FORSVARET
Forsvarets sikkerhetstjeneste

Vår saksbehandler
MAJ Bjarte Malmedal, bmalmedal@mil.no
+4755 50 59 47, 0540 5947
FOST/INFO S-AVD/

Vår dato
2010-05-04

Vår referanse
2010/013338-003/FORSVARET/ 433

Tidligere dato
2010-03-30

Tidligere referanse
2010/00794-1

Til
Forsvarsstaben

Kopi til
Forsvarsdepartementet
INIST

Høring - 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 varslet[1] om at deler av strategiforslaget kan være i strid med den militære folkeretten.

2 Drøfting

Det er åpenbart viktig for Forsvaret at det i Norge etableres en helhetlig strategi på strategisk nivå for Cybersikkerhet.

IKT gjennomsyrer hele det norske samfunn, og det er nødvendig å beskytte seg mot cyberanslag 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. FOST ser det som naturlig at en nasjonal strategi for cybersikkerhet skal bidra til å ivareta dette.

Strategiforslaget slår fast[2] at cyberspace er en attraktiv arena for kriminalitet, spionasje og i ytterste konsekvens krigføring. IKT-trusselbildet er basert på EOS-tjenestenes[3] vurderinger, hvor etterretningstrusselen fra utenlandske staters etterretningstjenester fremheves. Det understrekes at statsdrevede informasjonsoperasjoner opererer i hele konfliktspennet, også i fredstid, og utgjør trolig den mest alvorlige formen for anslag mot kritiske IKT-systemer. Forsvaret trekkes her frem som et

[1] 2010/003945-001/FORSVARET/ 433
[2] Pkt 2.5 Etterforske og bekjempe IKT-hendelser
[3] Etterretningstjenesten, Politiets sikkerhetstjeneste og Nasjonal sikkerhetsmyndighet

typisk mål for slike anslag. Trusselvurderingen viser til Estland-saken i 2007, Gaza-konflikten i 2008, Georgia-krigen i 2008 og valget i Iran i 2009 der cyberangrep og offensive informasjonsoperasjoner ble anvendt som en del av konflikten. FOST sine egne observasjoner og analyser samsvarer med det trusselbildet som beskrives i strategiforslaget.

FOST er imidlertid kritisk til at strategiforslaget i så stor grad legger informasjonsoperasjoner og cyberanslag 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[4].

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[5] 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 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). FOST 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[6].

En nasjonal strategi for cybersikkerhet kan derfor ikke se bort fra Forsvarets ansvars- og myndighetsområder 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

[4] St.prp. nr 42 (2003-2004)

[5] Håndbok i militær folkerett, Del G – pkt 2.2

[6] Støtte og samarbeid – Det moderniserte totalforsvarskonseptet, Forsvarsdepartementet, 2007

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.

2.1 Forsvarets ansvar og myndighet ved fiendtlige informasjonsoperasjoner og cyberanslag

Det er utviklet både nasjonale og internasjonale doktriner for anvendelse av militære informasjonsoperasjoner.

NATO beskriver sine prinsipper for informasjonsoperasjoner i AJP-3.10 *NATO Information Operations Doctrine*[7]. 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 sin *Concept for Computer Network Operations in EU-led military operations*[8] anvendt samme definisjon for CNO som NATO.

Forsvarets fellesoperative doktrine (FFOD) beskriver domenemodellen som en del av stridsevnemodellen. Domenemodellen beskriver det kognitive domenet, informasjonsdomenet, det sosiale domenet og det fysiske domenet. Domenemodellen ble utviklet med tanke på et nettverksbasert forsvar (NbF) og informasjonsoperasjoner. Disse beskrives[9] som en viktig del av alle militære operasjoner, og som har til hensikt å beskytte egne styrker og å påvirke motstanderen eller andre aktører i operasjonsområdet. Sentrale elementer i slike operasjoner angis[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. 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.

Det ovennevnte viser at både nasjonal og internasjonal doktrine definerer både offensive og defensive informasjonsoperasjoner som militære aktiviteter. Jf. 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 kommando for

[7] DCDC/NATO/AJP3.10 - 2007
[8] 13537/1/09 REV 1 – 17 mars 2010
[9] FFOD - 0592
[10] FFOD - 0596
[11] FFOD - 0597
[12] FFOD - 05101
[13] Håndbok i militær folkerett, Del G - pkt 3

gjennomføring av egne og bekjempelse av fiendtlige informasjonsoperasjoner. Nødvendig hjemmelsgrunnlag bør blant annet sikres gjennom å utvikle en *Rules Of Engagement*-struktur for slike operasjoner. Dette bør etableres som egne tiltak i strategien.

2.1.1 Etablering av 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. FOST 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 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.

2.2 Det nasjonale cybersenterets mandat, oppgaver og organisering

FOST 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). VDIs mandat 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 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. FOST 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 cyberanslag fra fremmede stater og ikke-regulære militante grupperinger uten at det bryter med kombattantbegrepet i den militære folkeretten. FOST 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 å ikke 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.

2.2.1 Organisering av et nasjonalt cybersenter

FOST 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. FOST er 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.

2.3 Økonomiske og administrative kostnader

FD ber i tidligere referanse om innspill til økonomiske og administrative konsekvenser som ikke har kommet til uttrykk i NSMs 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. CSIRT-rollen bør legges til Forsvarets CND-enhet som allerede har en deployerbar og døgnbemannet kapasitet for bekjempelse av datanettverksangrep. Kravstilling, kartlegging og verdivurdering av IKT-systemer i Forsvaret bør legges til avdeling for informasjonssikkerhet i FOST som i ivaretar virksomhetens ansvar for sikkerhetsgodkjenning av informasjonssystemer. FOST antar at også øvrige foreslåtte tiltak kan tillegges eksisterende strukturer og prosesser i Forsvaret for å redusere de økonomiske konsekvensene. FOST imøteser en ytterligere konkretisering av hvilke krav som stilles til de enkelte tiltakene.

3 Konklusjon

FOST er enig i at det er behov for en nasjonal strategi for cybersikkerhet, og imøteser at denne skal forbedre sikkerheten for nasjonens kritiske informasjonsinfrastruktur og evne til effektiv krisehåndtering.

Ovennevnte drøfting oppsummeres i følgende anbefalinger:

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

1. Med bakgrunn i tidligere varsel om forhold som kan være i strid med den militære folkeretten anbefaler FOST at det utredes hvorvidt kombattantbegrepet eller andre forhold forhindrer at det foreslåtte cybersenteret kan planlegge, lede eller delta i bekjempelse av informasjonsoperasjoner og cyberanslag fra fremmede stater og ikke-regulære militante grupperinger
2. Forsvarets ansvar og myndighet innen stats- og samfunnssikkerheten må beskrives i en nasjonal strategi for cybersikkerhet, herunder ansvaret ved bekjempelse av informasjonsoperasjoner og cyberanslag fra fremmede stater og ikke-regulære militante grupperinger i både militær og sivil infrastruktur
3. Etablering av en militær kommando for planlegging og ledelse av egne CND og CNA operasjoner bør vurderes etablert som et eget tiltak i strategien. Alternativt kan dette legges til sjef E eller sjef FOH som allerede har grunnlag og infrastruktur til å gjennomføre operasjoner. Det bør etableres en Rules Of Engagement-struktur som skal bidra til å sikre hjemmelsgrunnlag for den operative virksomheten
4. Strategiforslaget må eksplisitt slå fast at den enkelte sektor eller virksomhet selv er ansvarlig for egen cybersikkerhet
5. Cybersenterets mandat må avgrenses til kun å omfatte rådgiving, varsling og informasjonsutveksling
6. FOST anbefaler at det utredes om en alternativ organisering av det foreslåtte cybersenteret vil gi vesentlige gevinster innen nasjonal kriseberedskap og evne til å sikre og forsvare nasjonens kritiske informasjonsinfrastruktur.

Geir Gade
Kommandør
Sjef Forsvarets sikkerhetstjeneste