FORSVARSMINISTERIET
DANISH MINISTRY OF DEFENCE

NOTAT

CYBERSIKKERHED

8. april 2013

I forlængelse af Forsvarsministeriets orientering af Nordisk Råds danske delegation og repræsentanter fra Forsvars- og Udenrigsudvalget tirsdag den 2. april fremsendes hermed som ønsket et statusnotat om cybersikkerhed samt andre tiltag, der er planlagt igangsat på cyberområdet.

Cybersikkerhed er især i de senere år kommet på dagsordenen, og beskyttelsen af samfundsvigtig informations- og kommunikationsinfrastruktur bliver givet øget prioritet. Flere og flere lande tillægger således i stigende omfang området prioritet og også internationalt, eksempelvis i EU og NATO er emnet højt på dagsordenen.

Cybersikkerhed
Regeringen tillægger området stor betydning og har ved kgl. resolution af 3. oktober 2011 tildelt Forsvarsministeriet ansvaret for cybersikkerhed. Som konsekvens heraf er Center for Cybersikkerhed oprettet, hvor centeret, der er placeret i rammen af Forsvarets Efterretningstjeneste, bl.a. skal bidrage til beskyttelsen af samfundets kritiske informations- og kommunikationsinfrastruktur.

Det nye Center for Cybersikkerhed er under opbygning og består bl.a. af en civil og en militær varslingstjeneste for internettrusler, en såkaldt GovCERT og en MilCERT[1]. Centeret har

[1] GovCERT: Governmental Computer Emergency Response Team.
MilCERT: Military Computer Emergency Response Team.

HOLMENS KANAL 42
1060 KØBENHAVN K
TELEFON: 33 92 33 20
TELEFAX: 33 32 06 55
MAIL: FMN@FMN.DK
WEB: www.FMN.DK
CVR: 25-77-56-35
EAN: 5798000201200

således det overordnede ansvar for, at der træffes de fornødne foranstaltninger til beskyttelse af samfundets og forsvarets kritiske informations- og kommunikationsteknologiske infrastruktur. MILCert er i den forbindelse udelukkende et defensivt element, der indgår som et bidrag i den samlede militære kapacitet, som er beskrevet nedenfor. Når det er fuldt etableret, vil det samlede cybersikkerhedscenter bestå af ca. 85 personer.

Både GovCERT og MilCERT indgår i forskellige former for internationalt samarbejde med henholdsvis civile og militære samarbejdspartnere. Der er eksempelvis et nordisk og et baltisk samarbejde på cyberområdet, hvor der på forskellige niveauer jævnligt gennemføres møder. Eksempelvis afholdes der den 24.-25. april i år et nordisk-baltisk seminar i Tallinn, hvor embedsmænd og eksperter mødes for at drøfte en række cyber-relaterede emner. Det konkrete operative nordiske samarbejde mellem GovCERT'erne bygger blandt andet på Stoltenberg-rapportens[2] anbefaling nummer 7 om cybersikkerhed. I den sammenhæng er der bl.a. oprettet et såkaldt kompetencenetværk mellem landenes varslingstjenester, som muliggør udveksling af informationer om hændelser og trusler i cyberspace. På det militære område er det nordiske samarbejde primært forankret i NATO, hvor det tillige omfatter samarbejde med NATO-partnerskabslandene Sverige og Finland.

For at underbygge prioriteringen af cybersikkerhed, er der i den nyligt indgåede forsvarsaftale tilført centeret op til 50 mio. kr. årligt over den 5-årige aftaleperiode.

Militær cyberkapacitet
Som det også fremgår af forsvarsaftalen, skal der etableres en militær kapacitet til defensive og offensive operationer i cyberspace. Kapaciteten vil kunne støtte og indgå i de militære operationer, som danske styrker indsættes i. Den organisatoriske forankring og fysiske placering af kapaciteten er endnu ikke fastlagt.

I den nye forsvarsaftale er der samlet afsat op til 75 mio. kr. i 2013, 90 mio. kr. i 2014 og 2015, samt 150 mio.kr. i 2016 og 2017 til den militær cyberkapacitet.

[2] Thorvald Stoltenbergs rapport af 9. februar 2009 om "Nordisk samarbeid om utnriks- og sikkerhetspolitikk".