Representantforslag 147 S

(2011–2012)

fra stortingsrepresentantene André Oktay Dahl, Ine M. Eriksen Søreide, Anders B. Werp, Lars Myraune og Svein Harberg

Dokument 8:147 S (2011–2012)

Representantforslag fra stortingsrepresentantene André Oktay Dahl, Ine M. Eriksen Søreide, Anders B. Werp, Lars Myraune og Svein Harberg om målrettet og forsterket innsats for informasjons- og cybersikkerhet

Til Stortinget

Bakgrunn

Dagens samfunn blir i økende grad avhengig av datateknologi og digital infrastruktur. Teknologien er en forutsetning for mange viktige funksjoner og tjenester, og tilgang til mye viktig informasjon. Men dette er teknologi og nettverk som også har svakheter og som potensielt er sårbart for kriminell utnyttelse og angrep som setter systemer og viktige samfunnsfunksjoner helt eller delvis ut av spill.

NATO vurderer cyberangrep som en av de mest alvorlige truslene medlemsstatene står overfor, med noen av de mest alvorlige økonomiske og nasjonale sikkerhetsutfordringene i det 21. århundre (Kilde: DSB, Nasjonal sårbarhets- og beredskapsrapport (NSBR) 2011).

NorCERT, Norges nasjonale senter for håndtering av alvorlige dataangrep, melder om en årlig vekst på 33 pst. i antall saker de håndterer.

Fra Politiets sikkerhetstjenestes (PSTs) trusselvurdering fremgår det at det er økende aktivitet fra andre lands etterretningstjenester og private selskaper rettet mot Norge. Internett-basert etterretning brukes i stadig større grad. Stadig mer sensitiv informasjon ligger tilgjengelig på nettet.

Cyberkriminalitet har vokst kraftig de siste årene, og det er flere internasjonale, kriminelle organisasjoner som er svært aktive. Det er her tale om enorme verdier i denne sammenhengen. Det finnes ikke eksakte tall som beskriver omfanget, men anslagene indikerer at det i global sammenheng dreier seg om årlige forretningstap som følge av cyberkriminalitet på rundt 1 000 mrd. kroner. Og tallet øker raskt.

Fagmiljøene melder om at langt fra alle hendelser av datainnbrudd og dataangrep blir rapportert. Dette skyldes for det første at bedriftene eller organisasjonene aldri oppdager at uvedkommende har vært inne i deres systemer. For det andre er det mange som unnlater å rapportere hendelsen av frykt for tap av omdømme.

Trusselbildet har en stor spennvidde. Fra identitetstyveri på sosiale medier, som kan oppleves svært ubehagelig og krenkende for de berørte, og helt til detonasjon av en kjernefysisk ladning i høyere luftlag (HEMP-High-Altitude Electromagnetic Pulse), hvor den elektromagnetiske pulsen vil ødelegge både elektrisk infrastruktur og elektronikk i et enormt omfang over store områder. De fleste scenarier beskriver at resultatet av et vellykket HEMP-angrep vil være et sammenbrudd i nesten alle samfunnsfunksjoner i de land som rammes.

I tillegg til de bevisste, menneskeskapte truslene mot informasjonssystemer og infrastruktur ser man at ekstremvær, naturkatastrofer, solstormer og menneskelig svikt ved kritiske anlegg også utgjør en reell trussel.

Langtidsmeldingen for Forsvaret, «Et forsvar for vår tid», Prop. 73 S (2011–2012), legger opp til at cyberforsvaret blir en fullverdig forsvarsgren i vår militære styrkestruktur. Forslagsstillerne understreker at dette er et positivt tiltak, og at det i den militære strukturen må føre til at oppmerksomhet og innsats konsentreres og koordineres på en effektiv måte.

Erfaring fra nyere tids krigs- og konfliktsituasjoner viser at cyberoperasjoner rettet mot sivil IKT-infrastruktur kan forventes å være en del av et militært

anslag fra en statspart. I andre tilfeller er det uhyre vanskelig å identifisere hvorvidt angriper er en sivil eller militær aktør. I begge typer situasjoner er tradisjonelle grenser mellom sivil og militær sektor å anse som tilnærmet irrelevante, og tilgjengelige responsmuligheter må være tilpasset dette.

På denne bakgrunn mener forslagsstillerne det er viktig med målrettet og forsterket innsats for å bedre informasjons- og cybersikkerheten.

Overordnet nasjonal koordinering og ansvar

Den nasjonale strategien for informasjonssikkerhet er fra 2003. I denne fordeles ansvaret for å ivareta informasjonssikkerheten på elleve departementer, basert på daværende departementsstruktur:

- Arbeids- og administrasjonsdepartementet
- Finansdepartementet
- Fiskeridepartementet
- Forsvarsdepartementet
- Helsedepartementet
- Justisdepartementet
- Kommunal- og regionaldepartementet
- Nærings- og handelsdepartementet
- Olje- og energidepartementet
- Samferdselsdepartementet
- Sosialdepartementet

I 2007 ble det utarbeidet nasjonale retningslinjer for å styrke informasjonssikkerheten. Disse retningslinjene gjaldt fram til 2010. Fire departementer stod bak disse retningslinjene: Justisdepartementet, Forsvarsdepartementet, Samferdselsdepartementet og det daværende Fornyings- og administrasjonsdepartementet. Retningslinjene er nå utgått på dato, men arbeidet med å oppdatere disse pågår.

I tillegg er det en lang rekke statlige etater som arbeider med informasjons- og cybersikkerhet, enten som en del av et større arbeidsområde eller som spesialfelt.

Dette forslaget konsentreres om det overordnede, nasjonale nivået.

Forslagsstillerne mener det på departementalt nivå må klargjøres på en tydeligere måte enn i dag hvem som har det overordnede ansvaret for å ivareta landets informasjons- og cybersikkerhet, og dermed hvem som har ansvaret for å håndtere hendelser og kriser på dette området.

Forslagsstillerne vil presisere at dette åpner for forsterkning og etablering av fagmiljøer flere steder i offentlig forvaltning, både i sivil og militær sektor, men at det ikke skal være tvil om hvor det overordnede ansvaret ligger. Dette er for å sikre at ressurser og kompetanse blir brukt på en mest mulig målrettet og effektiv måte.

Forslagsstillerne etterlyser også en helhetlig og overordnet strategi for å forsterke innsatsen innen forebygging, oppdagelse og hendelseshåndtering, informasjonsdeling, etterretning og etterforskning av hendelser innen cyberområdet.

For forslagsstillerne står noen emner sentralt i utformingen av en nasjonal strategi for bedre informasjons- og cybersikkerhet:

- En strategi må beskrive samarbeidet mellom privat og offentlig sektor. I det norske næringslivet er det flere kompetansemiljøer av høy internasjonal standard. En strategi for økt informasjonssikkerhet bør omhandle hvordan man kan organisere et samspill basert på felles interesser, herunder gjerne etablere et gjensidig forpliktende samarbeid.
- Utdanning og forskning. Oppbygging av kompetanse på dette fagfeltet er av avgjørende betydning. Noen miljøer utmerker seg, blant annet Høgskolen på Gjøvik, men målrettet innsats og virkemiddelbruk fra overordnet myndighet etterlyses.
- En strategi for cybersikkerhet må beskrive ønsket nivå for utholdenhet og robusthet i samfunnskritiske datasystemer ut fra kjente trusler fra cyberkriminalitet og belastning som følge av cyberangrep. Nivået for utholdenhet og robusthet må beskrives for opprettholdelse av tjenestetilbud, den fysiske maskinparkens funksjonalitet og ikke minst for den digitale infrastrukturens kommunikasjonsevne.
- Videre må en strategi legge til rette for å delta i et bredt internasjonalt samarbeid. Målrettede datakriminelle, hackere og angripere opererer helt uten hindring av geografiske landegrenser. Det foregår mye internasjonalt arbeid som er viktig og nyttig, særlig i NATO, men også i EU.
- En gjennomgang og vurdering av lovverket er også nødvendig, for å se om dette er tilpasset de aktuelle utfordringene og truslene mot informasjonssikkerheten. I internasjonal rett er det en diskusjon og økende styrke i argumentasjonen for at man på nasjonalt nivå kan bli gjort indirekte medansvarlig dersom man ikke har iverksatt tilstrekkelige tiltak for å hindre cyberangrep. For eksempel at en hacker-gruppe i et land kompromitterer en norsk server, og fjernstyrer denne til å utføre at cyberangrep mot et tredjeland. Dermed kan Norge bli indirekte ansvarlig for hendelsen. Alle konklusjoner er ikke trukket i diskusjonen om et lands indirekte ansvar. Men diskusjonen aktualiserer betydningen av de juridiske virkemidlene i norske myndigheters arbeid for å styrke informasjonssikkerheten (Kilde: NATO Defence College: Research paper ISSN 2076-0949).

Forslag

På denne bakgrunn fremmer forslagsstillerne følgende

f o r s l a g :

Stortinget ber regjeringen legge fram en nasjonal strategi for styrket informasjons- og cybersikkerhet. Strategien må klargjøre ansvars- og oppgavefordelingen innen dette feltet på departementsnivå.

15. juni 2012