FORSVARET
Forsvarets Informasjonsinfrastruktur

Vår saksbehandler
Sr̊dg Knut Storvik, kstorvik@mil.no
+47 23 09 54 31, 0510 5431
INIST/I&N-avd

Vår dato 2010-06-25
Vår referanse 2010/013338-005/FORSVARET/ 433

Tidligere dato
Tidligere referanse

Til
Forsvarsdepartementet

Postboks 8126 Dep
0032 OSLO
NORGE

Kopi til
Forsvarsstaben

Høringsuttalelse fra INI - Forslag til strategi for Cybersikkerhet

1 Bakgrunn

Forsvarsdepartementet (FD) har i tidligere referanse lagt frem Nasjonal sikkerhetsmyndighet (NSM) sitt forslag til nasjonal strategi for cybersikkerhet på høring. Strategiforslaget trekker opp hovedlinjene for videreutvikling av nødvendige samordnende og sektorovergripende tiltak for helhetlig beskyttelse av kritiske IKT-systemer mot alvorlige IKT-hendelser. Med helhetlig beskyttelse menes så vel forebygging som effektiv håndtering av hendelser.

NSM ble i IVB2009 gitt i oppdrag å fremme et koordinert forslag til nasjonal strategi for Cyber Defence. NSM begrunner begrepsendringen fra Cyber Defence til cybersikkerhet med at Cyber Defence er en militær aktivitet. FD skriver i tidligere referanse at strategien ikke dekker militære tiltak mot IKT-angrep innenfor rammen av væpnet konflikt.

Forsvarets sikkerhetstjeneste (FOST) har tidligere kommentert[1] at deler av strategiforslaget kan være i strid med den militære folkeretten.

2 Drøfting

Forsvarets informasjonsinfrastruktur (INI) anser at den uttalte begrensning av strategien – at den ikke skal dekke militære tiltak mot IKT-angrep innefor rammen av væpnet konflikt – er en vesentlig svakhet ved forslaget.
Forslaget til strategi for cybersikkerhet er svært konkret på en rekke punkter, til dels mer konkret enn hva man normalt kan forvente i en overordnet nasjonal strategi, og gir i mange henseende mer uttrykk for å være en implementeringsplan enn en strategi. Siden man i stor grad benytter de militært rettede sidene ved cybersikkerhet og informasjonsoperasjoner som argumentasjon for å opprette et Cybersenter, ser vi oss nødt til å være tilsvarende konkrete i våre kommentarer også.

2.1 Begrepsavklaringer og definisjoner

2.1.1 Definisjon av Cyberspace

Det finnes en rekke definisjoner av Cyberspace, og INI kan ikke se at den definisjonen som NSM har hentet fra Wikipedia og lagt til grunn i utkast til nasjonal strategi for cybersikkerhet er den som best

[1] DL 2010/003945-001/FORSVARET/ 433

beskriver dette domenet.
Noen av de beste definisjonene av Cyberspace[2] og andre cyber relaterte begreper som har blitt fremlagt så langt, er de som professor Dr. Daniel T. Kuehl ved det amerikansk National Defence University (NDU)har kommet opp med og som er basert på en utvikling av de siste amerikanske forsøk på å definere dette domenet.

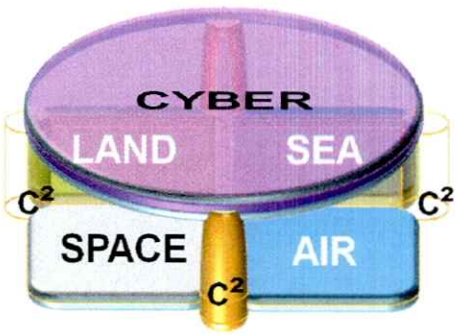
INI har ikke oversatt disse definisjonene pga begrensninger i tid til disposisjon, men vi vil kunne påta oss å forestå en slik oversettelse, og gjøre disse allment tilgjengelige.

"**Cyber Space** is an operational domain characterized by the use of electronics and the electronic spectrum to create, store, modify, exchange and exploit information via networked and interconnected information systems and their associated infrastructures."

"**Cyber Power** is the ability to use cyberspace to create advantages and influence events in the other operational environments and across the instruments of power."

"**Cyber Strategy** is the development and employment of capabilities to operate in Cyber Space, integrated and coordinated with the other operational domains, to achieve or support the achievement of objectives across the elements of national power."

"**Cyber Superiority** is the degree to which one can gain advantage from the use of Cyber Space while if necessary preventing one's adversaries from gaining advantage from it. Cyber Superiority includes offensive/proactive and defensive/protective operations."



Figur 1: De fem operasjonelle fysiske domenene, her vist med kommando og kontroll (C^2) som limet som sørger for at vi kan operere samordnet på tvers av domene.

2.1.2 The Information Environment.

Dette er det begrepet som det opereres med i gjeldende[3] doktrine for informasjonsoperasjoner, AJP 3.10 Information Operations, og som kan best beskrives av de tre distinkte men likevel innbyrdes forbundne dimensjonene som vi kan betegne som konneksjon (connectivity), innhold (content), and kognisjon (cognition). Dette er det "rommet" hvor Informasjonsoperasjoner gjennomføres og som vi må forholde oss til også i en cybersikkerhetssammenheng.
Konneksjon (connectivity) kan best beskrives som de fysiske plattformene, systemene og infrastrukturen som gir global konnektivitet for å koble sammen informasjonssystemer, nettverk og brukere. **Innhold (content)** kan beskrives som de massive mengdene med informasjon som digitalt og elektronisk kan sendes hvor som helst, når som helst, til neste hvem som helst. En tilstand som har blitt svært påvirket, og forsterket, av konvergensen av a en rekke informasjonsteknologier. **Kognisjon (cognition)** er resultatet av den sterke økningen i tilgang til innhold, og noe som på en dramatisk måte kan gi utslag i menneskelig oppførsel og beslutningstaking.

[2] From Cyberspace to Cyberpower: Defining the Problem; Dr Daniel T. Kuehl, NDU.
[3] Approbert av Norge og under innføring i Forsvaret.

2.1.3 Sammenhengen mellom Cyberspace og informasjonsoperasjoner

For det første vil det være feilaktig å sette likhetstegn mellom Cyberspace og informasjons-operasjoner. Isteden vil den mest dekkende beskrivelsen av Cyberspace være å se det som et kritisk aspekt av det totale "Information Environment[4]", hvor informasjonsoperasjoner gjennomføres, men ikke som hele "Information Environment". Mens informasjonsoperasjoner derfor inkluderer alle tre dimensjonene av "Information Environment", så omfatter Cyberspace bare deler – skjønt kanskje meget store deler – av dimensjonene konneksjon og innhold.
Informasjonsoperasjoner er evnen til å gjennomføre koordinerte og integrerte operasjoner som gir effekter innenfor det som kalles "Information Environment". For å gjennomføre slike operasjoner kan operativ myndighet benytte seg av en rekke kapasiteter, blant annet elektronisk krigføring (EK), psykologiske operasjoner (PSYOPS) og Computer Network Operations (CNO).
Informasjonsoperasjoner er slik INI ser det ikke bare en integrerende og rådgivende funksjon, men er en evne og en militær kjernekompetanse på linje med evne til land-, sjø- og luft-, ytre rom- og cyberoperasjoner. Dette bør beskrives i overordnede termer i en slik nasjonal strategi for cybersikkerhet.

2.2 Generelt om strategiens innhold

IKT gjennomsyrer hele det norske samfunn, og det er nødvendig å beskytte seg mot cyber-anslag som vil ramme kritiske samfunnsfunksjoner, verdiskaping og den enkeltes rettigheter og behov. Det er derfor behov for å utvikle en strategi som skal sette nasjonen i stand til å motvirke at kritiske samfunnsfunksjoner, verdiskaping og den enkeltes behov blir alvorlig skadelidende. INI ser det som naturlig at en nasjonal strategi for cybersikkerhet skal bidra til å ivareta dette.
INI er imidlertid kritisk til at strategiforslaget i så stor grad legger informasjonsoperasjoner og cyber-anslag fra fremmede stater og ikke-regulære militante grupperinger til grunn, samtidig som Forsvarets ansvar og myndighet innen stats- og samfunnssikkerheten er mangelfullt beskrevet. Forsvarets ansvar og myndighet ligger normalt innen det man oppfatter som statssikkerhet, mens politiet (justissektoren) har et overordnet ansvar for krisehåndtering relatert til samfunnssikkerheten.
Statssikkerhet er et helt grunnleggende sikkerhetsbehov som, når staten stilles overfor en eksistensiell trussel, kan legitimere innsats av alle dens tilgjengelige ressurser. Statssikkerheten kan også utfordres gjennom politisk og militært press mot norske myndigheter eller gjennom mer begrensede anslag og angrep mot norske myndigheter og interesser. Samfunnssikkerhet dreier seg om å ivareta sivilbefolkningens trygghet og å sikre sentrale samfunnsfunksjoner og viktig infrastruktur mot angrep og annen skade der statens eksistens som sådan ikke er truet. Det er en nær sammenheng og glidende overganger mellom disse sikkerhetsdimensjonene, og det er vanskelig å trekke klare skiller[5].
Organisering og bruk av den nasjonale informasjonsinfrastrukturen fører til særlige problemer med å adskille militær og sivil bruk. Et og samme system kan brukes til både sivile og militære formål, og militære og sivile systemer kan være knyttet sammen på en måte som gjør at angrep på det ene får virkninger i det andre. Dette er tilsvarende øvrig infrastruktur, der veier, jernbane, flyplasser osv har både sivil og militær anvendelse. I Håndbok i militær folkerett hevdes[6] det at en fiendtlig informasjonsoperasjon kan ha et så alvorlig omfang at det må regnes som et væpnet angrep, og at dette berettiger at en kan forsvare seg ved å bruke de midler som er nødvendige for å stoppe angrepet eller forhindre gjentagelse. Dette kan innebære datanettverksmotangrep, men kan også innebære at man i ytterste konsekvens utløser et fysisk motangrep for å nøytralisere trusselen.
Et datanettverksangrep fra fremmede stater eller ikke-regulære militante grupperinger mot militær eller sivil infrastruktur, som er av en slik karakter at det sidestilles med væpnet angrep, kan medføre at selvforsvarsretten i FN-paktens artikkel 51 trer i kraft. I en slik situasjon er det en selvstendig militær

[4] I mangel av en god norsk oversettelse av dette begrepet har vi inntil videre valgt å benytte den engelske originalversjonen.
[5] St.prp. nr 42 (2003-2004)
[6] Håndbok i militær folkerett, Del G – pkt 2.2

oppgave å håndtere krisen, herunder å iverksette mottiltak. Nødvendigheten av å bekjempe fiendtlige datanettverksangrep kan ikke utelukkende avgrenses til å gjelde militær informasjonsinfrastruktur, så lenge sivil informasjonsinfrastruktur direkte eller indirekte støtter militære operasjoner eller behov, eller at statssikkerheten er truet som følge av angrepene.
I andre deler av krisespennet kan fiendtlige datanettverksangrep rettet mot sivil infrastruktur være av et så alvorlig omfang at Forsvaret må bistå politiet med å ivareta samfunnssikkerheten. Forsvaret bidrar i dag til samfunnssikkerheten ved å bistå politiet med å beskytte annen kritisk infrastruktur (oljeinstallasjoner, veinettet, kraftverk osv). INI kan ikke se at det foreligger noen prinsipielle grunner til at Forsvaret ikke kan bistå med bekjempelse av datanettverksangrep eller ulovlig innsamling av etterretninger som rammer viktig sivil informasjonsinfrastruktur. Tvert imot synes dette å være i henhold til intensjonen i det moderniserte totalforsvarskonseptet som omfatter gjensidig støtte og samarbeid mellom Forsvaret og det sivile samfunn i hele krisespekteret fra fred via sikkerhetspolitisk krise til krig. Det er ikke lenger en forutsetning at beredskapslovgivningen trer i kraft for at støtten kan sies å være innenfor rammen av totalforsvarskonseptet[7].
En nasjonal strategi for cybersikkerhet kan derfor ikke se bort fra Forsvarets ansvars- og myndighets-områder ved bekjempelse av datanettverksangrep og ulovlig etterretningsinnsamling fra fremmede stater og ikke-regulære militante grupperinger, eller støtte til det sivile samfunn. Forsvaret må uansett sikres et nødvendig hjemmelsgrunnlag for å forsvare seg mot og bekjempe datanettverksangrep og ulovlig etterretningsinnsamling mot egen infrastruktur og infrastrukturer som eventuelt også benyttes av andre sektorer. Spesielt fordi angrep som berører Forsvaret potensielt kan få statssikkerhetsmessige konsekvenser uavhengig om de innledningsvis kan bære preg av kriminalitet.

2.3 Forsvarets ansvar og myndighet ved fiendtlige informasjonsoperasjoner og Cyber-anslag

Det er utviklet både nasjonale og internasjonale doktriner for anvendelse av informasjonsoperasjoner. NATO beskriver sine prinsipper for informasjonsoperasjoner i AJP-3.10 *NATO Information Operations Doctrine*[8]. NATO knytter muligheten for og effekten av datanettverksoperasjoner (CNO) til motstanderens bruk av IKT i militære operasjoner og prosesser. CNO består i denne sammenheng av Computer Network Attack (CNA), Computer Network Exploration (CNE) og Computer Network Defence (CND). Den europeiske union (EU) har i sitt *Concept for Computer Network Operations in EU-led Military operations*[9]anvendt samme definisjon for CNO som NATO.
Sentrale elementer i informasjonsoperasjoner angis i Forsvarets fellesoperative doktrine (FFOD)[10] å være informasjonssikkerhet, psykologiske operasjoner, villedning, elektronisk krigføring, datanettverksoperasjoner og fysisk ødeleggelse av informasjonsinfrastruktur. Informasjonssikkerhet er i denne sammenheng en viktig del av operasjonssikkerheten (OPSEC) som skal forhindre at en motstander skaffer seg informasjon om våre operasjoner, objekter, kapasiteter og intensjoner. Dette omfatter[11] blant annet overvåking av egne systemer og forsvar av datanettverk (CND). FFOD beskriver videre[12] datanettverksoperasjoner (CNO) hvor en søker å beskytte sin egen informasjonsinfrastruktur (CND) og/eller å forstyrre eller ødelegge (CNA) motstanderens evne til å anvende sin. Slike operasjoner kan brukes som både strategisk og operasjonelt verktøy, og de har økt sin betydning innen fellesoperasjoner.
Utviklingen innen doktriner i dag, og da spesielt innen NbF, Cyberspace som eget operasjonelt domene og innen informasjonsoperasjoner som kapabilitet, går så raskt at FFOD (som ble utviklet før 2007 og ikke siden er revidert) åpenbart er moden for revisjon.
Strategiforslaget hevder at Cyberspace aldri vil bli et virtuelt territorium som kan okkuperes og at det strategiske utfallet av en konflikt heller ikke vil avgjøres i Cyberspace. NSM gir ingen begrunnelse for dette standpunkt, og det fremstår som noe naivt og løsrevet fra etablerte nasjonale og internasjonale doktriner for informasjonsoperasjoner.

---

[7] Støtte og samarbeid – Det moderniserte totalforsvarskonseptet, Forsvarsdepartementet, 2007
[8] DCDC/NATO/AJP3.10 - 2007
[9] 13537/1/09 REV 1 – 17 mars 2010
[10] FFOD - 0596
[11] FFOD - 0597
[12] FFOD - 05101

Det ovennevnte viser at både nasjonal og internasjonal doktrine definerer både offensive og defensive informasjonsoperasjoner som militære aktiviteter. Jfr. Kombattantbegrepet[13] synes det åpenbart at kun militære styrker kan planlegge, lede og delta i slike operasjoner.
Forsvaret står i en særstilling hva gjelder ansvar for å bekjempe fiendtlige datanettverksoperasjoner og myndighet til å gjennomføre mottiltak i form av egne CND og CNA operasjoner. Strategiforslaget beskriver i liten grad Forsvarets ansvar, myndigheter eller kapasiteter innen dette området. En nasjonal strategi må også omhandle bekjempelse av fiendtlige datanettverksangrep og ulovlig etterretningsinnsamling, og bør ha som et mål at Forsvaret etablerer en militær enhet for gjennomføring av egne og bekjempelse av fiendtlige informasjonsoperasjoner. Nødvendig hjemmelsgrunnlag bør blant annet sikres gjennom å utvikle en engasjementsregelstruktur (RoE) for slike operasjoner. Dette bør etableres som egne tiltak i strategien.

2.3.1 Etablering av militær CERT-/ CSIRT-funksjon i Forsvaret

Strategiforslaget skisserer en nasjonal struktur hvor det etableres et nasjonalt Cybersenter og egne Computer Security Incident Response Team (CSIRT) i de mest samfunnsviktige sektorer og enkeltvirksomheter. Dette synes å være en fornuftig innrettning, men strategiforslaget er ikke tydelig nok i sin beskrivelse av hvor ansvaret for sikkerhet og risikohåndtering skal plasseres. INI mener at det bør etableres et militært Computer Emergency Response Team (CERT) i Forsvaret, ikke bare et CSIRT, ganske enkelt fordi vi i Forsvars-sammenheng ikke snakker kun om Computer Security Incidents, men om operasjoner som kan ha langt større omfang.
Den militære CERT-rollen bør legges til INI, etter at det er foretatt en konsolidering av CND-funksjonene som i dag ivaretas av FOST (FSA), inn i CNO-enheten.
INI viser til de nasjonale prinsipper for krisehåndtering mellom departementene: ansvarsprinsippet, nærhetsprinsippet og likhetsprinsippet. Ansvarsprinsippet innebærer at det er det enkelte departement som har ansvaret for å håndtere en krisesituasjon som berører eget ansvarsområde. Nærhetsprinsippet medfører at krisen skal håndteres på lavest mulig nivå, mens likehetsprinsippet medfører at organiseringen under en krise skal være mest mulig lik organiseringen en opererer med til daglig. Ut fra den struktur som er foreslått, og prinsippene for krisehåndtering, må derfor strategiforslaget være helt tydelig på at det er den enkelte sektor eller virksomhet som er ansvarlig for egen cybersikkerhet. Strategiforslaget må også være tydelig på hvilke minimumskrav som skal stilles til CERT/ CSIRT-strukturen og hva en eventuell koordinerende myndighet på toppen konkret skal omfatte. I militær sammenheng er koordinerende myndighet beskrevet i FFOD vedlegg B "myndighet til å kreve rådslagning, men ikke myndighet til å framtvinge en felles beslutning". Dette er helt i tråd med det konstitusjonelle ansvar som er nedfelt i ansvarsprinsippet.

2.4 Det nasjonale Cybersenterets mandat, oppgaver og organisering

INI støtter behovet for en nasjonal enhet som kan ivareta visse sektorovergripende funksjoner innen cybersikkerhet. *Etablere en felles situasjonsoversikt og forståelse, Bygge og opprettholde robuste og sikre IKT-systemer, Bevisstgjøre, opplyse og påvirke, Styrke evnen til å oppdage og varsle IKT-hendelser og Styrke samordningen av cybersikkerhetsarbeidet* er oppgaver som bør tillegges en slik enhet. Å avgrense det foreslåtte Cybersenterets mandat til det ovennevnte synes å være i tråd med det mandat som St. meld. nr. 39 (2003-2004) ga Varslingssystem for digital infrastruktur (VDI). Mandat til VDI er her avgrenset til identifisering og varsling av datanettsangrep.
NSM skriver i sitt strategiforslag at hensikten er å styrke Norges evne til å forebygge og håndtere alvorlige IKT-hendelser. Det gis ingen definisjon på hva som menes med håndtering, men *Pkt 2.4 Styrke evnen til å oppdage, varsle og håndtere IKT-hendelser* og *Pkt 2.5 Etterforske og bekjempe IKT-hendelser* viser at begrepet håndtering i strategiforslaget omfatter kriminalitetsbekjempelse og bekjempelse av fremmede etterretnings- og informasjonsoperasjoner. Annen type håndtering som ikke faller inn under dette kan være, i nasjonal målestokk, mindre alvorlige hendelser i den enkelte virksomhet eller sektor. Håndtering må derfor forstås som den bruk av makt og myndighet som tilligger politiet eller

[13] Håndbok i militær folkerett, Del G - pkt 3

Forsvaret, eller nødvendig bruk av menneskelige, finansielle eller tekniske ressurser i den enkelte virksomhet og sektor.
Som tidligere nevnt er samfunnssikkerheten, herunder etterforsking og kriminalitetsbekjempelse, i hovedsak et politiansvar. Forsvarets ansvar og myndighet innen håndtering og bekjempelse av fiendtlige informasjonsoperasjoner er drøftet tidligere. INI kan ikke se at Cybersenteret, som er foreslått som en videreføring av NorCERT, har - eller kan gis politimyndighet. Det synes åpenbart at et Cybersenter heller ikke kan planlegge, lede eller delta i bekjempelse av informasjonsoperasjoner og cyber-anslag fra fremmede stater og ikke-regulære militante grupperinger uten at det bryter med kombattantbegrepet i den militære folkeretten. INI kan heller ikke se at det foreslåtte Cybersenteret har - eller bør gis nødvendig myndighet til å håndtere hendelser i den enkelte virksomhet som omfattes av en slik nasjonal overvåking.
Cybersenterets mandat må av ovennevnte grunn avgrenses til ikke å omfatte håndtering av IKT-hendelser slik strategiforslaget legger opp til. Strategiforslaget må omarbeides slik at ansvar og myndighet for håndtering legges til den virksomhet og etat som har det faktiske ansvaret. Om begrepet håndtering skal brukes, må det klart defineres til kun å omfatte rådgiving, varsling og informasjonsutveksling.
Ettersom krisespennet er glidende og det faktiske ansvar for håndtering av alvorlige IKT-hendelser tilligger politiet, Forsvaret eller den enkelte sektor/virksomhet, synes det uhensiktsmessig å legge håndteringsoppgaver til et nasjonalt Cybersenter. Dersom Cybersenteret likevel skal ha håndteringsoppgaver ved beredskaps eller krisesituasjoner hvor fiendtlige datanettverksangrep og ulovlig etterretningsinnsamling truer nasjonal infrastruktur, må det i de tilfeller underlegges militær kommando og dets ansatte må gis status som kombattante i de militære styrker.

2.4.1 Organisering av et nasjonalt Cybersenter

INI mener at det kan være betydelige gevinster for nasjonal kriseberedskap, og evne til å forebygge og varsle om IKT-hendelser, dersom en velger en annen organisering av det foreslåtte Cybersenteret. Strategiforslaget tar til orde for å etablere Cybersenteret som en videreføring av NorCERT som i dag ligger i NSM. INI er svært bekymret for at etablering av Cybersenteret i NSM, med det mandatet som strategiforslaget legger til grunn, vil utydeliggjøre de faktiske ansvars og myndighetsforhold som eksisterer. NorCERT sitt administrative oppheng er tidligere drøftet[14] i FD.

En mulighet er å samlokalisere Cybersenteret med NorSIS som nå ligger under Fornyings-, administrasjons- og kirkedepartementet (FAD). FAD har sektoransvar for IT-politikk og utøver samordning av IT-sikkerhet og sårbarhet knyttet til samfunnsmessig bruk av IT. En slik organisering vil kunne gi store gevinster ved at den nasjonale evnen til å forebygge og varsle om IKT-hendelser blir vesentlig styrket. Denne organiseringen vil også bidra til å tydeliggjøre den rolle og det mandatet Cybersenteret bør ha, forutsatt avgrenset mandat til kun å omfatte rådgiving, varsling og informasjonsutveksling.

En annen mulighet kan være at Cybersenteret underlegges Direktoratet for samfunnssikkerhet og beredskap (DSB) for å trekke veksler på denne organisasjonens eksisterende ekspertise innen totalforsvarsberedskap og samfunnssikkerhet. Denne organiseringen vil også bidra til å tydeliggjøre den rolle og det mandatet Cybersenteret bør ha, på samme måte som i det første forslag til organisering. Dog mener INI at koblingen mot totalforsvar og samfunnssikkerhet er bedre ivaretatt gjennom dette opphenget, enn gjennom det forrige. Mandat som for alternativ 1.

En tredje mulighet er å etablere det foreslåtte Cybersenteret som en enhet i Forsvaret. Det vil på mange måter imøtegå alle over drøftede problemstillinger, samtidig som overgang fra fredsmessig håndtering av anslag (som støtte til politiet), til bekjempelse av informasjonsoperasjoner og cyber-anslag fra fremmede stater og ikke-regulære militante grupperinger vil være sømløs.
Videreføring av den støtte som dagens NorCERT yter, og et evt fremtidig Cybersenter er forutsatt å yte, overfor sivil sektor vil heller ikke være en utfordring så lenge det klargjøres gjennom sektorvise avtaler hvilke leveranser Cybersenteret er forutsatt å stå for og dekning av de økonomiske forhold ift disse

[14] S-gruppens rapport, Forsvarsdepartementet, 23 januar 2009

leveransene. Noe som uansett oppheng vil måtte gjennomføres.
Det vil også i gitte tilfeller være uproblematisk å gi medlemmer av de væpnede styrkene begrenset politimyndighet ifm støtte til politiet, slik det gjøres i lignende tilfeller i dag, ref avtale om Forsvarets støtte til Politiet. Dette forslaget ivaretar også totalforsvars- og samfunnssikkerhetsaspektene på en utmerket og helhetlig måte. Utvidet mandat iht opprinnelig forslag til strategi for cybersikkerhet.

2.5 Økonomiske og administrative kostnader

FD ber i tidligere referanse om innspill til økonomiske og administrative konsekvenser som ikke har kommet til uttrykk i NSM sin overordnede oversikt. Flere av de foreslåtte tiltakene vil medføre økonomiske og administrative kostnader for Forsvaret, herunder Tiltak 1 – Kartlegge og verdivurdere kritiske IKT-systemer i alle sektorer, Tiltak 6 – Stille felles krav til kritiske IKT-systemer, Tiltak 12 – arrangere og delta i øvelser (sektorvise, nasjonale og internasjonale) og Tiltak 15 – Etablere sektorvise CSIRT-miljøer i samfunnsviktige sektorer og i de største enkeltvirksomheter. Listen er ikke uttømmende.

De økonomiske og administrative kostnadene lar seg ikke kvantifisere fordi strategiforslaget i liten grad stiller krav til de enkelte tiltak. Forsvaret vil imidlertid kunne redusere de økonomiske konsekvensene ved å legge funksjoner og aktiviteter til allerede eksisterende strukturer i Forsvaret. Den militære CERT-rollen bør som tidligere drøftet legges til INI, etter at det er foretatt en konsolidering av CND-funksjonene som i dag ivaretas av FOST (FSA), inn i CNO-enheten. Kravstilling, kartlegging og verdivurdering av IKT-systemer i Forsvaret bør legges til den avdeling i Forsvaret som blir ansvarlig for å ivareta virksomhetens ansvar for sikkerhetsgodkjenning av informasjonssystemer. Hvor dette ansvaret plasseres vil fremkomme av de utredninger som gjøres ifm utarbeidelsen av ny instruks for Sjef FOST (SJ FSA).
INI antar at også øvrige foreslåtte tiltak kan tillegges eksisterende strukturer og prosesser i Forsvaret for å redusere de økonomiske konsekvensene. INI imøteser en ytterligere konkretisering av hvilke krav som stilles til de enkelte tiltakene.

3 Konklusjon

INI støtter fullt ut tanken om en nasjonal strategi for Cybersikkerhet, og imøteser at denne skal danne grunnlaget for, på en helhetlig og koordinert måte, det videre arbeidet for å forbedre sikkerheten innenfor Cyberspace domenet. Vi snakker i denne sammenheng om sikkerhet i vid forstand, både statssikkerhet og samfunnssikkerhet.
Samtidig er det essensielt at den tas frem innefor totalforsvarskonseptets rammer. Det er bare slik at den blir det overordnede og helhetlige grunnlaget nasjonen Norge trenger for å forbedre sikkerheten – og evnen til helhetlig og koordinert håndtering av hendelser i hele konfliktspennet – i informasjons-infrastrukturen, i det elektromagnetiske spektrum og ifm gjennomføring av informasjonsoperasjoner.

Ovennevnte drøfting oppsummeres i følgende innspill/anbefalinger:

1. INI slutter seg til FOST (FSA) sine betenkninger ift forslag om at det foreslåtte Cybersenteret skal kunne planlegge, lede eller delta i bekjempelse av informasjonsoperasjoner og cyber-anslag fra fremmede stater og ikke-regulære militante grupperinger. Dette kan bare utføres av enheter under militær kommando, ref kombattant begrepet, annet vil kunne innebære brudd på internasjonale konvensjoner som Norge har forpliktet seg til å følge.
2. Forsvarets ansvar og myndighet innen stats- og samfunnssikkerheten må beskrives i en nasjonal strategi for cybersikkerhet, herunder ansvaret ved bekjempelse av informasjonsoperasjoner og cyber-anslag fra fremmede stater og ikke-regulære militante grupperinger i både militær og sivil infrastruktur.

3. Det er etablert en egen militær sjef (Sjef INI) som i dag har ansvar for å bla utvikle og styrkeprodusere Forsvarets enhet for datanettverksoperasjoner (CNO), og gjennom FD sin Instruks[15] om sikkerhetstjenesten i Forsvaret skal det utøvende ansvar for totalsikkerheten i systemene de forvalter, herunder ansvaret for drifts- og sikkerhetsmessig overvåking av graderte og ugraderte informasjonssystemer, samt utøvende ansvar for hendelseshåndtering av drifts- og sikkerhetsmessige hendelser tillegges samme organisasjon. Dette vil utvilsomt styrke vår evne til samordnet og helhetlig innsats på området.
4. Det bør etableres en engasjementregelstruktur (RoE) som skal bidra til å sikre hjemmelsgrunnlag for den operative virksomheten.
5. Strategiforslaget må eksplisitt slå fast at den enkelte sektor eller virksomhet selv er ansvarlig for egen cybersikkerhet.
6. Cybersenterets mandat må avgrenses til kun å omfatte rådgiving, varsling og informasjonsutveksling, med mindre senteret organiseres som en del av Forsvaret.
7. INI anbefaler at det utredes om alternative organiseringer av det foreslåtte Cybersenteret vil gi vesentlige gevinster innen nasjonal kriseberedskap og evne til helhetlig og sømløst å sikre og forsvare nasjonens kritiske informasjonsinfrastruktur.
8. Videre arbeid med strategien må involvere alle berørte departementer/etater slik at man kan få til et omforent dokument. Det er spesielt viktig å få med de tyngste aktørene som forsvars- og justis-, men også de som representerer energi- og næringssektorene.

Roar Sundseth
Generalmajor
Sjef INI

[15] Instruks om sikkerhetstjeneste i Forsvaret, fastsatt 29. april 2010 av Forsvarsdepartementet i medhold av instruksjonsmyndighet.