FORSVARET
Forsvarets sikkerhetsavdeling

Vår saksbehandler
MAJ MALMEDAL BJARTE, bmalmedal@mil.no
+4761 10 38 50, 0500 3850
FSA/ INFO S-AVD/ Senter BKI

Vår dato 2010-02-11

Vår referanse 2010/003945-001/FORSVARET/ 433

Tidligere dato

Tidligere referanse

Til
Forsvarsstaben

Kopi til
Forsvarsdepartementet

Varsel om mulig brudd på den militære folkeretten i Nasjonal strategi for cybersikkerhet

1 Bakgrunn

Forsvarets sikkerhetstjeneste (FOST) er kjent med at Nasjonal sikkerhetsmyndighet (NSM) i IVB2009 ble gitt i oppdrag å fremme et koordinert forslag til Nasjonal strategi for Cyber Defence.

Gjennom en pressemelding 18. januar 2010 ble Forsvaret orientert om at NSM har fremmet et forslag til Nasjonal strategi for Cybersikkerhet[1] til Forsvarsdepartementet og Justisdepartementet. FOST sin gjennomgang av strategien reiser spørsmål hvorvidt deler av innholdet kan være i konflikt med den militære folkeretten.

Det antas at Forsvarsdepartementet har til hensikt å gjennomføre en bred og grundig høring av strategiforslaget. FOST oppfatter imidlertid at spørsmålene som reises i dette brev er av en slik karakter at det bør vurderes om det skal igangsettes utredning av de folkerettslige spørsmålene før dokumentet sendes ut på høring.

2 Drøfting

FOST gjør oppmerksom på at Forsvaret ikke var invitert til å delta i eller bidra til utarbeidelsen av strategiforslaget og anser ikke forslaget å være koordinert med Forsvaret.

Imidlertid vil FOST gi sin støtte til at det etableres en Nasjonal strategi for Cybersikkerhet.

IKT gjennomsyrer hele det norske samfunn, og det er et åpenbart nødvendig å beskytte seg mot cyberanslag som vil ramme kritiske samfunnsfunksjoner, verdiskaping og den enkeltes rettigheter og behov. Det er 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 beskriver et IKT-trusselbilde som er basert på EOS-tjenestenes[2] vurderinger. I vurderingen fremheves etterretningstrusselen fra utenlandske staters etterretningstjenester. 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

[1] NSM begrunner navneendringen med behovet for å skille Cybersikkerhet fra Cyber Defence som er en militær aktivitet

[2] *Etterretningstjenesten, Politiets sikkerhetstjeneste og Nasjonal sikkerhetsmyndighet*

frem som et 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.

Strategiforslaget slår fast[3] at cyberspace er en attraktiv arena for kriminalitet, spionasje og i ytterste konsekvens krigføring. I tiltakene[4] vises det til at Forsvaret har *"utviklet en deployerbar enhet for militære informasjonsoperasjoner (CNO-enheten)"*.

Strategiforslaget unnlater imidlertid å omtale Forsvarets totale kapasitet innen domenet for informasjonsoperasjoner. I tillegg til det operative ledelseselementet for informasjonsoperasjoner ved Forsvarets operative hovedkvarter og nevnte CNO-enhet, er det i FOST etablert en operativ enhet for militære Computer Network Defence (CND) operasjoner. Sjef FOST er i sin instruks gitt kompetanse innen militær kontra-etterretning og CND. Forsvarets kapasiteter innen informasjonsoperasjoner er etablert innen rammen av nasjonale[5] og NATO-doktriner[6], og er et virkemiddel som når synkronisert med tradisjonelle land, sjø og luft operasjoner skal etablere og opprettholde et relativt informasjons- og beslutningsfortrinn i forhold til en motstander.

Strategiforslaget beskriver [7] etablering av et Cybersenter som en videreføring av dagens NorCERT[8]. Det planlegges å tillegge cybersenteret et koordineringsansvar for håndtering av alvorlige dataangrep. Det hevdes at det nasjonale cybersenteret er et viktig virkemiddel for å styrke evnen til å etterforske og bekjempe IKT-hendelser, og det henvises her til strategiforslagets pkt 2.5 som omtaler de offensive kapasiteter som Forsvaret har etablert.

FOST oppfatter det slik at informasjonsoperasjoner slik de omtales i strategiutkastet og slike de er definert i nasjonal og NATO doktrine kun kan utføres av militære styrker. Håndbok i militær folkerett[9] drøfter anvendelsen av informasjonsoperasjoner og datanettverksangrep, og FOST retter en bekymring vedrørende kombattant-begrepet i forhold til den strukturen som strategiforslaget legger opp til. FOST kan vanskelig se at Forsvaret kan avgi militære kapasiteter til et sivilt direktorat for å bekjempe fiendtlige informasjonsoperasjoner. Om sivile enheter eller personer kan underlegges militær kommando i slike tilfeller er noe FOST mener må utredes nærmere.

3 Konklusjon

FOST er positiv til at det utarbeides en nasjonal strategi for Cybersikkerhet, men stiller seg kritisk til at strategiforslaget unnlater å beskrive Forsvarets ansvars- og myndighetsområde ved bekjempelse av informasjonsoperasjoner og cyberanslag fra fremmede stater og ikke-regulære militante grupperinger. Defensive og offensive informasjonsoperasjoner er militære virkemidler, og den militære folkeretten setter begrensninger i forhold til hvem som kan lede eller delta i slike operasjoner. FOST anbefaler at det igangsettes en militærfaglig og folkerettslig vurdering vedrørende strukturen som er fremmet i strategiforslaget.

Strategiforslaget fremstår som mangelfullt i sin behandling av Forsvarets ansvars- og myndighetsområde. FOST mener at det er grunn til å hevde at Forsvaret har både rett og plikt til å bekjempe informasjonsoperasjoner og cyberanslag fra fremmede stater og ikke-regulære militante grupperinger, og at slike operasjoner også kan omfatte sivil infrastruktur dersom disse direkte støtter militære operasjoner. Strategiforslagets mangelfulle behandling av disse spørsmål kan føre til at høringsinstansene uttaler seg på mangelfullt grunnlag. FOST anbefaler at det vurderes om strategiforslaget må koordineres med Forsvaret før det fremmes på nytt.

---

[3] Pkt 2.5 Etterforske og bekjempe IKT-hendelser
[4] Tiltak 20. Offensive kapasiteter
[5] Forsvarets fellesoperative doktrine, Forsvarsstaben, 2007
[6] AJP-3.10 Allied Joint Doctrine for Information Operations, 2009
[7] Pkt 2.6 Styrke samordning av cybersikkerhetsarbeidet, Tiltak 22 Etablere et nasjonalt cybersenter
[8] Organisatorisk plassert i Nasjonal sikkerhetsmyndighet
[9] Håndbok i militær forlkerett, Generaladvokat Arne W Dahl, 2008

Geir Gade
Kommandør
Sjef Forsvarets sikkerhetstjeneste