FÖRSVARSMAKTEN

Doktrinansats

Cyberförsvar

2024

Doktrinansats Cyberförsvar

DA CYBER

Omslag:	Fotograf: Joel Thungren, Försvarsmakten. Grafisk bearbetning: Anna-Karin Wetzig, Försvarsmakten
Handläggare:	Cyberförsvarsledningen (FST STRA CFL)
Publikationsklass:	F
Tillgängliggörande:	Försvarsmaktens intranät, www.forsvarsmakten.se
Beslutsfattare:	Generalmajor Johan Pekkari C FST STRA
Produktionsformat:	Indesign, G5
Tryck:	Försvarsmakten, FMLOG 2024

Versionshistorik

OBSERVERA
Om du läser denna publikation i pappersform så kontrollera att du har den senaste versionen. Fastställd och gällande version finns alltid publicerad på Försvarsmaktens intranät.

Version	Best. kod	Datum för när versionen börjar gälla/ska tillämpas	Vidarhandling för beslut	Anmärkning
1.0	F	2024-09-20	FM2024-21569:1	Utgivningsår 2024
1.1	F	2024-12-01	FM2024-21569:2	Formaterad för tryck i G5 samt mindre korrektur

Förslag på ändringar och förtydliganden insänds i RFF-mallen linjevägen till FST STRA CFL.

Publikationstypen doktrinansats

Om ett område eller ämne uppfattas sakna doktrinär styrning kan en doktrinansats skrivas. En doktrinansats ska främja diskussion om ämnet och utgöra underlag till beslut om hur området doktrinärt ska vidareutvecklas. En doktrinansats har en beslutad livslängd inom vilken behovet ska analyseras och Försvarsmakten bestämma hur behovet av doktrinär styrning ska tillgodoses. Exempel på åtgärder:

1. Utveckla doktrinansatsen till en doktrin (doktrintillägg).
2. Inarbeta saknade delar i annan doktrin (om Försvarsmakten ska tillämpa ”hybrid-doktrin”, det vill säga svenska element i Nato-doktriner, är under utredning).
3. Inarbeta saknade delar i annan publikation eller dokument.
4. Det finns inget behov av doktrinär styrning och ärendet avslutas.

En doktrinansats är inte ett styrande dokument som en doktrin är. Med vetskap om det så bör ändå doktrinansatsens inriktningar och vägledningar tillämpas för att få underlag att bedöma nyttan och behovet av dessa. Till skillnad från Försvarsmaktens doktrin, som fastställs av överbefälhavaren, fastställer chefen för Försvarsstabens strategienhet (C FST STRA) en doktrinansats.

Målgruppen för doktrinansatsen är Försvarsmaktens medarbetare på militärstrategisk, operativ och taktisk nivå. Doktrinansatsen riktar sig även till aktörer inom totalförsvaret som i sin verksamhet kan komma att samverka med Försvarsmakten och därmed har behov av utökad förståelse för området.

Doktrinansats Cyberförsvar beskriver verksamhet som genomförs i fred och hela konfliktskalan.

Innehållet i denna publikation omfattas inte av sekretess.

Förord C FST STRA

Försvarsmaktens huvuduppgift är att försvara Sverige och allierade mot ett väpnat angrepp med utgångspunkt från det kollektiva försvaret inom Nato. Cyberförsvaret utgör en integrerad del av det militära försvar som ska kunna möta ett väpnat angrepp. Försvarsmakten har en ledande roll i Sveriges cyberförsvar och ansvarar särskilt för Sveriges offensiva cyberförmåga.

Doktrinansats Cyberförsvar är den första i sitt slag och min förhoppning är att den både kommer att utgöra ett stöd vid genomförande av verksamheten och ett verktyg för att fortsätta den snabba utvecklingen av cyberförsvarsförmågan. Doktrinansatsen ska också främja diskussion om ämnet och utgöra underlag till beslut om hur cyberförsvaret doktrinärt ska utvecklas.

Johan Pekkari

C FST STRA

Sammanfattning och läsanvisning

Cyberförsvar är en integrerad del av det militära försvaret och är en väsentlig del av den moderna krigföringen. Försvarsmakten ansvarar för Sveriges offensiva cyberförmåga. Cyberförsvaret dimensioneras för höjd beredskap och väpnat angrepp samtidigt som cyberdomänens särskilda förutsättningar innebär att stora delar av cyberförsvaret är aktivt i samtliga konflikt- och beredskapsnivåer.

Cyberförsvaret ska upprätthålla överbefälhavarens handlingsfrihet med Försvarsmaktens system och plattformar samt skapa effekter i cyberdomänen som en del av det nationella och kollektiva försvaret.

Ett effektivt cyberförsvar kräver förebyggande aktiviteter på bredden i hela samhället och ett upprätthållande av en stark cybersäkerhet.

Doktrinansatsen bör läsas från början till slut av den som önskar fördjupa sin förståelse för cyberförsvar. För användning som referensverk inför framtagande av underliggande publikationer eller genomförande av verksamhet framgår de olika områdena som doktrinansatsen omfattar av innehållsförteckningen.

En process är inledd där analys kommer att göras av hur Försvarsmaktens doktrin förhåller sig till Natos doktrin. Inom ramen för det arbetet kommer även Doktrinansats Cyberförsvar att analyseras med motsvarande styrande dokument inom Nato.

Innehåll

1 Inledning

I detta kapitel redogörs för syfte, sammanhang och målgrupp för Doktrinansats Cyberförsvar.

1.1 Syfte

Syftet med doktrinansatsen är att skapa en doktrinär grund för cyberförsvaret inklusive en gemensam begreppsapparat. I den doktrinära grunden ingår en fördjupning av cyberdomänen och dess karaktäristik samt strukturer, ledningsprinciper och förutsättningar för genomförandet av cyberoperationer.

1.2 Målgrupp

Målgruppen för doktrinansatsen är Försvarsmaktens personal på militärstrategisk, operativ och taktisk nivå. Doktrinansatsen riktar sig även till aktörer inom totalförsvaret som i sin verksamhet kan komma att samverka med Försvarsmakten och därmed har behov av utökad förståelse för området.

1.3 Doktrinansatsens sammanhang

Doktrinansats Cyberförsvar kompletterar Militärstrategisk doktrin (MSD) och Doktrin för Gemensamma operationer (DGO).

I doktrinansatsen ges övergripande inriktningar av hur cyberförsvaret bedrivs utifrån ett militärstrategiskt perspektiv. Vidare beskriver doktrinansatsen grundläggande teori och begrepp som är inriktande för cyberförsvaret. Cyberförsvarets verksamhet styrs i detalj genom reglemente och handböcker.

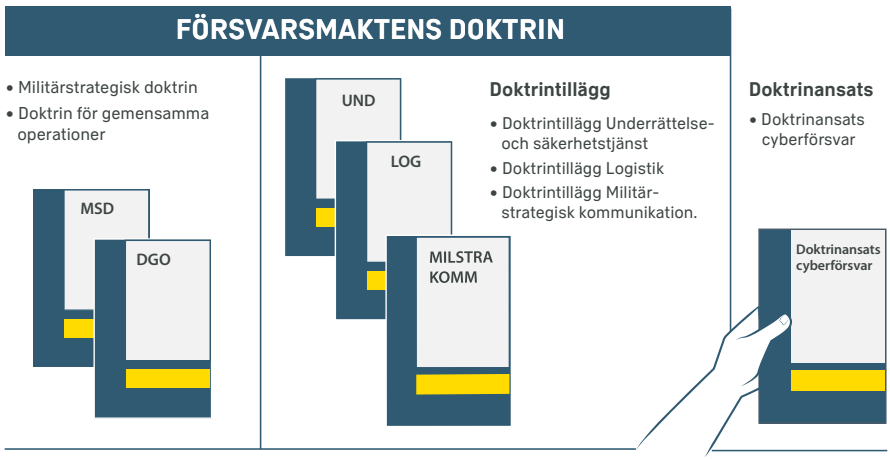

Bild 1.1 Försvarsmaktens doktrin består av MSD, DGO och doktrintilläggen. Doktrinansats Cyberförsvar är inte en formell del av Försvarsmaktens doktrin. Illustration: Anna-Karin Wetzig, Försvarsmakten.

2 Grunder

I detta kapitel redogörs för cyberförsvarets grunder och begrepp vilka är centrala för förståelsen av doktrinansatsen. En mer utförlig begreppslista återfinns i slutet av doktrinansatsen.

2.1 Cyberdomänen

Cyberdomänen definieras i Militärstrategisk doktrin (MSD22) och är tillsammans med mark- sjö-, luft- och rymddomänen de domäner som ingår i operationsmiljön. Cyberdomänen består av digitala system och elektroniska kommunikationstjänster samt de data som lagras i, bearbetas med, eller förmedlas genom dessa system och tjänster. En djupare beskrivning av cyberdomänen återfinns under kapitel 3.

2.2 Cyberförsvar

Cyberförsvar är en integrerad del av det militära försvaret och är en väsentlig del av den moderna krigföringen. Cyberförsvaret ska upprätthålla överbefälhavarens handlingsfrihet med Försvarsmaktens system och plattformar samt skapa effekter i cyberdomänen som en del av det nationella och kollektiva försvaret. Försvarsmakten ansvarar för Sveriges offensiva cyberförmåga. Cyberförsvar omfattar den verksamhet som krävs för att, enskilt eller tillsammans med andra, i samtliga konfliktnivåer kunna

- avskräcka och förneka en motståndare att i eller genom cyberdomänen påverka det militära försvarets förmåga att försvara Sverige och allierade stater mot ett väpnat angrepp, upprätthålla den territoriella integriteten eller värna Sveriges suveräna rättigheter
- försvara svensk kritisk infrastruktur som Försvarsmakten är beroende av
- vidta åtgärder i cyberdomänen för att bidra till att totalförsvaret och det kollektiva försvaret inom Nato som helhet är krigsavhållande
- upptäcka och möta ett väpnat angrepp i eller genom cyberdomänen
- genom offensiva cyberoperationer påverka en motståndares verksamhet i samtliga domäner.

Till följd av cyberdomänens särskilda förutsättningar är stora delar av cyberförsvaret aktivt i samtliga konflikt- och beredskapsnivåer. Genom ett aktivt och integrerat cyberförsvar upprätthålls handlingsfrihet i samtliga domäner samtidigt som cyberförsvarsförmågan utvecklas i takt med omvärldsförändringar och teknologiska framsteg.

Bild 2.1 Cyberförsvar är en integrerad del av det militära försvaret.
Foto: Hampus Hamberg, Försvarsmakten.

Cyberförsvarsförmågan utgörs av mänskliga aspekter i form av kompetensförsörjning och samverkan med partners och allierade såväl som av säkerställandet av spetsteknologi och säkra system och plattformar. För att kunna möta de mest kvalificerade antagonisterna är det nödvändigt att cyberförsvarets materiel och metoder befinner sig i teknikens och forskningens framkant. Striden i cyberdomänen präglas av en ständig kompetenskamp där verkansdelar och motmedel kontinuerligt skapas, omformas och utvecklas med mycket korta tidsförhållanden. Teknik-, kompetens- och metodutveckling är en essentiell del av stridstekniken inom cyberförsvaret.

2.3 Cybersäkerhet

Cybersäkerhet är som verksamhet skilt från cyberförsvar samtidigt som det finns likheter, beroenden och gränsytor mellan områdena. Cybersäkerhet beskrivs i doktrinansatsen enligt följande:

> Åtgärder för skydd av kommunikations-, informations- och andra elektroniska system samt den information som är lagrad i, bearbetad eller förmedlad av dessa system med avseende på konfidentialitet, riktighet, tillgänglighet, autenticitet och oavvislighet.[1]

Cybersäkerhet inkluderar eller överlappar till del informations- och it-säkerhet, vilket beskrivs och regleras i andra publikationer. I doktrinansatsen och i relation till cyberförsvar ska cybersäkerhet tolkas i ett sammanhang som sammanfattas av nedanstående punkter:

1. Cybersäkerhet är funktions- och systemcentriskt med en tydlig tyngdpunkt mot systemens korrekta funktionalitet och tillgänglighet som möjliggörare för den verksamhet de stödjer. Informationen som hanteras i eller passerar genom systemen skyddas som en effekt av att systemen är tillräckligt säkra.
2. Cybersäkerhet omfattar alla typer av system. Förutom styr- och reglersystem och andra funktioner som är av betydelse för totalförsvaret, omfattas produkter och tjänster som inte primärt är it-system men som ändå innehåller eller är beroende av informationsteknik.

Varje verksamhetsutövare inom totalförsvaret som upprätthåller den egna cybersäkerheten stödjer samhällets samlade robusthet och bidrar indirekt till cyberförsvaret. För att minska risken att cyberattacker mot dessa verksamheter blir ett effektivt medel att slå ut eller begränsa försvarsförmågan behöver system och funktioner som utgör beroenden för det militära försvaret

- upprätthålla tillräcklig cybersäkerhet i samtliga konfliktnivåer

1 Beskrivningen är en anpassad översättning från definitionen i Nato AJP-3.20 ver 1 från 2020. I den svenska versionen har *authentication* översatts till *autenticitet* snarare än *autentisering* i syfte att åstadkomma en konsekvent uppräkning där alla element utgör informationssäkerhetsegenskaper.

- förberedas för att vid höjd beredskap kunna förstärkas med krigsplacerade cybersäkerhetsspecialister genom de frivilliga försvarsorganisationerna
- förberederas för att kunna ta emot stöd och i vissa fall försvaras av resurser ur Försvarsmaktens cyberförsvarsförband.

2.4 Skydd, försvar och förutsättningsskapande verksamhet

För att upprätthålla handlingsfrihet i cyberdomänen krävs ständig samverkan mellan verksamheterna *skydd* och *försvar*. Ett effektivt försvar är vidare beroende av förutsättningsskapande verksamheter som bland annat inkluderar över tid upprätthållen *försvarbarhet* och god lägesuppfattning som försörjs av *cyberlägesbilder*.

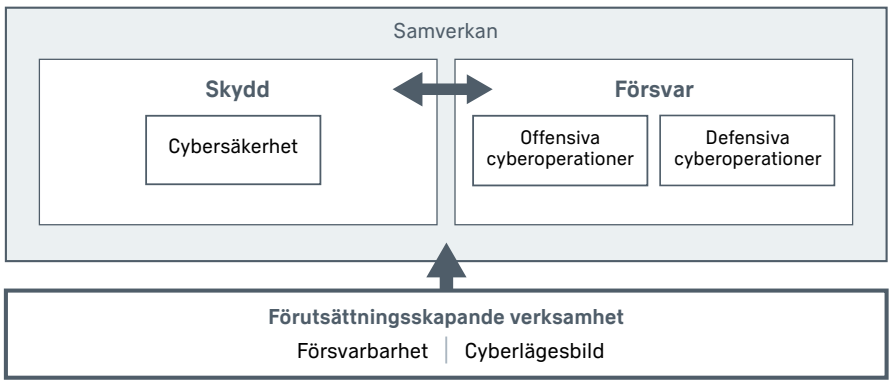

Bild 2.2 Skydd, försvar och förutsättningsskapande verksamhet.
Illustration: Anna-Karin Wetzig, Försvarsmakten.

Både skydd och försvar genomförs över tid, samverkar och är ömsesidigt förstärkande. En förutsättning för både skydd och försvar är att det inom varje verksamhet finns kunskap om vilka system och infrastrukturer som i cyberdomänen utgör beroenden för verksamheten.

2.4.1 Skydd

Området skydd består av verksamhet och resurser som angränsar till både it-produktion, drift och förvaltning samt säkerhetstjänst. Skyddet är proaktivt och reaktivt och syftar till att försvåra eller förhindra att en motståndare ska kunna påverka Försvarsmaktens system samtidigt som förutsättningar för försvar skapas. Skyddet utgörs av åtgärder för att upprätthålla och stärka cybersäkerheten. Ett sätt att öka cybersäkerheten är att genomföra övervakning och sårbarhetsanalys.

OBSERVERA
Det är skillnad på *skydd* som substantiv där det används för att beskriva en verksamhet samt verbet *skydda* som används som ett uppdragsord inom exempelvis operationsorder.

2.4.2 Försvar

Försvar är både proaktivt och reaktivt och en del av det aktiva försvar som genomförs i valda delar enligt förberedande planering eller på förekommen anledning. Försvar i cyberdomänen bedrivs genom *offensiva* eller *defensiva cyberoperationer* i system och plattformar. Försvar kan genomföras inom ramen för militära operationer och ofta för att möta ett specifikt hot. Försvar kan förstärka skyddet under en bestämd tidsrymd genom planerade operationer. Cyberoperationer beskrivs djupare i kapitel 4.

2.4.3 Förutsättningsskapande verksamhet

Cyberlägesbilder beskrivs mer ingående i kapitel 3.4 och återges därför inte i det här delkapitlet.

2.4.3.1 Försvarbarhet

Försvarbarhet kan både ses som en egenskap och ett mått på i vilken utsträckning ett system är utformat för eller på annat sätt möjliggör cyberförsvar. Grunden för försvarbarheten i ett tekniskt system skapas i det tidiga krav- och designarbetet och behöver därefter kontinuerligt upprätthållas och vidareutvecklas under hela systemlivscykeln.

2.4.3.2 Forskning, utveckling och innovation

Ett starkt cyberförsvar behöver ha tillgång till världsledande materiel och metoder för att kunna upptäcka och möta statliga eller statsunderstödda antagonister. En kvalificerad cyberförsvarsförmåga kräver därför en innovationsdriven organisation och en kontinuerlig utveckling för att omsätta forskning och idéer till nya produkter och arbetssätt. Detta förutsätter ett nära samarbete med utvalda organisationer i både privat och offentlig sektor och i såväl nationell som internationell kontext. En nära samverkan mellan myndigheter, akademi och näringsliv stärker även Sveriges konkurrenskraft vilket på sikt bidrar till att utveckla Sveriges roll som tekniknation.

2.4.3.3 Cyberförsvarspyramiden

För att de mest kvalificerade cyberförsvarsresurserna ska kunna nyttjas för att bemöta de mest kvalificerade antagonisterna krävs stöd från och samverkan mellan andra funktioner och aktörer inom totalförsvaret. Genom cyberförsvarspyramiden[2] illustreras hur ett antal centrala samverkande funktioner och förutsättningsskapande delar tillsammans skapar ett sammanhållet system.

Cyberförsvarspyramidens förutsättningsskapande beståndsdelar är

- underrättelse- och säkerhetstjänst
- säkra och robusta kommunikationstjänster
- informations- och cybersäkerhet, inklusive brottsbekämpning och samverkan med rättsvårdande myndigheter
- proaktiv drift, förvaltning och behörighetsstyrning
- användbara, robusta och försvarbara system i alla konfliktnivåer
- säkerhetsmedvetande och säkerhetskultur.

2 Cyberförsvarspyramiden är ursprungligen beskriven i artikeln *Sveriges cyberförsvar tar form – en struktur för fortsatt förmågeutveckling mot 2030 i KKrVAHT* nr 1 2022, s 80–106.

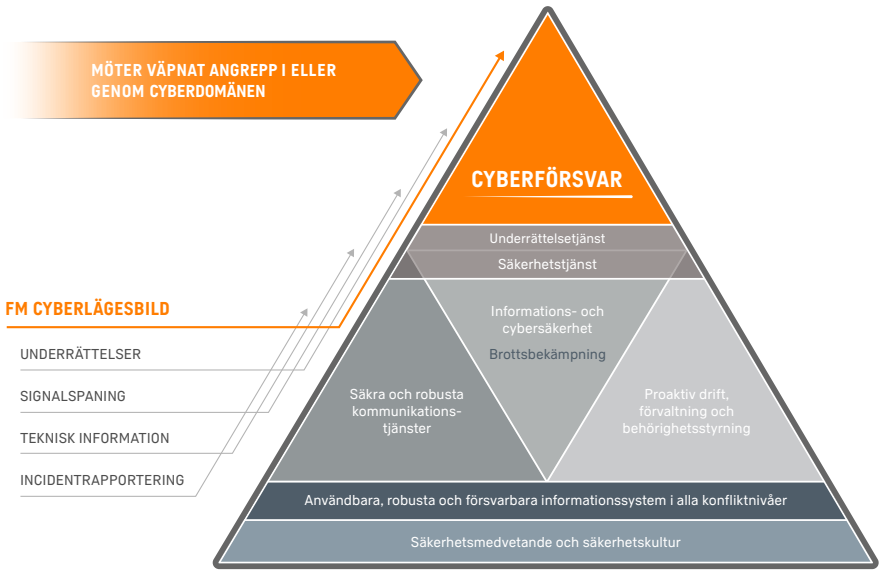

Bild 2.3 Cyberförsvarspyramiden. Illustration: Cecilia Nygren, Försvarsmakten.

Inom verksamheter relaterade till samtliga ovanstående beståndsdelar kan olika typer av information finnas eller händelser uppstå som är av relevans för Försvarsmaktens samlade cyberlägesbild.

Cyberförsvarspyramidens beståndsdelar är konceptuella och på en övergripande nivå. Det finns därmed ingen koppling mellan beståndsdelar och organisationsgränser. Inom Försvarsmakten ingår exempelvis flera områden i verksamheten *skydd*. De olika områdena är vidare reglerade i olika lagar, förordningar och föreskrifter och föremål för tillsyn beroende på verksamhet och aktör.

De olika beståndsdelarna är tätt integrerade och ofta beroende av varandra. För att cybersäkerheten ska kunna upprätthållas genom hela systemlivscykeln krävs till exempel proaktiv drift, förvaltning och behörighetsstyrning. En förutsättning för både framtagande och vidmakthållande av säkra, robusta och användbara system och kommunikationstjänster är att cybersäkerhet och förvaltningsbarhet omhändertas från början i krav- och designarbetet.

Säkra och robusta kommunikationstjänster är också en förutsättning för att cyberförsvaret ska kunna agera i rätt tid på underrättelser och incidentrapporter. Slutligen är en god säkerhetskultur en viktig förutsättning för att minska antalet incidenter och allvarlighetsgraden av dessa samt att totalförsvarets personal över tid bedriver all den verksamhet som cyberförsvarspyramiden beskriver på ett säkert sätt.

3 Cyberdomänen

Detta kapitel beskriver cyberdomänen med dess utformning och karaktäristik. Vidare beskrivs i kapitlet cyberdomänens terräng samt vikten av lägesuppfattning och cyberlägesbilder.

OBSERVERA
Äldre svenska publikationer kan använda begreppet cyberrymd för att beskriva cyberdomänen. Begreppet har sitt ursprung i det engelska *cyberspace* vilket nyttjas i många engelskspråkiga publikationer och sammanhang, till exempel inom Natos verksamhet.

En domän beskrivs i MSD 22 som ett tematiskt avgränsat område där strid mellan militära styrkor kan bedrivas. Cyberdomänen ingår tillsammans med domänerna sjö, mark, luft och rymd i Försvarsmaktens domänkoncept och utgör tillsammans med det elektromagnetiska spektrumet och informationsmiljön Försvarsmaktens operationsmiljö. I MSD 22 framgår att cyberdomänens fysiska delar ingår i operationsmiljöns fysiska miljö och befinner sig inom de övriga domänerna.

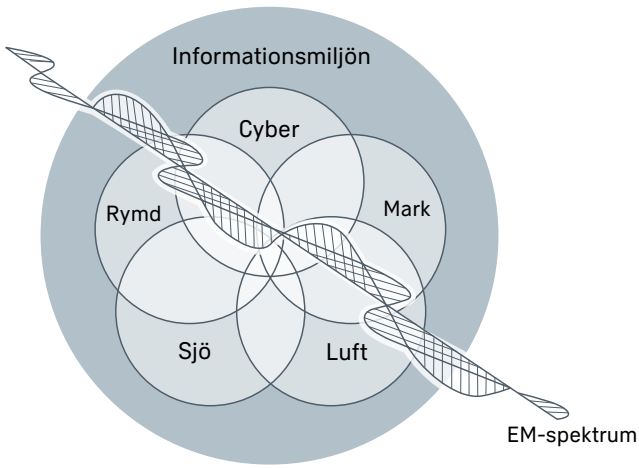

Bild 3.1 Operationsmiljön. Illustration: Anna-Karin Wetzig, Försvarsmakten.

Försvarsmaktens del av cyberdomänen utgörs exempelvis av Försvarets telenät (FTN), ledningsstödssystem, stridsledningss- och verkanssystem, plattformar, sensorkedjor, informationssystem, kryptoutrustning, styr- och reglerfunktioner i drivmedelstationer och anläggningar, bildvisningssystem och enskilda datorer. En cyberattack på system som Försvarsmakten är beroende av kan få stora konsekvenser för Försvarsmaktens förmåga att verka i samtliga domäner.

3.1 Cyberdomänens tre lager

Cyberdomänen kan beskrivas utifrån tre *lager* – det fysiska lagret, det logiska lagret och cyberpersona-lagret. Begreppet *lager* är en översättning av det engelska begreppet *layers* vilket används inom Nato vid beskrivning av cyberdomänens indelning. Lagerindelningen utgör ett stöd i planering och vid genomförande av operationer.

Infrastrukturen som cyberdomänen bygger på är till största del internationellt sammankopplad men omfattas av nationella lagar och regler inom de geografiska områden där infrastrukturen finns. Samtliga lager påverkas i olika grad av nationsgränser samt nationell och internationell rätt. Regleringen för jurisdiktion och tillämplig lag är tydligast avseende det fysiska lagret. Som en del av den pågående kampen i cyberdomänen försöker olika stater skapa egna fördelar genom att politiskt och juridiskt påverka utformningen och regleringen av exempelvis internet. Sveriges och Försvarsmaktens samverkan med internationella partners inom området är därför av stor vikt för handlingsfriheten såväl som för lägesuppfattning avseende händelser som sker inom andra staters ansvar av domänen.

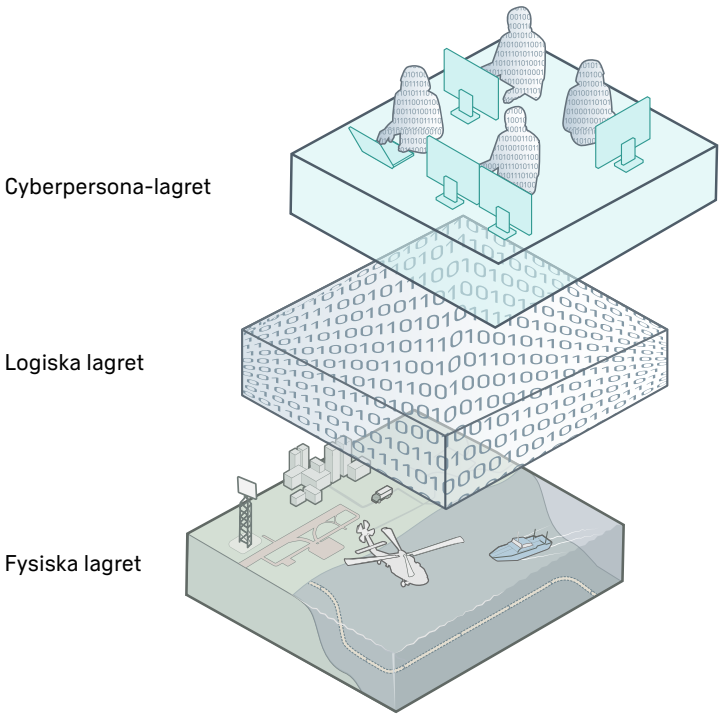

Bild 3.2 Cyberdomänens tre lager. Illustration: Anna-Karin Wetzig, Försvarsmakten.

3.1.1 Det fysiska lagret

Det fysiska lagret innehåller hårdvara. Här inkluderas datorer, servrar, nätverksutrustning, sensorer, länkar och annan utrustning som behövs för lagring, bearbetning och transmission av data. Dessa återfinns exempelvis i styr- och reglersystem, plattformar och vapensystem. Transmission är antingen trådbunden eller trådlös. För kommunikation över IP-nät (till exempel internet) gäller att trafiken kan ta olika vägar från fall till fall. Detta innebär att samma informationsmängd antingen kan gå genom luften via radiolänk eller trådlösa nätverk eller genom en fiber- eller kopparkabel på havsbotten såväl som på land.

3.1.2 Det logiska lagret

Det logiska lagret består av olika typer av data inklusive programkod, till exempel fast programvara, operativsystem, applikationer och andra mjukvarukomponenter. Det logiska lagret existerar inte utan det fysiska lagret. Förändringar i det logiska lagret kan samtidigt påverka det fysiska lagret och därmed ge effekter i operationsmiljön.

Bild 3.3 En bit är den minsta logiska dataenheten i en dator. En bit kan innehålla två värden; 1 eller 0. Bild: Försvarsmakten.

3.1.3 Cyberpersona-lagret

Cyberpersona-lagret innehåller representationer av virtuella identiteter som används av fysiska individer eller organisationer. En virtuell identitet kan vara en e-postadress, en användar-ID, ett konto på sociala media eller ett alias. En person eller en organisation kan ha eller kontrollera flertalet cyberpersona samtidigt som flera personer eller organisationer kan nyttja en och samma cyberpersona. Fysiska personer använder därmed cyberpersona-lagret som ett gränssnitt för att kommunicera och agera i cyberdomänen. Cyberpersona-lagret existerar inte utan det logiska lagret.

3.2 Cyberdomänens terräng

Specifika avsnitt eller områden av cyberdomänen benämns som *cyberterräng* eller *terräng i cyberdomänen*. Begreppet *terräng* är en översättning av det engelska begreppet *terrain* och har valts för att harmonisera språkbruket med allierade och partners.

Cyberdomänens terräng utgörs av hård- och mjukvara som ingår i system samt den information som lagras i, bearbetas med, eller förmedlas genom dessa system och tjänster. Cyberterrängen är både logisk och fysisk och spänner över alla tre lager. Det innebär att terrängen som cyberoperationer genomförs i inte begränsas av formella systemgränser utan kan spänna över flera sammankopplade system och tjänster. Två plattformar som i det fysiska lagret kan uppfattas vara oberoende av varandra kan i det logiska lagret ha ett beroende eller vara sammankopplade, exempelvis genom att de delar terräng i cyberdomänen.

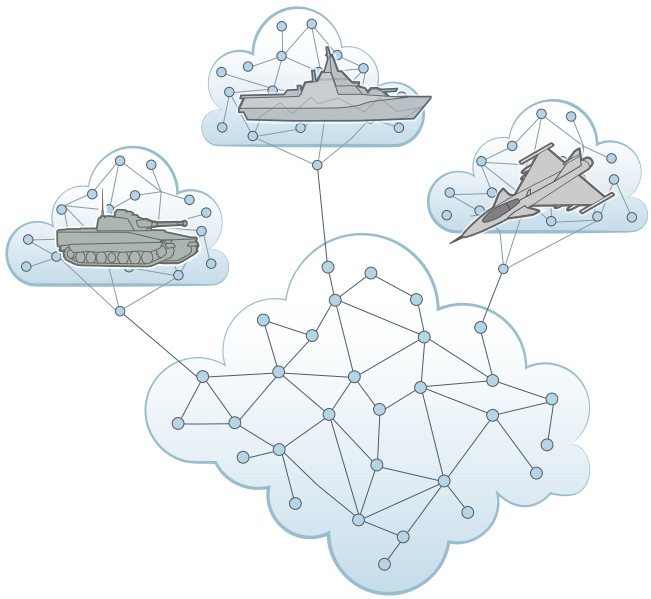

Bild 3.4 System som fysiskt kan se ut att vara oberoende av varandra kan dela cyberterräng i cyberdomänen. Illustration: Anna-Karin Wetzig, Försvarsmakten.

3.2.1 Nyckelterräng i cyberdomänen

Cybernyckelterräng avser avgränsade avsnitt ur cyberdomänen där kontroll eller insyn skapar fördelar för en aktör att uppnå sina mål. Begreppet *cybernyckelterräng* härstammar av det engelska begreppet *key terrain cyber* och har valts för att harmonisera språkbruket med allierade och partners.

Cybernyckelterräng liknar viktig terräng i de andra fysiska domänerna på så sätt att inneha kontroll eller insyn i den, ger en stridande en fördel. I cyberdomänen kan det räcka att upprätthålla närvaro på en särskild plats eller process istället för att erövra och hålla den exklusivt gentemot den andre parten.

Varje verksamhet behöver förberedande och kontinuerligt identifiera både sin egen och motståndarens cybernyckelterräng. Nyckelterrängen kan variera och förändras över tiden. I militära operationer behöver den som planerar verksamhet själv avgöra vilken avgränsad del av cyberdomänen som är nyckelterräng. Genom att ha identifierat cybernyckelterräng i de system och plattformar som är centrala för operationen kan handlingsfrihet upprätthållas genom att förstärka skydd eller försvar. Samma princip gäller vid planering av offensiva cyberoperationer men då identifieras cybernyckelterräng i motståndarens system.

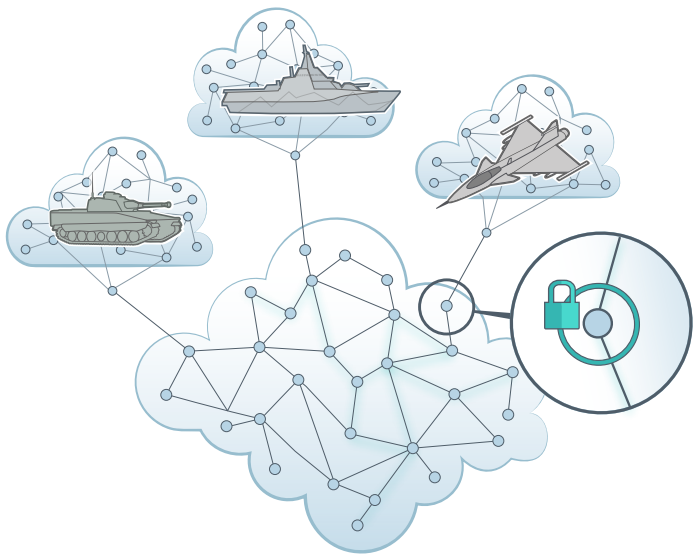

Bild 3.5 Nyckelterräng i cyberdomänen. Illustration: Anna-Karin Wetzig, Försvarsmakten.

För åtkomst till nyckelterräng kan exempelvis datacenter, kommersiella internettjänsteleverantörer, undervattenskablar, försörjningskedjor eller individer vara av intresse. Dessa individer avser personer med åtkomst eller inflytande av betydelse för den militära operationen. För att kontrollera och behärska nyckelterräng i cyberdomänen kan det därmed krävas åtgärder i andra domäner.

3.2.2 Cyberterrängens indelning

Cyberterrängen kan delas in i tre olika färger; *blå, grå* och *röd*. Indelningen används för att beteckna vem som har rådighet över olika delar av terrängen. Med rådighet avses dels vem som utnyttjar en komponent, dels vem som har ett fysiskt ägarskap och kontrollerar dess livscykel. Indelningen är inte juridisk utan utgör ett metodstöd vid planering, beslutsfattande, lägesbildsförståelse och genomförande.

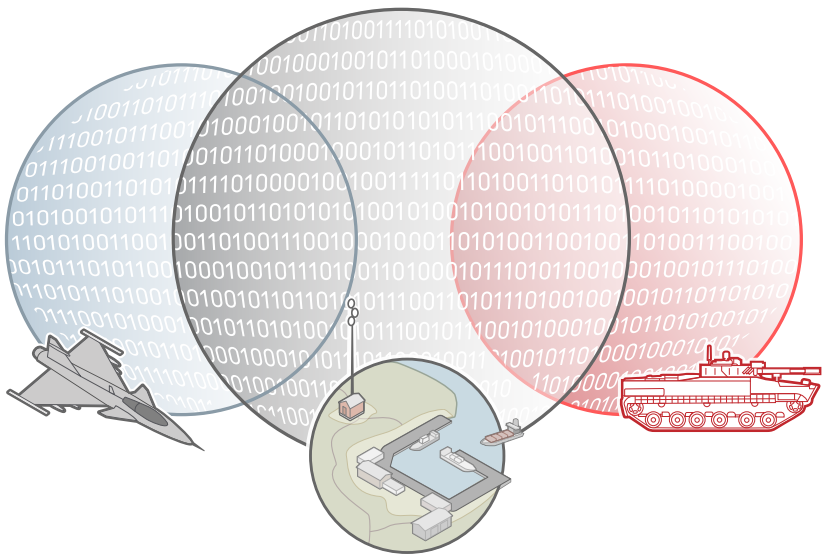

Bild 3.6 Cyberterrängens tre färger. Illustration: Anna-Karin Wetzig, Försvarsmakten.

3.2.2.1 Blå terräng

Blå terräng utgörs av terräng i cyberdomänen som Försvarsmakten har rådighet över. Det inkluderar hård- och mjukvara ingående i materielsystem och plattformar.

Utöver Försvarsmaktens terräng ingår även allierades terräng och terräng som Försvarsmakten ges i uppgift att försvara, vilken kan inkludera system och infrastrukturer som ägs av andra myndigheter, samarbetspartners och leverantörer.

3.2.2.2 Grå terräng

Grå terräng utgörs av sådan terräng som inte kan betecknas som blå eller röd och utgör majoriteten av cyberdomänen. Grå terräng knyter samman blå och röd terräng och kan även underbygga dessa genom exempelvis infrastruktur och tjänster som ägs av externa leverantörer.

Olika lager i domänen kan utgöra olika typer av terräng. Ett exempel på detta kan vara molnlösningar, där system som ingår i blå terräng utnyttjar fysisk infrastruktur som Försvarsmakten inte har rådighet över. Där kan det logiska och cyberpersona-lagret klassas som blå terräng och det fysiska lagret som grå terräng.

Ett annat exempel är system och plattformar i blå terräng som är spridda geografiskt och sammankopplade med en VPN[3]-lösning över internet. Transmissionen över internet går i grå infrastruktur som Försvarsmakten är beroende av för att system och plattformar i blå terräng ska fungera.

3.2.2.3 Röd terräng

I röd terräng har en motståndare rådighet över terrängen. I den röda terrängen ingår bland annat motståndarens system och plattformar. Att avgöra om en terräng är grå eller röd kan vara mycket svårt och kräva omfattande teknisk kartläggning och underrättelser.

3 Virtuellt privat nätverk.

3.3 Cyberdomänens karaktäristik

I det här delkapitlet ges en översiktlig beskrivning av cyberdomänens särskilda karaktäristik.

3.3.1 Anonymitet

Eftersom aktörer agerar genom cyberpersona-lagret möjliggörs ett anonymt uppträdande. Det innebär att det vid ett angrepp, särskilt i ett tidigt skede, kan vara svårt att identifiera upphovspersonen. Det är även möjligt att flera parter befinner sig i samma cyberterräng utan att känna till den andres närvaro. Inom cyberdomänen finns ett stort spektrum av aktörer vilka utgörs av statliga, statsunderstödda samt icke-statliga aktörer. En aktör som har avsikt och förmåga att agera illvilligt i eller genom cyberdomänen benämns i doktrinansatsen *antagonist*.

3.3.2 Asymmetri

Att cyberdomänen är världsomspännande och att det logiska lagret är lättillgängligt för den som har rätt resurser möjliggör närvaro i cyberdomänen för flertalet aktörer. En aktör med motivation, resurser och teknisk kapacitet kan agera i cyberdomänen och åstadkomma strategiska och storskaliga effekter som är oproportionerliga till aktörens storlek.

3.3.3 Flexibilitet och återanvändbarhet

Effekter i eller genom cyberdomänen kan utformas för att vara tillfälliga och därmed möjliga att återställa eller för att vara permanenta. En verkansdel kan exempelvis utgöras av skadlig kod som ligger latent i ett system innan den exekveras. Ett beslut om när och hur verkan ska ske kan fattas även efter att en verkansdel levererats om den har utformats på lämpligt sätt. När en verkansdel har blivit känd kan skyddsåtgärder i form av exempelvis mjukvaruuppdateringar förhindra att samma sårbarhet återanvänds. Att återanvända verkansdelar för att skapa effekter i eller genom cyberdomänen kan öka risken för upptäckt och innebära förlust av anonymitet. Det är därför viktigt att misstänkta angrepp rapporteras – dels för att kunna vidta adekvata åtgärder, dels för att informationen kan utgöra underlag till cyberlägesbilden och en kategorisering av hotaktörer. Genom att återanvända en verkansdel från en annan aktör och sedan förändra den kan den användas mot andra mål eller mot den ursprungliga aktören.

Bild 3.7 Cyberförsvaret är beroende av flexibla metoder.
Foto: Hampus Hamberg, Försvarsmakten.

3.3.4 Föränderlighet

Terrängen skiljer sig från den i andra domäner genom att den dels är skapad och kontrollerad av människor, dels är formbar och föränderlig. Den aktör som äger eller på annat sätt ansvarar för en del av terrängen har därför möjlighet att förändra den delen av terrängen till sin egen fördel i domänens alla lager utan att en motpart nödvändigtvis märker det.

3.3.5 Cyberdomänens omfattning

Cyberdomänens omfattning medför att operationer i cyberdomänen inte är begränsade till det geografiska närområdet utan av logiska anslutningar. Inte heller är operationsområdet geografiskt sammanhängande utan det kan utgöras av flera fysiskt oberoende men av varandra logiskt beroende komponenter. Detta möjliggör att aktörer kan uppnå effekt på en helt annan plats än där de själva fysiskt befinner sig. Internet är en stor del av cyberdomänen och eftersom alla internetanslutna system och tjänster är direkt eller indirekt ihopkopplade kan önskade effekter i ett specifikt system snabbt sprida sig och ge upphov till

oväntade eller oönskade konsekvenser i andra system. Domänens omfattning är däremot inte begränsad av internet utan den sträcker sig bortom internet och uppkopplade system.

3.3.6 Tid och hastighet

För att verka i cyberdomänen krävs resurser vilka kan utgöras av relativt enkla tekniska medel som utvecklats snabbt eller av sofistikerade verktyg som utvecklas och underhålls under lång tid. Komplexiteten hos och tekniknivån i ett verktyg beror framför allt på den önskade effekten och målets egenskaper.

Förberedelsetiden är längre om målets komplexitet är hög eller om underrättelseinhämtning, specifika effekter, kontinuerlig tillgång till målet och anonymitet är av vikt. Tiden från beslut att skapa en effekt, genom utveckling och leverans av verkansdelar, till att effekten uppnås kan således vara mycket lång. Samtidigt kan denna tid vara mycket kort om faktorerna ovan inte behöver beaktas. Effekten från en verkansdel kan vara omedelbar eller avsiktligt fördröjd.

3.4 Cyberlägesbilder

Cyberdomänens föränderlighet, dess svåröverblickbara terräng och korta tidsförhållanden gör att lägesuppfattning är vitalt. En *cyberlägesbild* beskriver läget i en specifik del av cyberdomänen vid en specifik tidpunkt. Cyberlägesbilder är därmed ett stöd för – men inte det samma som – lägesuppfattningen.

Med *cyberlägesbild* avses en strukturerad informationsmängd som för en given ledningsnivås intressesfär vid en given tidpunkt beskriver och bedömer konsekvenserna av tillståndet för och hoten mot utvalda delar av cyberdomänen. Lägesbild kan föras analogt, digitalt eller genom en kombination av de två.

OBSERVERA
En cyberlägesbild är en produkt. För att kunna ta fram relevanta cyberlägesbilder regelbundet såväl som vid uppkomna behov krävs personal, rutiner, informationsflöden och systemstöd.

3.4.1 Cyberlägesbilder på flera nivåer

Cyberlägesbilder förekommer inom olika verksamheter och nivåer i totalförsvarets militära och civila delar. En cyberlägesbild kan vara tematisk eller beskriva läget för en viss verksamhet, händelse eller operation. Olika cyberlägesbilder såväl som den information de är baserade på kan i sin tur försörja andra cyberlägesbilder.

Försvarsmaktens militärstrategiska cyberlägesbild eller den *militärstrategiska cyberlägesbilden* är myndighetens samlade beskrivning av tillståndet för och hoten mot Försvarsmaktens intressen i cyberdomänen. Den militärstrategiska cyberlägesbilden utgör ett stöd för Försvarsmaktens samlade militärstrategiska lägesuppfattning och beslutsfattande och omfattar lägesinformation med betydelse för den strategiska och militärstrategiska nivån. Exempel på innehåll är:

- Underrättelser om okända, neutrala och fientliga aktörers aktiviteter och modus inom cyberdomänen.
- Information om Försvarsmaktens verksamhet med betydelse för cyberförsvaret.
- Information om allierade och partners aktiviteter med betydelse för cyberförsvaret.

En förutsättning för att bibehålla en relevant lägesuppfattning är att den militärstrategiska cyberlägesbilden försörjs med rapportering från andra delar av Försvarsmakten och andra aktörer i samhället. Denna rapportering består av information om indikationer av sårbarheter eller angrepp, teknisk information och status för system och tjänster, incidentrapporter samt öppen information om sårbarheter och andra potentiella hot med bäring på systemen och tjänsterna i fråga. Att Försvarsmakten kontinuerligt försörjs med rapportering från olika aktörer möjliggör tidigt agerande. Säkerhetstjänsten bidrar till cyberlägeslägesbilden genom incidentrapporter från de verksamheter som står under säkerhetstjänstens föreskrifts-, tillsyns- och kontrollområden. Underrättelsetjänsten bidrar till cyberlägesbilder genom sammanställda underrättelseunderlag.

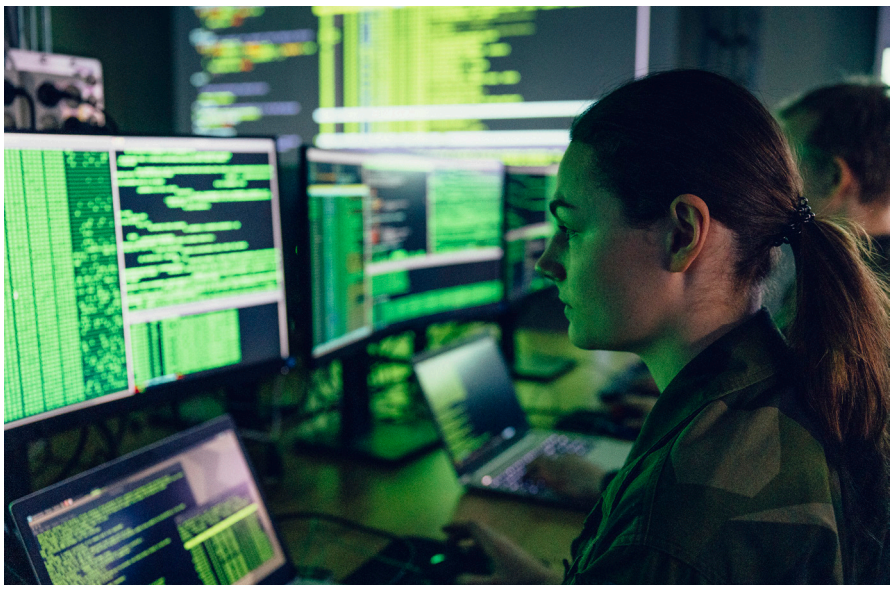

Bild 3.8 Att bibehålla en uppdaterad cyberlägesbild är en förutsättning för att kunna upprätthålla cyberförsvaret. Foto: Daniel Sanchez, Försvarsmakten.

Det är endast genom att aggregera information utifrån den expertkompetens om de egna systemen och de samlade iakttagelser som byggs upp lokalt, som en relevant bedömning kan göras på strategisk nivå. Detta gäller alltifrån förekomsten av specifika komponenter till händelser som detekterats, för att kunna kartlägga såväl potentiell sårbarhet som uppnådd effekt för aktuella operationer. Cyberlägesbilden kompletteras med information om exempelvis offentligt kända sårbarheter och it-säkerhetsincidenter samt relevant information tillhandahållen av myndigheter, organisationer och stater Försvarsmakten samarbetar med.

Den *operativa cyberlägesbilden* skapas genom att betrakta, kontextualisera och värdera de taktiska detaljerna i ljuset av de egna uppdragen och det egna handlandet. Information om motståndare, dess intention och kapacitet samt pågående aktiviteter används för att värdera olika cyberhot mot de egna operationerna.

Den *taktiska cyberlägesbilden* omfattar lägesinformation och systemstatus från försvarsgrenarnas och stridskrafternas egna system, plattformar och infrastruktur. Den taktiska cyberlägesbilden kan även inkludera observationer om hotaktörers infrastruktur, verktyg och tillvägagångssätt samt relaterade händelser i cyberdomänen av betydelse för verksamheten. Denna lägesbild delas med Försvarsmaktens operativa och strategiska nivå.

Eftersom antagonistiska aktiviteter i cyberdomänen kan vara indikatorer för ett möjligt kommande angrepp på Sverige, såväl som annan hotande verksamhet mot svenska intressen, stödjer cyberförsvaret genom sin verksamhet Försvarsmaktens samlade lägesbild och uppgiften strategisk förvarning.

3.4.2 Delgivning och aggregering

Den militärstrategiska cyberlägesbilden aggregeras på central nivå och delges den militärstrategiska ledningen samt berörda delar inom operativ och taktisk nivå. Delar av lägesbilden delges också andra myndigheter och organisationer som Försvarsmakten samarbetar med, exempelvis inom ramen för Nationellt cybersäkerhetscenter (NCSC).

3.5 Kategorisering av hotaktörer

Att identifiera vilken aktör som står bakom ett angrepp är viktigt som underrättelseunderlag och benämns *kategorisering av hotaktörer*. Försvarsmakten och cyberförsvaret genomför kontinuerligt bedömningar av händelser i cyberdomänen och kategoriserar dessa till olika hotaktörer. Kategorisering av hotaktörer görs i syfte att stödja genomförandet av egna operationer. Genom att försöka klargöra vem motståndaren är kan inriktning av genomförandet och dimensionering av den egna förmågan göras.

Försvarsmaktens kategorisering av hotaktörer kan även bidra till underlag som lämnas till regeringen för vidare hantering inom den politiska nivån. Som del i Sveriges utrikes- och säkerhetspolitik kan regeringen vilja peka ut vem som genomfört en viss handling. Detta benämns att *attribuera*. Attribuering görs i enlighet med de folkrättsliga reglerna om statsansvar.[4]

4 Position Paper on the Application of International Law in Cyberspace, Government Offices of Sweden (Ministry for Foreign Affairs), 2022, s. 5–6.

Regeringen är ansvarig för att fatta beslut om attribuering med stöd av berörda myndigheter, exempelvis Försvarsmakten. För ett beslut om attribuering krävs omfattande underlag, bland annat teknisk information och analys av en antagonists tillvägagångssätt både i cyberdomänen och i andra domäner. Detta skiljer sig från kategorisering av hotaktörer.

3.6 Incident

Begreppet *incident* har olika innebörd i olika verksamheter. Med incident avses i doktrinansatsen en händelse eller en aktivitet i cyberdomänen som direkt eller indirekt kan påverka system som utgör beroenden för Försvarsmakten och som kan misstänkas ha utnyttjats alternativt ha orsakats av en antagonist.

Uttrycken *kan påverka* och *kan misstänkas* förmedlar att det i incidentens tidiga skede ofta är svårt att med säkerhet fastslå förekomsten av en antagonist, den fullständiga omfattningen samt allvarlighetsgraden. Detta leder till två bärande principer för incidenthantering i cyberdomänen:

1. Åtgärder baseras på antagandet att en antagonist kan finnas i systemet fram till dess att motsatsen bedöms mer sannolik.
2. Hantering av misstänkta händelser inleds omedelbart inom den försvarsgren eller stridskraft som ansvarar för systemet. Den ansvariges egna resurser kan beroende på incidentens natur förstärkas med resurser ur cyberförsvarsförbanden.

4 Operationer

I det här kapitlet beskrivs olika operationer i cyberdomänen samt hur cyberoperationer kan utföras både som autonoma operationer och som ingående delar i gemensamma operationer.

4.7 Cyberoperationer

En *operation* är en sammanfattande benämning på militära insatser, handlingar, eller genomförandet av uppdrag eller uppgifter som oavsett ledningsnivå syftar till att nå en bestämd målsättning inom ett område.

En *cyberoperation* är en operation vars målsättningar uppnås genom aktiviteter i cyberdomänen. Cyberoperationer som militärt maktmedel kan användas i samtliga konfliktnivåer.

Cyberoperationer genomförs endast i det logiska lagret av cyberdomänen men kan i en gemensam operation koordineras med aktiviteter i det fysiska lagret. En operation som sker i den fysiska delen av cyberdomänen är en operation i cyberdomänen men inte en cyberoperation. Cyberoperationer skiljer sig slutligen från *informationsoperationer* vilket definieras i Doktrintillägg Militärstrategisk kommunikation.

> *”Operation som syftar till att uppnå effekter genom att förmedla en specifik informationsmängd till en eller flera utvalda målgrupper.”*
>
> Försvarsmakten, Doktrintillägg Militärstrategisk kommunikation 2023
> Sida 59

FAKTA
I äldre handlingar förekommer begreppet dator- och nätverksoperationer. Till följd av försvarsbeslut 2020 samt för internationell anpassning har en övergång till cyberoperationer skett. På samma sätt används *defensiva cyberoperationer* istället för det tidigare engelska begreppet *computer network defense* (CND).

Cyberoperationer delas upp i två kategorier: *offensiva* och *defensiva*:

1. Offensiva cyberoperationer syftar till att påverka motståndarens förmågor genom effekter i eller genom cyberdomänen.
2. Defensiva cyberoperationer syftar till att säkerställa egen handlingsfrihet och tillgänglighet i system av betydelse för egen verksamhet.

4.7.1 Offensiva cyberoperationer

Offensiva cyberoperationer (OCO) sker mot system som motståndaren behöver för att genomföra sin verksamhet. Dessa kan genomföras för att stödja operationer i övriga domäner. OCO delas in i *cyberexploatering* (CE) och *cyberattack* (CA).

Cyberexploatering innebär inhämtning och andra förberedelser i cyberdomänen till stöd för underrättelsebehov och planering av cyberattack.

Cyberattack[5] innebär planerade aktiviteter som leder till önskade effekter. Effekterna syftar till att aktivt påverka motståndarens vilja och krigföringsförmåga. Detta kan ske genom att

- förvägra motståndaren tillgång till system och plattformar genom att i olika grad degradera, störa alternativt förstöra hela eller delar av dessa
- manipulera data och information eller funktionellt påverka system och tjänster som motståndaren nyttjar i cyberdomänen.

Offensiva cyberoperationer beslutas och leds på militärstrategisk nivå. Militärstrategisk nivå kan understödja alternativt avdela resurser till operativ nivå för effekter i cyberdomänen.

5 Begreppet avser inte den folkrättsliga definitionen av cyberattack, se begreppslistan.

4.7.2 Defensiva cyberoperationer

Defensiva cyberoperationer (DCO) kan genomföras både i Försvarsmaktens egna system och i system utanför myndigheten som Försvarsmakten fått i uppgift att försvara.

DCO delas in fyra primära verksamheter:

1. *Sensoranalys (SA)* innebär att loggar och larm för system eller sensorer korreleras och analyseras för att upptäcka antagonistisk verksamhet.
2. *Uppsökande verksamhet (UV)* syftar till att upptäcka och hantera en antagonists verksamhet i system där en antagonist kan ha tagit sig förbi en eller flera säkerhetsfunktioner utan att ha detekterats.
3. *Incidenthantering (IH)* inom cyberförsvar syftar till att återställa tillförlitlig funktionalitet och utreda händelsekedjor i system efter att en händelse påverkat eller bedöms ha påverkat systemets tillgänglighet eller riktighet och där händelsen bedöms ha antagonistiskt ursprung.
4. *Motåtgärder*[6] *(MÅ)* syftar till att förhindra, påverka eller avbryta en motståndares verksamhet i eller mot egna system.

Verksamheterna kan genomföras var och en för sig eller kombinerat. Resultatet från en given aktivitet i en verksamhet kan automatiskt leda till att en annan verksamhet initieras.

Försvarsmakten genomför försvar av cyberdomänen i blå terräng genom defensiva cyberoperationer. DCO möter riktade och aktörsdrivna hot för att bibehålla eller öka Försvarsmaktens eller allierades handlingsfrihet.

DCO kan genomföras i operationsområden bestående av allt från små avskilda system till stora och komplexa system av system. DCO genomförs på samtliga ledningsnivåer.

6 Begreppet motåtgärder avser här en verksamhet inom defensiva cyberoperationer och avser inte den folkrättsliga betydelsen av begreppet.

Bild 4.1 Cyberoperationer som militärt maktmedel kan användas i samtliga konfliktnivåer. Foto: Försvarsmakten.

4.7.3 Cyberoperationer som autonoma och gemensamma operationer

Cyberoperationer kan dels utgöra en del av och syfta till att stödja den gemensamma operationen och dels utgöra autonoma cyberoperationer. Syftet med att genomföra autonoma cyberoperationer kan vara att med korta tidsförhållanden omsätta militärstrategiska inriktningar till operativ effekt eller när det är särskilt viktigt med exempelvis operationssekretess, möjlighet till okonventionellt uppträdande, tempo eller flexibilitet.

Syftet med cyberoperationer som integrerad del av en gemensam operation är att säkerställa tillgänglighet i egna system samt att förhindra eller begränsa en motståndares verkan. Offensiva cyberoperationer inom ramen för gemensamma operationer syftar till att påverka motståndarens krigföringsförmåga eller inhämta underrättelser till stöd för den egna förmågan. Den gemensamma operationen kan till exempel innefatta fokuserade och tidsbegränsade cyberoperationer i syfte att säkerställa eller öka handlingsfrihet i andra domäner. Att ha god terrängkännedom om både den egna och motståndarens cyberterräng är därför vitalt vid genomförande av en gemensam operation.

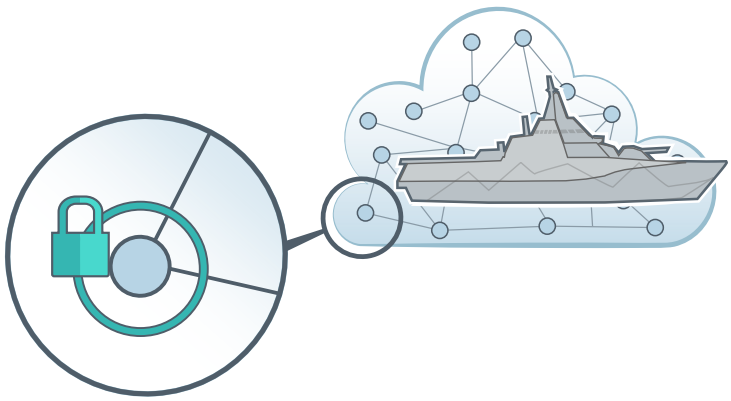

Bild 4.2 Cybernyckelterräng. Innan och under en operation kan skydd och försvar av egen cybernyckelterräng förstärkas. Illustration: Anna-Karin Wetzig, Försvarsmakten.

5 Ledning

Cyberförsvaret leds, inriktas och samordnas från militärstrategisk nivå genom chefen för cyberförsvaret och cyberförsvarsledningen. Inom cyberförsvaret kan det pågå flera samtidiga operationer på olika ledningsnivåer med cyberförsvarsresurser. Exempelvis kan det pågå en cyberoperation på militärstrategisk nivå samtidigt som andra delar av cyberförsvaret samordnas i en gemensam operation – nationellt eller med allierade och partners. Sammantaget ställer dessa ledningsförhållanden särskilda krav på cyberförsvarsledningens förmåga att leda och samordna flera olika typer av cyberoperationer samtidigt. Detta går att sammanfatta i sex ledningsprinciper vilka återges under kapitel 5.3.

5.1 Ledning av cyberoperationer som autonoma operationer

En *autonom cyberoperation* är en operation som initieras av och leds från den militärstrategiska nivån i syfte att uppnå militärstrategiska målsättningar. Operationsformen genomförs av kvalificerade cyberförsvarsresurser och kan genomföras självständigt eller samordnat med specialoperationer och militärstrategisk kommunikation. Autonoma cyberoperationer kan utgöras av såväl offensiva som defensiva cyberoperationer. Chefen för cyberförsvarsledningen utgör operativ chef under chefen för cyberförsvaret.

5.2 Ledning av cyberoperationer som del i gemensamma operationer

En *gemensam operation* är en operation där stridskrafter i olika domäner samordnas för att uppnå synergier, i ett gemensamt syfte. I den gemensamma operationen avdelas cyberförsvarsresurser från militärstrategisk nivå till operativ chef. Chefen för cyberförsvarsledningen utgör då taktisk chef under operativ chef. Inom den gemensamma operationen ryms både defensiva och offensiva cyberoperationer. För att optimera effekten av cyberförsvaret i en gemensam operation ska cyberoperationer integreras tidigt i operationsplaneringen.

Bild 5.1 Cyberoperationer genomförs både som autonoma operationer ledda från militärstrategisk nivå och som en del av gemensamma operationer. Foto: Försvarsmakten.

5.3 Cyberförsvarets ledningsprinciper

Sex principer utgör vägledning för ledning och styrning av cyberförsvaret. Genom att tillämpa dessa ledningsprinciper möjliggörs att cyberförsvaret leds effektivt i förhållande till cyberdomänens karaktäristik.

5.3.1 Lägesuppfattning

Cyberdomänens karaktäristik innebär att läges-, sårbarhets- och hotinformation behöver ha hög tillgänglighet på alla nivåer i Försvarsmakten. Ansvaret för att upprätthålla system- och terrängkännedom vilar alltid på den chef som ansvarar för ett system. Information behöver kunna samlas in från tillgängliga källor, analyseras, bearbetas och delges i nära realtid. Hög förmåga att aggregera, och med tekniskt stöd behandla, information krävs för att upprätthålla aktuella cyberlägesbilder för att skapa lägesuppfattning.

5.3.2 Flexibilitet

Beslut måste kunna fattas med snäva tidsförhållanden, vilket förutsätter en hög grad av delegerade mandat och kompetens för att kunna agera i rätt tid. Beslut om skydd och försvar av enskilda system behöver vara delegerade så långt som möjligt och fattas driftnära.

Flexibilitet och snabbhet är avgörande egenskaper för att cyberförsvaret ska kunna möta den snabbt föränderliga cyberdomänen och den sofistikerade naturen hos cyberhot. Det krävs förmåga att snabbt anpassa sig till nya hot, tekniker och taktik genom kontinuerlig utbildning, träning och övning. En flexibel ledning inom cyberförsvaret kan snabbt mobilisera resurser för att agera mot angrepp och förebygga framtida angrepp.

5.3.3 Ansvar

Tydliga roller och ansvarsområden är nödvändiga för att säkerställa effektiv koordinering och genomförande av cyberoperationer. Detta inkluderar att definiera befogenheter, ansvar och rapporteringslinjer för att säkerställa enhetlighet och transparens i beslutsprocesser. Samtliga inom cyberförsvaret är ansvariga för att säkerställa efterlevnad av lagar, regler och etiska riktlinjer vid genomförandet av cyberoperationer och för att hållas ansvariga för sina handlingar och beslut.

Utan tillräckligt delegerade mandat riskerar beslutskedjor att ta för lång tid för att kunna agera på uppkomna situationer. Olika typer av cyberoperationer har olika ledningsbehov, vilket ställer särskilda krav på militärstrategisk nivå som ska kunna sammanhålla samtliga typer av cyberoperationer. Alla ledningsnivåer ska ha förutsättningar att leda de operationer som faller inom eget verksamhetsansvar.

5.3.4 Proaktivitet

Proaktivitet i hanteringen av cyberhot ska eftersträvas genom att identifiera och åtgärda sårbarheter innan de utnyttjas av motståndaren. Detta kräver förebyggande åtgärder som uppdaterad teknik, kontinuerlig utbildning och utveckling av cyberförsvarsstrategier. Genom proaktivitet minskar risken att sårbarheter och potentiella hot utvecklas till allvarliga incidenter.

Bild 5.2 Aegis är Cyberförsvarets emblem. Aegis omnämns i Illiaden som ett attribut som bärs av både Zeus och hans dotter Athena. ”Att stå under Aegis beskydd” betyder att något görs under kraftfullt, skickligt och välgörande beskydd. I Illiaden beskrivs Aegis som ovärderlig och odödlig som under strid frambringade den kraft som en myriad drakars vrål.
Foto: Hampus Hamberg, Försvarsmakten.

5.3.5 Integration

Effektiv integration av cyberoperationer med övriga försvarsåtgärder är avgörande för att uppnå övergripande strategiska mål och säkerställa ett samordnat och enhetligt agerande mot hot. Detta kräver nära samarbete och integration inom Försvarsmakten och med andra aktörer i totalförsvaret för att dela information, resurser och erfarenheter.

Genom att integrera cyberoperationer med operationer i andra domäner kan Försvarsmakten på ett effektivt och samordnat sätt förutsäga, förebygga och svara på cyberhot.

5.3.6 Samverkan

Cyberförsvaret kräver en hög grad av samverkan för att effektivt kunna motverka globala cyberhot och att utbyta information och erfarenheter. Civil-militär samverkan, nationellt såväl som internationellt, mellan myndigheter men också med näringsliv och företag är centralt. Internationell militär samverkan med allierade och partners är en förutsättning och sker genom strategisk inriktning.

Begrepp

I denna publikation beskrivs flera begrepp i den löpande texten. Uppställningen här är gjord i bokstavsordning.

Begrepp	Förklaring och exempel
Cyberattack	Cyberattack kan antingen syfta till - illvillig aktivitet i cyberdomänen syftande till att inhämta, förneka, försämra eller förstöra ett system eller dess information. - specifik aktivitet inom ramen för en offensiv cyberoperation som beskrivs i kapitel 4.1.1.
Cyberdomänen	Cyberdomänen består av digitala system och elektroniska kommunikationstjänster samt de data som lagras i, bearbetas, eller förmedlas genom dessa system och tjänster. I domänen ingår bland annat ledningsstödsystem, stridsledning- och verkanssystem, intranät, styr- och reglersystem, telekommunikationssystem, de uppkopplades sakernas internet, inbyggda system i anläggningar, fordon och farkoster, samt internet i sin helhet. Cyberdomänens fysiska delar befinner sig i de övriga domänerna.
Cyberförsvarsförband	Försvarsmaktens cyberförsvarsförband (CFF) är en förbandstyp särskilt utformad och resurssatt för att genomföra kvalificerade cyberoperationer.
Cyberlägesbild	Med cyberlägesbild avses en strukturerad informationsmängd som inom en given ledningsnivås intressesfär, för en given tidpunkt, beskriver tillståndet för och hoten mot utvalda delar av cyberdomänen.
Cyberoperation	En cyberoperation är en operation vars målsättningar uppnås genom aktiviteter i det logiska lagret av cyberdomänen.
Cybersäkerhet	Åtgärder för skydd av kommunikations-, informations- och andra elektroniska system samt den information som är lagrad i, bearbetad eller förmedlad av dessa system med avseende på konfidentialitet, riktighet, tillgänglighet, autenticitet och oavvislighet. Beskrivningen är en anpassad översättning från definitionen i Nato AJP-3.20 ver 1 från 2020. I den svenska versionen har ***authentication*** översatts till ***autenticitet*** snarare än ***autentisering*** i syfte att åstadkomma en konsekvent uppräkning där alla element utgör informationssäkerhetsegenskaper.
Cyberterräng	Cyberterräng utgörs av hård- och mjukvara som ingår i system samt den information som lagras i, bearbetas med, eller förmedlas genom dessa system och tjänster. Cyberterrängen är både logisk och fysisk och spänner över alla tre lager.
Försvarbarhet	Förutsättningar att genomföra cyberoperationer i ett system.
Verkansdel	En verkansdel i cyberdomänen kan exempelvis utgöras av skadlig kod som ligger latent i ett system innan den exekveras.

Redaktionell information

Doktrinansats Cyberförsvar är en nyutgåva. Cyberdomänen och cyberförsvar beskrivs översiktligt i den militärstrategiska doktrinen samtidigt som det precis som för andra områden finns ett behov av en fördjupad doktrinär beskrivning i en annan publikation. Därför har C FST STRA gett i uppdrag att ta fram denna doktrinansats för cyberförsvar.

Doktrinansatsen är framtagen under ledning av cyberförsvarsledningen i en för arbetet sammansatt arbetsgrupp. I arbetsgruppen har representanter från cyberförsvarsledningen och cyberförsvarsförbanden deltagit. Arbetsgruppen har löpande samverkat med AG Doktrinutveckling.

Doktrinansatsen har genomgått internremiss inom Försvarsmakten, utvecklats genom Fältövning Cyberförsvar 2023 och varit föremål för särskilda fokusdiskussioner med berörda chefer. I arbetet har internremiss, samverkan och beredning gjorts inom Högkvarteret (FST EVS, FST STRA, FST GEN, FST STÖD, FST CIO, FST RHE, FST JUR, FST KOMM, FST SFL, MUST, OPL) samt med Arméstaben, Marinstaben, Flygstaben och FMTIS.

Inför C FST STRA beslut har beredning skett med C FST STRA PLAN överste Mikael Beck och dessförinnan C FST STRA CFL överste Thomas Höglund.

Bildförteckning

I den här publikationen förekommer följande bilder med verkshöjd:

Bildnr.	Fotograf/illustratör	Hur FM säkrat rätten att använda bilden
Omslag	Fotograf: Joel Thungren, Försvarsmakten; Grafisk bearbetning: Anna-Karin Wetzig	Bild hämtad från www.forsvarsmakten.se
1.1, 2.2, 3.1, 3.2, 3.4, 3.5, 3.6, 4.1	Anna-Karin Wetzig, Försvarsmakten	Försvarsmaktens bild
2.1, 3.7, 5.2	Hampus Hamberg, Försvarsmakten	Försvarsmaktens bild
2.3	Cecilia Nygren, Försvarsmakten	Försvarsmaktens bild
3.8	Daniel Sanchez, Försvarsmakten	Försvarsmaktens bild
3.3, 4.1, 5.1	Försvarsmakten	Försvarsmaktens bild

Källförteckning

Den här publikationen baseras på följande källor:

Dokumenttyp	Källor
Externt upprättade styrande dokument	-
Internt upprättade styrande dokument	• Militärstrategisk doktrin, MSD22, M7739-354028, gällande från och med 2022-07-01. • Doktrin för gemensamma operationer, DGO, M7739-354030, gällande från och med 2020-07-01. • Doktrintillägg Militärstrategisk kommunikation, DTLG MILSTRATKOM, M7739-350432, gällande från och med 2023-01-01.
Externt upprättade övriga dokument	• AJP-3.20 Edition A, Version 1, Allied Joint Doctrine For Cyberspace Operations. The Nato Standardization Office (NSO). 2020. • Cyber Commanders' Handbook. A. Dalmjin, V. Banse, L. Lumiste, J. Teixeira, A. Balci (Red.). NATO CCDCOE Publications. 2020. • Position Paper on the Application of International Law in Cyberspace. Government Offices of Sweden (Ministry for Foreign Affairs). 2022. • Sveriges cyberförsvar tar form – en struktur för fortsatt förmågeutveckling mot 2030. Kungliga Krigsvetenskapsakademiens Handlingar och Tidskrift (KKrVAHT) nr 1 2022, s 80–106. • Delar av doktrinansatsen innehåller AI-genererat innehåll. OpenAi. (2024). ChatGPT för IOS 1.2024.177 (9670299302) [Large language model].
Internt upprättade övriga dokument	-

Doktrinansats Cyberförsvar förklarar och förmedlar ett gemensamt förhållningssätt inklusive gemensamma begrepp för planering och genomförande av cyberförsvar.

Doktrinansatsen bidrar till att öka förståelsen för vad cyberdomänen är och hur cyberförsvaret leds. Även om doktrinansatsen inte är en formell del av Försvarsmaktens doktrin bör doktrinansatsens inriktningar och vägledningar ändå tillämpas. En doktrinansats ska främja diskussion om ämnet och utgöra underlag till beslut om hur området doktrinärt ska vidareutvecklas.

FÖRSVARSMAKTEN

107 85 Stockholm
www.forsvarsmakten.se

DA CYBER 2024
Versionsnr: 1.1