SVERIGES RIKSDAG

INTERPELLATION TILL STATSRÅD

Från Riksdagsförvaltningen
2017-10-09
Besvaras senast
2017-10-23

Till försvarsminister Peter Hultqvist (S)

2017/18:22 Offensiv cyberförmåga

I försvarsinriktningspropositionen kan man på s. 112 läsa: ”Försvarsmakten lyfter fram vikten av att utveckla en offensiv cyberförmåga för att kunna möta angrepp mot egna system samtidigt som det ger möjlighet att möta hot och angrepp i andra arenor, vilket sammantaget påverkar en motståndares förmåga att angripa Sverige och svenska intressen.”

Försvarsministern har i ett flertal fall uttryckt att han instämmer i detta, bland annat i en DN-intervju den 18 mars 2015 där han citeras: ”Vi måste också kunna genomföra aktiva aktioner i cybermiljön. Den aktiva förmågan är en form av motanfall.” Liknande uttalanden har också gjorts på Folk och Försvars rikskonferens i Sälen i januari 2016 och vid ett besök på Försvarshögskolan den 4 februari samma år, där försvarsministern uttalade att ”vi kommer att gå från passiv till aktiv cyberförmåga och kapacitet”.

Detta har också hörsammats av vapenindustrin, däribland Säkerhets- och försvarsföretagen, som anordnat ett seminarium med rubriken *Sveriges framtida cyberförsvar – ett seminarium om nya marknader och möjligheter*.

Det är inte helt enkelt att förstå vad som avses med denna offensiva cyberförmåga, än mindre hur detta i praktiken ska kunna utföras utan att bryta mot svensk lagstiftning. Lämpligt nog beskriver Försvarsmakten lite närmare vad det handlar om i sin redovisning av perspektivstudien 2013: ”Med offensiv förmåga kan underrättelseverksamhet bedrivas och förband eller system fördröjas, hindras, vilseledas eller slås ut. Underrättelseverksamhet i cybermiljön ger möjligheter till snabb och dold inhämtning av stora mängder information som kan vara tillgänglig i realtid. Mjuk- och hårdvara kan, redan innan de tas i bruk, förberedas för att samla underrättelser eller öka effekten av attacker med svåra konsekvenser som följd. Försvarsmakten måste kunna hantera att sådan förmåga används.” Man efterfrågar också att man ska få i uppgift att utveckla förmågan till offensiva cyberoperationer.

Försvarsmaktens klargörande ställer ett antal frågor på sin spets. Offensiva åtgärder och cyberoperationer handlar förstås om att verka utanför de egna systemen, det vill säga i andras system. Problemet är att för att i rimlig tid aktivt kunna slå till mot andra länders eller motståndares it-system krävs förberedelser. Det innebär att man i praktiken öppnar upp för att till exempel tillåta utplacering av malware som trojaner eller maskar i förberedande syfte.

Det skulle innebära att dessa förberedelser görs i fredstid, vilket strider mot svensk lag.

Mot bakgrund av ovanstående skulle jag vilja fråga försvarsminister Peter Hultqvist:

1) Är ministerns bedömning att Sverige nu har skaffat den aktiva cyberförmåga som ska verka avskräckande på angripare?

2) Hur ser analysen ut av de juridiska svårigheterna och de folkrättsproblem ministern själv pekat på?

……

Stig Henriksson (V)

Överlämnas enligt uppdrag

Johan Welander