# Aktiv cyberförmåga kräver cyberförståelse

*av Stefan Varga*

**Résumé**

The cyber domain is pervasive in modern society. Militaries are seeking cyber missions where there are both defensive and offensive possibilities. Cyber differs from other domains such as air, land and sea because it has an abstract logical layer that in a sense collapses space and time, making geography irrelevant, and enabling instant effects on attacked targets. The domain is complex and hard to describe. There is a need to develop an understanding of the domain and its opportunities. At a minimum, the Armed Forces need to have situational awareness, operational concepts that are aligned with overarching doctrine as well as deliberately designed resources with sufficient operational capabilities in order to be successful in the cyber mission.

ARTIKELN AVSER ATT belysa tre grundläggande frågor som sammantagna kan påvisa vad militär cyber kan omfatta, nämligen vad cybermiljön är, vad som händer i den och vad Försvarsmakten kan och bör göra i denna miljö. Ambitionen är att ge läsaren ett perspektiv på hur man kan betrakta cybermiljön, i stort påvisa vilka möjligheter cyberoperationer kan ge, samt ge några idéer till hur Försvarsmakten doktrinärt och förmågemässigt kan gå vidare med att etablera och bygga ut sin närvaro i miljön. Artikeln behandlar dator- och nätverksoperationer, särskilt cyberattacker.

Människor lever i ökande omfattning sina liv parallellt i det fysiska rummet och på ”nätet”, internet, med alla de bekväma informationsteknologiska, d v s IT-tjänster som finns tillgängliga där. Vi kan kommunicera med vänner, läsa tidningar, titta på filmer m m. I ena stunden kan uppmärksamheten riktas mot kassören i den lokala affären, för att i den andra riktas mot en vän i Japan som man kommunicerar med. Även i affärsvärlden är beroendet av modern kommunikationsteknologi stor, ibland av avgörande betydelse för hur affärer genomförs samt för hur varor och tjänster produceras, marknadsförs och distribueras. Ibland utgörs dessutom tjänsterna av internettjänster i sig. IT och modern kommunikationsteknologi i övrigt, IKT, utgör också ett betydande segment i ekonomin.

Ny teknologi gör att ekonomin omvandlas genom att gamla företag som inte förmår anpassa sig till omvärldens krav försvinner, samtidigt som nya tillkommer.[1] Exakt hur stor andel av ekonomin som kan hänföras till internet är dock svårt att säga. Att vårt moderna samhälle med sin komplexa struktur av flöden av exempelvis information, elenergi, vatten, varor och tjänster etc skulle kunna fungera tillfredsställande utan IKT är svårt att föreställa sig. Det är därför viktigt att ”nätet” fungerar på avsett vis.

Rationalisering av informationshantering, eller informationalisering som utvecklingen också kan kallas, är något som också pågår i många militära organisationer, inte bara i väst utan även i Kina[2] och Ryssland. En försmak av vad sådan informationalisering kan leda till kunde man få under Irakkriget 2003, där en utmärkt lägesuppfattning och ändamålsenliga ledningssystem med funk-

tionella sambands- och informationssystem medgav precisionsbekämpning och graderad verkan samt bekämpning av rörliga mål med avancerade vapensystem. Konkret kan effekten av informationalisering illustreras av skillnaden i träffsannolikhet[3] för en B-17 under andra världskriget som var 3 300 fot, och den för en F-117 med en laserguidad bomb under andra Irakkriget som var i storleksordningen tio fot.[4] Sedan dess har denna utveckling fortsatt.

## Cybertermer

Artiklar som handlar om cyber brukar ofta inledas med ett förord som innehåller begreppsdefinitioner. Men tyvärr har nästan inga gängse globalt accepterade definitioner av så kallade cybertermer.[5] Stater[6] och organisationer definierar och tolkar cyber annorlunda. Generellt verkar termen användas som ett prefix som vagt refererar till områden som kontroll, kommunikation, datorer och nätverk samt verksamheter kopplade till detta såsom cyberkrig, cyberattack, cyberförsvar, cyberförmåga, cyberspionage etc. Oklarheter om olika cybertermers närmare innebörd bidrar till att skapa osäkerhet och ibland förvirring. Författaren avser därför inte försöka att ge en allomfattande definition här, utan i stället väljs att i denna artikel undersöka cybertermens ursprung och uppkomst.

På 1940-talet var vetenskapsmännen Norbert Wiener och Arturo Rosenblueth intresserade av problem i skärningspunkten mellan matematik och fysiologi. Den amerikanske matematikern och universalgeniet Wiener och den mexikanske fysiologen Rosenblueth hade funnit att både människor och maskiner har en sak gemensamt: existensen och beroendet av återkopplingsloopar (eng *feedback*). I vidare undersökningar fann de att det saknades en universell terminologi för problemställningar rörande vad man kallade *communication, control and statistical mechanics*. De ansåg att det troligen berodde på att matematik och de sociala vetenskaperna utgör så disparata fält.[7] Som en följd fann sig Wiener och Rosenblueth tvingade att "mynta minst ett artificiellt nygrekiskt uttryck för att fylla luckan".[8] Efter inspiration av en artikel med titeln "On Governors" av James Maxwell, som behandlade återkoppling som koncept,[9] där en *governor* var en del av en maskin som såg till att hastigheten förblev närapå konstant, kom de att benämna fälten reglerteknik och kommunikationsteori för cybernetik. Ordet cybernetik kommer från grekiskans κυβερνητική *(kybernetike)* som betyder rorsman.[10]

Med valet av detta ord återfinns därmed analogin till styrning av fartygs framdrivningsanordningar, vilken de betraktade som en tidig men väl utvecklad form av återkopplingsmekanism.[11] Den etymologiska kopplingen till grekiskan synes utgöra ett undantag då det inom IT-branschen nästan uteslutande förekommer termer på engelska eller influerade av engelskan (vilket sedermera kommer att framgå i denna artikel). En möjlig start för de anglosaxiska influenserna inträffade några decennier senare då science fiction-författaren William Gibson myntade termen *cyberspace*. Den användes ursprungligen, men endast perifert, i hans bok *Burning Chrome* från 1982.[12] Mer centralt förekommer den i boken *Neuromancer.*[13] Enligt Gibson själv låter ordet som att det betyder eller skulle kunna betyda något, men i själva verket betyder det absolut ingenting.[14] På svenska kom denna term med sitt vaga innehåll att översättas till *cyberrymden*, eller *datarymden*. Personer som ifrågasätter vad cyber betyder, gör det alltså med rätta.

*Cyberspace* definierades av det amerikanska försvaret flera decennier efter Gibsons ursprungliga poetiska definition.[15] I amerikanska U.S. Army Field Manual 3-38 Cyber

Electromagnetic Activities[16] kan man läsa att *cyberspace* definieras som:"... a man-made construct of systems of systems in that many small and diverse systems comprise the structure as a whole. These systems exist in the physical world. Cyberspace, which continually evolves, facilitates the use and exploitation of information, human interaction, and intercommunication through computers and telecommunication systems". Vidare konstateras att cyberspace och det elektromagnetiska spektrumet konvergerat till ett globalt korsberoende nätverk.[17] Det betyder bl a att de underliggande transmissionsnätverken kan bestå både av fysiska kablar och radiolänkar på olika frekvenser. Man kan i definitionen utläsa att cyber består av fysiska delar, människor, information och kommunikation. 2016 fastslår Försvarsmakten för sin del att cyberrymden är en del av "...informationsmiljön som består av de sammanlänkade och av varandra beroende IT-infrastrukturer med tillhörande data och information. Den inkluderar internet, intranät, telekommunikations-system, datorsystem samt inbyggda processorer och styrenheter."[18]

I svensk militär terminologi används begreppet dator- och nätverksoperationer med de ingående delarna dator- och nätverksförsvar, dator- och nätverksexploatering och dator- och nätverksattack[19] för vad man kan göra i cyberrymden, men i den här artikeln används de motsvarande termerna cyberoperationer och cyberförsvar, cyberspionage och cyberangrepp.[20]

## Cyber – ett relativt omoget område

Om man räknar IBM System/360 som den första kommersiellt väl spridda datorn så har datorer varit tillgängliga för industrin och konsumentledet i ungefär femtio år.[21] Internet gjorde sitt intåg i Sverige i mitten av 1980-talet, men fick inte sitt stora genomslag förrän cirka tio år senare, och är därmed cirka tjugofem år gammalt. Datavetenskap som akademisk disciplin är inte heller gammal, t ex fick KTH inte en fyraårig utbildning i matematik och datavetenskap förrän 1979.[22] Med andra ord är hela datavetenskapsområdet, åtminstone som akademiskt fält, relativt ungt.

Med den ökande betydelsen av IT för myndigheters kärnverksamheter i kombination med bristen på beprövade metoder, levererade (och levererar) en hel del IT-projekt inte vad som utlovats enligt plan.[23] Beroende på bristfällig kravuppfyllnad och dess i allmänhet styvmoderliga behandling tillkom i USA år 1996 Clinger-Cohen Act, en lag för att strama upp IT-verksamheten i federala myndigheter. En del i lagen föreskrev att amerikanska myndigheter skulle etablera en CIO – Chief Information Officer – en funktion som skulle ha övergripande ansvar över hela organisationens IT-resurser och informationssäkerhet (eng information assurance). År 1998 kom Presidential Decision Directive 63, sektion VII (1998),[24] där det föreskrevs att även en CIAO, Chief Infrastructure Assurance Officer, med ansvar över alla aspekter rörande ett departements så kallade kritiska infrastruktur skulle tillsättas efter det att amerikanska politiker sett en möjlig hotbild mot en sådan.

Trots att det moderna samhället är beroende av, och blir alltmer beroende av IT, är det fortfarande uppenbarligen svårt att ta fram stora ändamålsenliga IT-system. Detta innebär att vi på mikronivå kan se att IT löser många problem, men att det på makronivå fortfarande finns en stor andel storskaliga komplexa IT-projekt som inte levererar avsedd effekt.[25]

## Hot mot informationssäkerhet

Hantering av information är en integrerad del av de flesta verksamheter. Eftersom informationshanteringen numera nästan uteslutande genomförs i IT-system är det därför av stor vikt att IT-system fungerar på avsett vis. Informationssäkerhet handlar, uttryckt i en mening, i grunden om att säkerställa att endast rätt personer får tillgång till oförvanskad information (data) i den utsträckning detta är specificerat. Med andra ord handlar informationssäkerhet om skydd av informationens konfidentialitet, riktighet och tillgänglighet.[26]

Hot mot denna s k informationssäkerhetstriad kan naturligtvis realiseras på flera olika sätt. Hoten kan delas in i två huvudgrupper: oavsiktliga och avsiktliga. Oavsiktliga hot som kan få skadliga konsekvenser kan röra sig om naturkatastrofer som jordbävningar, tornados, bränder, hårdvarufel och andra oönskade händelser som inte avsiktligt initierats av en människa. Avsiktliga, eller antagonistiska, hot är sådana hot som realiseras av mer eller mindre kvalificerade motståndare. I praktiken kan en skicklig motståndare dessutom maskera sina angrepp till att efterlikna oavsiktliga fel i syfte att försvåra eller försena upptäckt av angreppen och därigenom skapa ytterligare förvirring.

## Militärt samband och informationshantering

Historiskt har militära sambandssystem ofta byggts för att vara robusta och kunna utstå någon nivå av fientlig bekämpning. Man har dessutom byggt reservsystem, ibland i flera underliggande nivåer. Ofta har militära organisationer också ägt sin egen tekniska infrastruktur. På grund av den tekniska utvecklingen går vi från äldre tiders kretskopplade punkt till punkt-förbindelser till att data i transmissionslagren förmedlas i form av datapaket i nätverk. Allt fler sambandslösningar använder sig av IP-trafik vars paketförmedling i TCP och UDP är en teknisk grundbult för internet. Ibland passerar numera åtminstone en andel av den militära sambandstrafiken också kommersiell infrastruktur.[27]

En annan konsekvens av den tekniska utvecklingen är att långräckviddiga vapensystem får ökade bekämpningsavstånd. I modern krigföring måste man ofta förlita sig på fjärrspaning där tekniska system mäter in mål och för över information genom datorer och nätverk för att kunna genomföra sådan fjärrbekämpning. Insatsbeslut och bekämpning grundas på en förmedlad bild (lägesbild) av situationen, och inte på direkta observationer. Angrepp på informationssäkerheten som t ex påverkar integriteten på målinformationen i en sådan lägesbild kan få allvarliga konsekvenser.

## Cybermiljön

Bland många förslag till definitioner tecknas i en amerikansk militär doktrin, Joint Publication 3-12 Cyberspace Operations,[28] en bild av cyberspace som bestående av tre lager, som är i linje med tidigare nämnda Field Manual 3-38:[29]

1. *Det fysiska nätverkslagret*, i vilka fysiska nätverkskomponenter finns i geografin.

I det fysiska nätverkslagret transporteras data i form av olika signaler mellan nätverkskomponenter. Transmission kan ske både i fysisk infrastruktur, t ex i kablar av olika slag, och i det elektromagnetiska spektrumet, t ex i form av radiovågor. Det här lagret samexisterar med de traditionella militära miljöerna mark, sjö och luft (rymd).

2. *Det logiska nätverkslagret*, i vilka noder är sammankopplade, ibland utan en enhetlig koppling till de andra nätverkslagren.

Det logiska lagret är en abstraktion som existerar i dataminne, men som binder ihop och utgör ”kittet” mellan den fysiska hårdvaran och människorna i de två andra konkreta lagren. Här finns algoritmer, protokoll, portar och program etc av olika slag.

3. *Cyber persona*[30]*-lagret*, vilket utgörs av ”avtryck” eller ”digitala representationer” av människor[31] (kopplade till det logiska lagret).

Cyber persona utgörs av t ex identiteter, t ex användarnamn och liknande, kopplade till e-postkonton, sociala nätverkstjänster etc. Människor kan ha flera cyber persona, men en cyber persona kan också representera en grupp av individer.[32]

Denna indelning har således två lager som är mer eller mindre påtagligt konkreta: det fysiska nätverkslagret och cyber persona som relaterar till människor. De är sammanbundna av det abstrakta logiska nätverkslagret. För att komplettera och förtydliga hela bilden är det möjligt att lägga till ytterligare två lager:

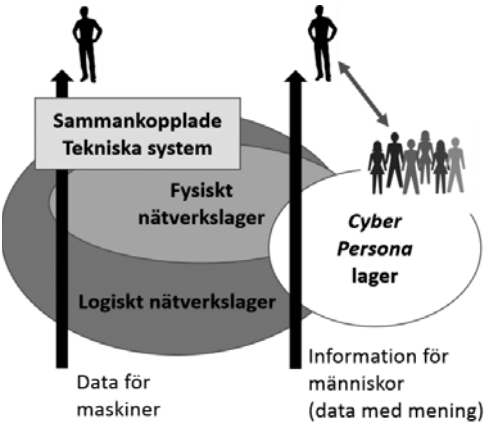
4. *Sammankopplade tekniska system*

Tekniska system som är kopplade till internet. Numera kan detta vara nästan vad som helst. Exempel är industriella kontrollsystem (SCADA-system[33]) i fabriker, telefonväxlar, bilar, kylskåp, tv-apparater, militära sambandssystem m m.

5. *Människor (beslutsfattare)*

Människan är det yttersta målet för alla typer av cyberoperationer.

Om vi ser de sammankopplade tekniska systemen och människor som måltyper framträder följande bild baserat på ovanstående resonemang:




*Figur: Cybermiljön och huvudtyper av cyberangrepp.*

Det innebär att cybermiljön är både ett (del) mål och ett medel. När operationerna syftar till att påverka människor genom maskiner, d v s tekniska system, med fysiska effekter som explosioner, strömavbrott, förorenat vatten etc handlar det om att med rätt data styra tekniska system till att åstadkomma sådana effekter. Då är cybermiljön, antingen med de sammankopplade tekniska systemen eller med cyberinfrastrukturen, ett mål i sig. När angreppen syftar till att påverka människor med information, tolkade data, utgör den mänskliga kognitionen målet. I detta fall är cybermiljön endast ett medel för att nå detta mål. Miljön används som ett medium för masskommunikation eller för operationer riktade mot enskilda individer eller grupper, t ex påverkan genom sociala medier. Poängen med cyber är att man genom att ansluta till det logiska nätverkslagret i princip kan angripa, eller bli angripen av vem som helst på jorden varsomhelst på jorden.

Cyber är alltså på ett sätt oberoende av geografi. Att utveckla cyberförmågor är dess-

utom troligen stridsekonomiskt gynnsamt, d v s kostnadseffektivt. Inträdesbiljetten – tröskeln att överskrida – till miljön består i huvudsak av två delar, nämligen att man har möjlighet att ansluta till internet, eng *connectivity*, samt tillgång till kompetent personal. Det behövs ingen dyr speciell hårdvara. En ytterligare fördel är att det tekniskt är mycket svårt att med säkerhet härleda en cyberattack tillbaka till en bakomliggande ansvarig vilket innebär att en angripare kan ha förnekbarhet. Kopplat till detta kan cyber också ge utmärkta möjligheter för vilseledning.[34] Vidare kan också cyberattacker genomföras genom ombud,[35] i så kallad proxykrigföring, där kopplingen till kontrahenten är ännu svårare att fastställa. Ibland kan man själv dra förhastade slutsatser om detta, vilket är något som inträffade i USA 1998 då ett antal militära baser utsattes för dataintrång. De amerikanska myndigheterna FBI och NSA misstänkte i tur och ordning en entitet i mellanöstern, Irak, Kina och Ryssland innan det uppdagades att två tonåringar i norra Kalifornien genomfört angreppen från den enes pojkrum.[36]

## Cyberoperationer

Det finns många möjligheter att åstadkomma effekter på fientliga system med hjälp av cyberoperationer, antingen som enskilt verkansmedel eller i kombination med andra. En indelning i cyberförsvar, cyberspionage och cyberangrepp är vanligt förekommande. Cyberförsvar, som är defensivt till sin karaktär, syftar till att skydda egen information, egna datorer och nätverk. Cyberspionage genomförs i syfte att stjäla information, d v s att bryta konfidentialitet i den tidigare nämnda informationssäkerhetstriaden, för att kartlägga datorer och nätverk för kommande cyberangrepp eller av andra skäl. Det är en verksamhet som ständigt pågår i mycket stor omfattning. Cyberspionage genomförs av både statliga och kriminella aktörer av olika snitt. Cyberattacker syftar till att angripa ett eller flera ”ben” i informationssäkerhetstriaden. Några exempel på målsättningar för cyberattacker är:[37]

- röja personlig information och på så sätt hota den personliga integriteten för människor,
- förneka legitima användare åtkomst till elektroniska tjänster,
- störa eller degradera samhällsviktiga funktioner,
- manipulera elektronisk handel,
- degradera eller slå ut kritisk infrastruktur, och
- andra typer av informationsläckage.

Antagonistiska cyberattacker kan alltså medföra allvarliga konsekvenser för de utsatta. Risker förknippade med IT-system i detta sammanhang är därmed inte något man bör ta lätt på, eller betrakta som ”bekvämlighetsrisker”[38] som saknar reell betydelse.

Som exempel på cyberattacker som kan genomföras av nationalstater givna utifrån de effekter de avser skapa föreslår Lukasik[39] följande [författarens översättning]:

- Mindre attacker som återupprepas frekvent i syfte att
  - skada eller förstöra en hel ekonomi,
  - genomföra ekonomiska bedrägerier eller utpressning.
- Större attacker som återupprepas mindre frekvent i syfte att
  - skada eller förstöra en enskild infrastruktur (inkl cyberinfrastruktur[40]),
  - skada eller förstöra flera infrastrukturer genom att exploatera samberoende mellan dessa,

och

- Attack på en befolkning (större grupp av individer) i syfte att
  - erodera ömsesidig tillit i populationen,
  - nöta ner motstånd mot förändrad politik.
- Attack på individer eller mindre grupper i syfte att
  - svärta ledares goda rykte (image),
  - urholka förtroendet för eliter.

Med tanke på den bild av cybermiljön som tecknats tidigare och de operationstyper som föreslagits av Phil Williams och Stephen Lukasik kan man dra slutsatsen att det finns två huvudtyper av cyberattacker: sådana som har människor och mänsklig kognition som (slut) mål, och sådana genom maskiner, inklusive cyberinfrastrukturen, har människor som mål. Dessa två typer av cyberattacker kan benämnas informationspsykologiska operationer, ”inform and influence operations” och informationstekniska operationer, ”information technical operations”.[41] Cyberangrepp kan genomföras i alla konfliktskeden, mot såväl militära som civila mål, såväl militär personal som civilbefolkning samt mot militära likaväl som civila system, inte minst s k kritisk infrastruktur. Det man kan åstadkomma med cyberattacker kan därmed gå långt utöver vad militära organisationer traditionellt sysselsatt sig med. Följaktligen är hotet från cyberattacker också betydligt mer omfattande än vad militära organisationer tidigare har haft att hantera.

Förutom de osäkerheter som uppstår på grund av svårigheterna med att positionera och identifiera angripare, som ibland också kallas attribuering, präglas cybermiljön av andra osäkerhetsfaktorer för den som önskar klarhet:

- En del aktörer hemlighåller sina intentioner och sin kapacitet inom området.
- Det finns ingen internationellt samstämmig tolkning av IT-juridik, och särskilt inte sådan som är kopplad mot cyberangrepp.
- Nationella myndigheter har generellt oklara mandat rörande cyberförsvar.
- Det finns inga knivskarpa gränser mellan konfliktnivåerna fred, kris och krig.

Även om det verkar finnas åtskilliga fördelar med cyberattacker som gynnar en angripare finns det flera kritiker mot synsättet att cyberattacker är en enkel universallösning för krigförande parter i framtida konflikter. Flera skeptiker har utmanat den inte minst i medier förekommande närmast bombastiska retoriken om ett förestående cyberkrig som enbart kommer att utkämpas i cybermiljön.[42] De hävdar bland annat att det är svårare än vad det verkar vara att genomföra framgångsrik offensiv cyberkrigföring. Det krävs t ex djup teknisk kompetens för att tillskansa sig åtkomst till målsystem,[43] men också en rad andra kompetenser, inte minst systemförståelse för hela det målsystem i vilket man avser åstadkomma effekter. Det är vidare svårt att verifiera att man nått önskad verkan och att de effekter man når blir bestående under tillräckligt lång tid i förhållande till de övergripande operativa målsättningarna.

Ett annat argument som lyfts fram är att det finns väldigt få exempel på konflikter där man kan peka på att cyberangrepp genomförts. Under anfallsfasen för Rysslands angrepp och illegala annektering av Krim förekom det sannolikt varken angrepp mot ukrainsk s k kritisk infrastruktur eller militära system i någon avgörande omfattning.[44] Bortsett från i huvudsak överbelastningsattacker som syftar till att förneka legitima

användare åtkomst till IT-resurser, finns det få exempel på när stater överhuvudtaget kan antas ha använt cyberattacker för att degradera eller slå ut fysiska mål. Några exempel är dock den påstått amerikanska operationen Olympic Games som var riktad mot Irans påstådda kärnvapenprogram som använde sig av mjukvaran Stuxnet,[45] samt den påstått ryska operationen riktad mot ukrainsk elförsörjning[46] som inträffade efter den högintensiva anfallsfasen vid annekteringen av Krim.

Det finns också faktorer som verkar avhållande för att använda cyberangrepp som verkansmedel. En sådan faktor är då stater doktrinärt deklarerat att de inte utesluter möjligheten att svara med massförstörelsevapen. En annan är då nationer unilateralt förbehåller sig rätten att peka ut vilka de anser vara ansvariga eller att vidta svarsåtgärder utan att för den sakens skull presentera några bindande bevis. Så skedde t ex år 2014 då USA pekade ut Nordkorea som ansvarigt för dataintrång med efterföljande informationsläckage riktat mot Sony,[47] samt då USA officiellt pekade ut Ryssland som ansvarigt för dataintrång med tillhörande datastöld riktat mot det amerikanska demokratiska partiet[48] under 2016. Även Storbritannien förbehåller sig rätten att svara på statsunderstödda cyberattacker med de medel de väljer, inklusive cyberangrepp.[49]

## Situationsuppfattning i cybermiljön

Det råder inga tvivel om nyttan med att ha en god lägesuppfattning om vad som händer på slagfältet. I den amerikanska armén är det en prioriterad uppgift att skapa en lägesbild som kan leda till en sådan lägesuppfattning även för cybermiljön,[50] och flera länder som har cyberstrategier eller cybersäkerhetsstrategier lyfter särskilt fram behovet av att skydda kritisk cyberinfrastruktur, men också behovet av att utveckla eller förbättra sin lägesuppfattning inom området.[51]

Med lägesuppfattning menar Försvarsmakten ”Den subjektiva uppfattning som rollinnehavare skapat sig grundad bland annat på presenterad lägesinformation.”[52] I engelskspråkig litteratur förekommer termen *situation* eller *situational awareness*, här: SA. I denna artikel antas lägesuppfattning vara ekvivalent med SA.[53] SA handlar helt enkelt om att veta vad som händer runt omkring dig.[54] Det finns flera olika modeller som beskriver SA.[55] En modell som vunnit vida acceptans[56] är Mica Endsleys, vars definition lyder: (en persons)”perception of the elements in the environment within a volume of time and space, the comprehension of their meaning and the projection of their status in the near future.”[57] Av detta följer att SA handlar om en persons kognitiva uppfattning snarare än om ett tekniskt system. Utöver detta måste personen, som t ex kan ses som en operatör av något slag, förstå i vilket sammanhang (system) hon själv verkar.[58] Vidare antas en god SA vara en förutsättning för effektivt handlande, d v s hur väl uppgifter löses, även om det för alla fall inte kan visas vara så. SA ska inte ses isolerat, utan som sammanhängande med (efterföljande) beslutsfattande och handlingar.

De tre nivåerna i SA enligt Endsley är således:

1. Förnimma/Upptäcka (eng perceive).

Här är det frågan om att överhuvudtaget kognitivt ta in och medvetandegöra sådant som är av vikt.

2. Förstå (eng comprehend).

Här gäller det att sätta in saker i sitt sammanhang och klarlägga betydelser.

3. Förutsäga (eng project).

I den mest utvecklade nivån handlar det om att förutspå den (omedelbara) framtiden och bedöma vad som kommer att hända härnäst.

De tre nivåerna bygger på varandra såtillvida att en högre nivå är beroende av den lägre. Man kan dock ha samtidig SA på flera olika nivåer i olika avseenden. SA är alltså en subjektiv uppfattning, och vad som är relevant i denna uppfattning är som nämnts beroende av vilken uppgift man har. Därmed finns det också skillnader mellan olika verksamhetsområden.[59] Vad som generellt är relevant för Försvarsmaktens del återfinns i dess definition av lägesbild: den ska innehålla ”Information avseende aktörers och i tillämpliga delar övriga resursers tillstånd i olika avseenden såsom geografisk position, förmåga, pågående verksamhet, lydnadsförhållande, uppdrag/order och/eller syftet med agerandet, samt information avseende miljön. Lägesinformation kan vara historisk, aktuell eller planerad/prognosticerad.”[60]

För ett mekaniserat förband går sådan information att sammanställa även om det är en grannlaga uppgift. Geografisk position kan mätas in med hjälp av tekniska sensorer, förbandets förmåga kan antas till del ges av dess vapensystems effekt, maximal förflyttningshastighet baserat på dess fordonsflotta, lydnadsförhållande enligt den fientliga kommandostrukturen som kan vara inhämtad sedan tidigare etc. För flygförband kan flygplanens geografiska position hämtas in med hjälp av radar eller signalspaning för att sedan presenteras på en lägeskarta. Sammantaget har forskningen rörande SA arbetat med någorlunda väl avgränsade ”situationer” inom flera olika verksamhetsområden.[61] När det gäller att avgränsa en ”situation”, eller definiera ett intresseområde för cybermiljön blir det mer komplicerat.

För att man ska kunna manövrera och verka i ”terrängen”, i detta fall cybermiljön, behövs en ingående förståelse för hur den ser ut. Det behövs en lägesuppfattning i cybermiljön – *Cyber Situational Awareness*, CSA.

Det geografiska intresseområdet för CSA utgörs av det egna nätverket, men också av sammankopplade enheter varifrån det kan genomföras attacker. Dessa kan finnas varsomhelst globalt. Tidsförhållandena är sådana att man måste intressera sig för vad som händer i realtid, eller nära realtid, t ex i samband med IP-trafik, men också för processer som tar betydligt längre tid i anspråk.[62] Efterföljande beslutsfattande kommer också att behöva ske på olika sätt, t ex med hänsyn tagen till riskaptit, juridik och nödvändighet, och i olika form, t ex av operatörer, eller semiautomatiskt med hjälp av operatörer, eller helt automatiskt.[63] Även etiska och moraliska överväganden bör spela in.

Kombinationen av vad som tidigare nämnts avseende en angripares utmärkta möjligheter att förbli anonym och ha förnekbarhet, att cyber utgörs av en union mellan en fysisk och en abstrakt domän, samt vad som nämnts här med geografiska och tidsmässiga gränser gör att jobbet att designa en cyberlägesbild således inte kan antas vara trivialt. Snarare är det en formidabel utmaning. En cyberlägesbild måste innehålla information om både den fysiska världen och det man kallar det ”virtuella slagfältet”, d v s om de tre lager vi stött på tidigare, det fysiska och det logiska nätverkslagret samt cyber persona-lagret.[64] Informationen som presenteras måste dessutom vara användbar såtillvida att den kan ligga som grund för beslutsfattande.[65] Det är inte heller så att ju mer information man har tillgång till, även om den är relevant för uppgiften, förbättrar resultatet när uppgiften löses.[66] Det gäller

alltså att välja relevant information och att presentera den på ett funktionellt sätt. Vad som måste lösas är dels ett tekniskt informationsfusionsproblem, dels ett kognitivt problem.

Inom CSA-forskningen har man behandlat olika delproblem,[67] men ingen verkar ha en komplett lösning på hur en militär cyberlägesbild för att nå CSA bör se ut. När det gäller att sammanställa och presentera vad som händer i nätverken konstaterade Tim Bass att bl a ämnesområdena statistik, artificiell intelligens, signalbehandling, mönsterigenkänning, kognitionsvetenskap och beslutsteori är kompetensområden som behövs för framgång.[68]

Men eftersom grundskälet för att överhuvudtaget ha en militär cyberlägesbild och CSA är att möjliggöra effektivt beslutsfattande och efterföljande åtgärder är det också nödvändigt att man intresserar sig för omgivande system och andra faktorer.

Om vi rekapitulerar innehållet i Försvarsmaktens definition av lägesbild,[69] bör den således dessutom innehålla historisk, aktuell eller prognosticerad information om aktörer, övriga resursers tillstånd i olika avseenden, t ex geografisk position, dess förmåga, pågående verksamhet, lydnadsförhållande, uppdrag/order och/eller syftet med agerandet, samt annan information avseende miljön.

Thomas Rid och Ben Buchanan[70] hävdar att det behövs kunskap om flera områden om man vill kunna attribuera cyberattacker och presenterar en modell för detta, sin s k Q-modell. Tabellen nedan ger exempel på relevanta aspekter på tre olika abstraktionsnivåer som sinsemellan förefaller vara konsistenta:

| **Aspekt** | **Lägre abstraktion Mer konkret** | **Mediumabstraktion** | **Hög abstraktion Mindre konkret** |
|---|---|---|---|
| Questions | What? How? | How? | Why? |
| Levels | Tactical/technical | Operational | Strategic |
| Staff | Forensic experts | Analysts | Leaders |
| Goals | Technical analysis | Understanding | Response |
| Responsibility | Individual | Agency/group | Government |
| Target | Data, docs, processes | Org, individuals | Government |
| Certainty | Higher | Medium | Lower |
| Detail | Detailed | Synthesis | Concise |
| [for communication to stakeholders] | Description | Hypotheses | Estimates |

*Tabell: Extraherad ur Rid och Buchanans Q-modell, Ibid., Rid; Buchanan 2015, pp. 34. Rubriksatt av författaren.*

Conti m fl tecknar kopplat till detta ett behov av 27 övergripande förmågor i form av deluppgifter som måste lösas att man ska få en funktionell lägesbild. Exempel är underrättelser, beslutsstöd, planering av vilseledning, försvar mot vilseledning, visualisering av stridsfältet, egen nätverksanalys, planering och genomförande av egna operationer etc.[71] Den kravbild på vilka kompetenser som behövs för att utveckla en cyberlägesbild blir därför mycket bred och omfattar dels militär kompetens, dels djup spetskompetens inom

flera områden som kan vara svår att finna i Försvarsmakten.

## Diskussion

Vi har sett att cyber är en stor och komplex fråga. Cybermiljön är komplicerad och har både abstrakta och konkreta domäner där både mycket korta och långa tidsförhållanden är lika relevanta att beakta. Flera typer av cyberattacker med både människor och maskiner som mål kan genomföras. Vi har också sett att cybermiljön inte är isolerad, utan att den utgör en integrerad del av de andra miljöerna mark, sjö och luft. Det är därför utsiktslöst att diskutera cyber enbart sett ur ett defensivt cyberförsvarsperspektiv i termer av antivirusprogram, intrångsdetekteringssystem, brandväggar m m. När det gäller offensiva cyberattacker finns det inte heller något större värde i att betrakta fenomenet som något isolerat cyberkrig där det handlar om att symmetriskt angripa mjukvara med annan mjukvara utan att fundera på vilka effekter som ska åstadkommas. Det är naivt och dysfunktionellt i en större militär kontext.

Modern krigföring handlar om att planera operationer så att de når avsedda effekter i förhållande till övergripande politiska och militära målsättningar. Man måste därför sätta in cyber i ett större sammanhang. Det kan vara aktuellt med både informationspsykologiska och informationstekniska cyberattacker. Flera exempel på sådana ges ovan, men det finns även ett spelrum att med god uppfinningsrikedom planera och sjösätta skräddarsydda operationer som är anpassade efter aktuella strategiska och operativa målsättningar. Dessutom kan man i militära operationer kombinera cyberattacker med andra verkansmedel. Exempelvis kan man:

- som en del i en cyberoperation nyttja kinetisk vapenverkan för att slå ut ett datacenter (datorhall) där skyddsvärd informationen finns lagrad,
- med hjälp av telekrigsåtgärder slå ut transmissionsinfrastruktur för att omöjliggöra för fienden att ta del av den information han behöver,
- inom ramen för krigets lagar bekämpa teknisk driftpersonal som utgör kritiska resurser, flaskhalsar, i komplexa tekniska system,
- röja konfidentiell information för ickebehöriga i syfte att misskreditera tredje part, jämför Wikileaks m fl så kallade visselblåsar-sajter, som offentliggör omfattande s k data dumps,
- i nämnda större informationsläckor plantera avsiktligt falsk och/eller vilseledande information, etc.

## Avslutning

Vi kommer inte att få se något cyberkrig som enbart utspelar sig i cybermiljön i framtiden. Vi börjar förstå att internet kan användas och används för inflytelseoperationer både genom både masskommunikation och riktade informationsoperationer t ex i s k sociala medier, d v s för informationspsykologiska cyberoperationer. Vi börjar också alltmer inse att cyberoperationer även har en användbar potential som fjärrbekämpningssystem för att degradera eller slå ut anslutna tekniska system. För att sluta cirkeln till Wiener och Rosenblueth, rör cyber både människor och maskiner, och cyberoperationer är något som ingår i och är integrerat med annan verksamhet. Oavsett vilka uppgifter och vilken ambitionsnivå Försvarsmakten har, anser författaren att det är viktigt att ha en situationsuppfattning grundad på en läges-

bild över cybermiljön. Att ta fram en sådan är mycket svårt.

Med en cyberlägesbild som grund kan Försvarsmakten som en miniminivå skydda ”sin” cybermiljö inklusive skyddsvärd information och infrastruktur.[72] Ett sådant cyberförsvar bör omfatta såväl de delar som tecknats ovan, men också det elektromagnetiska spektrumet. I skyddet bör det alltså ingå skydd mot informationstekniska cyberoperationer som syftar till att degradera eller slå ut vår cyberinfrastruktur, våra andra militära system, samt mot informationspsykologiska cyberoperationer som syftar till att påverka Försvarsmaktens personal.

Försvarsmakten ska dessutom utveckla vad man kallar ”...aktiv cyberförmåga och kapacitet...” enligt försvarsminister Peter Hultqvist.[73] Ordet ”aktiv” återstår att definiera, men används i rubriken för denna artikel. Inom ramen för detta uppdrag anser författaren att Försvarsmakten bör ta fram verkansdelar samt utveckla förmågan för planering av komplexa cyberattacker för alla de möjligheter som finns både beträffande informationspsykologiska-, och informationstekniska operationer.

Det är relativt enkelt att genom cyberangrepp orsaka någon skada, men att uppnå predikterbara och väl avgränsade effekter kräver tillgång till en rad olika delförmågor. Utvecklingen av cyberförmåga bör baseras på rigorös forskning med vetenskapliga metoder, så att inte lösningar för cyberoperationer riskerar bli lika ineffektiva som andra komplexa IT-projekt. Det finns som visats ett antal olika tänkbara typer av cyberangrepp. Det kan vara rimligt att också ha, och ge uttryck för, en doktrinär idé om vilka typer av cyberoperationer som står i samklang med ens övergripande ledningsfilosofi. Det krävs också att man resursmässigt överskrider en kritisk massa avseende de i cyber ingående delförmågorna för att få en användbar cyberförmåga. Cyber är inte en bisak, utan en viktig del av all verksamhet i organisationer idag. Även om tröskeln att överskrida för att kunna agera i cybermiljön är låg, är frågan om hur väl man leder, organiserar, bemannar, utrustar samt utvecklar förmågan som en militär förmåga, avgörande för hur effektiv den kan bli. Kalkylen som gjorts i flera länder gör är att det trots allt är stridsekonomiskt gynnsamt.

Författaren är major i flygvapnet och f n doktorand vid KTH i datalogi.

## Noter

1. Eliasson, Gunnar: *Den nya och omedelbara ekonomin – ett Internet-perspektiv*, 2002, Vinnova-rapport VR 2002:12, Stockholm 2012. *http://www.vinnova.se/upload/epistorepdf/vr-02-12.pdf*. (2016-10-20)
2. Blasko, Dennis J: *The Chinese army today – Tradition and transformation for the 21st century,* 2nd edition, Routledge 2012.
3. Med CEP = 50%, d v s att hälften av bomberna förväntas träffa inom det specificerade avståndet (radien).
4. Cordesman, Anthony M: *The Iraq war – Strategy, tactics and military lessons*, Pentagon Press 2012.
5. För olika länders och organisationers definitioner, se Natocentret Cooperative Cyber Defence Centre of Excellence (CCDCOE) sammanställning: *https://ccdcoe.org/cyber-definitions.html*.
6. Giles, Keir och Hagestad, William II: ”Divided by a Common Language: Cyber Definitions in Chinese, Russian and English”

i Podins, Karlis; Stinissen, Jan och Maybaum, Markus (red): *2013 5th International Conference on Cyber Conflict*, NATO CCD COE Publications, Tallinn 2013, s 413-429.

7. Wiener, Norbert: *Cybernetics – or control and communication in the animal and the machine*, 2nd edition, MIT Press 1985, första utgåva 1948.
8. Författarens översättning av "...forced to coin at least one artificial neo-Greek expression to fill the gap"; ibid, s 11.
9. Maxwell, James C: "On Governors", *Proceedings of the Royal Society*, London 1868, vol 16, s 270-283, *http://www.jstor.org/stable/112510?seq=1#fndtn-page_scan_tab_contents*. (2016-11-03)
10. Op cit, Wiener, Norbert, se not 7.
11. Ibid.
12. Gibson, William: *Burning Chrome,* Harper Voyager-Collins, New York 2003, första utgåva 1982.
13. Gibson, William: *Neuromancer*, Ace Books, New York 2000, första utgåva 1984.
14. Inspelad intervju med William Gibson, okänd tidpunkt, *https://www.brainpickings.org/2014/08/26/how-william-gibson-coined-cyberspace/*. (2016-11-01)
15. "Cyberspace. A consensual hallucination experienced daily by billions of legitimate operators, in every nation, by children being taught mathematical concepts . . . A graphic representation of data abstracted from the banks of every computer in the human system. Unthinkable complexity. Lines of light ranged in the non space of the mind, clusters and constellations of data. Like city lights, receding....", op cit, Gibson, William, se not 13, s 51.
16. *Cyber electromagnetic activities. Field Manual 3-38*, U.S. Department of Defense, Headquarters, Department of the Army, Washington DC febr 2014.
17. Ibid.
18. *Handbok Nomenklatur Ledning (H Nomen Led 2016),* Försvarsmakten, Högkvarteret, Stockholm 2016, s 16.
19. Ibid.
20. *Militärstrategisk Doktrin – MSD 16,* M7735-354028, Försvarsmakten, Högkvarteret, Stockholm 2016.
21. Försvarsmakter och universitet har haft tillgång i ytterligare några decennier.
22. *KTH:NADAs historia,* Kungliga Tekniska Högskolan, Stockholm 2012, *https://www.kth.se/csc/om/historia/nadas-historia-1.14418*, (2016-10-20).
23. En granskning av stora statliga IT-projekt i Sverige för år 2009 visade att över hälften inte levererade avsedd effekt. *Statliga IT-projekt som överskrider budget,* Riksrevisionen, RiR 2011:5, Stockholm 2011. *http://www.riksrevisionen.se/PageFiles/8542/Anpassad_11_5%20Statliga%20IT-projekt%20som%20%c3%b6verskrider%20budget.pdf*. (2016-11-12)
24. Presidential Decision Directive/NSC-63, hämtad från Federation of American Scientists, *http://fas.org/irp/offdocs/pdd/pdd-63.htm*. (2016-10-13)
25. Se t ex "The worst IT project disasters of 2013", *Infoworld*, 2013-12-30, *http://www.infoworld.com/article/2609011/applications/the-worst-it-project-disasters-of-2013.html*. (2016-11-18)
26. Eng *Confidentiality, Integrity and Availability.*
27. En enskild uppgift från år 1998, som är svår att verifiera, gör gällande att 95% av all amerikansk militär telekommunikation vid tillfället passerade kommersiell infrastruktur vid någon punkt. Pritulsky, Philip S: *Strategic Military Communications of the Future: Leveraging Civilian Operations,* U.S. Army War College, Carlisle Barracks, Pennsylvania mars 1998.
28. *Cyberspace operations. Joint Publication 3-12(R)*, U.S Department of Defense, Joint Chiefs of Staff, Washington DC febr 2013.
29. Op cit, *Cyber electromagnetic activities*, 2014, se not 16.
30. Notera att termen *persona* används med en annan betydelse inom området användarcentrerad design. Se t ex Cooper, Alan*: The Inmates Are Running the Asylum: Why High Tech Products Drive Us Crazy and How to Restore the Sanity*, 2nd edition, Sams Publishing, Indianapolis 2004.
31. Op cit, *Cyberspace operations*, se not 28.
32. Fanelli, Robert och Conti, Gregory: "A Methodology for Cyber Operations Targeting and Control of Collateral Damage in the Context of Lawful Armed Conflict" i Czossek, Christian; Ottis, Rain och Ziolkowski, Katharina (red): *2012 4th International Conference on Cyber Conflict,*, NATO CCDCOE Publications, Tallinn 2012.
33. SCADA = *Supervisory Control And Data Acquisition.*

34. Rowe, Neil C: ”A Taxonomy of Deception in Cyberspace” i *2006 International Conference in Information Warfare and Security*, Princess Anne, Maryland mars 2006, *http://calhoun.nps.edu/bitstream/handle/10945/35976/Rowe_A_Taxonomy_of_Deception.pdf?sequence=1&isAllowed=y.* (2016-11-06)
35. Op cit, *Militärstrategisk Doktrin*, 2016, se not 20.
36. Kaplan, Fred: *Dark Territory – The Secret History of Cyber War,* Simon and Schuster, New York 2016. Händelsen avhandlas på s 73-78.
37. Williams, Phil; Shimeall, Timothy och Dunlevy, Casey: ”Intelligence Analysis for Internet Security”, *Contemporary Security Policy*, vol 23, nr 2, 2002, s 1-38.
38. Fåk, Viveke: ”IT – risker och säkerhet” i Grimvall, Göran och Jacobsson, Per och Thedéen, Torbjörn (red): *Risker i tekniska system*, Studentlitteratur, Stockholm 2003.
39. Lukasik, Stephen J: ”A Framework for Thinking About Cyber Conflict and Cyber Deterrence with Possible Declaratory Policies for These Domains” i *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy*, Georgia Institute of Technology 2010, *http://nap.edu/12997.* (2016-11-09)
40. Cyberinfrastruktur – Ännu en term som jag anser inte har en bra fastställd definition. I denna artikel avses datorer och nätverk inklusive transmissionsutrustning, -media (inklusive kablar radioutrustningar m m), och andra nätverkskomponenter som utgör det fysiska nätverkslagret tillsammans med programvara som medger datakommunikation. I Försvarsmaktens *Handbok Nomenklatur Ledning 2016*, s 35, anges betydelsen av termen informationsinfrastruktur, som skulle kunna vara användbar i sammanhanget, i alltför vid bemärkelse anser jag: [det är] ”... en infrastruktur som tillsammans med specifika mekanismer möjliggör att flera funktioner på ett strukturerat sätt kan överföra information.”
41. Porche, Isaac R; Christopher, Paul; York, Michael; Serena, Chad C; Sollinger, Jerry M; Axelband, Elliot; Daehner, Endy M och Held, Bruce J: *Redefining Information Warfare Boundaries for an Army in a Wireless World*, RAND Corporation, Santa Monica, CA 2013. *http://www.rand.org/pubs/monographs/MG1113.html.* (2016-11-06)
42. Rid, Thomas: ”Cyber War Will Not Take Place”, *The Journal of Strategic Studies*, Routledge, vol 35, nr 1, febr 2012 (2016-11-06), s 5–32; Gartzke, Erik: ”The Myth of Cyberwar – Bringing War in Cyberspace Back Down to Earth”, *International Security,* vol 38, nr 2, hösten 2013, s 41-73; Lee, Robert M och Rid, Thomas: ”OMG CYBER! Thirteen reasons why hype makes for bad policy”, *RUSI Journal,* vol 159, nr 5, okt/nov 2014, s 4-12.
43. Libicki, Martin: ”The Cyber War that Wasn’t”, i Geers, Kenneth (red):*Cyberwar in perspective: Russian aggression against Ukraine*, NATO CCDCOE Publications, Tallinn 2015, *https://ccdcoe.org/sites/default/files/multimedia/pdf/CyberWarinPerspective_Libicki_05.pdf.* (2016-11-01)
44. Geers, Kenneth (red): *Cyberwar in perspective: Russian aggression against Ukraine*, NATO CCDCOE Publications, Tallinn 2015.
45. Sanger, David E: *Confront and Conceal: Obama’s Secret Wars and Surprising Use of American Power*, Broadway Books, New York 2013.
46. Lee, Robert M; Assante, Michael J och Conway, Tim: *TLP: White – Analysis of the Cyber Attack on the Ukrainian Power Grid – Defense Use Case*, E-ISAC – Electricity Information Sharing and Analysis Center, 2016-03-18, Washington DC 2016, *http://www.nerc.com/pa/CI/ESISAC/Documents/E-AC_SANS_Ukraine_DUC_18Mar2016.pdf.* (2016-11-01)
47. *Update on Sony Investigation*, Federal Bureau of Investigation, FBI, 2014-12-19, *https://www.fbi.gov/news/pressrel/press-releases/update-on-sony-investigation.* (2016-10-20)
48. Nakashima, Ellen: “U.S. government officially accuses Russia of hacking campaign to interfere with elections”, *Washington Post*, 2016-10-07, *https://www.washingtonpost.com/world/national-security/us-government-officially-accuses-russia-of-hacking-campaign-to-influence-elections/2016/10/07/4e0b9654-8cbf-11e6-875e-2c1bfe943b66_story.html.* (2016-10-20)
49. Uttalande av Philip Hammond: ”UK will retaliate against state-sponsored cyber attacks, Chancellor warns”, 2016-11-01,

*http://www.theregister.co.uk/2016/11/01/uk_state_sponsored_cyber_counter_offensive_plan/*. (2016-11-07)
50. "Army launches innovation challenge on cyber situational awareness", U.S. Army, 2015-11-20, *http://www.army.mil/article/158919*. (2016-10-13)
51. Franke, Ulrik och Brynielsson, Joel: "Cyber situational awareness – A systematic review of the literature", *Computers & security*, nr 46, s 18-31, Elsevier Ltd 2014.
52. Op cit, *Militärstrategisk Doktrin*, se not 20, s 47.
53. I Försvarsmaktens Handbok Nomenklatur Ledning 2016, s 65, uppges "Situation Awareness" olyckligtvis vara något helt annat, nämligen en specifik programvaruprodukt som ingår i ett informationssystem. Se not 18.
54. Endsley, Mica R: "Theoretical underpinnings of Situation Awareness: A critical review", Endsley, Mica R och Garland, Daniel J (red): *Situation Awareness Analysis and Measurement*, Lawrence Erlbaum Associates, Mahwah, NJ 2000.
55. Salmon, Paul M; Stanton, Neville A; Walker, Guy H; Baber, Chris; Jenkins, Daniel P; McMaster, Richard och Young, Mark S: "What really is going on? Review of situation awareness models for individuals and teams", *Theoretical Issues in Ergonomics Science,* vol 9, nr 4, 2008, s 297–323.
56. Wickens, Christopher D: "Situation Awareness: Review of Mica Endsley's 1995 Articles on Situation Awareness Theory and Measurement", *Human Factors*, vol 50, nr 3, juni 2008, s 397-402.
57. Endsley, Mica R: "Toward a Theory of Situation Awareness in Dynamic Systems", *Human Factors*, vol 37, nr 1, mars 1995, s 32-64. Citat från s 36.
58. Endsley, Mica R: "Measurement of situation awareness in dynamic systems", *Human Factors,* vol 37, nr 1, mars 1995, s 65-84.
59. Endsley, Mica R: "A survey of situation awareness requirements in air-to-air combat fighters", *International Journal of Aviation Psychology,* vol 3, nr 2, 1993, s 157-168.
60. Op cit, *Militärstrategisk Doktrin*, se not 20, s 47.
61. Patrick, John och Morgan, Philip L: "Approaches to understanding, analysing and developing situation awareness", *Theoretical Issues in Ergonomics Science*, vol 11, nr 1-2, 2010, s 41-57. Citat från s 42.
62. Brynielsson, Joel; Franke, Ulrik och Varga, Stefan: "Cyber Situational Awareness Testing", i Akhgar, Babak och Brewster, Ben (red): *Combatting Cybercrime and Cyberterrorism*, *Advanced Sciences and Technologies for Security Applications*, Springer International Publishing, Schweiz 2016, s 209-233.
63. Hew, Patrick; Lewis, Edward; Radunz, Penelope och Rendell, Sean: "Situation Awareness for Supervisory Control: Two Fratricide Cases Revisited" i *15th International Command and Control Research and Technology Symposium*, Santa Monica, Californien 2010.
64. Även op cit, Fanelli, Robert och Conti, Gregory, se not 32.
65. Conti, Gregory; Nelson, John och Raymond, David: "Towards a Cyber Common Operating Picture" i Podins, Karl; Stinissen, Jan och Maybaum, Markus (red): *2013 5th International Conference on Cyber Conflict*, NATO CCD COE Publications, Tallinn 2013, s 279-295.
66. Marusich, Laura R; Bakdash, Jonathan Z; Onal, Emrah; Yu, Michael S; Schaffer, James; O'Donovan John; Höllerer Tobias; Buchler, Norbou and Gonzalez, Cleotilde: "Effects of information availability on command-and-control decision making: performance, trust, and situation awareness", *Human Factors*, vol 58, nr 2, 2016, s 301-321.
67. Op cit, Franke, Ulrik och Brynielsson, Joel, se not 51.
68. Bass, Tim: "Intrusion detection systems and multisensor data fusion", *Communications of the ACM*, vol 43, nr 4, 2000, s 99-105.
69. Op cit, *Militärstrategisk Doktrin*, se not 20.
70. Rid, Thomas och Buchanan, Ben: "Attributing Cyber Attacks", *Journal of Strategic Studies*, vol 38, nr 1-2, 2015, s 4-37.
71. Op cit, Conti, Gregory m fl, se not 65.
72. Op cit, *Handbok Nomenklatur Ledning*, se not 18.
73. Försvarshögskolan, tal av försvarsminister Peter Hultqvist, Stockholm 2016-02-04, *http://www.fhs.se/sv/nyheter/2016/forsvarsministern-besokte-forsvarshogskolan/*. (2016-11-09)