Säkerhet i cybermiljön

Johan Sigholm
Militärtekniska avdelningen
Militärvetenskapliga institutionen

Sammanfattning

Den snabba utvecklingen inom IT-området under de senaste decennierna har haft stor betydelse för Försvarsmaktens verksamhet men har samtidigt även inneburit många nya möjligheter för det civila samhället. I synnerhet har framsteg inom sensorteknik, datateknik och kommunikationsteknik inneburit att man idag kan inhämta, överföra, lagra och analysera stora mängder data på ett snabbare och mer effektivt sätt än tidigare. Detta har kommit till nytta inom bland annat system för ledningsstöd, stridsledning, underrättelsetjänst och logistik.

På samma gång har dock komplexiteten, de inbördes systemberoendena och volymerna data som hanteras i informationssystemen ökat kraftigt. I kombination med att karaktären på Försvarsmaktens verksamhet medför särskilda krav på systemsäkerhet och skydd mot antagonistiska hot, är upprätthållandet av en tillräcklig säkerhetsnivå i cybermiljön en utmaning. Att kunna skydda viktiga informationstillgångar mot förekommande risker är samtidigt en nödvändighet för att den nya tekniken ska kunna bidra till militär nytta. Förmågan att kunna verka i cybermiljön måste utvecklas och regelbundet tränas i fredstid, för att denna ska kunna stå till förfogande vid behov.

Försvarsmakten är på väg mot en högre grad av mognad och förståelse för cybermiljöns förutsättningar och krav. Det krävs dock ett kontinuerligt arbete inom flera områden för att cybermiljön och de system som ingår i denna ska bidra till en reell effekt. De aspekter som belyses i denna rapport bedöms vara av särskild vikt.

Inledning

Denna rapport identifierar och beskriver ett antal aspekter som bedöms vara betydelsefulla för att kunna upprätthålla en godtagbar säkerhetsnivå i cybermiljön. Rapporten fokuserar i detta avseende främst på de behov och utmaningar som bedöms vara relevanta för Försvarsmakten.

De aspekter som belyses i denna rapport som bedöms vara av särskild vikt berör områdena: informationshantering, systemutveckling, hot och aktörer, samverkan, infrastrukturer för information, rättsliga aspekter och helhetssyn.

Bakgrund

Under senare delen av 1990-talet beskrevs ofta de möjligheter som den snabba civila utvecklingen inom informationsteknik då kommit att medge som ett tekniskt-taktiskt paradigmskifte för militär verksamhet, ett så kallat *Revolution in Military Affairs* (RMA). Man jämförde bland annat denna snabba utveckling inom ledning av väpnad strid med pansarvapnets framväxt som en konsekvens av den civila bilismen, samt hur den nazityska arméns senare utnyttjande detta för rörlig anfallsstrid på ett för tiden revolutionerande sätt.[1] Inom Försvarsmakten konkretiserades dessa tankar under början av 2000-talet genom

[1] Svensson, 1999

utvecklingskonceptet Nätverksbaserat försvar (NBF), samt försöks- och utvecklingsverksamhet inom Ledsyst-projektet. Huvudsyftena med denna verksamhet var att, genom att införa avancerade IT-baserade stödsystem samt anamma ett processinriktat arbetssätt, uppnå en högre total effekt av de insatta militära resurserna och öka effektiviteten i försvarsförmågan.

Senare studier av denna utveckling konstaterar emellertid att NBF-konceptet blev för teoretiskt, att ansvars- och lydnadsförhållandena blev oklara i den nya organisationen, samt att det fanns en övertro till vad civil, kommersiell informationsteknik kunde åstadkomma.[2] I kombination med ekonomiska neddragningar, samt beslutet om att delta i EU:s snabbinsatsstyrka (NBG-08), blev resultatet att implementeringen av konceptet NBF kom att helt avbrytas år 2006.

Flera av de erfarenheter som drogs under denna tid kom dock att leva vidare, såsom trenden att flera mindre, specialiserade och plattformsspecifika system ersatts av ett fåtal större, som exempelvis PRIO, SWECCIS och Stridsledningssystem bataljon (SLB). Dessa mer generella system har istället utvecklats som *system av system*, där helheten byggs upp av olika moduler vilka kan uppgraderas och förändras oberoende av varandra. På detta sätt minskas risken för att utvecklingen av systemen försenas och överskrider budget.

Utvecklingen och utbredningen av informations- och kommunikationsteknik, i synnerhet internet, har lett till att det i dagsläget är såväl enkelt som billigt att ”koppla upp” de flesta typer av tekniska produkter. Detta gäller allt ifrån traditionella hemdatorer till stora industriella system som kan vara av samhällskritisk betydelse. Att ett system har en internetanslutning kan även ibland krävas för att kunna erhålla olika systemuppdateringar och andra stödtjänster från produktens leverantör. Av denna anledning skapas nätverk av alltmer sammankopplade system, vilket medför såväl möjligheter som stora utmaningar vad gäller säkerhet. Den ”miljö” eller ”arena” som uppstår då nätverken breder ut sig ges ibland olika namn beroende på vilket perspektiv man anlägger.

Utveckling och definitioner

Frågan om hur man ska definiera det sammanhang som skapas genom att allt fler system ansluts till internet eller motsvarande parallella informationsinfrastrukturer är vanligt förekommande och ibland uppstår därför en viss begreppsförvirring.[3,4] I Försvarsmaktens Grundsyn informationsoperationer[5] definierades begreppet *informationsarenan*, vilken senare utvecklades till *informationsmiljön* i Försvarsmaktens Handbok Informationsoperationer [6] och Militärstrategisk doktrin, 2012 års utgåva.[7]

Det pågår dock för närvarande ett arbete inom Högkvarteret med att vidareutveckla begreppet informationsmiljön till ett nytt – *cybermiljön*. Syftet är dels att harmonisera det svenska begreppet med det inom NATO vedertagna ”cyberspace”, men även att betona att man i större grad även åsyftar ett stridsrum i vilket reella militära effekter kan uppnås och specifika förmågor definieras. Försvarsmaktens förmåga i cybermiljön lämnar således, tillsammans med förmågor inom de traditionella miljöerna (mark, hav, luft och rymd), ett bidrag till den samlade operativa förmågan. Då denna rapport fokuserar på nyttan för Försvarsmakten

[2] Hamberg, 2010
[3] Lundholm et al., 2011
[4] Biverot, 2012
[5] Försvarsmakten, 2007a
[6] Försvarsmakten, 2008
[7] Försvarsmakten, 2011

kommer begreppet cybermiljö användas istället för informationsmiljö, då det senare i större utsträckning beskriver kognitiva aspekter.

Cybermiljön avser här den IT-miljö som direkt eller indirekt sammankopplar informationssystem och nätverk, men även själva de fysiska systemen och nätverken i sig. Den virtuella delen av cybermiljön är global och gränsöverskridande, medan den fysiska delen är bunden till en viss geografisk plats och består av den tekniska utrustning och infrastruktur som används för att inhämta, överföra, bearbeta, lagra och presentera information. Cybermiljön är tillgänglig via olika tekniska system och är beroende av mänsklig interaktion för konfiguration och styrning.

Militär nytta

Försvarsmakten identifierar idag information som en av sina viktigaste tillgångar och som en förutsättning för att kunna bedriva verksamheten.[8] En av anledningarna till att information har så stor betydelse är, som militärhistorien har visat, att den part i en konflikt som snabbast lyckas skapa ett informationsöverläge även ofta är den som gått segrande ur striden.[9] För att bli användbar måste dock informationen kunna samlas in, bearbetas, distribueras och lagras – något som vanligtvis sker med hjälp av ett informationssystem. Genom ett sådant system kan informationen även förädlas och fusioneras för att därigenom kunna bidra till en förståelse för den situation man befinner sig i. Först då kan en lägesbild erhållas, vilken medger effektiv ledning av insatta resurser.

Sett ur ett utvecklingsperspektiv innebär detta att komplexiteten i teknik som används för militär ledning ofta är hög. Förutom att militära system för ledning innehåller avancerade funktioner ställs det höga krav på kvalitet (bl.a. systemsäkerhet, användbarhet och informationssäkerhet) jämfört med exempelvis civila affärssystem eller olika industriella styr- och övervakningssystem. Till skillnad från många civila tillämpningar ställs ofta höga krav även på maskinvaran i systemet då den ska användas i speciella och krävande miljöer som i stridsfordon, på fartyg eller i flygplan.

En effektiv operation kräver avancerade realtidssystem för samordning mellan de grundläggande militära förmågorna, såsom nätverk för ledning, underrättelser och sensordata. En stor utmaning är att dels skapa en acceptabel nivå av säkerhet i dessa system, utan att på grund av detta begränsa dess effektivitet, samtidigt som de kan användas i situationer som kräver nationell- eller internationell samverkan. För att uppnå militär nytta av framtida system, tjänster och funktioner i cybermiljön som Försvarsmakten nyttjar krävs därför kontinuerlig visshet om att informationssäkerheten kan upprätthållas, samtidigt som aspekter såsom användbarhet, effektivitet, legalitet, tilltro, acceptans, personlig integritet och kostnadsutveckling beaktas.

Informationssäkerhet

När internet först utvecklades under 1970- och 1980-talen var säkerheten inte i huvudsakligt fokus. Egenskaper som effektivitet, transparens och flexibilitet prioriterades snarare än möjlighet till kontroll över den överförda informationens innehåll, dess riktighet, identitet på sändare och mottagare, samt garantier för tjänstekvalitet och tillgänglighet. Denna öppna approach har starkt bidragit till internets snabba tillväxt och till att göra tekniken attraktiv för såväl företag som privatpersoner, men har samtidigt öppnat för destruktiva beteenden, där

[8] Försvarsmakten, 2006
[9] Nylander, 2009

ondsinta aktörer kan välja mål, metod och medel för olika former av angrepp. På grund av cybermiljöns natur kan dessa angrepp ske på stora avstånd, dolt, relativt enkelt och billigt, samtidigt som aktörerna kan vara svåra att identifiera. Behovet av att skydda de informationstillgångar som finns åtkomliga i eller genom cybermiljön är därför i dagsläget en angelägen utmaning.

Begreppet informationssäkerhet innefattar två huvudsakliga delar – *administrativ säkerhet* och *teknisk säkerhet*. Försvarsmaktens gällande definition av informationssäkerhet avser att information ska finnas tillgänglig när den behövs, att den är och förblir riktig, att den endast är tillgänglig för den som är behörig att ta del av och använda den, samt att hanteringen av informationen är spårbar.[10] Det övergripande målet med att upprätthålla informationssäkerhet är att säkerställa ett tillräckligt skydd för myndighetens informationstillgångar såväl inom som utom landet, så att rätt information är tillgänglig för rätt person i rätt tid på ett spårbart sätt.[11]

Historiskt har stort fokus lagts på de tekniska aspekterna av informationssäkerheten, såsom system för behörighetskontroll, antivirusprogramvara och skydd mot röjande signaler. Den administrativa säkerheten är dock lika viktig, där komponenter som regelverk, rutiner och utbildning ingår. Speciellt tydligt blir detta eftersom det ofta är människan som är den svagaste länken i informationssäkerhetskedjan.[12] Då det är de enskilda medarbetarna som ansvarar för att hantera tekniken måste dessa bibringas kunskap och förståelse för teknikens möjligheter och begränsningar, samt ges adekvat utbildning på hur systemen utnyttjas på bästa sätt som stöd för operationer.

Det måste även finnas en lyhördhet gentemot slutanvändarna, så att erfarenheter av brister och outnyttjad potential kan tas omhand i framtida uppgraderingar och vidareutvecklingsarbeten. I jämförelse med att skydda informationstillgångar mot externa hot är det vanligtvis mycket svårare att skydda dessa mot det så kallade *insiderhotet*, d.v.s. hotet från att en betrodd användare medvetet eller omedvetet exponerar tillgången. Detta har nyligen blivit aktuellt genom de informationsläckor som utförts av Bradley Manning och Edward Snowden.

En vidare utmaning är att kunna upprätthålla en tillräckligt hög grad av tillit till den information som finns i informationssystemen, vilket är av stor vikt för användarnas tilltro till systemen, i synnerhet i pressade och tidskritiska situationer, samtidigt som dessa uppfyller användarnas krav på tillgänglighet och användbarhet. Exempel på system som kan riskera att ratas av användare är kommunikationssystem som har för omständliga krypteringsfunktioner eller vilka endast kan användas på vissa i förväg bestämda geografiska platser.

Försvarsmaktens informationssystem måste även bidra till att stödja verksamhetens syfte och mål, så att inte denna måste anpassa sig efter de tekniska systemen. Om detta inte uppnås kan säkerheten hotas genom att användaren väljer andra, mindre säkra verktyg eller kommunikationsformer, regler och rutiner till trots. Utmaningarna blir även särskilt tydliga genom påbudet att Försvarsmakten i ökande grad ska implementera civilt utvecklad teknik. Detta eftersom civila produkter ofta inte är designade med avseende på militära krav och förutsättningar utan måste anpassas för att leva upp till gällande regelverk, något som kan bli såväl kostsamt som tidskrävande.

[10] Försvarsmakten, 2007b, s.38
[11] Försvarsmakten, 2006, s.187
[12] Försvarsmakten, 2007b, s.35

Antagonistiska hot

Antalet avsiktliga intrång och intrångsförsök i cybermiljön ökar ständigt och de bakomliggande avsikterna är många. En trend som tidigare kunnat urskiljas är att den tidigare så vanliga drivkraften bakom angreppen, nyfikenhet och viljan att demonstrera teknisk expertis, alltmer övergått i en strävan efter ekonomisk eller politisk vinning. Attackerna har övergått från att i princip ha varit relativt oskyldiga ”pojkstreck”, mot att bli alltmer fokuserade på organiserad, ekonomisk brottslighet. På senare år har dock angrepp i syfte att komma över information som gynnar nationella intressen vuxit. Det rör sig alltså om en form av spionage, vilken med hjälp av cybermiljön kan genomföras på distans, i skydd av anonymitet och till en relativt låg kostnad. Angreppen är vanligtvis fokuserade mot enskilda företag, organisationer eller myndigheter i syfte att komma över företagshemligheter, sekretessbelagda dokument tillhörande militär eller statliga myndigheter, resultat från forskning och utveckling, insiderinformation, dokument rörande internationella upphandlingar, eller tekniska resurser såsom källkod.

I dagsläget används i stor utsträckning traditionellt passiva tekniska funktioner för att skydda informationstillgångar på många myndigheter och företag. Det rör sig ofta om olika former av trafikfilter, såsom brandväggar och system för intrångsdetektering, och applikationer för detektion och oskadliggörande av främmande kod, såsom antivirusprogramvara. Trots att dessa funktioner i och för sig fortfarande är nödvändiga för att hindra att tillgångar exponeras som konsekvens av vanligt förekommande hot, är de inte tillräckliga för att förhindra ett angrepp från en antagonist som använder sig av avancerade metoder. Genom kunskap om ännu inte tilltäppta säkerhetsluckor i operativsystem eller tredjepartsprogramvara, i kombination med förfalskade digitala certifikat och omdirigering av nätverkstrafik, kan en angripare med stora ekonomiska resurser kringgå de flesta skydd som idag finns tillgängliga. Det krävs därför nya, tvärvetenskapliga metoder och tekniker för att möta dessa framväxande hot, för att erhålla en förmåga till effektivt cyberkontraspionage.[13] Dessa nya hotbilder växer fram samtidigt som den traditionella problematiken med virus, maskar, trojaner, överbelastningsattacker m.m. alltjämt består.

Samverkan och interoperabilitet

En av insatsförsvarets uppgifter är att värna civilbefolkningen och under svåra påfrestningar säkerställa de viktigaste samhällsfunktionerna. Denna uppgift ställer krav på att Försvarsmakten, under såväl fredstid som under olika former av oroligheter och påfrestningar, kan kommunicera och samverka med andra myndigheter, organisationer, och internationella partners. Då cybermiljön har en tydlig internationell karaktär där hot, risker och olika former för angrepp till delar är gemensamma och ständigt utvecklas i snabb takt är det väsentligt att Försvarsmakten är en aktiv part inom ramen för internationellt samarbete. Sådant samarbete behöver omfatta såväl ömsesidig delgivning av inträffade incidenter och dragna erfarenheter som utveckling av system, medel och metoder.

Samverkan kan dels ske genom i förväg upprättade och ackrediterade informationskanaler, men kommer sannolikt i framtida insatser alltmer ske genom hastigt upprättade nätverk, så kallade ”Hastily Formed Networks”.[14] Sådana nätverk utgör exempel på ett område där avancerad nätverksteknik och organisation av humanitära insatser möts. Nätens förmåga att fungera effektivt i krissituationer är beroende av forskning, planering och förberedelser inom dels områden som organisationsteori, sociologi och ledningsvetenskap, men även inom

[13] Sigholm & Bang, 2013
[14] Sigholm, 2010

datalogi, informationsteknologi och -säkerhet. Då denna typ av verksamhet troligtvis kommer att öka i betydelse för Försvarsmakten i framtiden, är det ett angeläget område att bevaka. Införande av dynamiska säkerhetsfunktioner, som genom riskhantering bland annat medger justering för balans mellan säkerhet, effektivitet och personlig integritet, är även ett område som kan komma att bidra till såväl flexibilitet och effektivitet i framtida operationer.[15]

Det finns även många beröringspunkter med andra samverkansoperationer, i både nationell och internationell miljö, där det finns behov av kommunikation och informationsutbyte med allierade parter. Många av de hot och risker som kan drabba samhället genom angrepp i cybermiljön kan riktas mot verksamhet som inte har med Försvarsmakten att göra. Sådana angrepp kan få indirekta konsekvenser för Försvarsmakten men framförallt skada andra samhällsfunktioner och svenska intressen. Det är därför nödvändigt att Försvarsmakten tillsammans med andra myndigheter gemensamt utvecklar förmågan att skydda samhället från angrepp i cybermiljön. Myndigheten för samhällsskydd och beredskap har det övergripande ansvaret för samordning av sådan förmåga. Vad avser underrättelse- och säkerhetstjänst är Försvarsmaktens samverkan med Försvarets radioanstalt och Säkerhetspolisen av särskilt stor betydelse.

En stor del av Försvarsmaktens verksamhet i cybermiljön är beroende av infrastruktur som ägs av privata svenska och utländska aktörer. Det är därför av stor betydelse att Försvarsmakten säkerställer att dessa aktörer kan och kommer att leverera de tjänster som erfordras för Försvarsmaktens verksamhet i samtliga konfliktnivåer. Det finns även ett behov av att kontinuerligt undersöka vilka konsekvenser olika sammanlänkningar av militära och civila informationssystem får för informationssäkerheten.

Nya infrastrukturer för information

I framtiden kommer sannolikt allt hårdare krav ställas på Försvarsmakten att leverera ett användbart, flexibelt och kostnadseffektivt försvar. Som ett led i denna omställning måste allt fler uppgifter lösas av allt färre personer, samtidigt som graden av komplexitet och specialisering ökar. För att åstadkomma detta måste olika nya tekniker tas i bruk. Ett exempel är en utökad användning av obemannade farkoster för uppgifter som spaning och inhämtning av underrättelser. Ett annat exempel är den enskilde soldaten i fält, som med olika tekniska hjälpmedel ska kunna göras allt mer effektiv.

För att förbanden i ovan givna exempel ska kunna lösa sina uppgifter krävs avancerade system, för information, ledning och verkan, såsom positionsangivelser, överföring av sensordata, underrättelserapportering osv. Traditionellt används radio- eller trådburen kommunikation för detta ändamål, men i fientliga eller störda miljöer, eller i områden där täckning saknas, är det önskvärt att enskilda enheter kan ansluta sig till varandra och skapa lokala, temporära nätverk för direktkommunikation. Denna typ av spontana nätverk, vanligen kallade Ad-hoc-nät, har visat sig vara effektiva i många sammanhang. Främst gäller detta miljöer med många rörliga enheter, där det finns systembegränsningar i form av exempelvis tillgång till bandbredd, arbetsminne eller strömförsörjning, och där alla enheter har ett kommunikationsbehov, men inte nödvändigtvis har direktkontakt med en basstation.

Det bedrivs en hel del forskning runt om i världen inom området mobila Ad-hoc-nät (förkortat MANET), främst vad det gäller att ta fram robusta och effektiva protokoll för nätstyrning. Precis som vid internets initiala utveckling utgick mycket av forskningen inom Ad-hoc-nät ursprungligen från antagandet att näten befann sig i en vänligt inställd miljö, där alla noder

[15] Sigholm & Andersson, 2011

samarbetade efter bästa förmåga. Det är först på senare tid som frågor har väckts angående säkerheten i Ad-hoc-näten, när dessa upprättas i miljöer där noder med fientliga avsikter existerar. Behovet av att bedriva utökad och fördjupad forskning på detta område är därför stort. Problem som är intressanta och viktiga att studera är hur man kan säkerställa sekretess, integritet och tillgänglighet då Ad-hoc-tekniker används i militära tillämpningar, under operationer i potentiellt fientliga miljöer, av obemannade system eller vid enskild soldats kommunikation. Samtidigt är det, mot bakgrund av tidigare erfarenheter, av betydelse att förväntningarna på vad tekniska system, såsom Ad-hoc-nät och mjukvarubaserad radio, ska kunna åstadkomma är realistiska och verklighetsförankrade.[16]

Trots att man sedan tidigare har lyckats ta fram relativt effektiva algoritmer för intrångsdetektering så återstår flera utmaningar med att anpassa dessa för specifika, specialiserade system, såsom Hastily Formed Networks och system för övervakning och styrning av elnät, vattendistribution m.m. (så kallade SCADA-system). Ett viktigt mål är därför att utreda de speciella behov som finns här, och göra analyser av trafikmönster, för att på så sätt kunna generera en modell, med relevanta testdata, genom vilken men kan göra åtskillnad mellan legitim och illegitim nätverkstrafik.

Aktörer

Cybermiljön är en global arena, tillgänglig för i princip vem som helst som har tillgång till en internetansluten dator, en smart mobiltelefon eller någon annan sorts uppkopplad IT-utrustning. I denna miljö existerar många olika sorters aktörer, alla med olika behov, intressen, mål och intentioner. Några agerar individuellt, andra i löst sammansatta grupperingar eller i mer formella strukturer. Rollerna kan också variera beroende på den aktuella situationen och kan överlappa mellan olika aktörskategorier. Aktörer kan även röra sig mellan olika kategorier över tiden, beroende på hur deras mål och övriga förutsättningar förändras.

De positiva konsekvenserna av cybermiljöns utbredning till trots så har denna samtidigt utvecklats till en arena för konflikter, såväl små som stora. Utöver protester, virtuell vandalism och annan vanligt förekommande vardagsbrottslighet som spiller över i denna miljö, såsom trakasserier, bedrägerier och upphovsrättsbrott förekommer även allvarligare organiserad brottslighet. Denna inkluderar bland annat pengatvätt, omfattande handel med stulna kreditkortsuppgifter och kapade identiteter, drogrelaterad verksamhet, trafficking och terrorism. Länder och regioner som har en avancerad informationsinfrastruktur är särskilt sårbara för denna verksamhet.

En annan trend som kan skönjas är att allt fler av de dataintrång som genomförs syftar till att främja nationella intressen. Enligt den årliga rapporten ”Data Breach Investigations Report”[17], sammanställd av det amerikanska telekombolaget Verizon, är nu statligt sponsrade informationsstölder och spionage i cybermiljön den näst vanligaste orsaken till intrång som genomförts under det gångna året, näst efter ekonomisk brottslighet. Aktörerna inom denna kategori, ibland även kallade cyberspioner, drivs inte av något kortsiktigt ekonomiskt incitament utan är snarare intresserade av att komma över information som gynnar nationella intressen. Trots att länder som Kina och Ryssland ofta i media pekats ut som de stora spelarna inom denna kategori har den senaste tidens avslöjanden, som ett resultat av den information som läckts av Edward Snowden, antytt att även västländer som USA och Storbritannien avsätter avsevärda resurser för att uppnå effekt genom operationer i cybermiljön.

[16] Sigholm & Raciti, 2012
[17] Verizon, 2013, s.21

Tabell 1 nedan sammanställer de viktigaste aktörerna i cybermiljön, grupperade i kategorier efter motiv, mål, samt använda medel och metod. Aktörskategorierna finns även närmare beskrivna i en tidigare publicerad artikel.[18]

Aktör	Motiv	Mål	Metod/medel
Vanliga medborgare	Inget (eller svagt)	Godtyckligt	Indirekt
Script kiddies	Nyfikenhet, spänning, ego	Individer, företag, myndigheter	Förtillverkade skript och verktyg
Hacktivister	Politiska, eller social förändring	Beslutsfattare, helt godtyckliga mål	Protester genom vanställande av webbsidor eller överbelastnings-attacker
Svarthatts-hackare	Ego, personligt agg, ekonomisk vinning	Godtyckligt	Skadlig kod, virus, utnyttjande av okända sårbarheter
Vithattshackare	Idealism, kreativitet, laglydighet	Godtyckligt	Penetrationstestning, tilltäppning av luckor och rättande av sårbarheter
Gråhattshackare	Tvetydiga	Godtyckligt	Varierande
Patriotiska hackare	Patriotism	Motståndare till den egna staten	Överbelastningsattacker, vanställande av webbsidor
Insiders	Ekonomisk vinning, hämnd, bitterhet	Arbetsgivare	Social ingenjörskonst, bakdörrar, manipulation
Terrorister	Politiska, eller social förändring	Oskyldiga offer	Datorbaserat våld eller materiell förstörelse
Författare av skadlig kod	Ekonomisk vinning, ego, personligt agg	Godtyckligt	Utnyttjande av olika orättade sårbarheter
Bedragare	Ekonomisk vinning	Individer, småföretagare	Social ingenjörskonst
Organiserad brottslighet	Ekonomisk vinning	Individer, företag	Skadlig kod, identitetsstöld, överbelastningsattacker
Företag	Ekonomisk vinning	IT-baserade system och infrastrukturer (privata eller publika)	Olika tekniker för angrepp, påverkan eller underlättande av operationer
Spioner och agenter	Politiska eller ekonomisk vinning	Individer, företag, statliga institutioner	Olika tekniker för att komma over information
Hemvärn/milis	Patriotism, personlig utveckling	Motståndare till den egna staten	Baseras på gruppens gemensamma förmågor

Tabell 1. Aktörer i cybermiljön

Rättsliga aspekter

I de flesta länder regleras verksamhet som bedrivs i eller med hjälp av cybermiljön av nationell lagstiftning. När det gäller militär användning av cybermiljön är dock rättsläget något mer oklart. Det föreligger en bred acceptans för att regler och principer för krigföring i internationell rätt t.ex. Genèvekonventionerna är tillämpliga även på väpnade konflikter som utspelas i cybermiljön. Moderna tolkningsbidrag av reglerna anpassade till cybermiljön har även kommit på senare tid genom t.ex. *The Tallinn Manual on the International Law Applicable to Cyber Warfare*).[19] Däremot saknas fortfarande tydliga internationella konventioner och uppförandekoder för militär verksamhet i cybermiljön i situationer som ligger under tröskeln för en väpnad konflikt. Detta innebär att statligt sponsrade aktörer kan sträva efter att utnyttja cybermiljön i syfte att nå egna säkerhets- eller utrikespolitiska mål. Internationella avtal skulle kunna begränsa hur stater kan använda cybermiljön i antagonistiska syften och hur dessa samarbetar om olika hot och vid upptäckt av överträdelser i det överenskomna regelverket. En utmaning är dock att det sannolikt är svårt att kunna

[18] Sigholm, 2013
[19] Schmitt, 2013

genomföra kontroller av hur regelverken efterlevs, samt ännu svårare att implementera konsekvenser av identifierade överträdelser.

De rättsliga förutsättningarna för Försvarsmaktens mandat inom cyberområdet utgörs, i allt väsentligt, av att utveckla och vidmakthålla ett militärt försvar som ska kunna agera inom cybermiljön, med de begränsningar som Sveriges folkrättsliga åtaganden under krig och väpnad konflikt ger. I första hand avses krigets folkrätt (se 15 kap. 13 § Regeringsformen). Försvarsmaktens uppgifter inom cyberområdet måste stå i överensstämmelse med de åligganden som där anges. Försvarsmakten kan endast vidta aktiva motåtgärder på cyberområdet som kan kopplas till underrättelse- och säkerhetstjänst, krigföring, hävdandet av Sveriges territorium, eller värnandet av Sveriges suveräna rättigheter och nationella intressen. Regeringen har inte gett Försvarsmakten något särskilt uppdrag att värna Sveriges nationella intressen utomlands genom insatser på cyberområdet.

Försvarsmaktens fredstida uppgifter i cyberområdet är alltså i realiteten begränsade till underrättelse- och säkerhetstjänst och förutsättningar för att ingripa aktivt på cyberområdet saknas vid hävdandet av Sveriges territorium och vid värnandet av Sveriges nationella intressen utanför landets gränser. Eftersom såväl defensiva som offensiva militära insatser i cybermiljön kan krävas även i andra delar av konfliktskalan än krig, exempelvis som stöd till att uppnå olika säkerhetspolitiska effekter, finns ett behov av ett juridiskt regelverk som styr verksamheten i även dessa situationer. Förmågan att kunna verka i cybermiljön måste dock likväl utvecklas och regelbundet tränas i fredstid, för att denna ska kunna stå till förfogande vid behov.

Diskussion och slutsatser

Cybermiljön är komplex och verksamhet som bedrivs i eller med hjälp av denna påverkas av ett flertal olika faktorer. För Försvarsmaktens vidkommande är det främsta målet med att använda cybermiljön att få effektiv tillgång till och användande av information, i syfte att upprätthålla och utveckla ett militärt försvar. Grunden för detta är förmågan att leda och föra väpnad strid, vilken även innefattar cybermiljön. Förmågan ska vara tillgänglig och användbar samt successivt utvecklas i paritet med omvärlden, samt ska i likhet med andra förmågor även kunna ställas till samhällets förfogande i händelse av andra samhällskriser än krig.

Att uppnå en tillräcklig grad av säkerhet i cybermiljön är, som vi har sett ovan, av avgörande betydelse för att de existerande förmågorna ska kunna resultera i militär nytta. Om informationssystemen kan påverkas så att sekretess, riktighet eller tillgänglighet av informationstillgångarna inte längre kan garanteras, minskar användbarheten av systemen helt eller delvis. Samtidigt kan en överdriven implementering av olika säkerhetsfunktioner även bidra till att nyttan minskar, då systemen blir orimligt svåra för användaren att förstå eller hantera, eller ineffektiva vid lösandet av en given uppgift. Det krävs därför en noggrann analys av såväl den teknik som de regelverk och policys som implementeras i verksamheten för att resultatet ska bli acceptabelt och för att maximera den militära nyttan.

Försvarsmakten är på väg mot en högre grad av mognad och förståelse för cybermiljöns förutsättningar och krav. Det krävs dock ett kontinuerligt arbete inom flera områden för att cybermiljön och de system som ingår i denna ska bidra till en reell effekt. De aspekter som belysts i denna rapport bedöms här vara av särskild vikt:

- **Informationshantering**. Information är en av Försvarsmaktens viktigaste tillgångar och en förutsättning för att verksamheten ska kunna genomföras. Läckage av skyddsvärd information måste förhindras för att undvika allvarliga men, samtidigt som den alltid ska

vara tillgänglig för behöriga personer vid behov. Information ska kunna flöda sömlöst mellan olika egna system, samt kunna utbytas med samarbetspartners på ett kontrollerat vis.

- **Systemutveckling**. Erfarenheten från tidigare utveckling av informationssystem inom Försvarsmakten visar att dessa bör utvecklas etappvis, i moduler, samt ha ett tydligt användarfokus, för att kunna ge militär nytta. Systemen måste även vara användarvänliga och de regelverk som omgärdar dem får inte göra dem ineffektiva. Tillitens till systemens informationsinnehåll, funktionalitet och tillgänglighet måste även kunna upprätthållas i de olika situationer och miljöer där nyttjas.

- **Hot och aktörer**. Hoten som riktas mot Försvarsmakten i cybermiljön blir alltmer avancerade och kan riktas från många olika typer av aktörer. En trend som kan skönjas är att angrepp allt oftare emanerar från resursstarka aktörer, sannolikt i åtnjutande av statligt stöd. Försvarsmakten måste därför kontinuerligt följa utvecklingen och utveckla såväl en defensiv som en offensiv förmåga i cybermiljön. Det krävs även ett förebyggande arbete i syfte att minska risken för angrepp eller informationsläckage som en följd av insiderproblematik.

- **Samverkan**. Många av de hot och risker som kan drabba samhället genom angrepp i cybermiljön kan riktas mot verksamhet som inte har med Försvarsmakten att göra. Detta kräver att Försvarsmakten är en aktiv samarbetspartner till såväl externa myndigheter och företag som ansvarar för drift och underhåll av samhällskritiska infrastrukturer, samt tillsammans med dessa organisationer utvecklar förmågan att skydda samhället från angrepp i cybermiljön. Ett utökat samarbete med de nordiska grannländerna och EU när det gäller cyberförsvarsförmåga bör vara prioriterat, särskild mot bakgrund av den av Sverige uttryckta solidaritetsdeklarationen.

- **Infrastrukturer för information**. Utvecklingen av nya avancerade tekniska plattformar, såsom trådlösa sensornätverk och obemannade farkoster, driver även på implementering av nya infrastrukturer för kommunikation. I detta sammanhang bör Försvarsmakten därför studera hur säkerhet kan upprätthållas i framväxande tekniker såsom mjukvarubaserad radio och mobila Ad-hoc-nätverk.

- **Rättsliga aspekter**. Det saknas i dagsläget tydliga internationella konventioner och uppförandekoder för militär verksamhet i cybermiljön under tröskeln för väpnad konflikt. Det oklara läget kan utnyttjas av antagonistiska krafter och Försvarsmakten bör därför ta initiativ till att stödja och påskynda ett internationellt arbete med en utveckling av folkrättsliga regelverk och standarder i syfte att gemensamt kunna hantera framväxande hot och risker. En förmåga att verka såväl defensivt som offensivt i cybermiljön måste vidare tränas regelbundet för att kunna användas i krig.

- **Helhetssyn**. Eftersom i stort sett alla förband och enheter i Försvarsmakten nyttjar cybermiljön måste förmågan att upprätthålla dess funktionalitet bli en integrerad del av Försvarsmaktens normala verksamhet. Grundläggande principer och metoder för militärstrategisk, operativ, taktisk och stridsteknisk planering, genomförande och uppföljning bör i framtiden även tillämpas med avseende på cybermiljön. Förmågor i cybermiljön bör även utvecklas med fokus på de dimensionerande hoten och riskerna.

Referenser

Biverot, E. (2012) *Cyber Security, Cyberkrigföring och Cyberförsvar i ett militärtekniskt perspektiv*, Teknisk prognos 2012, Försvarshögskolan.

Försvarsmakten (2006) *Handbok för Försvarsmaktens säkerhetstjänst, Informationsteknik (H SÄK IT)*, M7745-734062.

Försvarsmakten (2007a) *Grundsyn Informationsoperationer*, M7739-350004.

Försvarsmakten (2007b) *Handbok för Försvarsmaktens säkerhetstjänst, Säkerhetsskyddstjänst (H SÄK Skydd)*, M7739-352005.

Försvarsmakten (2008) *Försvarsmaktens Handbok Informationsoperationer*, M7739-352014.

Försvarsmakten (2011) *Militärstrategisk doktrin med doktrinära grunder (MSD 12)*, M7739-354023.

Hamberg, U. (2010) *NBF: Förmågan att se på andra sidan kullen eller ”Kejsarens nya kläder”*, C-uppsats, Försvarshögskolan.

Lundholm, K., Löfvenberg, J., Hunstad, A. & Karlzén, H. (2011) *Lägesbild på informationsarenan: Översikt och diskussion*, Totalförsvarets Forskningsinstitut, FOI-R--3240--SE.

Nylander, M. (2009) *Militärteknik för ledning*, i M. Reberg: ”Lärobok i Militärteknik, vol. 3: Teknik till stöd för ledning”, Försvarshögskolan.

Schmitt, M. (Gen. ed.) (2013) *Tallinn Manual on the International Law Applicable to Cyber Warfare*, Cambridge University Press.

Sigholm, J. & Andersson, D. (2011) *Privacy on the Battlefield? Ethical Issues of Emerging Military ICTs*, Proceedings of the 9th International Conference of Computer Ethics: Philosophical Enquiry (CEPE 2011).

Sigholm, J. & Bang, M. (2013) *Towards Offensive Cyber Counterintelligence: Adopting a Target-Centric View on Advanced Persistent Threats*, Proceedings of the 4th European Conference in Intelligence Security Informatics (EISIC 2013).

Sigholm, R. & Raciti, M. (2012) *Best-Effort Data Leakage Prevention in Inter-Organizational Tactical MANETs*, Proceedings of the 2012 IEEE Military Communications Conference.

Sigholm, J. (2010) *Reconfigurable Radio Systems: Towards Secure Collaboration for Peace Support and Public Safety*, Proceedings of the 9th European Conference on Information Warfare and Security (ECIW 2010).

Sigholm, J. (2013) *Non-State Actors in Cyberspace Operations*, Journal of Military Studies, vol. 4, no. 1.

Svensson, P. (1999) *Rad av misslyckade storprojekt visar att ledningssystem måste byggas etappvis*, FOA-tidningen, nr 4, 1999.

Verizon (2013) *2013 Data Breach Investigations report*.