Motion till riksdagen
2010/11:Fö221

av Anna SteeleKarlström (FP)

Nytt vapenslag: e-krig/telekrig

Förslag till riksdagsbeslut

1. Riksdagen tillkännager för regeringen som sin mening vad som anförs i motionen om att man inom Försvarsmakten från existerande vapenslag bör organisera de enheter som huvudsakligen utför uppgifter relaterade till telekrig i ett nytt vapenslag: e-krig.
2. Riksdagen tillkännager för Regeringen som sin mening vad som anförs i motionen om att det nya vapenslaget e-krig bör få det huvudsakliga ansvaret i samhället i såväl fredstid som krigstid för en effektiv samverkan mellan samtliga civila och militära insatser relaterade till e-krig, telekrig, signalspaning, elförsörjning och datakommunikation.

Motivering

Det svenska samhället är mycket sårbart för störningar i infrastruktur av alla slag. Det gäller naturliga störningar av typen snö, is, stormar och aska från vulkanutbrott, men i allt högre grad också störningar i kommunikationsnät för datakommunikation och elförsörjning. Exempelvis anger Elsäkerhetsverket i en årsrapport för 2008 att ”den faktiska förmågan att klara en kris är osäker”[1]. Först år 2009 införde Elsäkerhetsverket en krisplan[2]. Konsekvenser av strö-

[1] ”Årsredovisning 2008”, Elsäkerhetsverket (http://www.elsakerhetsverket.se/Global/PDF/%C3%85rsredovisningar/%C3%85rsredovisning_2008_webb.pdf).
[2] ”Årsredovisning 2009”, Elsäkerhetsverket. (http://www.elsakerhetsverket.se/Global/PDF/%C3%85rsredovisningar/%C3%85rsredovisning_2009_webb.pdf).

mavbrott för exempelvis sjukvården kan studeras i ett exempel från Karolinska sjukhuset 2007[3].

Störningar i datorsystem av ”naturligt” slag, dvs. felaktigheter (”buggar”) i de system som finns i drift, visar sig några gånger per år då exempelvis någon av Sveriges större banker inte är tillgänglig för inloggning via Internet. Det brukar allt som oftast ge rubriker i olika medier, trots att skadan inte är större än att räkningarna för några hundra tusen personer betalas en dag eller två senare än normalt.

Störningar i datakommunikation kan också bero på den mänskliga faktorn, som exempelvis när kablar grävs av, eller som när samtliga webbadresser inom hela Sverige-domänen ”.se” blev onåbara en kort tid[4]. Konsekvenserna av kommunikationsavbrotten blir ofta stora på mobilteletrafik och på datakommunikation mellan privatpersoner, företag och offentliga verksamheter. Varje år utreder PTS ett tiotal haverier i teleoperatörernas datanät där konsekvenserna inte sällan varit att det är omöjligt att använda telefon, inklusive att nå larmnumret 112.

Intresset i världen för att skydda sig mot attacker på infrastruktur för el och kommunikation ökar. Under hösten 2010 finns rapporter om organiserade attacker på specifika system för drift av kärnkraftverk (”Stuxnet”)[5], och USA beslutade i juni 2009 att inrätta ”U.S. Cyber Command”, aktivt från maj 2010, som skall vara fullt operationsdugligt oktober 2010[6]. Ett dokument om en ny nationell säkerhetsstrategi för Storbritannien anger att telekrigföring ”kan ha förödande effekter i samhället genom att slå ut datanätverk som används för vital säkerhet, finanssystem och transporter”[7].

I Sverige finns ett civilt IT-incidentcentrum inom PTS, som skall flyttas till MSB från 1 januari 2011 enligt en statlig utredning[8]. När det gäller rent militär kapacitet finns den främst inom Telekrigbataljonen som är ett insatsförband inom Ledningsregementet i Enköping. De är exempelvis operativa i Afghanistan[9]. Till dessa kommer naturligtvis också de insatser som görs inom

[3] ”Strömavbrottet på Karolinska Universitetssjukhuset, Huddinge den 7 april 2007” (http://www.socialstyrelsen.se/Lists/Artikelkatalog/Attachments/8758/2008-126-15_200812616.pdf).

[4] ”Misstag slog ut .se-domänen”, branschorganisationen Elektronikbranschen, 2009-10-13 (http://www.elektronikbranschen.se/index.php?categoryid=45&articleid=5739).

[5] ”Svenska kraftbolag håller ögat på Stuxnet”, IDG (http://www.idg.se/2.1085/1.342931/svenska-kraftbolag-haller-ogat-pa-stuxnet).

[6] ”U.S. Cyber Command fact sheet”, United States Strategic Command (http://www.stratcom.mil/factsheets/cc/).

[7] ”UK warns on growing threat of cyberwar”, Financial Times, tisdag 19 oktober 2010, huvudartikel på förstasidan. Refererar till dokument gällande ny säkerhetsstrategi som publicerades 18 oktober 2010. Texten i artikeln lyder på engelska”… In a national security strategy document, published on Monday, the UK government said attacks in cyberspace ’could have a potentially devastating real world effect’ shutting down computer networks used to run vital security, financial and transport systems.”

[8] ”Lokalisering av Sveriges IT-incidentcentrum (Sitic)”, Försvarsdepartementet, 1 februari 2010 (http://www.regeringen.se/sb/d/108/a/138836).

[9] ”Telekrig”, Försvarsmaktens webbplatser ”Förband och förmågor/Förband/Ledningsregementet (LedR)/Telekrig” (http://www.forsvarsmakten.se/ledr/Telekrig/).

övriga vapenslag samt av FRA och Säkerhetspolisen gällande olika former av signalspaning och avlyssning.

Kapacitetsuppbyggnaden i Sverige inom telekrigsområdet har skett under lång tid. Den har skett inom respektive vapenslag (Flygvapnet, Marinen, Armén) samt civila myndigheter som FRA och Säkerhetspolisen. De hot som idag diskuteras gäller främst det civila samhället och dess sårbarhet, och tiden kan vara mogen för att även Sverige skapar en mer sammanhållen struktur för att möta dessa hot.

Namnet på området för e-krig är på engelska ”electronic warfare”, vilket möjligen bättre översätts med ”e-krig” än ”telekrig” eftersom det omfattar all typ av elektrisk och elektromagnetisk verksamhet, såsom strömförsörjning, radar, mikrovågor, trådbunden datakommunikation osv. I USA indelas e-krig militärt i tre huvudområden: e-anfall, e-skydd, e-krigsunderstöd[10].

Det traditionella territoriella hotet mot Sverige har Försvarsmakten alltid haft till uppgift att bemöta. Riskerna kring dagens olika infrastrukturer för elförsörjning, betalningsöverföringar, värdepappershandel, allmän företags- och myndighetskommunikation skiljer sig från de traditionella hoten eftersom de är åtkomliga på nya sätt: Att påverka dem kan göras med tekniker som är helt fristående från svenskt territorium.

Attacker mot infrastruktur via e-krigföring är asymmetriska på samma sätt som gerillakrigföring: En förhållandevis liten grupp människor kan till en förhållandevis begränsad kostnad åsamka ett samhälle oproportionerligt stor skada. Det behövs inte livlig fantasi för att inse hur Svenska banker skulle påverkas internationellt om Riksbankens system inte var nåbart under en vecka, eller hur illa Sverige skulle fungera om Svenska kraftnäts ledningscentraler inte fungerade under en februarivecka då stora delar av landet har under –15 grader C.

Den nya typen av hot kräver både ökade resurser och ett sammanhållet ansvar. Inom det här området ställs några för Sverige komplicerade principiella frågor på sin spets: Dels har Sverige som nation sedan skotten i Ådalen varit mycket ambivalent i frågor kring militära insatser i det civila samhället, med undantag av livräddande operationer (sjuktransporter, transport av vatten och mat vid stormar och snöoväder). Dels har Sverige dragit en gräns kring terroristhot och så här långt angett Säkerhetspolisen som ansvarig för att bemöta dessa, snarare än Försvarsmakten. Ingendera svåra principiella fråga bör stå i vägen för att det här området stärks kraftigt!

Ett angrepp på exempelvis den finansiella infrastrukturen är att likställa med ett territoriellt angrepp på Sverige, eftersom bådadera kan leda till en total kollaps av nationen. Därför är det av yttersta vikt att hot som kan utövas via e-krig, från annan nation eller annan aktör, kan bemötas med största möjliga kraft när så behövs, och att det förebyggande arbetet utgår från Försvarsmakten som har ett perspektiv av nationellt försvar.

[10] ”Electronic Warfare”, USA Joint Chiefs of Staff, Joint Publication 3-13.1, 2007-01-25. De tre huvudområdena bemämns på engelska Electronic attack (EA), Electronic Protection (EP), Electronic Warfare Support (ES) (http://www.fas.org/irp/doddir/dod/jp3-13-1.pdf).

Att etablera ett nytt vapenslag är ingen okomplicerad fråga. Med tanke på hur omvärlden agerat och beskriver de risker som finns är det hög tid att Sverige kan bli ett av föregångsländerna på det här området och sätta fokus på samordnat preventivt arbete. Det skulle kraftigt minska risken för att Sverige måste bemöta redan inträffade allvarliga händelser reaktivt, utan samordning och utan övergripande kontroll.

Stockholm den 22 oktober 2010

Anna SteeleKarlström (FP)