GENERALADVOKATEN
Postboks 651 Sentrum, 0106 OSLO
Telefon 22 70 87 50 - Mil 510 5681 - Telefax 22 41 94 54
E-mail: postmottak.generaladvokaten@hpm.no
http://www.generaladvokaten.no

Vår referanse
0405/2010/GA/AWD/729 og 035.4

Dato
17. juni 2010

Deres referanse

Det kongelige forsvarsdepartement
Postboks 8126 Dep
0032 Oslo

Gjenpart: Det kongelige justis- og politidepartement,
Politiavdelingen
Postboks 8005 Dep
0030 Oslo

HØRING AV FORSLAG TIL NASJONAL STRATEGI FOR CYBERSIKKERHET

Det vises til Forsvarsdepartementets høringsbrev av 30. mars 2010 med vedlegg, oversendt hit fra Justisdepartementet for eventuell direkte uttalelse til Forsvarsdepartementet.

Generaladvokaten har begrenset egenkompetanse på fagfeltet. Denne uttalelsen vil derfor nødvendigvis måtte holde seg på et forholdsvis generelt plan.

Det er ingen tvil om at samfunnets sårbarhet for datanettverkskriminalitet, i vinnings hensikt, som skadeverk eller for terrorformål er økende. Det samme gjelder mht. angrep fra fiendtlig statlig aktør i tilfelle krig. Det er derfor meget prisverdig at Nasjonal sikkerhetsmyndighet griper fatt i denne saken.

Som strategi betraktet, synes forslaget å kunne karakteriseres som mottiltak på bred front basert på at det ikke foretas grunnleggende endringer i systemene. Med grunnleggende endringer tenker jeg på slikt som reversering av trenden mot sammenkobling (større vekt på lukkede nettverk) eller overgang til annet operativsystem (ikke Microsoft-basert) for funksjoner man særlig ønsker å beskytte. Dette kan for eksempel være kjernevirksomheter som politiet. Det er mulig at slike tiltak vil ha begrenset effekt og/eller innebære kostnader eller andre ulemper som vil være uforholdsmessig store. Jeg tillater meg likevel å etterlyse en drøfting av slike mer grunnleggende alternative strategier.

Det fremgår av Forsvarsdepartementets høringsbrev at strategien ikke dekker militære tiltak mot IKT-angrep innenfor rammen av væpnet konflikt. Hvis det siktes til tiltak av typen motangrep, er dette forståelig. Hvis man derimot tenker på defensive tiltak mot ondsinnet programvare som har tatt seg inn i eller truer med å ta seg inn i norske IKT-systemer, vil jeg tro at det kan være mye å tjene på samordnede tiltak fra militær og sivil side, uavhengig av om angrepet står i sammenheng med en væpnet konflikt, eller ikke.

For øvrig vil jeg peke på betydningen av at Forsvaret og andre offentlige eller private netteiere følger med på trafikken gjennom aktivitetslogging av eget nett, og at dette ikke vanskeliggjøres ved at utenforstående gis adgang til å bruke nettet uten at de opplyses om at noen har til oppgave å følge med på hvilke typer filer som passerer aktuelle målepunkter på vei til eller fra brukere. Fjorårets sak som rettet seg mot Forsvarets Sikkerhetsavdeling (nå FOST) var beklagelig i så henseende.

En generell lærdom kan være at man på nettet, likeså lite som på landeveien, ikke kan forvente full handlefrihet og frihet fra å bli sett av håndhevingsmyndigheter samtidig som man forventer sikkerhet mot å lide skade på grunn av andres uforsvarlige opptreden eller kriminelle handlinger. Spørsmålet om hvordan man skal avveie frihet mot sikkerhet kan falle forskjellig ut avhengig av hvorvidt man beveger seg i IKT-verdenens "utmark" eller "innmark". En bevisstgjøring av brukerne med hensyn til behovet for kontroll av trafikken på særlig beskyttelsesverdige nett (eller deler av nettet) kan muligens innpasses i tiltak nr. 11 "Styrke tiltak for bevisstgjøring, utdanning og holdningsskapende arbeid".

Med vennlig hilsen

Arne Willy Dahl
generaladvokat