og Forsvarets varsling til og fra NATO, og andre internasjonale aktører, skal for øvrig utføres iht. gjeldende avtaler og bestemmelser for dette.

Etterretningstjenesten (E-tjenesten) forestår tidlig varsling av mulige ytre cybertrusler fra fremmede stater, organisasjoner eller individer.

Cyberkoordineringsgruppen (CKG) som ledes av NSM, og som for øvrig består av E-tjenesten og Politiets sikkerhetstjeneste (PST), skal fremskaffe tidsriktig informasjon og beslutningsgrunnlag til den operative og strategiske ledelsen om trusler og sårbarheter i cyberdomenet. For det formål har CKG også informasjonsutveksling med sektororganer, herunder Forsvaret og Politiet. Ved alvorlige cyberhendelser vil etterretnings- og sikkerhetstjenestene (EOS-tjenestene)[4], på bakgrunn av sine respektive nasjonale sektorovergripende ansvarsområder, koordinere varsling, rådgivning og informasjonsutveksling innenfor sine fullmakter. I den enkelte sak, skal en av tjenestene være koordineringsansvarlig. Denne skal lede arbeidet og ta initiativ til å koordinere og avstemme tiltak mellom EOS-tjenestene, herunder i forhold til informasjonsdeling og samhandling med andre aktører i den enkelte sak. Det er utarbeidet en egen instruks for CKG.

[4] EOS-tjenestene er en samlebetegnelse på Etterretningstjenesten, Politiets sikkerhetstjeneste og Nasjonal sikkerhetsmyndighet.

3.5 Håndtering av cyberhendelser

Sikkerhetstruende hendelser skal, så langt det er hensiktsmessig, håndteres innenfor rammene av normal drift. Sektoren skal legge vekt på tidlig varsling av cyberhendelser, og rutiner for hurtig iverksettelse av tiltak for å hindre eller redusere skadevirkninger av slike hendelser.

Det må ved håndtering av kriser som omfatter cyberhendelser sikres nødvendig samordning med sivil sektor. NSM koordinerer innenfor rammen av sin myndighet håndteringen av alvorlige dataangrep. NSM skal inneha en tverrsektoriell oversikt over relevante tilgjengelige kompetansemiljøer og ressurser innen hendelseshåndtering til bruk i dette arbeidet..

Ved eskalering av en krise kan aktivitet som i en normalsituasjon håndteres som del av ordinær virksomhet, bli omfattet av en militær operasjon eller bli del av nasjonal krisehåndtering med andre fullmakter enn i normaltilstand. I en slik situasjon skal forsvarssektoren sørge for tett og løpende kontakt mellom strategisk og operasjonelt nivå i sektoren, samt mellom forsvarssektoren og sivil sektor, for å sikre at tiltak koordineres og at uønskede følgekonsekvenser unngås. NSMs koordinerende rolle endres ikke.

Cyberangrep som krever koordinering på sentralt nivå skal håndteres i henhold til gjeldende prinsipper for sentral krisehåndtering. Dette gjelder blant annet beslutningsmyndigheten knyttet til krisehåndteringen, som ligger på den enkelte fagstatsråd eller i regjeringen, og koordinering gjennom lederdepartement og kriseråd støttet av Krisestøtteenheten. Det enkelte departement har ansvar for krisehåndtering innenfor egen sektor, og for å samordne denne med øvrige departementer og sektorer.

Angrep i cyberdomenet kan i første rekke ramme samfunnssikkerheten ved at kritiske funksjoner utnyttes eller settes ut av spill. Avhengig av omfang og mål kan cyberangrep også true statssikkerheten. Sivile myndigheter har primæransvaret for å ivareta samfunnssikkerheten, mens Forsvarets primæroppgaver er å hevde Norges suverenitet og suverene rettigheter, og forsvare landet mot ytre angrep (statssikkerhet). Det er regjeringen som avgjør om et cyberangrep skal ansees å være et væpnet angrep. Cyberangrep som del av væpnet konflikt skal håndteres som del av FDs konstitusjonelle ansvar. En slik situasjon vil også involvere hele samfunnet og øvrige sektorers ansvar for å iverksette sektorvise tiltak og konsekvenshåndtering.

Selv om en krise er forårsaket av et cyberangrep, vil effekten av angrepet i mange tilfeller materialisere seg i det fysiske domenet. I slike tilfeller vil det være behov for at håndteringen av cyberangrep ses i sammenheng med, og i enkelte tilfeller underordnes, den øvrige krisehåndteringen.

3.5.1 Strategisk kommunikasjon

En alvorlig cyberhendelse som krever nasjonal håndtering kan også innebære behov for kommunikasjon med befolkningen og media, i henhold til etablerte prosedyrer for sentral krisehåndtering. Det skal utvises særlig forsiktighet i omtalen av rammede aktører for å forhindre unødig skade på omdømme og tillit. Videre skal omtale av trusselaktøren(e), særlig dersom det er andre stater involvert, vurderes som del av det bredere sikkerhetspolitiske bildet.

3.6 Sivilt-militært samarbeid

Forsvaret kan etter anmodning gi bistand til sivile myndigheter ved alvorlige cyberhendelser i henhold til gjeldende prinsipper og regelverk for Forsvarets bistand til politiet og øvrige sivile myndigheter.

Forsvarets bistand ved cyberhendelser kan eksempelvis innebære faglig rådgivning, støtte fra enheter med særskilt kompetanse, bistand til gjenoppretting av kommunikasjonsnettverk og støtte med mer generelle kapasiteter som vakthold, sikring og transport for å bistå med håndtering av cyberangrep og følgeskader av slike. Bistand knyttet til sivile virksomheters håndtering av alvorlige dataangrep skal være koordinert med NSM.

Forsvaret kan kreve pliktmessig støtte fra sivile myndigheter i alvorlige situasjoner der beredskapslovene tas i bruk. Under andre forhold må dette skje i form av avtaler om støtte og samarbeid, og gjennom kommersielle ordninger. Også i krisesituasjoner kan støtte og samarbeid i henhold til slike avtaler være hensiktsmessig.

3.7 Cyberoperasjoner

3.7.1 Generelt

Cyberoperasjoner gjennomføres som selvstendige operasjoner eller som støtte til land-, luft-, sjø- eller fellesoperasjoner. Cyberoperasjoner inkluderer ikke oppgaver som utføres som del av daglig drift eller oppgaver knyttet til utvikling av materiell, taktikk, organisasjon og personell samt utdanning og trening. Cyberoperasjoner omfatter ikke tiltak utenfor datanettverkene for å påvirke disse, eksempelvis i form av kinetiske maktmidler og elektronisk krigføring. Siden begrepet cyberoperasjoner forbeholdes militære operasjoner i selve datanettverkene, innebærer det at blant annet etablering av samband i operasjonsområdet ikke omfattes av begrepet.

Med mindre annet følger av gjeldende regelverk for gjennomføring av særlig sensitive etterretningsoperasjoner, skal planlegging og ledelse av cyberoperasjoner underlegges militære myndighets-, ansvars- og kommandoforhold, som nedfelt i Forsvarssjefens direktiv for operativ virksomhet og følge ordinære operasjonsplanprosesser som nedfelt i Beredskapssystem for forsvarssektoren. Cyberoperasjoner skal underlegges politisk styring og kontroll på lik linje med øvrige operasjoner.

Beslutningsmyndigheten for operasjoner som innebærer offensive tiltak i form av CNA ligger på strategisk nivå, og det samme gjelder for beslutninger som reiser politiske eller prinsipielle problemstillinger i en slik operasjon. Offensive innhentingstiltak (CNE) er tillagt Etterretningstjenesten gjennom lov og instruks. Også defensive tiltak som vil kunne ha strategiske og /eller sektorovergripende konsekvenser skal besluttes på strategisk nivå, og NSM skal trekkes inn som rådgiver ved slike beslutninger. Forsvaret skal etablere ordninger og mekanismer som sikrer rettidig, god og sikker kommunikasjon mellom strategisk nivå og utøvende nivå for å sikre politisk kontroll og strategisk styring av slike tiltak.

3.7.2 Defensive cyberoperasjoner

Defensive cyberoperasjoner skal under kriser og væpnet konflikt inngå som del av den helhetlige operasjonsplanleggingen og krisehåndteringen. CND er et av virkemidlene som planlegges som del av informasjonsoperasjoner i kampanjeplanlegging. Dersom situasjonen involverer NATO og/eller allierte skal koordinering av CND inngå som del av Forsvarets totale operative koordinering mot disse aktørene.

Defensive cyberoperasjoner må sikre nødvendig understøttelse av militære operasjoner og strategisk krisehåndtering. Forsvarssektoren skal derfor ha planer og beredskap for dette, samt gjennomføre øvelser for slik støtte.
CND kan medføre behov for tiltak med følgekonsekvenser ut over forsvarssektoren, f. eks. nedstenging av deler av sivil IKT-infrastruktur og militær rekvisisjon av telekommunikasjonslinjer. Slike tiltak skal være hjemlet i lovverk og bør, så langt de kan forutses, reflekteres i konkrete forhåndsplanlagt beredskapstiltak nedfelt i de nasjonale beredskapssystemene.

Ved eskalering av en krise vil det være et økende behov for koordinering og liaisonering. Etatene i forsvarssektoren skal avgi relevant gjensidig liaisonstøtte til hverandre, samt ved behov også gjensidig liaisonstøtte til sivile myndigheter, slik at det økende behovet for koordinering ved kriser kan ivaretas.

3.7.3 Offensive cyberoperasjoner

Forsvaret skal ha kapasitet for offensive cyberoperasjoner, som bl.a. bidrar til at vi kan beskytte oss mot angrep utenfra. Som all annen bruk av militære maktmidler er også disse kapasitetene underlagt politisk kontroll og strategisk styring, jf. også omtale av CNA og CNE i punkt 3.7.1. Ytterligere regulering av offensive cyberoperasjoner er gradert og fastsatt i annet regelverk og dokumentasjon.

3.8 Juridiske rammer

Forsvarssektorens aktivitet i cyberdomenet er underlagt en rekke lover og forskrifter. Nedenfor redegjøres det for de mest sentrale bestemmelsene som regulerer denne aktiviteten.

3.8.1 Nasjonalt regelverk

NSM kan, som nasjonal fagmyndighet for forebyggende sikkerhet, bistå virksomhetene ved spørsmål om juridiske rammer relatert til informasjonssikkerhet. Se vedlegg 2 for mer utfyllende informasjon om hjemmelsgrunnlag for informasjonssikkerhet og hendelseshåndtering.

E-tjenesten kan støtte andre virksomheters defensive cyberoperasjoner iht. eget lovgrunnlag, i kraft av fagmyndighet og utøvende ansvar for offensive cyberoperasjoner og i kraft av fagmyndighet for all etterretning i Forsvaret.

Virksomhetene har ansvar for egenbeskyttelse og for å gjennomføre tiltak for gjenoppretting av sikker tilstand i egne IKT-systemer. Slike tiltak må ligge innenfor rammene av gjeldende regelverk, og tiltak som kan være inngripende overfor enkeltindivider må ha et legalt grunnlag.

Dersom eksterne aktører skal være tilkoblet forsvarssektorens IKT-systemer eller informasjonsinfrastruktur, skal ansvar, roller og myndighet reguleres i en egen avtale.

3.8.2 Folkerettens regler for cyberangrep

3.8.2.1 Folkeretten og ansvar

Et digitalt angrep kan, avhengig av omstendigheter som angrepets formål og legitimitet, styrke og konsekvenser, regnes som ulovlig maktbruk etter FN-paktens artikkel 2(4). Et angrep i cyberdomenet kan utløse en stats rett til selvforsvar etter FN-paktens artikkel 51. Terskelen er høy, og vil eksempelvis først gjelde der staten er utsatt for et omfattende angrep

rettet mot kritisk infrastruktur, eller dersom cyberangrepet forårsaker betydelig tap av liv eller materiell skade. Dersom angrepet ikke er tilstrekkelig alvorlig til å utløse selvforsvarsretten, vil den rammede stat likevel kunne iverksette andre mottiltak som ikke innebærer bruk av makt.

3.8.2.2 Bruk av makt

Bruk av, eller trussel om bruk av offensive cyberkapasiteter som kvalifiserer som trussel om maktbruk eller maktbruk etter FN-pakten art 2(4) og anvendt mot den territoriale integriteten til en annen stat, eller som på annen måte er i strid med formålet til FN-pakten, kan bare benyttes hvis ett eller flere av følgende kriterier er tilfredsstilt:

- autorisasjon fra Sikkerhetsrådet
- som utøvelse av selvforsvar etter FN-paktens artikkel 51
- samtykke fra den stat på hvis territorium effekten av maktbruken vil materialisere seg

3.8.2.3 Regler for digital krigføring

Krigens folkerett kommer til anvendelse i cyberdomenet, forutsatt at terskelen for væpnet konflikt er overskredet. Dette får betydning både for planleggingen og gjennomføringen av operasjoner der digitale virkemidler er en del av forsvars- og angrepsmidlene. Det bør i forkant av en operasjon foretas en juridisk vurdering der de særskilte folkerettslige problemstillingene vedrørende digital krigføring vurderes nærmere. Det skal i denne vurderingen også tas stilling til om særskilte engasjementsregler vedrørende digital krigføring bør fastsettes for operasjonen.

3.9 Beredskap

Forsvarssektoren skal være forberedt på å håndtere cyberhendelser. Forberedelse for håndtering av alvorlige cyberhendelser må skje i fredstid. Det skal derfor gjennom beredskapsplanlegging på alle nivåer etableres relevante planer og tiltak som raskt kan iverksettes ved en cyberhendelse for å bringe kommunikasjonsinfrastruktur og IKT-systemer tilbake til en sikker og robust tilstand. Tiltakene skal videre gi grunnlag for best mulig håndtering av konsekvensene av hendelsen, herunder også å begrense skadeomfang. Virksomhetene skal beskrive tiltakene i sine beredskapsplanverk.

Inngripende tiltak må være hjemlet i lov, forskrift eller tilsvarende eller forberedte slike, på adekvat nivå. Beredskapstiltak som krever sentral beslutning skal reflekteres i Beredskapssystem for forsvarssektoren. Tiltakene må sees i sammenheng med, og samordnes med, tiltak på sivil side samt i NATO der det er relevant. Tiltakene skal også være samordnet med andre beredskapstiltak og -planer i forsvarssektoren. Det skal i planlegging av alle operasjoner foretas vurderinger av risikoen for cyberhendelser, og om nødvendige skal avbøtende tiltak iverksettes. Beredskapsplaner og -tiltak for cyberhendelser skal til enhver tid være oppdatert. Etter øvelser og reelle hendelser som omfatter cyberhendelser, og som berører innholdet i beredskapsplanene og -tiltakene, skal disse alltid evalueres. Erfaringene skal også danne grunnlag for revisjon av beredskapsplanverket.

Forsvarets deployerbare IKT- og CND-kapasiteter skal ha en beredskap som er tilpasset Forsvarets behov, og enhetene som etablerer og drifter disse kan ved behov benyttes til støtte for det sivile samfunn i henhold til gjeldende bestemmelser for slik støtte, jf. punkt 3.6.

3.10 Kompetanse, øving og trening

Virksomhetene i sektoren er ansvarlige for å ha personell med tilstrekkelig og tilpasset kompetanse i henhold til gjeldende krav og operative behov. Det skal innenfor relevante områder søkes strategisk samarbeid med sivile utdanningsinstitusjoner, samt samarbeid om utdanning i utlandet herunder med nære allierte, for å bidra til å dekke sektorens behov. Dette

ansvaret omfatter også etablering og vedlikehold av ordninger og mekanismer som sikrer nødvendig og sikker tilgang til relevant reservepersonell som kan øves og innkalles ved behov.

Forsvarsektorens ledelses- og kommandostruktur skal ha tilstrekkelig kompetanse til å planlegge og lede cyberoperasjoner, samt håndtere krisesituasjoner under trussel om eller bruk av cyberangrep. Denne kompetansen skal være tilpasset oppgaver og ansvar som er lagt til de ulike nivåer i forsvarssektoren.

For å oppnå effektiv evne til cyberoperasjoner og IKT-aktiviteter til støtte for operasjoner skal forsvarssektoren regelmessig trene prosedyrer og tiltak, samt gjennomføre øvelser. IKT-aktiviteter og cyberoperasjoner skal rutinemessig innarbeides i øvelser på alle nivåer. Sivilt-militært samvirke skal øves innenfor rammene av gjeldende bestemmelser og begrensninger for gjensidig sivil-militær støtte generelt og innen cyberdomenet spesielt. Virksomhetene skal holde hverandre gjensidig oppdatert på tverrsektoriell øvingsdeltakelse.

Internasjonalt samarbeid om øving, trening og evaluering, særlig med nære allierte, skal vektlegges der dette kan bidra til økt kompetanse og bedre utnyttelse av ressursene.

3.11 Internasjonalt samarbeid

3.11.1 NATO og Norge

Trusler i cyberdomenet kan nå en terskel som truer nasjonal og euro-atlantisk velferd, sikkerhet og stabilitet, og kan utløse en NATO artikkel 5-situasjon. NATO vil for å bevare fleksibilitet i sin respons, kunne iverksette både militære og andre tiltak for å beskytte Alliansen mot angrep. Forsvar mot digitale angrep inngår som del av Alliansens planverk og operasjoner.

NATO har ansvar for den informasjons- og kommunikasjonsinfrastrukturen som NATO eier. Medlemslandene har selv ansvar for å sikre nasjonal IKT, herunder systemer som opprettholder vitale nasjonale funksjoner så som regjering, forsvar og sikkerhet.

I tillegg til å bidra med forebyggende tiltak som standardisering, interoperabilitet, erfaringslæring med mer, kan NATO bidra med varsling og informasjonsdeling ved alvorlige cyberangrep som rammer NATO og/eller allierte. For å bidra til alliert informasjonsdeling om cyberhendelser via NATO skal Forsvaret og NSM dele relevant informasjon med NATO ved bruk av etablerte prosedyrer. For nærmere bestemmelser om varsling og rapportering, se 3.4.

Norge kan anmode NATO om støtte i forbindelse med cyberangrep rettet mot nasjonal IKT-infrastruktur. Ved alvorlige cyberangrep kan det være aktuelt å benytte artikkel 4 og/eller artikkel 5 i NATO-traktaten. Konkret hva som vil inngå i en anmodning om støtte vil vurderes fra hendelse til hendelse. Eksempler på støtte kan være økt informasjons- og etterretningsdeling, politisk støtte, eller støtte i form av sivil cyberekspertise gjennom Civil Emergency Planning Committee (CEPC).

For at NATO skal kunne planlegge, lede og gjennomføre sine operasjoner må nasjonale systemer som støtter opp om disse, fungere uhindret. Forsvaret skal derfor sørge for at IKT som er driftet av Forsvaret, og som er viktig for NATO, er tilstrekkelig sikret i forhold til systemenes konfidensialitet, integritet, tilgjengelighet og autentisitet iht. krav i relevant

regelverk og risiko- og sårbarhetsanalyser. Nasjonal IKT-infrastruktur som er viktig for NATO skal også inngå i nasjonale objektsikkerhetsregimer der dette er relevant.

3.11.2 Forholdet til andre land

Bilateralt samarbeid er viktig for informasjonsutveksling og kompetanseoverføring. Slikt samarbeid innen informasjonssikkerhet og cyberoperasjoner kan være nyttig i håndteringen av større cyberangrep. Prioriterte samarbeidsland vil i første rekke være avhengig av hvilke land som har relevant kompetanse, og følger retningslinjer for bilateralt samarbeid som angitt i gjeldende styringsdokumenter, herunder Iverksettingsbrev/Tildelingsbrev.

Etatene i forsvarssektoren skal koordinere internasjonal kontakt seg imellom, samt sørge for at relevant informasjon deles med hverandre og med FD, for å sikre at sektoren fremstår koordinert utad.

Ved en alvorlig cyberhendelse kan det være behov for økt strategisk koordinering på myndighetsnivå av kontakten med andre land.

3.11.3 Særlig om nordisk samarbeid

Det er etablert et samarbeid mellom de IKT-responsmiljøene i Norden som utøver en nasjonal funksjon. Hovedfokus for samarbeidet skal være erfaringsutveksling, rådgivning og samordning av nasjonenes innsats ved alvorlige cyberangrep mot kritisk infrastruktur. NSM er nasjonalt kontaktpunkt i samarbeidet. NSM skal følge opp og videreutvikle det nordiske samarbeidet koordinert med øvrige berørte aktører i forsvarssektoren.

4 Forsvarsdepartementets og underlagte etaters ansvar, oppgaver og myndighet

I det følgende beskrives på et overordnet nivå FDs og underlagte etaters ansvar, oppgaver og myndighet innen informasjonssikkerhet i cyberdomenet og cyberoperasjoner.

4.1 Forsvarsdepartementet

FD skal, som overordnet ansvarlig for sektoren, sørge for at informasjonssikkerhet i cyberdomenet og cyberoperasjoner er en integrert del av departementets planleggings-, ledelses- og styringsprosesser. På denne måten sikres en overordnet og helhetlig tilnærming til forsvarssektorens arbeid med fagområdet. Ansvaret for cybersaker følger linjeansvaret i departementet, og de enkelte avdelinger i FD skal ivareta cyberaspektet som en integrert del av avdelingens øvrige portefølje.

Avdelingenes arbeid, og ved behov også etatenes skal koordineres gjennom FDs Koordineringsgruppe for informasjonssikkerhet og cyberoperasjoner (KG Cyber) jf. egen instruks. Ved behov trekkes også etatene inn i KG Cyber.

4.2 Forsvaret

Forsvaret planlegger, leder og gjennomfører alle militære operasjoner i hele krisespekteret. Forsvaret planlegger, etablerer, drifter, forsvarer og utvikler Forsvarets kommunikasjonsinfrastruktur, samt leverer administrative og operative IKT-systemer til forsvarssektoren.

4.2.1 Forsvarssjefen

Forsvarssjefen (FSJ) har innenfor disse rammene ansvar for at Forsvaret:

a) ivaretar sitt selvstendige ansvar for militært forsvar av Norge, og opprettholdelse av landets forsvarsevne, dersom riket er i væpnet konflikt eller væpnet konflikt truer eller rikets selvstendighet eller sikkerhet står i fare, også innenfor cyberdomenet
b) innehar nødvendig kompetanse, kapasitet og kapabilitet til å planlegge med og benytte cyberoperasjoner i sin virksomhet
c) sikrer at forebyggende sikkerhet i cyberdomenet og evne til å utføre cyberoperasjoner blir ivaretatt i egen organisasjon i henhold til gjeldende lover og regelverk
d) integrerer forebyggende informasjonssikkerhet i cyberdomenet og cyberoperasjoner i sine planleggings-, ledelses- og styringsprosesser
e) har en tilstrekkelig evne til å beskytte seg mot cyberangrep, og kan yte bistand til sivile myndigheter med tilgjengelig kapasitet i henhold til gjeldende bestemmelser
f) har tilstrekkelig evne til å styrke kommunikasjonsinfrastruktur og IKT-systemer innen prioriterte områder
g) gjennom styrkeproduksjon ivaretar krav til informasjonssikkerhet og cyberoperasjoner, herunder at styrkebidrag er utdannet, utrustet, organisert og samtrent, og at kontroll av faglig standard gjennomføres
h) iverksetter de planverk og bestemmelser som FD utgir innen cyberoperasjoner og forebyggende informasjonssikkerhet i cyberdomenet, og følger opp de krav som stilles gjennom styringsdialogen med departementet, eller som på annen måte er pålagt Forsvaret

Forsvarssjefen utgir nødvendige direktiver som fastsetter ansvar, oppgaver og myndighet for de enkelte avdelinger i Forsvaret.

4.2.2 Særskilt om E-tjenesten

E-tjenesten omtales særskilt i disse retningslinjene, på grunn av tjenestens særlige hjemmelsgrunnlag og sektorovergripende ansvar.

Sjef E-tjenesten er ansvarlig for all norsk utenlandsetterretning og fagmyndighet og utøvende ansvarlig for etterretningsvirksomhet i Forsvaret, og skal ivareta oppgaver som følger av lov og instruks om E-tjenesten. Sjef E-tjenesten er fra forsvarssjefen også delegert fagmyndighet for offensive cyberoperasjoner.

Sjef E-tjenesten har innenfor disse rammene ansvar for E-tjenestens:

a) utførelse av tidlig varsling av mulige ytre cybertrusler fra fremmede stater, organisasjoner eller individer
b) bidrag til å produsere et oppdatert nasjonalt cyberrisikobilde innenfor rammen av Cyberkoordineringsgruppen (CKG), sammen med NSM og PST
c) koordinerende myndighet innen cyberoperasjoner
d) gjennomføring av offensive tiltak i cyberdomenet

4.3 Nasjonal sikkerhetsmyndighet

NSM er det sentrale direktoratet for beskyttelse av informasjon og infrastruktur av betydning for samfunnskritiske og andre viktige samfunnsfunksjoner.

Direktør NSM har ansvar for at NSM:

a) utøver funksjonen som nasjonal sikkerhetsmyndighet i henhold til sikkerhetsloven, herunder å være nasjonal fagmyndighet for forebyggende sikkerhet i cyberdomenet
b) bidrar til at IKT-sikkerhetstiltak utvikles gjennom iverksettelse av forskning og utvikling på områder av betydning for forebyggende sikkerhetstjeneste
c) utfører sikkerhetsgodkjenning av informasjonssystemer der dette er tillagt NSM
d) ivaretar oppgaven som nasjonal varslings-, informasjonsdelings- og koordineringsinstans for håndtering av alvorlige dataangrep mot samfunnskritisk infrastruktur eller andre viktige samfunnsfunksjoner, herunder drift av Varslingssystem for digital infrastruktur (VDI)
e) vedlikeholder og utgir et helhetlig cyberrisikobilde innen rammen av Cyberkoordineringsgruppen og i samarbeid med E-tjenesten og PST
f) ivaretar rollen som nasjonalt kontaktpunkt for varsling av cyberangrep til, og nasjonal viderevarsling fra, internasjonale organisasjoner, herunder NATO og andre land innenfor eget ansvarsområde
g) ivaretar rollen som sertifiseringsmyndighet for IKT-sikkerhet i produkter og systemer.
h) iverksetter de planverk og bestemmelser som FD utgir innen forebyggende informasjonssikkerhet, og følger opp de krav som stilles gjennom styringsdialogen med departementet, eller som på annen måte er pålagt NSM
i) understøtter JDs ansvar for forebyggende IKT-sikkerhet på sivil side

4.4 Forsvarets forskningsinstitutt

Direktør FFI har ansvar for at FFI:

a) gjennom egen forskning og utnyttelse av andres forskningsresultater, bidrar til å øke forsvarssektorens innsikt i cyberdomenet
b) gir råd til ledelsen i forsvarssektoren om den vitenskapelige og militærtekniske utvikling med konsekvenser for virksomhet i cyberdomenet
c) har kompetanse innenfor prioriterte områder innen informasjonssikkerhet og cyberoperasjoner, og benytter denne til å støtte forsvarssektoren med forskning innen virkninger av, og beskyttelse mot, cyberangrep i henhold til de til enhver tid gjeldende prosjektoppdrag
d) bistår forsvarssektoren med støtte til undervisning om effekter av, og beskyttelse mot, cyberangrep
e) støtter forsvarssektoren med forskning innen forbedring av informasjonsinfrastruktur i henhold til de til enhver tid gjeldende prosjektoppdrag
f) bistår forsvarssektoren med støtte til planlegging og gjennomføring av øvelser med relevans for informasjonssikkerhet i cyberdomenet og cyberoperasjoner
g) iverksetter de planverk og bestemmelser som FD utgir innen forebyggende informasjonssikkerhet, og følger opp de krav som stilles gjennom styringsdialogen med departementet, eller som på annen måte er pålagt FFI

4.5 Forsvarsbygg

Direktør FB har ansvaret for at FB:

a) etablerer nøkterne og fleksible løsninger ved fremskaffelse av EBA, med mulighet for tilpasning av funksjonalitet til endringer i sektorens behov, herunder blant annet strømkapasitet og fysisk sikring ved nyetablering eller utvidelse av informasjonsinfrastruktur
b) ivaretar krav til fysisk sikring av EBA
c) i samarbeid med bruker sikrer nødvendig redundans og driftssikkerhet, for eksempel kraftforsyning, for IKT-systemene i bygningsinstallasjonene
d) innehar nødvendig cyberkompetanse i egen organisasjon
e) iverksetter de planverk og bestemmelser som FD utgir innen forebyggende informasjonssikkerhet, og følger opp de krav som stilles gjennom styringsdialogen med departementet, eller som på annen måte er pålagt FB

5 Sluttbestemmelser

Etatene har ansvar for at retningslinjene gjøres kjent i egen organisasjon. Etatssjefene skal utarbeide nødvendige bestemmelser for egen organisasjon og eget myndighetsområde, og sørge for at etatens eksisterende regelverk blir oppdatert og tilpasset cyberretningslinjene.

FD har det overordnede ansvaret for å tolke og informere om retningslinjene samt gi veiledning om retningslinjenes virkeområde.

Forslag til endringer i disse retningslinjene skal rettes til FD, som har ansvaret for at de ved behov blir oppdatert og videreutviklet.

Vedlegg 1: Definisjoner med relevans for informasjonssikkerhet og cyberoperasjoner

Autentisitet
«Ekthet»

Autorisere
Gi en bruker tillatelse til å kommunisere med eller bruke en funksjon, ressurs eller objekt

Cyber
Prefiks for vise at det ordet prefikset benyttes sammen med henviser til noe i cyberdomenet. F.eks. *cyberangrep* eller *cybertrussel.*

Cyberangrep
Handlinger i eller gjennom cyberdomenet med hensikt å skade eller påvirke personell, materiell eller konfidensialiteten, integriteten, tilgjengeligheten eller autentisiteten til et informasjonssystem.

Cyberdomenet
Fysiske og logiske sammenkoblinger av informasjonssystemer, herunder nettverksenheter, kommunikasjonsinfrastruktur, lagringsmedia og data.
Synonym: Det digitale rom

Cyberforsvar
Anvendelsen av hensiktsmessige defensive tiltak for å oppnå cybersikkerhet

Cyberhendelse
Brukes i disse retningslinjene både om situasjoner der IKT-systemer blir utsatt for cyberangrep, og ved utilsiktet svikt forårsaket av ulykker eller uhell. Med alvorlige cyberhendelser menes cyberhendelser som rammer samfunnskritisk infrastruktur, samfunnskritisk informasjon eller samfunnskritiske funksjoner på en slik måte at det får betydning for samfunnets og befolkningens trygghet.

Cybermakt
Evne til å anvende eller projisere makt i eller gjennom cyberdomenet.

Cyberoperasjoner/Datanettverksoperasjoner
Datanettverksoperasjoner er et samlebegrep som tilsvarer det engelske begrepet Computer Network Operations (CNO). CNO er tiltak som gjennomføres i datanettverkene for å påvirke motstanders datanett og beskytte eget nett. Dette omfatter Computer Network Defence (CND), Computer Network Exploitation (CNE) og Computer Network Attack (CNA). CND er å anse som en defensiv aktivitet som skal sikre handlefrihet i egen

informasjonsinfrastruktur, til tross for offensive aktiviteter fra en motstander. CNE og CNA er å anse som offensive aktiviteter og gjennomføres normalt i en motstanders nettverk. CNE skal bidra til å søke etter, fange opp, identifisere og lokalisere aktiviteter og informasjon i cyberdomenet i den hensikt å oppnå situasjonsforståelse og for å kunne gjenkjenne trusler. CNA skal bidra til å redusere eller hindre en motstanders evne til å utnytte cyberdomenet til egne operasjoner. Informasjon fremskaffet gjennom CNE vil være av sentral betydning for både CNA- og CND-aktiviteter.

Cyberoperasjoner brukes i forsvarssektoren som et synonym til datanettverksoperasjoner. Cyberoperasjoner omfatter ikke IKT-aktiviteter. Cyberoperasjoner omfatter ikke tiltak utenfor datanettverkene for å påvirke disse, eksempelvis i form av kinetiske maktmidler og elektronisk krigføring. Cyberoperasjoner og operasjoner i det digitale rom kan benyttes som synonymer.

Computer Network Attack (CNA)
Angrep på motstanderens datasystem med sikte på å forstyrre, manipulere eller ødelegge som støtte til en militær operasjon.

Computer Network Defence (CND)
Tiltak for å opprettholde militær handlefrihet i en militær operasjon ved å overvåke, detektere, analysere og iverksette defensive mottiltak i egne informasjonssystemer ved CNA eller CNE mot egne informasjonssystemer. Synonym: *Datanettverksforsvar*

Computer Network Exploitation (CNE)
Tiltak for å oppnå adgang til motstanderens datasystem, tappe det for informasjon og utnytte denne informasjonen (uten at motstanderen er klar over det) som støtte til en militær operasjon.

Cybersikkerhet
Samme definisjon som informasjonssikkerhet, men i en digital kontekst.

Elektronisk krigføring (EK)
En militær aktivitet som gjør bruk av elektromagnetisk (EM) energi, for å utnytte og beherske spektrumet i offensive og defensive operasjoner. EK omfatter innhenting og identifikasjon av EM utstråling, bruk av EM energi for å redusere eller forhindre fiendtlig bruk av spektrumet og tiltak for å sikre egne styrkes bruk av dette.

Forsvarssektoren
Samlebetegnelse på Forsvarsdepartementet (FD), Forsvaret, Forsvarets forskningsinstitutt (FFI), Forsvarsbygg (FB) og Nasjonal sikkerhetsmyndighet (NSM).

IKT
Informasjons- og kommunikasjonsteknologi.

IKT-aktiviteter
Aktiviteter for å kunne utvikle og fasilitere et stabilt og sikkert cyberdomene. Dette inkluderer å utvikle, etablere, konfigurere, sikre, vedlikeholde, drifte og risikohåndtere cyberdomenet.

IKT-aktiviteter omfatter daglig drift og støtte til operasjoner.
Synonym: CIS-aktiviteter

Informasjon
Enhver form for opplysninger i materiell eller immateriell form

Informasjonssikkerhet
Sikkerhetstiltak for i nødvendig grad å oppnå konfidensialitet, integritet, tilgjengelighet og autentisitet ved behandling av informasjon i alle situasjoner, uavhengig av verktøy og metoder. Cyberretningslinjene er innrettet mot håndtering av digital informasjon og informasjonssystemer.

Informasjonssikkerhet omfatter både etablering av barrierer, deteksjon av sikkerhetstruende hendelser og reaksjon på slike med tanke på gjenoppretting av sikker tilstand for informasjon og systemer. Defensive datanettverksoperasjoner (CND) omfattes av begrepet informasjonssikkerhet, men utføres i en operativ kontekst.

Informasjonssystem
En organisert samling av periferiutrustning, programvare, datamaskiner og kommunikasjonsnett som knytter dem sammen.

Informasjonssystemsikkerhet
Omfatter både forebyggende tiltak, aktive og passive sikringstiltak, og hendelseshåndtering, herunder en rekke tiltak som i en operativ kontekst omtales som CND. De tiltak som skal iverksettes for å ivareta informasjonssystemsikkerhet omfatter forebyggende robusthetsskapende tiltak, men også tiltak som har til formål og detektere og håndtere hendelser med sikte på gjenopprettelse av systemets sikre tilstand. Offensive aktørrettede tiltak faller utenfor både begrepet informasjonssystemsikkerhet og CND.

Integritet
Sikkerhet for at informasjonen og informasjonsbehandlingen er fullstendig, nøyaktig og gyldig, og et resultat av autoriserte og kontrollerte aktiviteter

Konfidensialitet
Sikkerhet for at nærmere angitt informasjon ikke avsløres for uvedkommende, og at kun autoriserte personer får tilgang til denne.

Tilgjengelighet
Sikkerhet for at en tjeneste oppfyller bestemte krav til stabilitet, slik at aktuell informasjon er tilgjengelig ved behov.

Vedlegg 2: Hjemmelsgrunnlag for sikring av systemer og hendelseshåndtering

Dette vedlegget omhandler hjemmelsgrunnlag for forebyggende informasjonssikkerhet, herunder sikkerhetsmessig overvåking, innenfor rammen av sikkerhetsloven. Vedlegget omhandler ikke hjemmelsgrunnlag for etterretningsvirksomhet eller hendelseshåndtering ved bruk av offensive virkemidler, som kan følge både av folkeretten og nasjonal rett (herunder lov og instruks for Etterretningstjenesten).

Graderte systemer
Sikkerhetsloven med forskrifter fastsetter en rekke tiltak for å sikre systemene. Tiltakene skal bygge opp under målene for informasjonssystemsikkerhet, nemlig sikker plattform, sikker drift og vedlikehold, og sikker hendelseshåndtering og gjenoppretting. Dette forutsetter blant annet en sikkerhetsmessig overvåkning av system, med formål å avdekke «sikkerhetstruende hendelser» i sikkerhetslovens forstand. Sikkerhetstruende hendelser er definert som sikkerhetstruende virksomhet – kompromittering av skjermingsverdig informasjon og grove sikkerhetsbrudd. Sikkerhetsbrudd er brudd på bestemmelser gitt i og i medhold av sikkerhetsloven.

Ugraderte systemer
Det eksisterer en rekke ulike regelverk som stiller krav til sikkerhet også i ugraderte informasjonssystem, blant annet personopplysningsloven med forskrifter. Dette for å sikre systemenes konfidensialitet, integritet og tilgjengelighet.
Det forutsettes i personopplysningsforskriften en viss sikkerhetsmessig overvåkning av systemer som behandler personopplysninger. Formålet med denne sikkerhetsmessige overvåkning er å administrere systemet, og/eller avdekke/oppklare brudd på sikkerheten i systemet.

Særlig om sikkerhetsmessig overvåkning
Sikkerhetsmessig overvåkning av graderte systemer må ligge innenfor de rammer og det formål som følger av sikkerhetsloven. Det følger forutsetningsvis av personopplysnings-forskriften at formålet med sikkerhetsmessig overvåkning av ugraderte systemer er å ivareta systemet sikkerhet.

I tillegg må sikkerhetsmessig overvåkning skje innenfor rammene av annet lovverk, herunder personopplysningsloven og arbeidsmiljøloven, begge med forskrifter. Inngrep i den personlige rettssfære krever som utgangspunkt hjemmel i lov, jf. legalitetsprinsippet.

Det legges til grunn at det innenfor ovennevnte formål er adgang til å logge trafikkdata. Dette hjemles i personopplysningsloven § 8 bokstav f). Personopplysninger som behandles ved logging av trafikkdata vil i det alt vesentlige være IP-adresser. For forsvarssektorens systemer gjør sterke allmenne interesser seg gjeldende i forhold til å sikre systemene, og personvernulempen vurderes som beskjeden ved denne type overvåkning.

Det vil i enkelte tilfeller vil være behov for å «dumpe» innholdsdata for på en tilfredsstillende måte å ivareta systemenes sikkerhet. Hjemmelsgrunnlag for denne type overvåkning må vurderes konkret i det enkelte tilfelle, herunder opp mot personopplysningsloven § 8 bokstav f). Forhold av betydning ved denne vurderingen vil være blant annet systemets graderingsnivå, kritikalitet, omfang av innholdsdata som ønskes dumpet, om man står ovenfor en konkret trussel og denne trusselens potensielle alvorlighetsgrad. Ved dumping av

innholdsdata gjelder de generelle prinsippene i personopplysningsloven. I tillegg gjelder de prosedyrekrav som følger av arbeidsmiljøloven med forskrifter, herunder regler for innsyn i epostkasse mv.