Sveriges cyberförsvar tar form

En struktur för fortsatt förmågeutveckling mot 2030[1]

av Patrik Sternudd

Résumé

Cyber operations and the consequences of cyber attacks against critical military and civilian infrastructure are increasingly debated in the Swedish society. This article provides an analysis of what Cyber Defence entails within the Swedish Total Defence concept. Based on this, the *Cyber Defence Pyramid* is proposed as a model used to structure current and future capability development within the cyber domain for the Swedish Armed Forces as well as the civilian functions supporting the Armed Forces efforts.

BEHOVET AV ETT starkt cyberförsvar såväl som höjd nivå av cybersäkerhet i samhället påtalas allt oftare i olika sammanhang, inte minst i regeringens proposition *Totalförsvaret 2021–2025*.[2] Samtidigt är författaren inte medveten om att någon djupare analys av innebörden av vare sig begreppet cyberförsvar eller propositionens cyberförsvarskapitel har presenterats i ett offentligt sammanhang.

För att bidra till ökad förståelse och fortsatt diskussion beskrivs därför i artikeln hur cyberförsvar och cyberoperationer förhåller sig till Försvarsmaktens huvuduppgift samt det övriga totalförsvaret. Beskrivningen omfattar samtliga konfliktnivåer och inkluderar hybridaktiviteter med cyberkomponenter. Dessa beskrivningar mynnar ut i en sammanhängande förklaringsmodell, *cyberförsvarspyramiden*, som beskriver cyberförsvarets kärnuppgifter tillsammans med dess samverkande funktioner och förutsättningsskapande delar. Pyramiden utgår bland annat från tionde kapitlet i *Totalförsvaret 2021–2025*[3] och erbjuder en struktur för fortsatt förmågeutveckling under både innevarande och kommande försvarsbeslutsperiod. Artikeln avslutas med en kort redogörelse av några av Försvarsmaktens åtgärder för att vidareutveckla cyberförsvarsförmågan under innevarande och efterföljande försvarsbeslut.

Delar av det arbetsmaterial som utgör underlag till artikeln har även varit föremål för diskussion inom delar av Försvarsmakten och kan även komma att återanvändas i andra sammanhang. Författaren vill uttrycka sitt tack till de som lämnat synpunkter på underlaget samtidigt som ansvaret för eventuella felaktigheter i artikeln i sedvanlig ordning uteslutande ligger på författaren. Eftersom arbetsmaterialet inte är fastställt, utgör varken det eller artikeln Försvarsmaktens officiella hållning.

En viktig avgränsning i artikeln är att den endast översiktligt berör cybersäkerhetsområdet. Även om flera av de aktörer som har direkta eller stödjande uppgifter i Sveriges cyberförsvar i många fall också har ett omfattande ansvar för Sveriges informations- och cybersäkerhet så är cyberförsvar inte synonymt med cybersäkerhet.[4]

Regleringar, mandat och ansvar för Sveriges cybersäkerhet kommer istället att behandlas i en framtida skrift.

Cyberförsvar – en integrerad del av det militära försvaret

Innebörden av ordet cyberförsvar har under de senaste åren gått från att mer eller mindre ha varit en synonym till cybersäkerhet till att knytas allt närmare den nationella försvarsförmågan. Detta har skett parallellt med att cyberoperationer och cyberattacker har fått en ökad betydelse som ett statligt maktmedel, såväl internationellt[5] som i Sverige, där exempelvis propositionen *Totalförsvaret 2021–2025* innehåller följande konstaterande:

> Många stater har byggt upp avsevärda resurser i syfte att kunna verka offensivt genom cyberattacker. Förutom att dessa stater utvecklar avancerade metoder och offensiva verktyg har de skapat förmåga att slå brett mot många mål och att upprätthålla uthållighet över tid.[6]

Senare i avsnittet framgår att konsekvenserna av ett cyberangrepp kan likställas med effekterna av konventionell kinetisk verkan:

> Effekterna av ett antagonistiskt cyberangrepp kan få lika stora konsekvenser för samhällsviktiga funktioner och kritiska it-system som ett konventionellt väpnat angrepp.[7]

I kapitlet om cyberförsvar i *Totalförsvaret 2021–2025* skriver regeringen explicit att ”Ett cyberangrepp kan i vissa fall vara att betrakta som ett väpnat angrepp”.[8]

I *Inriktning för Försvarsmakten 2021–2025* framträder cyberoperationens roll som ett militärt maktmedel än tydligare:

> Ett väpnat angrepp mot Sverige kan komma att inledas med en förbekämpning av basområden, ledningsnoder och annan kritisk civil och militär infrastruktur. Angriparens förbekämpning kan genomföras med kryssningsrobotar, ballistiska robotar, attackflyg, nätverksattacker och cyberoperationer samt genom sabotage och likvidering av nyckelpersonal. […][9]

Försvarsmakten måste därför utgå från att cyberattacker kan komma att sättas in, inte bara mot Försvarsmaktens egna system utan också mot system och tjänster som är av vikt för totalförsvaret och ytterst rikets ledning. Till det kommer Försvarets telenät, FTN, som är av betydelse inte bara för Försvarsmaktens ledningsförmåga utan också används av andra aktörer inom totalförsvaret. Genom att Försvarsmakten är sin egen nätoperatör med ansvar för drift och förvaltning skapas möjligheter för en robust utformning med utgångspunkt från krigets krav, vilket inkluderar förberedelser för cyberförsvarsåtgärder inklusive cyberförsvarsoperationer.

Cyberförsvar ingår i Försvarsmaktens huvuduppgift

Försvarsmaktens huvuduppgift är att försvara Sverige mot ett väpnat angrepp.[10] Utifrån föregående citat om att cyberangrepp i vissa fall är att likställa med väpnat angrepp samt beskrivning om hur cyberoperationer kan nyttjas vid förbekämpning dras slutsatsen att cyberförsvar ingår i Försvarsmaktens huvuduppgift. Cyberförsvar är därmed en integrerad del av det militära försvaret.

Denna slutsats stärks genom följande skrivning i cyberförsvarskapitlet i *Totalförsvaret 2021–2025:*

> Försvarsmakten ska upprätthålla och utveckla ett militärt försvar som kan möta ett väpnat angrepp. Försvarsmakten ansvarar för Sveriges offensiva cyberförsvarsförmåga.

> Cyberdomänen är en av flera domäner där Försvarsmakten ska kunna möta ett antagonistiskt hot med stöd av andra myndigheter, t ex Försvarets radioanstalt och övriga försvarsunderrättelsemyndigheter, Säkerhetspolisen och MSB. Försvarsmakten ska, inom cyberdomänen, kunna verka i alla konfliktnivåer.[11]

Citatet innehåller ytterligare tre viktiga punkter:

- Försvarsmakten ansvarar för den offensiva cyberförsvarsförmågan, vilket är i analogi med ansvarsförhållandet för samtliga militära maktmedel.
- Försvarsmakten ska i cyberdomänen kunna verka i alla konfliktnivåer, vilket är i analogi med det militära försvaret i allmänhet och inte minst luft- och sjöstridskrafterna.
- Försvarsmakten behöver stöd från såväl andra försvarsmyndigheter som delar av totalförsvaret, precis som för övriga förmågor i det militära försvaret

I Försvarsmaktens doktrin framgår att cyberdomänen tillsammans med mark- sjö-, luft- och rymddomänen ingår i den operationsmiljö där Försvarsmakten ska kunna verka.[12] I doktrinen beskrivs också den nära kopplingen till den militärstrategiska nivån:

> [Cyberoperationer][13] leds med särskilda ledningsförhållanden och med en tydlig närhet till den högsta militärstrategiska ledningsnivån. Dessa ledningsförhållanden skapar förutsättningar för att tidigt i planeringen, vid framtagande av militärstrategiska optioner inom ramen för en nationell eller multinationell strategi, överväga möjligheter att genomföra cyberoperationer.[14]

Försvarsmaktens förmåga till verkan i domänen utgörs till stor del av dess it-försvarsförband:

> Försvarsmaktens it-försvarsförband är en förbandstyp designad och resurssatt för att genomföra [cyberoperationer]. It-försvarsförbanden tillför handlingsalternativ för den strategiska, militärstrategiska och operativa nivån, vilka ligger utanför de reguljära förbandens förmågor. It-försvarsförbanden består av stående krigsförband med hög tillgänglighet och genomför såväl defensiva som offensiva operationer.[15]

Cyberdomänen och cyberförsvaret kan således i all väsentlighet sägas ha gått från att vara nykomlingar med oklar innebörd till att bli integrerade delar av det militära försvaret och en naturlig del i den modern krigföringen. Detta återspeglas även i budgetpropositionen för 2022 där cyberförsvaret behandlas inom de avsnitt som rör det militära försvaret, medan informationssäkerhet placeras under civilt försvar och krisberedskap.[16]

En direkt konsekvens av att cyberoperationer utgör ett militärt maktmedel är att dess nyttjande omfattas av folkrättens principer om proportionalitet och distinktion[17] samt militära befälhavares straffansvar[18] för underordnades handlingar. Försvarsmakten måste därför säkerställa att det finns officerare som har erforderlig utbildning för att kunna fatta beslut om när och till vilken grad militärt våldsanvändande ska nyttjas i cyberdomänen.

I budgetpropositionens resultatredovisning av cyberförsvaret framhåller regeringen avslutningsvis att förmågan i sig är viktig för att undvika att hamna i ett väpnat angrepp:

> Det är regeringens bedömning att cyberförsvarsförmågan bidrar till att försvåra och höja tröskeln för en aktör som överväger att angripa eller utöva påtryckningar mot Sverige eller svenska intressen.[19]

Försvarsmaktens kvalificerade resurser, bland annat i form av dess it-försvarsförband,

är en väsentlig del av ovanstående tröskel. Till det tillkommer ytterligare förmågor och resurser både inom Försvarsmakten och i andra delar av totalförsvaret.

Cyberförsvarets omfattning ur tre perspektiv

I *Totalförsvaret 2021–2025* beskrivs cyberförsvar enligt följande:

> Cyberförsvar kan definieras som en nations samlade förmågor och åtgärder, såväl defensiva som offensiva, till skydd för dess kritiska samhällsfunktioner samt förmågan att kunna försvara sig mot cyberangrepp från kvalificerade motståndare. Defensiva operationer syftar till att försvara informationssystem inklusive elektroniska kommunikationsnät för att på så sätt förhindra motståndare att påverka information, informationssystem, datorer eller nätverk. Offensiva operationer syftar till att förhindra motståndaren att använda sina system eller att tvinga motståndaren att avbryta angrepp mot svenska system.[20]

Definitionen beskriver det väsentliga ur ett nationellt perspektiv samt kompletterar med kärnförmågan i form av defensiva och offensiva cyberoperationer. Samtidigt lämnar den ett visst mått av tolkningsutrymme avseende var gränsen mellan cyberförsvar och annan verksamhet går.

Betrakta ett scenario där ett befäl i sitt dagliga arbete upptäcker att det ledningsstödssystem denne arbetar med beter sig konstigt och ringer till it-supporten. Därifrån sker felsökning och en kedja av eskaleringar genom driftorganisationen som leder fram till att ärendet ändrar form till en it-säkerhetsincident. Ytterligare senare uppstår misstanke om att en statlig aktör ligger bakom varpå delar av Försvarsmaktens mest kvalificerade resurser sätts in.

Från detta scenario kan man diskutera huruvida befälet som vill ha hjälp med att lösa sitt it-problem är en del av cyberförsvaret. Är it-supporten det? Driftorganisationen inklusive dess it-säkerhetsspecialister? Hade svaren blivit annorlunda om det visat sig att det var ett enkelt problem som inte hade några it-säkerhetsimplikationer? Ändras svaren i efterhand beroende på att några statliga antagonister upptäcks och beror det dessutom på om den förmodade intentionen är förberedelser för ett väpnat angrepp eller spionage?

Scenariot belyser utmaningen att ta fram exakta definitioner med tydliga gränser för cyberförsvarets omfattning. Detta beror bland annat på att cyberförsvar skär genom flera andra funktioner och områden och att det är svårt att avgöra i förväg hur en incident kommer att utvecklas men framför allt beror det på att det finns flera olika perspektiv som existerar samtidigt och där svaret i ett givet fall kan vara ett av dessa perspektiv lika gärna som en kombination av dem.

Tre sådana perspektiv beskrivs i nedanstående avsnitt. Samtliga perspektiv omhändertas i cyberförsvarspyramiden som presenteras i kommande avsnitt.

Cyberförsvaret som funktion

Cyberförsvar som en funktion i Försvarsmakten är ett organisatoriskt perspektiv som syftar till att underlätta ledning och utveckling av Försvarsmaktens cyberförsvarsresurser. Funktionen omfattar både personal och verksamhet på alla nivåer i Försvarsmakten. Utifrån funktionsperspektivet går det förhållandevis enkelt att lista ingående förband, enheter och stabsresurser.

Verksamheten avgränsas till de aktiviteter, inklusive cyberoperationer, som leds eller utförs av personal som ingår i funktionen.

Funktionens verksamhet är både förmågenyttjande och förmågeskapande.[21]

Cyberförsvaret som verksamhet

Det bredare verksamhetshetsperspektivet omfattar all den verksamhet i Försvarsmakten och totalförsvaret, såväl förmågeskapande som förmågenyttjande, som krävs för att i samtliga konfliktnivåer:

- upptäcka och möta ett väpnat angrepp i eller genom cyberdomänen,
- säkerställa att en motståndares aktiviteter i eller genom cyberdomänen inte förhindrar Försvarsmaktens förmåga att försvara Sverige mot ett väpnat angrepp, inklusive att genomföra mobilisering,
- förstärka skyddet av kritiska samhällsfunktioner i cyberdomänen,
- upptäcka och möta hybridaktiviteter med ingående cyberkomponenter som utförs av andra staters väpnade styrkor,
- genom åtgärder i cyberdomänen bidra till att totalförsvaret som helhet är krigsavhållande.

Verksamhetsperspektivet inkluderar utöver cyberförsvarsfunktionen ett stort antal andra funktioner och individer som utgör stöd och förutsättningar för att uppgifterna ska kunna lösas. Bland annat ingår förmågan att efter incidenter återställa system och tjänster till ett säkert tillstånd.

Vilka som i varje tillfälle bedriver cyberförsvarsverksamhet kan dock variera, liksom vilken chef som är understödd respektive stödjande. Eftersom en stor del av Försvarsmaktens personal såväl som dess informationssystem har direkta kopplingar till försvaret av Sverige innebär det att många av dessa vid något tillfälle har åtminstone indirekta roller i cyberförsvaret. Detsamma gäller inom andra försvarsmyndigheter samt verksamheter inom totalförsvaret, dock i något mindre utsträckning än inom Försvarsmakten.

Cyberförsvar som totalförsvars- och samhällsangelägenhet

Det sista och mest omfattande perspektivet involverar alla de verksamheter som på kort och lång sikt skapar förutsättningar för ett starkt cyberförsvar i ett allt mer digitaliserat och uppkopplat samhälle.

En långt ifrån uttömmande lista inkluderar ett ökat säkerhetsmedvetande på alla nivåer i samhället, ökade utbildningsvolymer av ingenjörer med cybersäkerhetskompetens samt en inhemsk industri som kan producera säkra och försvarbara informationssystem och kommunikationstjänster.

Att anlägga detta breda perspektiv bör inte tolkas som att alla medborgare är en del av cyberförsvaret, men väl att de utgör en del i samhällets totala motståndskraft och robusthet. Däremot är de tveklöst en del av samhällets cybersäkerhet, vilket är en förutsättning för ett starkt cyberförsvar. Detta kan liknas med att den som låser sitt säkerhetsskåp eller rapporterar säkerhetshotande verksamhet är avgörande för säkerhetsskyddet utan att för den sakens skull vara en del av den Militära underrättelse- och säkerhetstjänsten (Must) eller Säkerhetspolisen.

För att undvika sammanblandning mellan cyberförsvar och cybersäkerhet, samt behålla cyberförsvarets koppling till det militära försvaret och totalförsvaret anser författaren att det här mest omfattande perspektivet bör användas med viss försiktighet.

Stöd från andra är nödvändigt

Slutsatsen att cyberförsvar och cyberoperationer ingår i Försvarsmaktens huvuduppgift samt utgör en integrerad del av det militära försvaret innebär att Försvarsmakten har en ledande roll i Sveriges cyberförsvar på samma sätt som för det militära försvaret i övrigt. Denna roll omfattar både förmågeskapande och förmågenyttjande.

Att Försvarsmakten har en ledande roll betyder inte att det är den enda aktören. Precis som för övriga delar av det militära försvaret är cyberförsvarsverksamheten beroende av stöd från både försvarsmyndigheter och det övriga totalförsvaret. Genom att cyberförsvaret ska kunna agera i samtliga konfliktnivåer och på samma sätt som luft- och sjöstridskrafterna bedriva skarp verksamhet även i fred innebär det att behovet av stöd inte bara omfattar förberedelser för höjd beredskap och krig.

En myndighet som utgör ett viktigt stöd för Försvarsmakten, både avseende dess cyberförsvar och andra funktioner, är Försvarets radioanstalt, FRA, vilket också framgår av *Totalförsvaret 2021–2025*:

> Försvarets radioanstalt har genom signalunderrättelsetjänsten en viktig roll i att stödja Försvarsmaktens underrättelsebearbetning. Detta gäller även för cyberförsvaret, där det är särskilt angeläget att upprätthålla en god lägesuppfattning inom ett område med korta ledtider. Regeringen delar Försvarsberedningens bedömning att en nära samverkan mellan Försvarsmakten och Försvarets radioanstalt är nödvändig för att kunna bibehålla och utveckla förmågan över tid.[22]

Regeringen har i samband med försvarsbeslutet också säkerställt Försvarsmaktens möjligheter till detta stöd genom den uppdaterade instruktionen till Försvarets radioanstalt:

> 3 e § Försvarets radioanstalt ska stödja Försvarsmakten i verksamhet som avser utveckling och vidmakthållande av Försvarsmaktens cyberförsvarsförmåga.[23]

Försvarsmaktens och Försvarets radioanstalts uppgifter liksom viljan att stärka dessa återspeglas även i budgetpropositionen:

> Regeringen avser stärka och utveckla cyberförsvarsförmågan i enlighet med propositionen *Totalförsvaret 2021–2025* (prop. 2020/21:30). Det inbegriper Försvarsmaktens förmåga att, med stöd av Försvarets radioanstalt, genomföra defensiva och offensiva operationer i cyberdomänen.[24]

Därutöver behöver cyberförsvaret exempelvis stöd i form av lägesbilder och incidentrapporter från bland annat säkerhetstjänsterna, Myndigheten för samhällsskydd och beredskap, MSB, och bevakningsansvariga myndigheter samt andra verksamheter som är viktiga för Försvarsmaktens förmåga. Behovet påtalas även i *Totalförsvaret 2021–2025*:

> En del i detta är en ökad rapportering av it-incidenter till MSB enligt förordningen (2015:1052) om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap, liksom anmälan vid säkerhetshotande händelser och verksamhet till Säkerhetspolisen och Försvarsmakten enligt säkerhetsskyddsförordningen (2018:658).[25]

För incidentrapporter som inte berör säkerhetskänslig verksamhet kan det ansvar som Myndigheten för samhällsskydd och beredskap har tillsammans med tillsynsmyndigheterna utifrån lagen om informationssäkerhet för samhällsviktiga och digitala tjänster[26] utgöra ett värdefullt stöd till upprätthållandet av Försvarsmaktens cyberlägesbild.

Den samverkan och informationsdelning som sker med andra myndigheter inom ra-

men för Nationellt cybersäkerhetscentrum (NCSC) kommer sannolikt att utgöra ett betydelsefullt stöd avseende information om händelser med relevans för cyberförsvaret som inträffar utanför Försvarsmaktens egna informations- och kommunikationssystem. Försvarsmakten, i sin tur, kan stödja övriga myndigheter i centret med det militära perspektivet, avdela kvalificerade resurser efter begäran utifrån stödförordningen,[27] samt delge sådan information ur Försvarsmaktens cyberlägesbild som är av betydelse för övriga aktörer.

Cyberförsvar respektive underrättelsetjänst

Cyberförsvaret är en konsument av underrättelser. Genom mottagna underlag kan cyberförsvaret vidta förebyggande och skadebegränsande åtgärder för att skydda och försvara informationssystem och elektroniska kommunikationstjänster från kvalificerade antagonister.

I *Totalförsvaret 2021–2025* framgår på flera ställen vikten av effektiv underrättelseförmåga i relation till cyberförsvaret. Ett exempel återges nedan:

> Utvecklingen av defensiv och offensiv cyberförsvarsförmåga bygger på tre samverkande delar: kunskap om hoten, skyddsåtgärder och motåtgärder. Det kräver i sin tur en stark säkerhetstjänst och försvarsunderrättelseförmåga för att kunna förebygga och identifiera hotande verksamhet, god förmåga att upptäcka, varna för och hantera intrång och angrepp, samt ett starkt skydd av de mest skyddsvärda verksamheterna i samhället.[28]

Genom försvarsmaktsinterna samarbeten skapas förutsättningar för säkerhetstjänsten och cyberförsvaret att inom sina respektive ansvarsområden kunna agera på hotinformation från underrättelsetjänsten. Genom Försvarsmaktens möjlighet att inrikta övriga försvarsunderrättelsemyndigheter kan respektive myndighet tillföra värdefull information inom sitt kompetensområde, som sedan sätts ihop till en kvalificerad helhet.

Försvarsmakten har genom sin instruktion även en särskild uppgift i att ta fram underlag för höjd beredskap:

> 3 § Försvarsmakten ska bedriva omvärldsbevakning och upptäcka och identifiera yttre hot mot Sverige och svenska intressen samt ta fram underlag för beslut om höjd beredskap.[29]

Eftersom antagonistiska aktiviteter i cyberdomänen kan vara indikatorer för ett kommande angrepp såväl som annan hotande verksamhet mot svenska intressen kan cyberförsvarsfunktionen genom sin verksamhet stödja Försvarsmaktens samlande bedömningar.

Cyberförsvar respektive säkerhetstjänst

Cyberförsvaret och säkerhetstjänsten är två funktioner som har många inbördes relationer och beroenden. Säkerhetstjänsten och cyberförsvaret kompletterar varandra och har ett gemensamt intresse i arbetet att förhindra obehörig åtkomst till informationssystem och elektroniska kommunikationstjänster som är av särskild vikt för Sveriges säkerhet. Det finns dock principiella skillnader avseende uppgifter, målsättningar och mandat.

Säkerhetstjänsterna (både den militära och den civila) har ett brett perspektiv med ansvar och mandat inom alla tre delarna av säkerhetsskyddet (informations-, personal- och fysisk säkerhet). Innebörden av säkerhetsskydd återges i säkerhetsskyddslagens första kapitel:

> 2 § Med säkerhetsskydd avses skydd av säkerhetskänslig verksamhet mot spionerі, sabotage, terroristbrott och andra brott som kan hota verksamheten samt skydd i andra fall av säkerhetsskyddsklassificerade uppgifter.[30]

Med utgångspunkt från säkerhetsskyddslagstiftningen leds arbetet genom bland annat föreskrifter, tillsyn samt uppföljning och analys av inträffade incidenter. Säkerhetstjänsternas arbete är i många avseenden nära förknippat med skyddet av Sveriges säkerhetskänsliga verksamhet.

Cyberförsvaret verkar framför allt i cyberdomänen och med utgångspunkt i Försvarsmaktens huvuduppgift att möta ett väpnat angrepp. Centralt i cyberförsvarets intressesfär är att förhindra att en antagonistisk statlig aktör genom aktiviteter i cyberdomänen kan påverka funktionalitet och tillgänglighet i informations-, kommunikations- och verkanssystem som är väsentliga för Försvarsmaktens förmåga att bedriva väpnad strid. Utöver att planera och genomföra cyberoperationer och incidenthantering i alla konfliktnivåer leder cyberförsvaret inom cyberdomänen planeringen för höjd beredskap och väpnat angrepp. Denna planering utgår från Försvarsmaktens uppgift att bedriva försvarsplanering och omfattar både Försvarsmakten och det övriga totalförsvaret.

Nedan återges några exempel som belyser några skillnader mellan säkerhetstjänsterna och cyberförsvaret.

- Säkerhetstjänsternas intressesfär omfattar all säkerhetsskyddsklassificerad information, oavsett om den är digital eller på papper. Cyberförsvaret verkar i cyberdomänen; information på papper är bara en angelägenhet om den röjer cyberförsvarets skyddsvärden och är även i det fallet i första hand en fråga för säkerhetstjänsterna.
- Säkerhetstjänsternas mandat och tillsynsområden är uppdelade i en militär (Försvarsmakten) och en civil (Säkerhetspolisen) del. Cyberförsvaret behöver kunna agera inom båda områdena för att exempelvis kunna försvara civila system som Försvarsmakten är beroende av för att kunna möta ett väpnat angrepp. Cyberförsvaret kan även behöva agera för att skydda eller försvara system som inte faller under säkerhetsskyddslagstiftningen.
- Att förhindra eller upptäcka legitima användare som utnyttjar erhållna privilegier i ett system för att obehörigt ta del av eller sprida säkerhetsskyddsklassificerad information är en uppgift för säkerhetstjänsten. Detta ligger utanför cyberförsvarets mandat och uppgifter.
- Cyberförsvaret dimensioneras för att möta statliga aktörer vid höjd beredskap och i krig, med fokus på den väpnade striden. Även för säkerhetstjänsterna är statliga aktörer den dimensionerande faktorn men de behöver också inrikta skyddet mot övriga hotaktörer såsom terrorism och kriminalitet. Ur ett cyberförsvarsperspektiv förväntas hoten från kriminella framför allt hanteras i det grundläggande cybersäkerhetsarbetet, även om cyberförsvaret givetvis kan stödja med kvalificerade resurser för exempelvis incidenthantering.

Ovanstående exempel belyser några av skillnaderna. Genom sina olika uppgifter och mandat kompletterar säkerhetstjänsten och cyberförsvaret varandra i skyddet av svenska intressen. En stor del av säkerhetstjänstens arbete är dessutom förutsättningsgivande för cyberförsvaret liksom annan skyddsvärd verksamhet inom totalförsvaret.

Säkerhetstjänsterna har exempelvis viktiga roller i säkerhetsprövningen av den personal som verkar inom cyberförsvaret, samt upprätthållande av fysisk säkerhet i exempelvis datorhallar och andra anläggningar för informationssystem och elektroniska kommunikationstjänster som används för säkerhetskänslig verksamhet.

Säkerhetsskyddslagen ger också Försvarsmakten och Säkerhetspolisen möjlighet att förhindra överlåtelser av säkerhetskänslig verksamhet. I relation till cyberförsvaret kan sådan verksamhet till exempel utgöras av elektroniska kommunikationstjänster eller styr- och reglersystem som Försvarsmakten direkt eller indirekt är beroende av för att kunna möta ett väpnat angrepp.

Cyberförsvar inom totalförsvaret

I *Inriktning för Försvarsmakten 2021–2025* finns en överordnad inriktning för totalförsvaret:

> Totalförsvaret ska vara krigsavhållande genom att ha en sådan styrka, sammansättning, ledning, beredskap, uthållighet och planering att det avhåller från försök att anfalla, kontrollera eller på annat sätt utnyttja vårt land.[31]

För att cyberangrepp inte ska vara det enklaste sättet att slå ut eller begränsa försvarsförmågan behöver särskilt viktiga system och funktioner i totalförsvaret dels ha tillräcklig grundsäkerhet, dels förberedas för att vid höjd beredskap kunna förstärkas med kvalificerade cyberförsvarsresurser.

En särskild utmaning för Försvarsmakten såväl som övriga totalförsvarsmyndigheter är det allt större beroendet av externa tjänster och funktioner, som i många fall i sin tur är beroende av flera olika informationssystem och elektroniska kommunikationstjänster.

Dessa system och tjänster kan i sin tur tillhandahållas av andra leverantörer än den som erbjuder den primära tjänsten eller funktionen. De kan också vara samlokaliserade i samma datorhallar utan att totalförsvarets aktörer är medvetna om detta och den risk som därmed uppstår att flera viktiga funktioner slås ut vid ett och samma angrepp. Dåligt skyddade system som har anslutningar till varandra kan också nyttjas som språngbrädor av en angripare.

I *Totalförsvaret 2021–2025* uttrycks utmaningen tydligt:

> De mest kvalificerade hotaktörerna kommer alltid att agera mot de svagaste länkarna i våra sammankopplade system och därför behöver hela hotskalan inom cybersäkerhetsområdet tas i beaktande ur ett totalförsvarsperspektiv.[32]

För att exemplifiera kan det ur en angripares perspektiv vara enklare att genom cyberdomänen försöka påverka det system som styr kylan i datorhallen för ett logistiksystem snarare än att verka kinetiskt mot logistikföretagets enskilda transporter till Försvarsmakten.

Försvarsmaktens uppgifter och ansvar

Genom § 2 a i myndighetsinstruktionen har Försvarsmakten, utöver att organisera krigsförband i uppgift att ”[…] vidta de förberedelser i övrigt som behövs för att kunna lösa myndighetens huvuduppgift.”[33]

Försvarsmakten behöver därför skapa förutsättningar för att kunna skydda och försvara prioriterade informationssystem och kommunikationstjänster som Försvarsmakten är beroende av för att möta väpnat angrepp och genomföra mobilisering, oavsett om systemet är myndighetsinternt, finns hos en annan totalförsvarsmyndighet eller

finns hos en enskild näringsidkare. Detta gäller i två samtidiga perspektiv:

1) Funktioner och tjänster som Försvarsmaktens samtliga stridskrafter är beroende av.
2) Funktioner och tjänster som cyberförsvarsfunktionen själv behöver för att genomföra sin verksamhet till stöd för punkt 1 ovan.

Utöver att säkerställa den egna förmågan ska Försvarsmakten i krig kunna förstärka skyddet av kritiska samhällsfunktioner:

> Försvarsmakten ska därutöver i händelse av krig med befintlig förmåga och resurser kunna förstärka skyddet av kritiska samhällsfunktioner.[34]

Till följd av samhällets beroenden till digitala informationssystem och elektroniska kommunikationstjänster utgår Försvarsmakten från att sådan förstärkning kan komma att krävas även i cyberdomänen.

Uppgiften att genomföra nödvändig planering för att åstadkomma ovanstående regleras genom Försvarsmaktens myndighetsinstruktions 3 och 7 §§ om försvarsplanering:

> 3 § […] Försvarsmakten ska ha en aktuell försvarsplanering. Planeringen ska omfatta alla resurser som är nödvändiga för att genomföra Försvarsmaktens verksamhet.
>
> [---]
>
> 7 § Försvarsmakten ska samordna försvarsplaneringen inom myndigheten med motsvarande planering inom övriga delar av totalförsvaret. […]
>
> Försvarsmakten får ta del av planeringen för höjd beredskap hos de myndigheter som är bevakningsansvariga myndigheter enligt förordningen (2015:1052) om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap.[35]

Försvarsmakten har vidare, av regeringen, fått inriktningen att planera för att stöd kommer att ges från övriga totalförsvaret.[36]

Försvarsmaktens ansvar gentemot övriga aktörer är framför allt samordnande och inriktande. Precis som för cybersäkerhet i allmänhet måste merparten av det förmågehöjande arbetet göras på bredden och av de aktörer som har verksamhet eller funktioner som utgör beroenden för att det militära försvaret ska kunna möta ett väpnat angrepp eller mobilisera.

Som ett verktyg i arbetet med att inrikta och samordna totalförsvarsplaneringen har Försvarsmakten i samverkan med MSB infört Stärkt informations- och cybersäkerhet som ett av sex fokusområden i den handlingsplan[37] som ÖB och vikarierande GD MSB undertecknade i augusti 2021.

Övriga totalförsvarsaktörers ansvar och uppgifter

Utöver specifikt stöd till delar som rör cyberförsvarets kärnverksamhet, kan totalförsvaret och resten av samhället, inklusive enskilda medborgare, bidra till ett robust samhälle genom att säkerställa att de egna systemen och tjänsterna fungerar även under påfrestande förhållanden. Detta inkluderar kontinuitetsplanering som hålls aktuell och regelbundet övas såväl som en tillräckligt god nivå av cybersäkerhet. Om detta görs kan de mest kvalificerade resurserna avdelas för att skydda och försvara de mest kritiska systemen i samhället.

Behovet att tillräcklig informations- och cybersäkerhet framgår av *Totalförsvaret 2021–2025:*

> En förutsättning för ett starkt cyberförsvar är, i enlighet med vad regeringen framhåller i budgetpropositionen för 2021, att samtliga aktörer inom totalförsvaret har en god informations- och cybersäkerhet.[38]

Som redan nämnts ingår detta sedan hösten 2021 som ett särskilt fokusområde i handlingsplanen för totalförsvaret. Grundnivån av cybersäkerhet är därutöver i stor utsträckning reglerad genom författningar och föreskrifter. En heltäckande redogörelse ligger utanför den här artikeln, men i sammanhanget kan följande paragraf från *förordningen om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap* nämnas:

> 19 § Varje myndighet ansvarar för att egna informationshanteringssystem uppfyller sådana grundläggande och särskilda säkerhetskrav att myndighetens verksamhet kan utföras på ett tillfredsställande sätt. Därvid ska behovet av säkra ledningssystem särskilt beaktas.[39]

Verksamhetsutövare vars system används för säkerhetskänslig verksamhet behöver dessutom förhålla sig till säkerhetsskyddsförordningen, där första stycket i 3 kap 4 § första stycke lyder:

> 4 § En verksamhetsutövare som ansvarar för ett informationssystem som ska användas i säkerhetskänslig verksamhet ska vidta lämpliga skyddsåtgärder för att kunna upptäcka, försvåra och hantera skadlig inverkan på informationssystemet samt obehörig avlyssning av, åtkomst till och nyttjande av informationssystemet. Verksamhetsutövaren ska också se till att spårbarhet finns för händelser som är av betydelse för säkerheten i systemet.[40]

Eftersom elektroniska kommunikationstjänster kommer att vara av minst lika stor betydelse under höjd beredskap och ytterst krig är det i sammanhanget värt att nämna Post- och telestyrelsen samt *förordningen om elektronisk kommunikation:*

> 5 § Post- och telestyrelsen får meddela sådana föreskrifter om den fredstida planeringen för totalförsvarets behov av elektroniska kommunikationer som avses i 1 kap. 8 § andra stycket lagen (2003:389) om elektronisk kommunikation. Post- och telestyrelsen ska då beakta frågor om prioriterade abonnemang och krigsabonnentplaner.[41]

Som komplement till lagstiftningen kan aktörer inom totalförsvaret skapa ytterligare förutsättningar för att omhänderta egna och Försvarsmaktens behov i upphandlingar och beställningar till leverantörer.

Det ska slutligen konstateras att de åtgärder och förberedelser som genomförs för höjd beredskap och väpnat angrepp i organisationer utanför Försvarsmakten i stor utsträckning också kommer att vara användbara i fred och därmed stärka Sveriges samlade motståndskraft inom cyberområdet.

Hybridaktiviteter och gränsdragningsproblem

I *Totalförsvaret 2021–2025* finns en utförlig beskrivning av hybridhot. I flera fall nämns i dessa sammanhang cyberattacker eller cyberangrepp:

> […] Cyberangrepp kan också utgöra en delmängd av eller en indikator för ett sammansatt antagonistiskt angrepp, s k hybridaktivitet. Detta är aktiviteter som sker i hela hotskalan, i fredstid, beredskap och då ytterst i krig. Hanteringen av sådana sammansatta aktiviteter förutsätter god lägesuppfattning och förmåga till förvarning.[42]

Det finns därför skäl att närmare beskriva Försvarsmaktens och andra myndigheters ansvar och uppgifter att möta hybridaktiviteter med cyberkomponenter. Det faktum att Försvarsmakten i cyberdomänen ska kunna verka i samtliga konfliktnivåer är i paritet med att hybridaktiviteterna sker i hela hotskalan.

Ordet *hybridaktivitet* används här för att beteckna något av de följande:

a) en *kombination* av medel som en antagonist nyttjar, ”[…] i såväl fred som i höjd beredskap och ytterst krig, för att avsiktligt störa samhällens funktionalitet eller påverka opinioner, beslutsfattare och demokratiska processer.”[43] Beroende på grad av konflikt kommer den militära komponenten att vara mer eller mindre påtaglig och ha varierande grad av förnekbarhet,

b) militära medel som används selektivt, via ombud, dolt eller med förnekbarhet, nyttjade på ett sådant sätt att de *samtidigt ingår* som komponenter i normal civil samhällsverksamhet.[44]

Hybridaktiviteter, liksom enskilda maktmedel, kan riktas direkt eller indirekt mot det militära försvaret eller totalförsvaret och ske med olika syften med både kort- och långsiktiga målsättningar. Aktiviteterna kan dock lika gärna, eller i vissa fall i större utsträckning, riktas mot det civila samhället. Utgångspunkten är att en antagonist kommer att försöka uppnå sina målsättningar med minsta möjliga resursutnyttjande, vilket innebär att en cyberkomponent kan vara ett attraktivt medel om försvararen bedöms ha en otillräcklig nivå av cybersäkerhet.

En vektor eller hävstång för hybridaktiviteter är de gränsdragningsproblem som återfinns i alla staters förvaltningsmodeller. Gränsdragningsproblemen uppstår där konceptuella kategorier överlappar. Tre exempel på sådana kategorier, som även har inbördes relationer är:

a) gränser mellan olika typer av maktmedel (militära respektive civila, olika typer av militära maktmedel, militära maktmedel som utnyttjas i ett civilt sammanhang och framför allt under gränsen för ett väpnat angrepp),

b) gränser mellan olika myndigheters ansvar och mandat,

c) samt gränsen för vilket nyttjande av maktmedel som utgör ett väpnat angrepp.

Dessa gränsdragningsproblem benämns ofta som gråzonsproblematik.[45] Notera dock särskilt att problematiken, även om den ibland framställs så, inte är ett särskilt skede utan något som förekommer i samtliga beredskaps- och konfliktnivåer.[46]

Genom att enskilt eller i en sammansatt hybridaktivitet exploatera ett eller flera gränsdragningsproblem gör angriparen det svårare för den utsatte att hantera problemen var för sig såväl som att avgöra om de ingår i en sammanhängande strategi som ytterst kan vara förberedelser för ett väpnat angrepp.

Ett exempel som tangerar alla ovanstående kategorierna är cyberattacker:

- En cyberattack utförd av statliga aktörers väpnade styrkor utgör ett militärt maktmedel. En stor del i utmaningen ligger i att klarlägga vem som ligger bakom; detta är dock inte unikt för cyberdomänen utan samma problematik föreligger i andra domäner.
- Cyberattacker kan också utföras av statliga eller statsunderstödda aktörer som inte är en del av landets väpnade styrkor samt av kriminella organisationer. Beroende på aktör, målval och konsekvenser kan attacken betraktas som ett väpnat angrepp eller som en kriminell handling.

Därtill förekommer it-relaterad brottslighet som sker i syfte att uppnå ekonomisk vinning och inte primärt avser att slå ut eller degradera funktionalitet. Som exempel

kan nämnas industrispionage, utpressning inklusive så kallad ”ransomware”,[47] bedrägerier och förfalskningar.

De medel som ingår i en hybridaktivitet är i sig inte nya. Det är därför ingen slump att de i många fall kan inordnas under säkerhetstjänstens traditionella säkerhetshot[48] i form av subversion, sabotage, främmande underrättelseverksamhet och kriminalitet:

- Påverkansoperationer i syfte att få beslutsfattare att agera på ett visst sätt (inklusive att inte agera alls) kan utgöra subversion, oavsett om informationen förmedlas via sociala medier eller på annat sätt. Det finns också stora likheter mellan subversion och påverkansoperationer avseende tillvägagångssätt även om påverkansoperationer är ett något vidare begrepp än subversion.
- Sabotage kan genomföras både direkt fysiskt och genom cyberdomänen, samt kombineras med subversiv verksamhet i en hybridaktivitet.
- Metoder för underrättelsehämtning kommer fortsätta att utvecklas i takt med att tekniken gör det. Att en sådan metod kan vara it-intrång omnämns exempelvis redan i 2007 år version av Försvarsmaktens handbok för säkerhetsskyddstjänsten.[49]
- Kriminalitet kan vara säkerhetshotande oavsett om förövaren gör det på uppdrag av en statsaktör eller ej och oavsett nyttjande av digitala verktyg.

Hybridaktiviteter och gränsdragningsproblematik förekommer i samtliga konfliktnivåer, även om intensiteten såväl som statsmaktens svar på dem kan variera utifrån rådande omvärldsläge. Gränsdragningsproblemens omfattning eller existens är inte heller konstanta. Lagar och förordningar förändras över tid och om riksdag eller regering beslutar om högsta beredskap eller att riket är i krig träder omedelbart ett antal lagar i kraft som ger omfattande förändringar i bland annat Försvarsmaktens mandat.

Att möta och hantera hybridaktiviteter med cyberkomponenter

På samma sätt som att hybridaktiviteter är en kombination av medel så möts dessa hot genom en kombination av egna förmågor. Precis som när det gäller cybersäkerhet är ansvarsförhållandena för att möta dessa hot till stor del reglerade.

På ett övergripande plan gör hybridaktiviteternas natur underrättelse- och säkerhetstjänsterna till centrala aktörer[50] i att upptäcka och identifiera dessa aktiviteter samt förmedla relevant information till de myndigheter och funktioner som har i uppgift att hantera dem. Detta poängteras också i *Inriktning för Försvarsmakten 2021–2025:*

> Förmågan att agera på underrättelser är en viktig del i utvecklingen av totalförsvaret, även avseende förmågan att hantera hybridhot. Den bredare hotbilden mot Sverige medför behov av att stärka samverkan mellan säkerhets- och underrättelsetjänsterna för att säkerställa en god gemensam lägesuppfattning över hela hotskalan.[51]

När det gäller hybridaktiviteter med cyberkomponenter[52] gäller, på samma sätt som att det är en förutsättning för ett starkt cyberförsvar, att hela samhället och inte minst aktörerna i totalförsvaret har tillräckligt god informations- och cybersäkerhet. Detta ger ett grundskydd som minskar manöverutrymmet för en potentiell antagonist. Därutöver gäller följande:

- För att möta ett väpnat angrepp i eller genom cyberdomänen ansvarar Försvars-

makten, oavsett om det sker som en hybridaktivitet eller som en del i ett storskaligt väpnat angrepp.

- För att möta subversion och främmande underrättelseverksamhet har Försvarsmakten och Säkerhetspolisen ett särskilt ansvar. För att möta subversiv verksamhet och påverkansoperationer på ett bredare plan har även Myndigheten för psykologiskt försvar en roll. Inom Försvarsmakten är cyberförsvarsfunktionens roll i båda fallen begränsad så länge inte en antagonist försöker komma åt något av de system som är av särskild betydelse för att möta ett väpnat angrepp.
- För att möta sabotage ansvarar framför allt Försvarsmakten, Säkerhetspolisen och Polismyndigheten. Cyberförsvarsfunktonen har ett särskilt intresse att möta sabotage som genom cyberdomänen riktas mot för försvarsförmågan kritiska system, inte minst till följd av den gränsdragningsproblematik som i sådana lägen uppstår mellan sabotage och väpnat angrepp.
- Hantering av kriminalitet utanför Säkerhetspolisens mandat är framför allt Polismyndighetens och andra rättsvårdande myndigheters ansvar, även om Försvarsmaktens militärpoliser har polismans befogenhet inom militärt område. Cyberförsvarsfunktionen har dock ett intresse att få kännedom om sådan brottslighet som kan påverka kritiska system och funktioner inom dess intressesfär.

För hybridaktiviteter med cyberkomponenter kommer även de möjligheter för förenklad informationsdelning som uppstår genom samlokaliseringen i Nationellt cybersäkerhetscentrum öka ansvariga myndigheters förutsättningar att snabbt identifiera misstänkta händelser. Kopplat till Försvarsmaktens uppgift att ta fram underlag för höjd beredskap har cyberförsvarsfunktionen en stödjande roll gentemot både den militära underrättelse- och säkerhetstjänsten och den militärstrategiska ledningen.

I samtliga fall ovan där cyberförsvarsfunktionen inte har en explicit roll kan dess resurser på begäran stödja de aktörer som i varje enskilt fall ansvarar för ärendet.

Cyberförsvarets stöd till samhället i fred

Vid högsta beredskap är totalförsvar den överordnade prioriteten och är all den samhällsverksamhet som då ska bedrivas. I det läget stödjer det civila samhället Försvarsmakten. I lägre beredskapsnivåer kan istället Försvarsmakten, under vissa förutsättningar, stödja det civila samhället.

Inom cyberförsvaret har Försvarsmakten kvalificerade resurser som i många fall är unika. Dessa resurser är i flera avseenden användbara när samhället utsätts för påfrestningar inom cyberområdet. Genom *Inriktning för Försvarsmakten 2021–2025* har Försvarsmakten fått följande uppgift:

> Försvarsmakten ska i fredstid ha förmåga att:
>
> […]
>
> – med befintliga resurser förstärka skyddet av prioriterade kritiska samhällsfunktioner,
>
> – med befintliga resurser kunna lämna stöd till civil verksamhet.[53]

Motsvarande uppgifter gäller, som redan konstaterats, även i krig. Den sista strecksatsen ingår även i Försvarsmaktens myndighetsinstruktion.[54]

Genomförande av sådana förstärkningar som nämns i inriktningen kan i fred kräva

särskilda beslut från regeringen och i vissa fall även författningsändringar. Däremot finns det sedan många år tillbaka förutsättningar för att lämna stöd genom lagen om Försvarsmaktens stöd till polisen vid terrorismbekämpning,[55] samt förordningen om Försvarsmaktens stöd till civil verksamhet.[56]

De huvudsakliga skillnaderna mellan dessa författningar rör i vilken utsträckning våld eller tvång får användas mot enskilda, vilka som får begära stödet, samt huruvida Försvarsmakten får eller ska avdela stöd. Möjligheten att avdela stöd gäller även enskild verksamhet som är av intresse för samhället:

> 5 § Försvarsmakten får på begäran även lämna stöd till enskilda om det är fråga om en verksamhet som är av intresse för samhället eller om Försvarsmaktens medverkan kan inordnas som ett led i den utbildning som bedrivs vid myndigheten.[57]

Somframgårfinnssåledesförfattningsmässiga möjligheter för Försvarsmakten att lämna stöd i form av cyberförsvarsresurser. Detta är dock en begränsad resurs som framför allt är dimensionerad för att möta de mest kvalificerade antagonisterna. Detta har en särskild betydelse utifrån stödförordningens begränsning i vilken utsträckning stöd får lämnas:

> 6 § Försvarsmakten får lämna stöd enligt 3–5 §§ endast om Försvarsmakten har resurser som är lämpliga för uppgiften och det inte allvarligt hindrar dess ordinarie verksamhet eller dess medverkan enligt lagen (2003:778) om skydd mot olyckor.[58]

Att Försvarsmakten har kvalificerade resurser som utan tvekan kan anses lämpliga inom cybersäkerhetsområdet är uppenbart. Däremot innebär det andra kriteriet att stödet framför allt behöver ske inom ramen för den ordinarie verksamheten. Detta kan omfatta stöd som lämnas på begäran av de myndigheter[59] som ingår i nationellt cybersäkerhetscentrum (NCSC) men framför allt till sådana totalförsvarsaktörer som ansvarar för informationssystem och kommunikationstjänster vilka är kritiska för Försvarsmaktens förmåga att försvara Sverige mot ett väpnat angrepp eller att genomföra mobilisering.

Ovanstående avser det direkta stödet. Indirekt stödjer Försvarsmakten inom cyberområdet dessutom totalförsvaret och samhället genom olika typer av samverkan, föreläsningar och inte minst övningsverksamhet. Inom personalförsörjningsområdet, där cybersäkerhetskompetens är en bristvara, förväntas många av de upp till 60 värnpliktiga cybersoldater som årligen utbildas fortsätta sina karriärer inom cybersäkerhetsområdet och då framför allt som anställda utanför Försvarsmakten. Detsamma gäller de planerade reservofficersutbildningarna, där officerarna i sina civila roller kommer att bidra till både den allmänna cybersäkerhetskompetensen men också förståelsen för cyberförsvaret. Hela samhället kommer också att kunna dra nytta av resultaten från forskningscentrumet för cyberförsvar och informationssäkerhet (CDIS) som Försvarsmakten och KTH etablerat.

Närliggande verksamhet utanför cyberförsvaret

Det finns, utöver cybersäkerhet, två ytterligare områden som ofta blandas ihop med cyberförsvar: telekrig samt psykologiskt försvar. Att kunna agera inom dessa områden är nödvändigt i samtliga konfliktnivåer och inte minst gentemot en högteknologisk motståndare. Det är dock andra funktioner än cyberförsvaret som ansvarar för dessa verksamheter. I vanlig ordning gäller att

funktionerna kan kombineras för att uppnå önskad effekt i en given operation.

Telekrig

Det finns en likhet mellan cyberoperationer och telekrigsåtgärder i det att båda kan användas för att degradera motståndarens ledningsstöds- och stridsledningssystem inklusive dess kommunikationslänkar. Båda disciplinerna nyttjar dessutom i olika utsträckning det elektromagnetiska spektrumet. Det finns dock flera principiella skillnader, där två framträdande sådana är att:

- för telekrig är *verkan i* det elektromagnetiska spektrumet det primära. För en cyberoperation är *transmission genom* det elektromagnetiska spektrumet *en av flera* möjliga transmissionstyper för att nå målet.
- telekrigsaktiviteter verkar mot specifika sändare eller mottagare i närheten. För cyberoperationer är fysisk närhet till målet mindre relevant till följd av cyberdomänens globala utbredning. Kommunikation i cyberdomänen sker typisk via flera sammankopplande länkar där de mellanliggande sändarna och mottagarna i många fall är ointressanta.

Psykologiskt försvar och påverkansoperationer

I *Totalförsvaret 2021–2025* beskrivs utmaningarna med påverkansoperationer i flera olika sammanhang. Till exempel:

> Påverkansoperationer för att störa förmågan att fatta beslut och försvarsviljan kommer att vara en del i krigföringen.[60]

Även om påverkansoperationer ofta nämns i samma sammanhang som cyberhot är de verksamheter som möter dem, cyberförsvar och psykologiskt försvar, skilda från varandra. Att möta påverkansoperationer kräver kompetens inom strategisk- och militärstrategisk kommunikation samt kognitionsvetenskap, medan cyberförsvarets tekniska kompetensprofiler framför allt har en grund inom datorteknik, datakommunikation och datavetenskap.

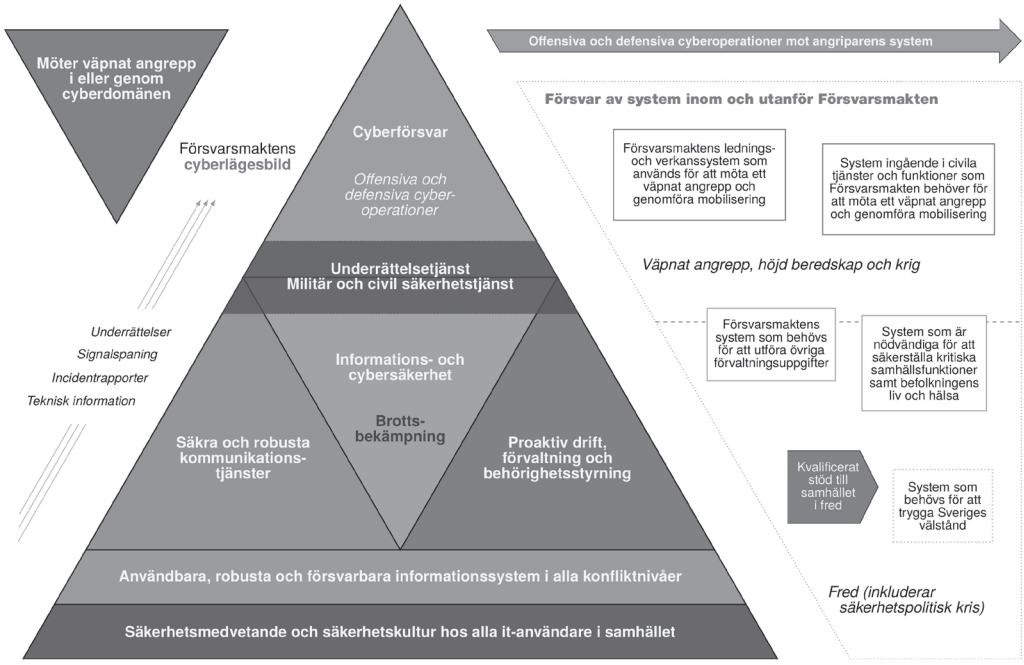
Naturligtvis kan en påverkansoperation använda digitala kanaler, men det är först om en angripare gör ett intrång i ett informationssystem, exempelvis i syfte att sprida ett budskap eller misskreditera den som ansvarar för systemet, som det blir en cybersäkerhetsfråga. Beroende på aktör eller andra omständigheter kan cyberförsvarsresurser i ett sådant läge stödja i incidenthanteringen.

Cyberförsvarspyramiden

Cyberförsvarspyramiden är en modell som på ett överskådligt sätt beskriver cyberförsvarets kärnuppgifter samt dess samverkande funktioner och förutsättningsskapande komponenter. Andra geometriska former har utvärderats, men pyramidformen har funnits ge flera fördelar i att skapa en sammanhängande förklaringsmodell. Bland annat är förhållandet mellan basen och spetsen väsentlig; basen är alltid bredare än spetsen.

De förebyggande aktiviteter som genomförs närmare basen och därmed på bredden i samhället har potential att markant höja ribban för en angripare och samtidigt minska allvarlighetsgraden i de incidenter som förr eller senare alltid kommer att uppstå. På samma gång frigörs de mest kvalificerade och därmed också de mest begränsade resurserna för att försvara de högst prioriterade systemen mot de mest kvalificerade hotaktörerna.

Spetsen och basen fyller således olika funktioner men tas någon bort blir pyramiden ofullständig. Detsamma gäller för övriga



delar. Pyramiden förmedlar därmed att alla delarna är nödvändiga för att upprätthålla ett svenskt cyberförsvar; varje del som underdimensioneras eller tas bort får konsekvenser för helheten. Det går samtidigt att resonera kring varje enskild del och vad som där särskilt behöver utvecklas eller upprätthållas för att ge nödvändigt stöd till andra delar av pyramiden.

Det ska slutligen påtalas att blocket för underrättelse- och säkerhetstjänst avsiktligt överlappar både ovan- och underliggande delar i pyramiden. Avsikten är att särskilt lyfta fram den viktiga roll dessa funktioner har samt visa att deras ansvarsområden delvis överlappar åt båda hållen.

Cyberdomänen

Cyberdomänen är tillsammans med mark-sjö-, luft- och rymddomänen de domäner där Försvarsmakten ska kunna genomföra operationer samt möta ett väpnat angrepp. Domänen består av digitala informationssystem och elektroniska kommunikationstjänster samt de data som lagras i, bearbetas med, eller förmedlas genom dessa system och tjänster.

En *cyberoperation* är en operation vars målsättningar uppnås genom aktiviteter i cyberdomänen. I domänen ingår bland annat ledningsstödsystem, stridsledningss- och verkanssystem, intranät, styr- och reglersystem, telekommunikationssystem, de uppkopplade sakernas internet, inbyggda system i anläggningar, fordon och farkoster samt inte minst Internet. Delar av cyberdomänen ingår i eller utgör beroenden för Sveriges kritiska infrastruktur och samhällsfunktioner.

Händelser och incidenter i cyberdomänen där cyberförsvarsresurser inklusive den militärstrategiska ledningen behöver involveras kan initieras inom alla delar i pyra-

miden. Beroende på typen av incident och framför allt bakomliggande aktör kan den fortsatta hanteringen sedan antingen ledas av Försvarsmakten eller någon av de rättsvårdande myndigheterna.

Cyberförsvar

Cyberförsvaret ska inom cyberdomänen kunna verka i samtliga konfliktnivåer men dimensioneras för att vid höjd beredskap och under väpnat angrepp kunna möta de mest kvalificerade aktörerna.

Kärnan i cyberförsvaret är förmågan till offensiva och defensiva cyberoperationer samt att upptäcka, identifiera och avvärja hot mot digitala informationssystem och elektroniska kommunikationstjänster som är väsentliga för att hävda Sveriges territoriella integritet, möta ett väpnat angrepp samt på andra sätt främja Sveriges säkerhet. Cyberförsvaret bidrar till att försvåra och höja tröskeln för en aktör som överväger att angripa eller utöva påtryckningar mot Sverige eller svenska intressen.

Vid höjd beredskap och under väpnat angrepp prioriteras försvaret av Försvarsmaktens lednings- och verkanssystem samt civila system som utgör beroenden för de tjänster och funktioner Försvarsmakten behöver för att kunna möta väpnat angrepp och genomföra mobilisering. Försvarsmakten ska även, med befintliga resurser, kunna förstärka skyddet av samhällskritiska funktioner.

Försvarsmaktens cyberförsvarsresurser kan i fred användas för att stödja samhället under kriser eller andra allvarliga händelser. Bland annat kan stöd avdelas för att bistå med skydd, försvar och incidenthantering för system som behövs för att säkerställa kritiska samhällsfunktioner, inklusive befolkningens liv och hälsa, samt system som i övrigt behövs för att trygga Sveriges välstånd.

Försvarsmaktens cyberlägesbild

Cyberdomänen är till sin natur komplex i sin uppbyggnad samtidigt som mycket korta tidsförhållanden föreligger vid attacker. Försvararen ligger därför nästan alltid i efterhand mot en kvalificerad antagonist. Samtidigt har försvararen möjlighet att kompensera angriparens fördelar genom tillgång till ständigt uppdaterad och lättillgänglig kunskap om de egna systemens status och konfiguration. Kombineras denna kunskap med förmåga att upptäcka attacker samt kännedom om hoten kan försvararen i vissa fall ha ett informationsöverläge gentemot angriparen.

I Försvarsmaktens cyberlägesbild integreras underrättelser och incidentrapporter med teknisk information om de system och tjänster Försvarsmakten är beroende av eller av andra anledningar ska kunna försvara. Cyberlägesbilden är ett viktigt verktyg för både lägesuppfattningen och som underlag för beslut om åtgärder för att möta aktuella hot. Lägesbilden försörjs även med information från teknisk omvärldsbevakning om exempelvis publikt kända sårbarheter och it-säkerhetsincidenter, samt annan relevant information som tillhandahålls av leverantörer och it-säkerhetsföretag.

Kvaliteten på cyberlägesbilden stärks slutligen genom de samarbeten Försvarsmaktens cyberförsvar har med andra försvarsmakter och mellanstatliga organisationer.

Underrättelsetjänst

För att kunna möta kvalificerade antagonister inom cyberdomänen är det nödvändigt med god underrättelseförmåga som kan kartlägga yttre hotaktörer och deras verksamhet. Underrättelsetjänsterna har dessutom en central roll i att kartlägga hybridhot

och identifiera hybridaktiviteter, vilket gäller oavsett om det ingår en cyberkomponent eller inte. Den militära underrättelsetjänsten stödjer cyberförsvarets verksamhet med underrättelser som ligger till grund för utveckling av förmågor, operationsplanering och strategisk förvarning. Till följd av cyberdomänens karaktäristik är underrättelser från signalspaningen av särskild betydelse för att cyberförsvaret snabbt ska kunna agera på uppkomna händelser.

Militär och civil säkerhetstjänst

Hotbilden från den militära underrättelsetjänsten kompletteras av den militära säkerhetstjänsten i form av säkerhetsunderrättelser avseende hot riktade specifikt mot Försvarsmakten.

Utöver kunskap om hoten är en stark militär och civil säkerhetstjänst en förutsättning för att genom föreskrifter, tillsyn och stödjande aktiviteter skapa ett tillräckligt säkerhetsskydd för de mest skyddsvärda verksamheterna. Säkerhetstjänsternas arbete omfattar alla aspekter av säkerhetsskyddet, som i säkerhetslagen delas upp i informationssäkerhet, fysisk säkerhet och personalsäkerhet. I den militära säkerhetstjänsten ingår signalskyddstjänsten som skapar förutsättningar för att på ett säkert sätt kommunicera skyddsvärda uppgifter genom elektroniska kommunikationstjänster.

Den militära och civila säkerhetstjänsten utgör slutligen ett viktigt bidrag till Försvarsmaktens cyberlägesbild genom incidentrapporter från de verksamheter som står under säkerhetstjänsternas föreskrifts- och tillsynsområden. Den kunskap om brister och sårbarheter som säkerhetstjänsterna genom sin verksamhet besitter kan också komplettera Försvarsmaktens cyberlägesbild, inte minst genom att synliggöra vilka kända risker i cyberdomänen som Sveriges säkerhetskänsliga verksamhet har valt att acceptera.

Säkra och robusta kommunikationstjänster

För många typer av system, oavsett om det är ett kontorssystem för totalförsvarsplanering eller ett taktiskt system för ledning och genomförande av operationer, uppstår nyttan och effekten framför allt när information snabbt kan förmedlas till de mottagare (både människor och maskiner) som har behov av den. Detta gäller oavsett verksamhet men är också en förutsättning för att cyberförsvaret ska kunna agera i rätt tid på underrättelser och incidentrapporter, inte minst eftersom händelseförloppet inom cyberdomänen ofta är mycket kort.

Elektroniska kommunikationstjänster spelar därmed stor roll för informationssäkerhetens tillgänglighetskriterium; informationen måste vara tillgänglig i rätt tid och på rätt plats. Kommunikationstjänster som ska användas i högre konfliktnivåer behöver därmed vara så robusta att en motståndare inte enkelt kan slå ut eller degradera kommunikationen och därmed de verksamheter som har behov av den. Tillräcklig nivå av robusthet förutsätter motståndskraft mot attacker i cyberdomänen såväl som för bekämpning av fysisk infrastruktur.

Robusthet är dock inte tillräckligt. Kommunikationstjänsterna måste dessutom förhindra att obehöriga kan ta del av eller förändra den informationen som förmedlas, samt förhindra att en angripare kan använda tjänsten som en väg in i de system som är anslutna till tjänsten. Tillräckligt sekretess-, riktighets-, och intrångsskydd kan uppnås genom att använda ett av Försvarsmakten godkänt signalskyddsystem, vilket vid för-

medling av säkerhetsskyddsklassificerad information också är ett författningskrav.[61]

En elektronisk kommunikationstjänst består slutligen av flera olika komponenter vilka precis som ett informationssystem behöver övervakas samt ha funktionalitet och personal som gör det möjligt att upptäcka och avvärja intrångsförsök från kvalificerade aktörer. Det innebär att tjänstens förmåga att skydda den förmedlade informationen är direkt beroende av att dess egen funktionalitet kan skyddas och i vissa fall förberedas för att kunna försvaras av kvalificerade cyberförsvarsresurser.

Informations- och cybersäkerhet

Cyberförsvarets och säkerhetstjänsternas kvalificerade resurser är varken avsedda eller tillräckliga för att på egen hand upprätthålla säkerheten i Sveriges samtliga informationssystem och elektroniska kommunikationstjänster. För att de mest kvalificerade resurserna ska kunna möta de mest kvalificerade antagonisterna krävs en tillräcklig grundnivå av informations- och cybersäkerhet i hela samhället.

Oavsett organisationsstruktur behöver därför verksamhetsutövare, såväl offentliga som enskilda, en funktion med utpekat ansvar för cybersäkerheten. I större organisationer kan det finnas flera sådana funktioner med olika inbördes ansvar och roller. Behovet av en dedikerad cybersäkerhetsfunktion undantar dock inte det ansvar som respektive verksamhetsföreträdare har för att säkerställa tillräcklig nivå på informations- och cybersäkerhet inom dennes ansvarsområde. En cybersäkerhetsfunktion kan utgöra ett viktigt och i många fall nödvändigt komplement men den kan inte på egen hand upprätthålla cybersäkerheten i en organisation.

Cybersäkerhetsfunktionen kan bland annat ansvara för att omsätta föreskrifter och inriktningar från säkerhetstjänsten och cyberförsvaret till tillämpade styrningar för it-verksamheten. Till det kommer den interna uppföljningen av att genomförda cybersäkerhetsåtgärder får önskad effekt.

Funktionen säkerställer vidare, tillsammans med drift- och förvaltningsorganisationen, att det finns resurser och metoder för att hantera alla sådana cybersäkerhetsincidenter som inte kräver stöd från kvalificerade cyberförsvarsresurser eller av andra skäl behöver koordineras från militärstrategisk eller strategisk nivå. För allvarligare incidenter är cybersäkerhetsfunktionen dessutom i många fall den naturliga kontaktytan för att kunna ta emot stöd från kvalificerade externa resurser.

Samhällets grundnivå av cybersäkerhet inkluderar slutligen en ordningsmakt och rättsvårdande myndigheter med kapacitet att utreda och lagföra individer som begår dataintrång, it-relaterade bedrägerier och andra brott som inte utgör ett väpnat angrepp. Ur ett cyberförsvarsperspektiv minskar detta utrymmet för kvalificerade antagonister att nyttja kriminella som ombud, liksom deras möjlighet att få deras egna aktiviteter att framstå som något annat än vad det är. Det skapar också en större medvetenhet i samhället om vilka beteenden som inom området är olagliga, vilket i bästa fall minskar risken för att enskilda av obetänksamhet begår it-brott som på olika sätt kan påverka samhällsviktiga funktioner.

Proaktiv drift, förvaltning och behörighetsstyrning

Tillräcklig cybersäkerhet är omöjlig att uppnå utan en proaktiv drift och förvaltning med tillhörande behörighetsstyrning. En stor del av det praktiska arbetet för att upprätthålla

cybersäkerheten utförs av drift- och förvaltningsorganisationerna, vilket gör kompetensområdena så tätt sammanvävda att det ibland är svårt att behandla dem var för sig.

Allvarliga sårbarheter i olika typer av it-komponenter kommer under överskådlig framtid att fortsätta upptäckas mer eller mindre frekvent. Varje sådan sårbarhet leder till en kapplöpning mellan antagonister och försvarare. Det är därför nödvändigt att drift- och förvaltningsorganisationen vid varje givet tillfälle snabbt kan svara på vilka produkter, tjänster och användare som finns i varje givet system, hur dessa system och tjänster är ihopkopplade och konfigurerade samt vilka versioner av mjukvaror som nyttjas. Till det kommer rutiner för att snabbt kunna installera säkerhetsuppdateringar när de tillgängliggörs av leverantören, alternativt att kunna ändra konfigurationen för att minska attackytorna i väntan på en uppdatering.

Om ovanstående saknas skapas istället attackytor som i det närmaste är öppna mål även för mindre kvalificerade angripare. När en angripare väl är inne i systemet krävs mycket omfattande arbete för att återställa det till ett säkert tillstånd, vilket också i vissa fall visat sig närmast omöjligt.

För de verksamheter som har egna informationssystem är drift- och förvaltningsorganisationen således den stabila grundplattan i cybersäkerhetsarbetet. Den utgör ett avsevärt hinder för en angripare genom att upprätthålla en god grundsäkerhet men också att genom sin djupa kännedom om systemen kunna upptäcka anomalier som kan tyda på intrång.

En proaktiv drift och förvaltning som därtill är integrerad med verksamhetens kontinuitetsplanering är vidare grundpelaren för att samhällsviktig verksamhet ska kunna fortsätta bedrivas även vid systembortfall, oavsett om dessa uppstår på grund av angrepp eller av andra orsaker. Som en del i förvaltningen krävs även rutiner och utbildad personal för behörighetsstyrning och uppföljning av resursnyttjande, vilket gäller oavsett om verksamheten nyttjar egna system eller externa molntjänster.

För organisationer som inte har drift och förvaltning i egen regi, antingen genom egna system hos externa it-leverantörer eller genom publika molnlösningar, blir kompetensbehovet delvis annorlunda. Förutom personal med kompetens för att kravställa och följa upp att leverantörernas säkerhetsåtgärder är tillräckliga hamnar tyngdpunkten i ännu större utsträckning på att styra behörigheter och identifiera avvikelser i resursutnyttjande.

Användbara, robusta och försvarbara informationssystem i alla konfliktnivåer

För informationssystem som ska användas i totalförsvarsverksamhet krävs att verksamhetens behov av användarvänlighet, robusthet, riktighet, tillgänglighet, sekretess och spårbarhet tillgodoses för samtliga konfliktnivåer som systemen eller tjänsterna ska användas i, oavsett säkerhetsskyddsklassificering på den behandlade eller förmedlade informationen. System som Försvarsmakten är beroende av för att möta ett väpnat angrepp eller mobilisera behöver vara särskilt utformade för att stödja försvarsåtgärder mot kvalificerade statliga antagonister.

Ett system som ska användas på ett säkert sätt i situationer med högt stresspåslag behöver dessutom från början utformas för en hög grad av användbarhet. Ett krångligt användargränssnitt riskerar till exempel att antingen leda till misstag eller att systemet undviks till förmån för alternativa lösningar som står helt eller delvis utanför verksamhe-

tens kontroll. Sådana alternativa lösningar kan upplevas som attraktiva eftersom det löser ett akut problem, men de medför ofta en stor uppsättning kända och okända risker för verksamheten.

System som tagits fram utan att beakta användbarheten och säkerheten kräver ofta, i den mån det alls är möjligt, omfattande personella och ekonomiska resurser för att kompensera bristerna. Konsekvensen blir därför antingen att bristerna kvarstår eller att de tillförda resurserna tränger ut andra systems behov. Det sistnämnda blir särskilt problematiskt om kvalificerade och därmed begränsade cyberförsvarsresurser behöver avdelas för att försvara system med bristande grundsäkerhet.

För att verksamheten inte ska invaggas i en falsk känsla av säkerhet är det sist men inte minst viktigt med säkra leverantörskedjor i alla led. Även den mest säkra och välgranskade mjukvara är helt beroende av den processor och de kretskort som exekverar den och en angripare kommer alltid välja det enklaste sättet att uppnå sina mål. Ett effektivt säkerhetsskyddsarbete i anskaffningsfasen är därför en förutsättning för att systemen ska vara säkra när väl används.

Alla ovanstående aspekter måste hanteras genom hela systemlivscykeln och inkluderar även att förutsättningarna för proaktiv drift och förvaltning omhändertas tidigt i kravställningen. Detta ställer i sin tur krav på utbildad personal med flera olika specialistkompetenser[62] inom utvecklings- och anskaffningsfunktionerna.

Säkerhetsmedvetande och säkerhetskultur hos alla it-användare i samhället

I *Totalförsvaret 2021–2025* framhåller regeringen vikten av en säkerhetskultur i hela samhället:

> Regeringen, liksom Försvarsberedningen, understryker vikten av det förebyggande arbetet och av att öka medvetenheten såväl som förmågan hos alla användare av it-system för att skapa förutsättningar för utvecklingen av en säkerhetskultur i hela samhället.[63]

En del i en sådan medvetenhet är förståelsen att även om en individ eller organisation inte anser sig ha någon viktig information som är värd att bevara så kan deras it-produkter och system vara av intresse för både kriminella organisationer och statliga antagonister som en del i en infrastruktur för fortsatta angrepp mot samhällsviktiga system.

Till det behövs en ökad medvetenhet om att det för en angripare är värdefullt att få tillgång till information som beskriver hur ett tekniskt system är utformat, eftersom detta i många fall underlättar att antingen slå ut systemet alternativt komma åt informationen i det. Denna ökade medvetenhet behöver sedan omsättas i relevanta skyddsåtgärder kring hur tekniska specifikationer inklusive förfrågningsunderlag vid upphandlingar hanteras.

När det kommer till säkerhetskultur framställs i många fall behöriga användare som ett av de största hoten mot säkerheten. Samtidigt är samma användare den första skyddslinjen mot många angreppsförsök. Även om insiderhotet alltid måste beaktas kan användarna med stöd av god säkerhetskultur och rätt utbildning utgöra en av de största tillgångarna i skyddet mot exempelvis skadlig kod.

En god säkerhetskultur kommer dock aldrig att uppstå av sig självt, utan är något som liksom övrigt cybersäkerhetsarbete kräver systematiskt och tålmodigt arbete. Det förutsätter också att både informationssystem och regelverk harmoniserar med den verksamhet som ska bedrivas. Om personalen hela tiden tvingas bryta mot regelverket för

att kunna genomföra sitt arbete är det svårt att skapa acceptans för säkerhetsarbetet och säkerhetskulturen blir då därefter.

I ett bredare perspektiv krävs ökad medvetenhet i hela samhället för att både privatpersoner och organisationer ska efterfråga, kräva och vilja betala för produkter och tjänster med tillräcklig säkerhet, där leverantörerna tar ansvar för att tillhandahålla säkerhetsuppdateringar under hela produktens tekniska livslängd. Om en sådan förväntan uppstår hos konsumenterna och därigenom resulterar i säkrare produkter minskar attackytorna på bred front. Detta reducerar i sin tur angriparnas möjlighet att undgå upptäckt eller använda en stor samling övertagna enheter för exempelvis överbelastningsattacker eller distribuerad upprepad systematisk lösenordsgissning.

Några av Försvarsmaktens åtgärder för att vidareutveckla cyberförsvarsförmågan

Artikeln har så här långt framför allt beskrivit vad cyberförsvar är och, genom cyberförsvarspyramiden, vilka samverkande komponenter som behöver finnas för att uppnå de förväntningar som beskrivs i propositionen *Totalförsvaret 2021–2025*.[64]

I det här avsnittet beskrivs tre större områden där Försvarsmakten etablerar nödvändiga strukturer för att över tid upprätthålla en relevant cyberförsvarsförmåga. Dessa åtgärder[65] berör framför allt toppen av pyramiden. Aktiviteter och strukturer för att upprätthålla förmåga i övriga delar av pyramiden är viktiga men ligger utanför artikeln såväl som cyberförsvarsfunktionens primära ansvarsområde.

En åtgärd som inte utgör ett eget område men som under de kommande tio åren är av stor vikt för Sveriges samlade cyberförsvarsförmåga är att Försvarsmakten under 2022 påbörjar etableringen av ytterligare ett it-försvarsförband (2. ITF). Det nya förbandet kommer att avsevärt öka Försvarsmaktens kapacitet att genomföra defensiva och offensiva cyberoperationer. Parallellt med etableringen tillförs cyberförsvarsofficerare till staber på taktisk och operativ nivå.

Samverkan och övningar

Nationell och internationell samverkan och samarbete samt övningsverksamhet är av stor betydelse för förmågeutvecklingen såväl som för tillgången till relevant information om status och händelser i cyberdomänen. En konkret åtgärd för att utöka tillgången till relevant information är att bli en fullvärdig medlem i NATO MISP *(Malware Information Sharing Platform)*. Försvarsmakten fortsätter därutöver samarbetet med andra nationers försvarsmakter samt mellanstatliga organisationer utifrån regeringens anvisningar.

För att vidareutveckla befintliga förmågor deltar Försvarsmaktens cyberförsvarsresurser regelbundet i olika övningar. Bland dessa kan nämnas NATO Cyber Coalition, Bold Quest och Locked Shields. Den sistnämnda är en prestigefylld cyberövning som arrangeras av Natos cyberförsvarcenter i Estland (NATO CCD COE). Försvarsmakten sammanhåller Sveriges deltagande i övningen och bjuder in både myndigheter och företag för att tillsammans öka Sveriges förmåga att hantera cyberattacker.

Försvarsmakten arrangerar dessutom sin egen årliga övning *SAFE Cyber* där myndigheter och företag som är särskilt viktiga för Försvarsmaktens förmåga inom olika sektorer bjuds in att under cyberförsvarsfunktionens ledning öva incidenthantering och incidentrapportering.

Ett cyberförsvar i forskningens och teknikens framkant

För att kunna möta de mest kvalificerade motståndarna är det nödvändigt att cyberförsvarets teknik och metoder befinner sig i teknikens och forskningens framkant. Detta återspeglas också i *Totalförsvaret 2021–2025:*

> Till följd av den snabba teknikutvecklingen krävs kontinuerlig forskning och utveckling för att bidra till vidmakthållande och utveckling av cyberförsvarsförmågan.[66]

Att realisera ovanstående ligger i linje med Försvarsmaktens uppgifter enligt myndighetsinstruktionen:

> 5 f § Försvarsmakten ska beställa forskning och utveckling, samt bedriva egna studier och försök, för inriktning och utveckling av det militära försvaret och för att säkerställa dess tillgång till integritetskritisk kunskap.[67]

Den förstärkning av cyberförmågan som beslutades under föregående försvarsbeslutsperiod gav Försvarsmakten tillsammans med KTH möjlighet att under 2019 och 2020 etablera *Centrum för cyberförsvar och informationssäkerhet,* CDIS. Under 2021 utökades centrumet genom att FHS ingick som medlem och på sikt kan ytterligare aktörer komma att ingå.

De forskningsprojekt som bedrivs inom CDIS involverar doktorander som under sina forskarstudier, utöver djup teknisk kompetens, också får förståelse för Försvarsmaktens och försvarssektorns behov av informations- och cybersäkerhet. Detta stärker Sveriges långsiktiga konkurrenskraft inom området.

Försvarsmaktens målsättning är att cyberförsvaret i alla lägen ska ha tillgång till världsledande produkter och tekniska system för att kunna upptäcka och möta statliga eller statsunderstödda antagonister. Detta förutsätter att både öppen och hemlig spetsforskning snabbt omsätts i produkter och metoder för it-försvarsförbanden och andra kvalificerade cyberförsvarsresurser. Genom att Försvarsmakten utifrån forskningsresultat från bland annat KTH och FOI lägger utvecklingsuppdrag på innovativa leverantörer med förmåga att kombinera kompetens, flexibilitet och säkra utvecklingsprocesser kommer cyberförsvaret att ligga i framkant av teknikutvecklingen. Uppdragen till industrin stärker även leverantörernas kompetens och konkurrenskraft vilket på sikt bidrar till att utveckla Sveriges roll som tekniknation.

Ett sammanhållet personalförsörjnings- och karriärsystem

Cyberförsvarets förmåga är till stor del en direkt effekt av kompetensen hos dess personal. Vikten av kvalificerad personal framhålls i *Totalförsvaret 2021–2025:*

> Kvalificerad personal krävs för att långsiktigt kompetensförsörja och stärka både den defensiva och offensiva cyberförsvarsförmågan.[68]

Som konstaterats i tidigare avsnitt behöver beslut om militär våldsanvändning enligt folkrätten ske i den militära orderkedjan. Därmed behöver cyberförsvaret officerare och specialistofficerare som har djup kompetens inom cyberoperationer och verkan i cyberdomänen. För att åstadkomma detta behövs utbildningsinriktningar där generella officersfärdigheter kombineras med teknisk förståelse för cyberdomänens särskilda karaktäristik och förutsättningar.

Officersprofessionen kombineras i cyberförsvaret med civila experter inom informationsteknologins olika deldiscipliner. För

att bibehålla relevansen i den snabba utvecklingen krävs i många fall djup teoretisk kunskap och det finns därför i funktionen många individer med datortekniska och datavetenskapliga utbildningar på avancerad nivå som exempelvis civilingenjörer. Till följd av teknik- och samhällsutvecklingen inom AI och andra områden kommer sannolikt behovet av personer med forskarexamen på sikt att öka.

Det personalförsörjnings- och karriärsystem för cyberförsvaret som Försvarsmakten etablerar syftar till att åstadkomma en struktur med grundutbildning av militär personal samt förutsägbara personalflöden för samtliga personalkategorier. Systemet utformas för att:

- ge värnpliktiga och officerare rätt utbildning från början, vilket minskar behovet av längre frånvaro från förband för att genomgå omfattande omskolning senare i karriären,
- ge cyberförsvarsfunktionens officerare som kollektiv kunskap om och praktisk erfarenhet från kritiska informations- och sambandssystem inom samtliga försvarsgrenar,
- undvika oplanerade vakanser i andra funktioner och samtidigt bibehålla möjligheten för befintlig personal med relevant kompetens att byta funktion,
- erbjuda ändamålsenlig kompetensutveckling för samtliga personalkategorier inom cyberförsvarsfunktionen, samt
- stärka den allmänna kompetensen och förståelsen för cybersäkerhet och cyberförsvar även utanför cyberförsvarsfunktionen.

Avslutande ord

I artikeln har författaren beskrivit sin syn på omfattning och struktur för Sveriges cyberförsvar, där cyberförsvarspyramiden illustrerar allt ifrån kärnförmågan att bedriva offensiva och defensiva operationer i cyberdomänen till behovet av en god säkerhetskultur i hela samhället. Båda dessa delar, som kan ses som spetsen respektive basen på pyramiden, förutsätter alla mellanliggande delar, som exempelvis försvarbara, robusta och användbara informationssystem och kommunikationstjänster och därtill kopplad drift- och förvaltning, cybersäkerhetsarbete, brottsbekämpning och inte minst starka underrättelse- och säkerhetstjänster.

För många av uppgifterna, och då särskilt i toppen av pyramiden, har Försvarsmakten genom sin myndighetsinstruktion och andra förordningar huvudansvaret och därmed en ledande roll. Samtidigt har cyberförsvaret som en del i det militära försvaret många beroenden till andra funktioner och förutsättningsskapande verksamheter inom totalförsvaret. Stöd från andra aktörer i totalförsvaret och ytterst hela samhället är därför nödvändigt på både kort och lång sikt för att cyberförsvarspyramiden ska kunna realiseras fullt ut.

Författaren ser med tillförsikt på den fortsatta uppbyggnaden av cyberförsvaret. Mycket återstår att göra, men mycket av grundarbetet är gjort. Försvarsmakten har redan idag förmågan att utföra alla typer av cyberoperationer; de medel som avdelats av regering och riksdag för den fortsatta utbyggnaden kommer att öka kapaciteten och robustheten och inte minst upprätthålla spetsförmågan i den snabba teknikutvecklingen.

Författaren är civilingenjör i informationsteknologi och tjänstgör inom Ledningsstabens CIO-avdelning vid Försvarsmaktens högkvarter.

Noter

1. Akademiledamoten överste Patrik Ahlgren har vid framtagandet av artikeln haft rollen som mentor och sakkunnig expert.
2. *Totalförsvaret 2021–2025,* Prop 2020/21:30, Regeringen, Stockholm 2020, *https://www.regeringen.se/4a965d/globalassets/regeringen/dokument/forsvarsdepartementet/forsvarsproposition-2021–2025/totalforsvaret-2021–2025-prop.-20202130.pdf,* (2022-01-09).
3. Ibid, s 151-153.
4. Däremot är, precis som regeringen konstaterar, god informations- och cybersäkerhet en *förutsättning* för ett starkt cyberförsvar. Ibid, s 153.
5. Se exempelvis Natostandarden *Allied Joint Doctrine for Cyberspace Operations (AJP-3.20 Ed A Ver 1)* från 2020 som också fastställts med nationella kommentarer av Storbritanniens försvarsministerium, samt danska *Joint Doctrine for Military Cyberspace Operations* från 2019 framtagen av Royal Danish Defence College.
6. Op cit, *Totalförsvaret 2021–2025,* se not 2, s 63.
7. Ibid.
8. Ibid, s 151.
9. *Inriktning för Försvarsmakten 2021–2025,* RB 30, Regeringen, Stockholm 2020, s 2.
10. *Förordning (2007:1266) med instruktion för Försvarsmakten,* Regeringen, 1 §.
11. Op cit, *Totalförsvaret 2021–2025,* se not 2, s 152.
12. *Doktrin för Gemensamma operationer (DGO 20),* Försvarsmakten, Stockholm 2020, s 15.
13. I doktrinen (ibid, s 127) används det äldre begreppet *dator- och nätverksoperationer* eftersom den är fastställd innan det senaste försvarsbeslutet. I nyare publikationer används företrädesvis begreppet *cyberoperationer.*
14. Ibid, s 127.
15. Ibid.
16. *Försvar och samhällets krisberedskap,* Prop 2021/22:1 Utgiftsområde 6, Regeringen, Stockholm 2021, *https://www.regeringen.se/4a6878/contentassets/bc0f4b1a4ce844f2aa59949d09c93f29/utgiftsomrade-6-forsvar-och-samhallets-krisberedskap.pdf,* (2022-01-16).
17. *Svensk manual i humanitär rätt m m* (SOU 2010:72, bilaga 7), Folkrättskommittén, Stockholm 2010, s 46-48.
18. Ibid, s 249-250.
19. Op cit, *Prop. 2021/22:1 Utgiftsområde 6,* se not 16, s 17.
20. Op cit, *Totalförsvaret 2021–2025,* se not 2, s 152.
21. När begreppet *cyberförsvarsfunktionen* används senare i artikeln åsyftas vad som beskrivs i det här avsnittet.
22. Op cit, *Totalförsvaret 2021–2025,* se not 2 s 152.
23. *Förordning om ändring i förordningen (2007:937) med instruktion för Försvarets radioanstalt* (SFS 2020:1236), Regeringen, 2020.
24. Op cit, *Försvar och samhällets krisberedskap,* se not 16, s 47.
25. Op cit, *Totalförsvaret 2021–2025,* se not 2, s 153.
26. *Lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster,* Riksdagen.
27. *Förordning (2002:375) om Försvarsmaktens stöd till civil verksamhet,* Regeringen.
28. Op cit, *Totalförsvaret 2021–2025,* se not 2, s 152.
29. Op cit, *Förordning med instruktion för Försvarsmakten,* se not 10, 2 §.
30. *Säkerhetsskyddslag (SFS 2018:585),* Riksdagen, 2 §.
31. Op cit, *Inriktning för Försvarsmakten 2021–2025,* se not 9, s 4.
32. Op cit, *Totalförsvaret 2021–2025,* se not 2, s 63.
33. Op cit, *Förordning med instruktion för Försvarsmakten,* se not 10, 2a §.
34. Op cit, *Inriktning för Försvarsmakten 2021–2025,* se not 9, s 6.
35. Op cit, *Förordning med instruktion för Försvarsmakten,* se not 10, 7 §.
36. Op cit, *Inriktning för Försvarsmakten 2021–2025,* se not 9, s 4.
37. *Handlingskraft – Handlingsplan för att främja och utveckla en sammanhängande planering för totalförsvaret 2021–2025,* Försvarsmakten; Myndigheten för samhällsskydd och beredskap, Stockholm 2021
38. Op cit, *Totalförsvaret 2021–2025,* se not 2, s 153.

39. Förordning (2015:1052) om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap, Regeringen, 19 §.
40. *Säkerhetsskyddsförordning (2018:658)*, Regeringen, 3 kap 4 §.
41. *Förordning (2003:396) om elektronisk kommunikation*, Regeringen, 5 §.
42. Op cit, *Totalförsvaret 2021–2025*, se not 2, s 151.
43. Ibid, s 61.
44. Ibid. Meningen är i en anpassning av första styckets fjärde mening under rubriken *"Hybridhot"*.
45. Lindqvist, Henrik: *Femtio nyanser av grått – Om gråzonsproblematik, hybridkrigföring och skymningsläge*, essä inom Taktisk stabskurs 19-20, Försvarshögskolan, 2020.
46. Ibid, s 9. Den refererade essän har även i övrigt utgjort en värdefull inspirationskälla för det här avsnittet i artikeln.
47. Begreppet används ofta i svenska texter utan översättning. Även om det är önskvärt med ett svensk begrepp är författaren av uppfattningen att uttryck som utpressnings- eller lösenprogramvara skulle skapa förvirring snarare än klarhet varför det engelska begreppet används även här.
48. *Reglemente Säkerhetstjänst 2021*, Försvarsmakten, M7739-353149, Stockholm 2021, s 24-25.
49. *Handbok för Försvarsmaktens säkerhetstjänst, Säkerhetsskyddstjänst (HSÄK Skydd)*, Försvarsmakten, M7739-352005, Stockholm 2007, s 12-13.
50. Bland annat har Försvarsmakten genom sin myndighetsinstruktion (op cit, *Förordning med instruktion för Försvarsmakten*, se not 10, 2 §) i uppgift att "[…] upptäcka och identifiera yttre hot mot Sverige och svenska intressen […]".
51. Op cit, *Inriktning för Försvarsmakten 2021–2025*, se not 9, s 5.
52. För att möta övriga delar i en hybridaktivitet krävs ett gott säkerhetsskydd på bredden, vilket är alla verksamhetsutövares ansvar, starka militära och civila säkerhetstjänster som inriktar och utövar tillsyn över säkerhetsskyddet samt en underrättelsetjänst som kan identifiera den sammanlagda verksamheten och de bakomliggande aktörerna.
53. Op cit, *Inriktning för Försvarsmakten 2021–2025*, se not 9, s 7.
54. Op cit, *Förordning med instruktion för Försvarsmakten*, se not 10, 2 § sista stycket.
55. *Lag (2006:343) om Försvarsmaktens stöd till polisen vid terrorismbekämpning*, Riksdagen.
56. Op cit, *Förordning om Försvarsmaktens stöd till civil verksamhet*, se not 27.
57. Ibid, 5 §.
58. Ibid, 6 §.
59. Några av dessa myndigheter har i sin tur, vilket framgår av senare kapitel, direkta uppgifter att stödja hela eller delar av samhället inom cybersäkerhetsområdet, både avseende förebyggande arbete och vid incidenter.
60. Op cit, *Totalförsvaret 2021–2025*, se not 2, s 60.
61. Op cit, *Säkerhetsskyddsförordning*, se not 40, 5 §.
62. Systemlivscykelstandarden *ISO/IEC/IEEE 15288:2015* beskriver till exempel ett antal kompetensområden som är nödvändiga för att skapa användbara, robusta och säkra sociotekniska system.
63. Op cit, *Totalförsvaret 2021–2025*, se not 2, s 153.
64. Ibid, se särskilt kapitel 10 "Cyberförsvar", s 151-153.
65. Samtliga åtgärder kan härledas från FM2020-18169:29 *Försvarsmaktens verksamhetsplan 2021-2030 (FMVP 21) Ä1*, bilaga 3 avsnitt 8.6. Den beskrivande textmassan är dock framför allt baserad på författarens diskussioner med överste Patrik Ahlgren under artikelns framtagande (se not 1).
66. Op cit, *Totalförsvaret 2021–2025*, se not 2, s 152.
67. Op cit, *Förordning med instruktion för Försvarsmakten*, se not 10, 5 f §.
68. Op cit, *Totalförsvaret 2021–2025*, se not 2, s 153.