Försvarbarhet i cyberdomänen

En intervjustudie

William de Brun Mangs, Martin Karresand,
Frankie Johansson, Ralf Alvarsson

FOI-R--5854--SE

Juni 2026

FOI

William de Brun Mangs, Martin Karresand, Frankie Johansson, Ralf Alvarsson

Försvarbarhet i cyberdomänen

En intervjustudie

Titel	Försvarbarhet i cyberdomänen – En intervjustudie
Title	Defensibility in the Cyber Domain – An Interview Study
Rapportnr/Report no	FOI-R--5854--SE
Månad/Month	juni
Utgivningsår/Year	2026
Antal sidor/Pages	38
ISSN	1650-1942
Uppdragsgivare/Client	Försvarsmakten
Forskningsområde	Cyberförsvar och cybersäkerhet
FoT-område	Operationer i cyberdomänen
Projektnr/Project no	E38559
Godkänd av/Approved by	Foteini Papiri
Ansvarig avdelning	Cyberförsvar och ledningsteknik
Exportkontroll	Innehållet är granskat och omfattar ingen information som är underställd exportkontrollagstiftningen.

Bild/Cover	Gail Johnson (Shutterstock)

Sammanfattning

Denna studie undersöker egenskaper som påverkar försvarbarheten hos system och plattformar i cyberdomänen. Undersökningen är baserad på intervjuer med tio individer verksamma inom Försvarsmaktens cyberförsvar med expertkunskap inom defensiva cyberoperationer (DCO). Specifikt har de erfarenhet inom minst ett av verksamhetsområdena sensoranalys (SA), uppsökande verksamhet (UV), incidenthantering (IH) eller motåtgärder (MÅ).

Det insamlade intervjumaterialet har utvärderats genom en tematisk analysprocess, där respondenternas utsagor resulterade i fem övergripande teman. Dessa teman innefattar *systemdesign med försvarbarhetsmekanismer i fokus*, *terrängkännedom som förutsättning för aktivt försvar*, *beredning av defensiva cyberoperationer genom organisatorisk förståelse av försvarbarhet*, *anpassning av den militära kontexten för integrering av försvarbarhet i cyberdomänen* och *samverkan mellan statiska skydd och aktivt försvar*.

Studiens resultat beskriver detektionsrelaterade systemegenskaper som möjliggörande för DCO samt förhöjande av försvarbarheten hos system och plattformar i cyberdomänen. Vidare behöver kravställningsprocesser för system och plattformar i cyberdomänen anpassas för att tillhandahålla nödvändiga försvarsåtgärder och därmed skapa balans mellan statiska skydd och aktivt försvar. Slutligen påvisar resultaten ett behov av grundläggande kunskap om försvarbarhet på organisationsnivå för att säkerställa att operatörer förses med tillräckliga resurser vid defensiva cyberoperationer.

Nyckelord: Försvarbarhet, defensiva cyberoperationer, DCO, cyberdomän, cyberangrepp

Summary

This study investigates properties which affect the defensibility of systems and platforms in the cyber domain. The research comprised a qualitative interview study where ten individuals with connections to the Swedish Armed Forces cyber defense and expert knowledge in the area of Defensive Cyber Operations (DCO) were selected as respondents. More specifically, the interviewees had hands on experience in at least one of the following operational areas: Sensor Analysis (SA), Deployed Actions (UV), Incident Response (IH) or Internal Countermeasures (MÅ).

The collected data was evaluated through a thematic analysis, where the respondents' descriptions resulted in five overarching themes. The identified themes consist of *system design with focus on defensibility mechanisms*, *terrain knowledge as a prerequisite for active defense*, *preparing defensive cyber operations through organisational understanding of defensibility*, *adapting the military context to integrate defensibility in the cyber domain* and *interaction between static protection and active defense*.

The results of the study describe system attributes related to detection as enabling for DCO and enhancing for the defensibility of systems and platforms in the cyber domain. Furthermore, processes for requirement specifications of systems and platforms in the cyber domain must be adapted in order to provide the necessary defense measures and thus ensure balance between static protection and active defense. Lastly, the results indicate a need for organisational understanding of defensibility in order to provide operators with sufficient resources during DCO.

Keywords: Defensibility, defensive cyber operations, DCO, cyber domain, cyber attack

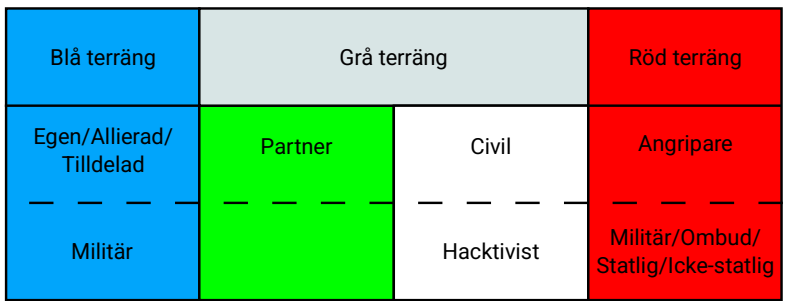
Innehåll

1 Inledning

Den snabbväxande cyberdomänen är i försvarssammanhang ny och därför relativt omogen, där angripare ständigt utvecklar nya och förfinar existerande taktiker, tekniker och procedurer (TTP). För att upprätthålla ett heltäckande skydd och minimera motståndarens förmåga att orsaka skada krävs att den defensiva sidans förmågor ständigt utvecklas och anpassas för att möta angriparens TTP:er.

Det är inte tillräckligt för den defensiva sidan att förlita sig på statiska skyddsåtgärder eftersom motståndaren gör kontinuerliga anpassningar för att kringgå skydden. Följaktligen är det viktigt att systemen och plattformarna även har förmågan att stödja ett aktivt och effektivt försvar i form av defensiva cyberoperationer (DCO). I *Cyber Commanders' Handbook 2* definieras DCO som ”Actions in or through cyberspace to preserve own and friendly freedom of action in cyberspace.” [1, s. 59].

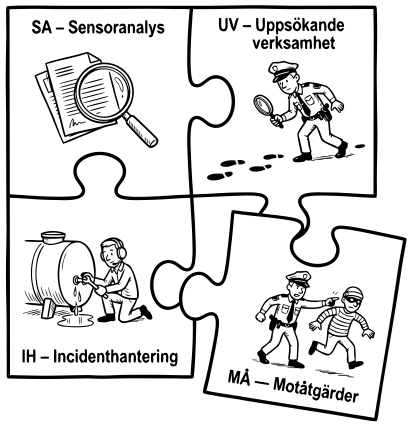
DCO utförs i vad som kallas *blå terräng*, vilket i *Cyber Commanders' Handbook 2* definieras som ”Own military/government/critical infrastructure, owned, operated and protected cyberspace vital to the mission” [1, s. 37]. Det finns totalt tre terrängtyper som sträcker sig över fyra aktörsområden. Dessa visas i figur 1. I den här studien behandlas endast blå terräng.



Figur 1: De tre terrängtyperna och deras förhållande till aktörsområdena som finns i cyberområdet. Bilden har tagit inspiration från *Cyber Commanders' Handbook 2* [1, fig. 3.3].

Enligt *Doktrinansats Cyberförsvar* nyttjas defensiva cyberoperationer i syfte att försvara Försvarsmaktens egna system och plattformar i cyberterrängen [2]. De

defensiva cyberoperationerna delas in i fyra operativa verksamhetsområden: sensoranalys (SA), uppsökande verksamhet (UV), incidenthantering (IH) och motåtgärder (MÅ) som visualiseras i figur 2 [2]. Det finns även stödjande verksamhetsområden, där terränganalys (TA) är av särskild vikt för studien. Huruvida dessa verksamheter kan fungera och prestera beror på en mängd organisatoriska och tekniska egenskaper relaterade till de system som DCO-verksamheten syftar till att försvara.



Figur 2: Visualisering av de fyra operativa verksamhetsområdena inom DCO. Bilden är genererad med *Shutterstocks* tjänst för AI-bildgenerering.

Begreppet *försvarbarhet* (engelska *defensibility*) utgör ett mått på hur väl ett systems egenskaper är anpassade för att möjliggöra aktivt försvar. En tidig användning av begreppet försvarbarhet har påträffats i masteruppsatsen ”Integrated Cyber Defenses: Towards Cyber Defense Doctrine” från 2007 av Cloud [3]. Trots att det är cirka 20 år sedan Cloud nämnde begreppet saknas fortfarande en generellt accepterad definition, vilket kan medföra variation i hur begreppet tolkas inom forskningsfältet. *Cyber Commanders' Handbook 2* definierar försvarbarhet som ”The ability of a given area of blue terrain to facilitate defensive actions” [1, s. 61].

Principerna för DCO är fortfarande under utveckling och mer forskning behövs därför inom området. I ”Defining, Measuring, and Analyzing Defensibility in The Defensive Cyber Operations Context” [4] föreslår Ekstorm användning av 66

parametrar[1] för att mäta försvarbarhet hos system. Parametrarna är dock inte praktiskt utvärderade och antalet kan behöva minskas för att göra det möjligt att använda dem i skarpa situationer.

Skydd (säkerhetsfunktioner) i ett IT-system utgörs av olika statiska och proaktiva åtgärder för att öka ett systems förmåga att stå emot intrång. Att utöka och förstärka systemets skydd benämns härdning av systemet, vilket är en förebyggande åtgärd. En användbar analogi är att betrakta systemets skydd som en borgs tjocka, höga och solida murar. Ju färre svagheter de har i form av hål, gluggar och fönster, desto bättre skydd ger de. En problematisk aspekt är att detta även hindrar försvararna från att övervaka och motverka angriparnas aktiviteter. Detta framhålls bland annat i *Försvarbarhet i cyberdomänen – En litteraturstudie*, vars resultat särskilt pekar ut härdning som negativt för försvarbarhet [5, s. 36].

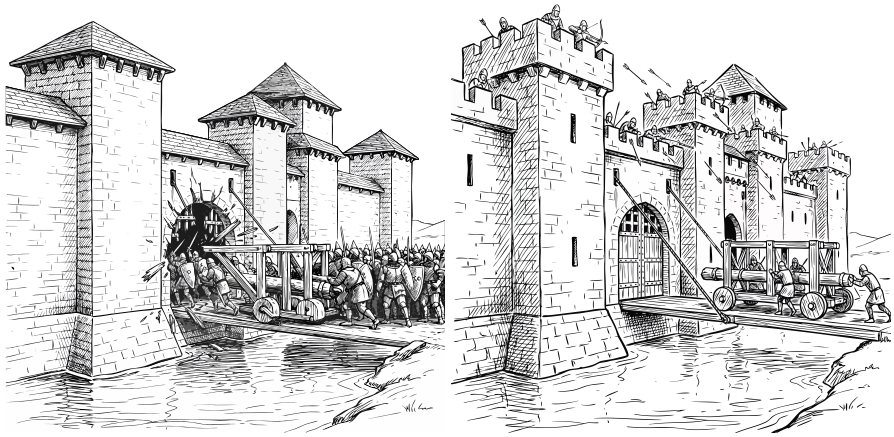
Försvarsåtgärder är, till skillnad från skyddsåtgärder, aktiva och tidsbegränsade och syftar till att avhysa angripare ur systemet. För att öka effekten av försvarsåtgärder kan system och plattformar förberedas med försvarbarhetshöjande åtgärder. Dessa åtgärder kan dock medföra att det statiska skyddet försvagas. För att återgå till analogin med borgar medför försvarbarhetshöjande åtgärder att murarna förses med gluggar och hål för att kunna spana, skjuta och hälla kokande olja på angriparna. Figur 3 skildrar vikten av att inte förlita sig enbart på skydd, utan att även integrera försvarbarhet som koncept. Med rätt balans mellan skyddsnivå och försvarbarhet ökar systemets motståndskraft mot angrepp, trots att det statiska skyddet har försvagats.

Tillgänglig forskning avseende försvarbara system och plattformar i cyberdomänen är i nuläget begränsad [5]. Den forskning som finns visar framför allt på vikten av detektion, det vill säga förmågan att se vad som händer i systemen. Den som besitter kunskap om både slagfältet och egna samt fientliga trupper, positioner och rörelser har en fördel framför motparten, vilket kallas informationsövertag.

Det finns dock flera närbesläktade initiativ som kan användas för att snabbare få fram ny kunskap inom området. Ett av initiativen är MITRE D3FEND, som utvecklas av MITRE[2]. MITRE D3FEND-ramverktet syftar till att bygga upp en

[1] Ekstorm [4, s. 64, tabell 3] presenterar i realiteten bara 65 parametrar, eftersom nummer 32 och 56 i listan är dubbletter. Deras svarsalternativ (mått) skiljer sig dock åt.

[2] `https://www.mitre.org/who-we-are`



(a) Låg försvarbarhet med enbart statiska skydd.

(b) Hög försvarbarhet med aktivt försvar, men försvagade statiska skydd.

Figur 3: Skildring av låg och hög försvarbarhet hos system. Bilderna är genererade med *Shutterstocks* tjänst för AI-bildgenerering.

kunskapsgraf av skydds- och försvarsmekanismer, där mekanismerna delas in i kategorierna *model*, *harden*, *detect*, *isolate*, *deceive*, *evict*, *restore* [6]. Varje kategori inkluderar ett flertal olika grupper av skydds- och försvarsmekanismer som i sin tur kan innefatta flera specifika mekanismer.

MITRE D3FEND används ofta som en minsta gemensamma nämnare när försvar av system och plattformar ska diskuteras. Exempelvis används MITRE D3FEND inom akademiska kretsar för att underlätta jämförelse av olika vetenskapliga resultat och upptäckter med bäring på cybersäkerhetsmässiga försvarsåtgärder. I denna studie nyttjas MITRE D3FEND i syfte att knyta identifierade egenskaper till ramverkets etablerade kategorier.

MITREs initiativ har sällskap av det ramverk som NICE[3] har utvecklat. NICE-ramverket tillhandahåller en beskrivning av nödvändiga roller och uppgifter inom cyberdomänen samt de färdigheter och den kunskap som varje roll kräver. Bland annat beskrivs rollen digital forensiker, vars uppgifter inkluderar inhämtning och analys av skadlig nätverkstrafik i syfte att identifiera avvikelser [7].

[3] `https://www.nist.gov/itl/applied-cybersecurity/nice/about`

Förmågan att motstå angrepp hos ett system är, precis som för borgar, beroende av samverkan mellan det statiska skyddet och de försvarsåtgärder som finns tillgängliga. För att uppnå största möjliga motståndskraft mot angrepp av ett system måste balansen mellan försvarbarhet och skydd optimeras. Hur detta ska gå till och kunna mätas är dock ännu inte utrett. Som ett komplement till *Försvarbarhet i cyberdomänen – En litteraturstudie* (FOI-R--5850--SE) [5], kommer denna studie att genom intervjuer undersöka vad ett antal experter inom DCO anser främjar och motverkar försvarbarheten hos system och plattformar i cyberdomänen.

Rapporten riktar sig till beslutsfattare, systemutvecklare, säkerhetsgranskare och andra som har behov av att veta mer om hur de som verkar inom området ser på de olika egenskaper som berör försvarbarhet i cyberdomänen. Studien är genomförd på beställning av Försvarsmakten och är anpassad till den militära kontexten som omfattar deras system och plattformar i cyberdomänen. Därmed bör studiens slutsatser tolkas från Försvarsmaktens perspektiv.

1.1 Syfte och mål

Syftet med föreliggande studie är att, baserat på expertkunskap från individer med erfarenhet av DCO, undersöka vilka egenskaper som kan påverka ett systems försvarbarhet samt vilka effekter dessa kan medföra. Vidare undersöks hur organisatoriska processer som exempelvis Krav på IT-säkerhetsförmågor hos IT-system (KSF)[4] påverkar försvarbarheten hos system och plattformar i cyberdomänen. Utöver detta berörs även frågeställningar kring förmågan att utföra framgångsrika defensiva cyberoperationer inom olika verksamhetsområden och vilka faktorer som påverkar detta, både positivt och negativt.

Studiens mål är att ge beslutsfattare och annan berörd personal mer kunskap om vad försvarbarhet i cyberdomänen är och hur den kan påverkas. Med tillgång till sådan kunskap kan de inkludera försvarbarhetsaspekter vid utveckling och

[4] ”KSF är de krav på IT-säkerhetsförmågor som militära underrättelse- och säkerhetstjänsten (MUST) tagit fram och som, enligt C MUST beslut, alla IT-system i Försvarsmakten måste uppfylla för att tillräckliga skyddsåtgärder ska anses föreligga. I detta perspektiv utgör KSF en del av MUST riskhantering avseende IT-säkerhetsförmågor för att reducera eller eliminera bedömda risker sett till IT-system.” [8, s. 4]

anskaffning av framtida system och plattformar inom Försvarsmakten. Målet är även att särskilt belysa de egenskaper som kan påverka förmågan att utföra DCO i syfte att kunna anpassa system och plattformar för detta på ett bättre sätt i framtiden. Vikt har även lagts vid hur DCO-förmågan påverkas inom de olika verksamhetsområdena.

1.2 Frågeställningar

De forskningsfrågor som har styrt arbetet som presenteras i den här rapporten är:

1. Vilka egenskaper i ett system eller en plattform i cyberdomänen är viktiga för att uppnå försvarbarhet?
2. Vad hindrar eller minskar försvarbarheten för ett system eller en plattform i cyberdomänen?
3. Vad möjliggör eller förstärker försvarbarheten för ett system eller en plattform i cyberdomänen?

Utifrån dessa forskningsfrågor har en intervjustudie utformats med frågor relaterade till defensiva cyberoperationer och försvarbarhet. Urvalet av respondenter har fokuserats på personer med erfarenhet inom DCO-området.

1.3 Avgränsningar

Studien är inriktad på den operativa sidan av försvarbarhet i cyberdomänen. Av den anledningen undersöks stödjande verksamheter endast till den utsträckning att behandla eventuella effekter på de operativa verksamhetsområdena SA, UV, IH och MÅ. Vidare har bara svenska förhållanden undersökts, vilket utelämnar eventuellt viktig internationell erfarenhet. Likaså baseras underlaget på tio intervjuer med experter inom olika områden av DCO, något som medför en risk för likriktning och missad information.

2 Metod

I denna studie har semistrukturerade intervjuer med sakkunniga inom området defensiva cyberoperationer genomförts i syfte att generera en ökad förståelse för hur försvarbarheten hos system och plattformar i cyberdomänen kan stärkas. Det insamlade materialet behandlades med hjälp av en tematisk analysprocess [9]. Kapitlet behandlar respektive metod för intervju och analys i separata avsnitt.

2.1 Intervju

Intervjuerna genomfördes i semistrukturerad form, vilket möjliggjorde att klargörande följdfrågor kunde ställas i de fall där respondenternas svar indikerade eventuella missförstånd. Ställda följdfrågor dokumenterades för att ge en tydligare förståelse av respondenternas svar och vinklingar.

Intervjufrågorna utformades med utgångspunkt i studiens forskningsfrågor. Ett initialt frågeutkast utvecklades och genomgick därefter en iterativ intern testprocess för att säkerställa relevans och tydlighet. Den slutgiltiga versionen av intervjufrågorna, som låg till grund för intervjuerna, presenteras i appendix A.

Respondenterna utgjordes av individer med anknytning till Försvarsmaktens cyberförsvar, expertkunskap inom DCO och betydande erfarenhet inom minst ett av områdena SA, UV, IH eller MÅ. Totalt intervjuades tio personer i 1,5 till 2 timmar vardera.

Intervjuerna genomfördes under perioden september till oktober 2025 och leddes av två personer, där den ena ansvarade för frågeställningen och den andra dokumenterade respondenternas svar och beskrivningar. Inför intervjutillfällena blev respondenterna ombedda att i förväg bekanta sig med ramverket MITRE D3FEND medan frågorna presenterades först under intervjun.

2.2 Analys

Detta avsnitt redogör för den metodologiska process som tillämpades vid analysen av det insamlade intervjumaterialet.

2.2.1 Teoretisk grund för analysmetod

Analysen av intervjuerna baserades på tematisk analys, där *Thematic Analysis – A Practical Guide* [9] av Braun och Clarke användes som inspiration. Tematisk analys bygger på att intervjuunderlaget i en iterativ process sammanställs och kategoriseras till teman som analytikern kan extrahera ur materialet. Processen kopplar hela tiden till de forskningsfrågor som styr undersökningen och är uppdelad i tre övergripande steg som kan repeteras inbördes innan nästa processteg. De tre stegen beskrivs enligt följande:

Familiarisering är det första steget i analysprocessen och kan beskrivas som en djupdykning i det insamlade materialet. Under familiariseringen bekantar sig analytikerna med materialet till den grad att de har allt i närminnet och intuitivt kan se mönster och kopplingar mellan respondenternas svar [9].

Kodning syftar till processen att komprimera sekvenser i det insamlade materialet till etiketter (koder) som beskriver innehållet i relation till studiens syfte och forskningsfrågor. Detta görs i iterationer där analytikerna vidare bekantar sig med materialet och koderna förfinas för att bättre gruppera respondenternas svar och beskrivningar [9].

Tematisering tar vid efter kodningssteget i analysprocessen och syftar till att ytterligare koncentrera det insamlade materialet. Under tematiseringen grupperas koder och slås samman till omfattande meningar som tydligt beskriver materialet. Processen utförs iterativt till dess att materialet har kondenserats och grupperats under ett fåtal övergripande kandidatteman. Dessa genomarbetas och förfinas därefter för att både representera materialets fulla innehåll och bibehålla relevans för studiens forskningsfrågor [9].

2.2.2 Praktisk tillämpning av analysmetod

Analysarbetet inleddes med familiarisering av det insamlade materialet, vilket innebar en genomläsning med enklare noteringar för att poängtera punkter av intresse. Familiariseringen genomfördes individuellt av samtliga deltagare i projektgruppen i syfte att varje deltagare skulle anskaffa en egen överblick av materialet.

Då en överblick av materialet var erhållen genomfördes en första kodning där respondenternas åsikter och reaktioner fångades i korta meningar. Den initiala kodningen genererade 782 koder som därefter systematiskt organiserades och raffinerades genom flera iterationer. Denna process genomfördes av en individ och resulterade i 32 kvarvarande koder.

De resulterande koderna användes som bas för tematiseringen, där koderna grupperades och samlades under övergripande kandidatteman. De initiala kandidattemana identifierades av samma individ som genomförde kodningen. Dessa teman diskuterades och justerades kollektivt inom projektgruppen i iterationer tills temana upplevdes sammanstråla med studiens forskningsfrågor. Vid processens slut hade fem teman identifierats.

3 Resultat

Detta kapitel presenterar de resultat som framkommit genom tematiseringen av intervjuerna. Resultaten beskriver identifierade teman som sammanställer intervjudeltagarnas åsikter och erfarenheter på en övergripande nivå.

Analysarbetet resulterade i fem stycken övergripande teman. Dessa är analytiskt sammanlänkade genom att de tillsammans synliggör olika organisatoriska och tekniska egenskaper som påverkar försvarbarheten hos system och plattformar i cyberdomänen. Varje tema fångar en specifik aspekt av respondenternas erfarenheter, samtidigt som temana tillsammans formar en helhetsbild av förutsättningarna för att öka försvarbarheten hos system och plattformar i cyberdomänen. De identifierade temana listas nedan.

- Systemdesign med försvarbarhetsmekanismer i fokus.
- Terrängkännedom som förutsättning för aktivt försvar.
- Beredning av defensiva cyberoperationer genom organisatorisk förståelse av försvarbarhet.
- Anpassning av den militära kontexten för integrering av försvarbarhet i cyberdomänen.
- Samverkan mellan statiskt skydd och aktivt försvar.

Varje tema presenteras i ett eget avsnitt, där resultatet beskrivs i detalj och sätts i sitt sammanhang. I anslutning till detta redogörs även för hur de identifierade temana härstammar från upptäckta mönster i respondenternas utsagor. Avslutningsvis beskrivs respondenternas rangordningar av MITRE D3FENDs kategorier i relation till försvarbarhet.

3.1 Systemdesign med försvarbarhetsmekanismer i fokus

Temat *systemdesign med försvarbarhetsmekanismer i fokus* ämnar att beskriva hur möjligheten att utföra aktivt försvar i ett system påverkas av hur systemet är uppbyggt, samt vilka verktyg och förmågor som tillhandahålls av systemet.

Framgång vid aktivt försvar har en stark omvänd korrelation till angriparens förmåga att orsaka skada i terrängen. Det är därför ytterst viktigt att försvararna lyckas avlägsna angriparen ur systemet inom ett rimligt tidsintervall, vilket underlättas om systemets egenskaper tillför nödvändig funktionalitet för operatörerna. Tabell 1 beskriver de mest framträdande systemegenskaperna i respondenternas utsagor.

Tabell 1: Sammanställning av systemegenskaper för aktivt försvar.

Egenskap	**Effekt**
Passiv inhämtning	Tillhandahåller forensisk data som kan nyttjas för detektion och spårning av eventuella angripare, vilket kan reducera tiden som krävs för att lokalisera och avlägsna angriparen.
Aktiv inhämtning	Möjligheten att utföra aktiv inhämtning bidrar med realtidsdetektion och en detaljerad överblick av systemens status.
Förberedda konton och anslutningspunkter	Direkt åtkomst till terrängen för operatörerna minimerar operationens startsträcka.

De egenskaper som sammanställs i tabell 1 bedömdes av respondenterna som viktiga, vilket motiveras av egenskapernas positiva inverkan på defensiva cyberoperationers startsträcka. Exempelvis kan passiv inhämtning bidra med forensiska spår av angriparen, vilket kan påskynda upptäckt och lokalisering av angriparen.

Analysen av intervjumaterialet visar att de systemegenskaper som stärker aktivt försvar i dagsläget är begränsade till favör för statiska skydd. Respondenterna uttrycker en önskan att systemdesign ska inkludera försvarbarhetsmekanismer i en större utsträckning.

3.2 Terrängkännedom som förutsättning för aktivt försvar

I detta avsnitt behandlas terrängkännedomens påverkan på försvarsoperatörernas förmåga att utföra DCO. Temat *terrängkännedom som förutsättning för aktivt försvar* belyser hur denna påverkan kommer till uttryck i respondenternas beskrivningar och resonemang.

Förmågan att utföra effektiva operationer i cyberdomänen kräver en väletablerad kunskap om terrängen där operationen ska genomföras. Detta då en välgrundad terrängkännedom bidrar till att öka synligheten i terrängen och därmed ge operatörerna en överblick av terrängens struktur och konfiguration.

Processen att anskaffa kännedom om terrängen benämns *terränganalys*. Analysprocessen kan vara tidskrävande i komplexa system, vilket ökar arbetsbelastningen på operatörerna. Verksamheten som ska försvaras bör därmed tillhandahålla information som på ett effektivt sätt ökar operatörernas förståelse om terrängen. Tabell 2 beskriver de mest framstående faktorerna som påverkar operatörernas terrängkännedom baserat på respondenternas beskrivningar.

Tabell 2: Sammanställning av bidragande faktorer till ökad terrängkännedom.

Faktor	Effekt
Systemdokumentation	Tillhandahåller information om systemets funktionalitet och uppbyggnad.
Systemkonfiguration	Tillhandahåller aktiv konfiguration för systemet.
Kommunikationsvägar till kunnig intern och extern personal	Skapar en direktväg för operatörerna att inhämta kunskap om målsystemet och eventuella tredjepartssystem på både teknisk- och verksamhetsnivå.

Samtliga faktorer listade i tabell 2 bör finnas tillgängliga innan försvarsoperatörerna anländer för att minimera tiden tills effektivt arbete kan påbörjas. Respondenternas utsagor visar dock att tillgången av dessa faktorer ofta är begränsad vid defensiva cyberoperationer.

3.3 Beredning av defensiva cyberoperationer genom organisatorisk förståelse av försvarbarhet

Ett centralt mönster i materialet avser hur förståelse av försvarbarhet på organisationsnivå påverkar processen att genomföra defensiva cyberoperationer. Detta avsnitt redogör hur respondenternas utsagor speglas i temat *beredning av defensiva cyberoperationer genom organisatorisk förståelse av försvarbarhet*.

Tidsaspekten är en kritisk faktor inom defensiva cyberoperationer. Följaktligen är det önskvärt om den lokala personalen inom verksamheten som ska försvaras bidrar maximalt för att underlätta operatörernas arbete. För att möjliggöra att den lokala personalen kan bidra i önskvärd utsträckning krävs en viss kunskapsnivå inom försvarbarhet och defensiva cyberoperationer. Respondenterna menar att de lokala förmågorna inte förväntas besitta tillräcklig kunskap för att på egen hand

genomföra en defensiv cyberoperation, men en grundläggande förståelse av försvarbarhet och DCO kan bidra med gynnsamma förutsättningar för operationen.

Kunskap om försvarbarhet och defensiva cyberoperationer behöver finnas i samtliga lager från beslutsfattande chefer till lokal personal i verksamheten som ska försvaras. Detta då höjd kunskap inom området bidrar till mer väletablerade operationsplaner och underlättar kommunikation av lägesbilden till operatörerna. Utökad förståelse om försvarbarhet inom organisationer bidrar även till en tydligare rollfördelning där mandat fördelas i enlighet med dess avsedda syfte. Tabell 3 beskriver respondenternas utsagor om organisatoriska förmågor som tillförs av utökad förståelse om försvarbarhet på organisationsnivå.

Tabell 3: Sammanställning av organisatoriska förmågor som bidrar till ökad försvarsförmåga.

Förmåga	**Effekt**
Tydlig roll- och mandatfördelning	Skapar tydliga riktlinjer om vilka uppgifter och mandat varje individ har. Motverkar tidskrävande anskaffningsprocesser av mandat.
Lokal DCO-kunskap	Påskyndar operationens effekt genom att inledande åtgärder utförs innan försvarsoperatörerna kopplas in.
Tydligt definierade operationsordrar	Motverkar tvetydighet under operationen och ger operatörerna en tydlig plan att arbeta efter.

Analysen av intervjuerna visar att det i dagsläget finns en generell brist på grundläggande kompetens vad gäller försvarbarhet inom organisationer. Utöver detta belyser analysen de förmågor som möjliggörs av en organisatorisk förståelse av försvarbarhet, där hinder för defensiva cyberoperationer undanröjs och ersätts av stärkande förmågor. Den centrala likheten mellan dessa organisatoriska förmågor är att de maximerar tiden som operatörerna kan spendera på sina huvudsakliga uppgifter. Exempelvis kan förmågorna reducera ledtiden från det att en möjlig ändring identifieras till dess att den påförs i systemet.

3.4 Anpassning av den militära kontexten för integrering av försvarbarhet i cyberdomänen

Temat *anpassning av den militära kontexten för integrering av försvarbarhet i cyberdomänen* beskriver identifierade mönster i respondenternas utsagor om hur Försvarsmaktens rutiner, regelverk och allmänna struktur påverkar försvarbarheten hos system och plattformar i cyberdomänen samt operatörers förmåga att genomföra DCO.

Under intervjuerna identifierades ett behov av att anpassa den militära kontexten i syfte att integrera konceptet försvarbarhet i cyberdomänen. Huvudsakligen beaktas inte behovet att utföra försvarsåtgärder som påverkar system och plattformars säkerhetsfunktionalitet. Exempelvis kan Försvarsmaktens aktiva regelverk kräva en full omackreditering av system när nödvändiga försvarsåtgärder har påförts, vilket kan hindra operatörerna från att påföra dessa ändringar då verksamheten värderar systemets tillgänglighet över dess säkerhet. Tabell 4 beskriver de mest frekventa militära faktorerna som påverkar operatörers förmåga att utföra försvar i cyberdomänen baserat på respondenternas beskrivningar.

Tabell 4: Sammanställning av militära faktorer som påverkar försvarbarhet i cyberdomänen.

Faktor	**Effekt**
Ackreditering av system och plattformar	Hindrar påförande av nödvändiga modifieringar i system.
Kravmassan i *KSF* [8]	Tillgodoser inte behovet av försvarbarhet i system och plattformar.
Bristfälliga processer vid anskaffning av mandat	Tidskrävande och kan hindra nödvändiga åtgärder från att påföras.

Analysen av det insamlade materialet indikerar att den militära kontexten inte

förser det aktiva försvaret med tillräckliga förutsättningar för att möjliggöra effektiva defensiva cyberoperationer. Respondenterna menar att KSF:en bidrar till en ökad förståelse av vad som kan förväntas av ett system men att försvarbarheten av systemet inte tas i åtanke. Utöver detta beskriver respondenterna att processen att anskaffa mandat ofta är otydlig och tidskrävande då det kan finnas osäkerhet om vem som besitter mandat att ta beslutet i fråga.

3.5 Samverkan mellan statiskt skydd och aktivt försvar

Säkerheten hos system och plattformar i cyberdomänen utformas av förebyggande skyddsåtgärder och möjligheten till att utföra aktivt försvar. Temat *samverkan mellan statiskt skydd och aktivt försvar* syftar till att redogöra respondenternas utsagor om hur skyddsåtgärder kan påverka det aktiva försvaret.

Statiska skydd syftar till åtgärder som kontinuerligt motverkar angripare i och runt målsystem, likt hur en vallgrav hindrar angripare från att nå borgen. Detta reducerar antalet angripare som behöver hanteras av det aktiva försvaret, vilket bidrar till en ökad försvarbarhet då systemets försvarsförmågor kan fokuseras på färre punkter.

Samtidigt som skydd genererar positiva effekter, kan de även tillföra negativ inverkan på försvarbarheten. Detta kan exemplifieras av att en brandvägg som hindrar angripares rörlighet i nätverket även begränsar försvararnas framkomlighet. Det är därför nödvändigt att analysera hur statiska skydd kan komma att påverka försvarbarheten och därefter värdera huruvida skyddet ses som fördelaktigt för systemets säkerhet. Tabell 5 presenterar respondenternas erfarenheter om skyddsåtgärder som upplevs hindra aktivt försvar vid defensiva cyberoperationer. I tabellen presenteras skyddsåtgärderna tillsammans med deras huvudsakliga positiva och negativa effekter på ett system eller plattforms försvarbarhet.

Tabell 5: Sammanställning av skyddsåtgärder och deras inverkan på försvarbarheten.

Skyddsåtgärd	**Positiv effekt**	**Negativ effekt**
Trafikkryptering	Motverkar avlyssning.	Hindrar upptäckt av antagonistisk trafik.
Luftgap	Reducerar attackytan.	Hindrar försvarares rörlighet mellan systemkomponenter.
Vitlistning av applikationer	Motverkar exekvering av skadlig kod.	Begränsar försvarares förmåga att påföra ändringar.
Segmentering	Reducerar attackytan.	Reducerar försvarares rörelseförmåga.
Brandväggar	Reducerar attackytan.	Reducerar försvarares rörelseförmåga.

Som illustreras i tabell 5 kan statiska skyddsåtgärder bidra med försvårande faktorer för angripare samtidigt som de introducerar begränsningar hos det aktiva försvarets förmågor. Det är därför viktigt att kravställningar innefattar både skydds- och försvarbarhetskrav för att säkerställa ett robust skydd som hindrar angripare från att ta sig in i systemet samtidigt som aktivt försvar möjliggörs. Analysen av respondenternas berättelser påvisar även att kravställningsprocesser, som exempelvis Försvarsmaktens ackrediteringsprocess, i dagsläget mer eller mindre saknar försvarbarhetsperspektiv. Dessa processer bör ses över för att tillhandahålla nödvändiga förutsättningar för aktivt försvar samtidigt som en godtagbar nivå av statiskt skydd kan upprätthållas.

3.6 Synlighet i system och plattformar

Ramverket MITRE D3FEND syftar till att öka försvarsförmågan hos system och plattformar i cyberdomänen genom att beskriva skydds- och försvarsmekanismer i en kunskapsmatris. För att undersöka ramverkets relevans inom defensiva cyberoperationer ombads respondenterna beskriva hur de ansåg att MITRE D3FEND kan anpassas till DCO ur ett konceptuellt perspektiv. Vid analys av respondenternas beskrivningar framgick det att frågan hade feltolkats. Respondenternas svar på frågan beskriver istället en rangordning av den översta nivån av kategorier i ramverket ur ett DCO-perspektiv. Eftersom detta ger insikter om vilka kategorier i ramverket som är viktigast vid defensiva cyberoperationer, baserat på respondenternas erfarenheter, behölls svaren och presenteras i tabell 6.

Tabell 6: Sammanställning av respondenternas svar på frågan: Hur kan de två översta kategorierna i MITRE D3FEND-ramverket anpassas till DCO-konceptet? Observera att de i praktiken rangordnade den översta nivån ur ett DCO-perspektiv. Skalan, som används för sammanställningen sträcker sig från 1 (lägst) till 7 (högst).

Givet svar	Median	Medelvärde	Min	Max
Detect	7	6.4	3	7
Model	6	5.8	4	7
Isolate	4.5	4.1	2	5
Evict	4	4	2	6
Deceive	1	1.9	1	4
Harden	3	3.33	2	5
Restore	2	2.79	1	6

Resultaten i tabell 6 visar en tydlig prioritering av kategorierna *detect* och *model*. Ur ett DCO-perspektiv kan detta tolkas som en önskan om hög synlighet för försvarssidan i system och plattformar, vilket i sin tur möjliggör övervakning och hantering av angripare.

4 Diskussion

I detta kapitel diskuteras den intervju- och analysmetod som har använts i studien. Vidare behandlas de organisatoriska och tekniska egenskaper som enligt studiens analys har inverkan på försvarbarheten hos system och plattformar i cyberdomänen. Avslutningsvis diskuteras studiens begränsningar.

4.1 Metod

Detta avsnitt behandlar de metoder som har använts i studien, däribland processen som användes vid tematiseringen samt några utvalda intervjufrågor som visade sig vara tvetydigt utformade.

4.1.1 Intervjuer

Resultaten i den här studien är främst baserade på analysen av respondenternas svar på intervjufrågorna (se appendix A). För att kunna redogöra för resultatens tillförlitlighet är det väsentligt att diskutera intervjufrågornas utformning samt de tekniker som intervjuarna har använt sig av.

En fallgrop med intervjustudier är att frågor feltolkas, vilket kan leda till uteblivna eller ovidkommande svar. I denna studie missuppfattades den nionde frågan (*Hur kan de två översta kategorierna i MITRE D3FEND-ramverket anpassas till DCO-konceptet?*). Respondenternas svar representerade en rangordning av MITRE D3FENDs kategorier ur ett DCO-perspektiv, snarare än hur kategorierna kan anpassas till DCO, vilket var vad som avsågs med frågan. Missuppfattningen kan bero på otydlighet i antingen utformningen av frågan eller hur den yttrades under intervjuerna. Ytterligare en möjlig orsak till feltolkningen är att tidigare ställda intervjufrågor innefattade frågor där respondenterna ombads rangordna faktorer som de ansåg påverka förmågan att utföra DCO, vilket även var en del av den nionde frågan.

Trots feltolkningen av den nionde frågan beslutades det att svaren skulle behållas då de ansågs tillföra viktig information om vilka kategorier som är närmast sammankopplade med DCO. Respondenternas rangordningar sammanställdes därför i tabell 6 där median, medelvärde och spridning användes för att visa deltagarnas graderingar av de olika kategorierna. En viktig sak att notera är att frågan stödjer resultaten från övriga intervjufrågor genom att peka ut de synlighetsrelaterade MITRE D3FEND-kategorierna *model* och *detect* som viktigast.

4.1.2 Tematisering

Respondenternas erfarenheter inom defensiva cyberoperationer och försvarbarhet analyserades genom tematisk analys, inspirerad av *Thematic Analysis – A Practical Guide* [9]. I boken belyser författarna att analytikerna kontinuerligt ska beakta forskningsfrågorna för att bibehålla analytiskt fokus. Följaktligen genomlästes studiens forskningsfrågor med jämna mellanrum under samtliga steg i tematiseringsarbetet. Det, tillsammans med det faktum att den inledande fasen i analysarbetet genomfördes i grupp, borgar för att det fortsatta arbetet fick en stadig grund att stå på.

Ett återkommande problem vid intervjustudier är att återge respondenternas svar korrekt i anteckningarna. Det är därför bra att spela in och transkribera alla intervjuer inför analysarbetet, vilket delvis gjordes även i denna studie. Materialet transkriberades dock först på begäran och efter en sekretessbedömning. Den processen visade sig vara mycket tidskrävande, vilket fick till följd att anteckningarna och de två intervjuarnas minnen av intervjuerna utgör det främsta materialet i tematiseringsprocessen. För att motverka bristen på detaljerat underlag diskuterades alla individuella tolkningar av respondentsvaren gemensamt tills konsensus nåddes.

4.2 Resultat

Analysen av det insamlade materialet visar att deltagarnas erfarenheter och beskrivningar kan förstås genom fem centrala teman, vilka tillsammans belyser hur försvarbarhet hos system och plattformar i cyberdomänen byggs upp. Avsnittet är uppdelat i delavsnitt som diskuterar försvarbarhetshöjande systemegenskaper samt förutsättningar och hinder för försvarbarhet i cyberdomänen.

4.2.1 Systemdesign med försvarbarhetsmekanismer i fokus

Temat *systemdesign med försvarbarhetsmekanismer i fokus* beskriver ett tydligt behov av att utöka verktygslådan som systemen och plattformarna tillhandahåller vid defensiva cyberoperationer. Behovet av utökade verktygslådor är en direkt konsekvens av att de tekniska förutsättningarna ofta är begränsade vid DCO. Detta tyder på en bristande prioritering av försvarbarhet vid utveckling av system och plattformar i cyberdomänen. Det kan finnas många orsaker till den bristande prioriteringen, till exempel okunskap, ekonomiska aspekter, tradition eller att systemutvecklingsområdet helt enkelt inte hängt med i den snabba utvecklingen. För att försvarssidan ska kunna ta in angriparnas försprång behöver orsakerna till den låga prioriteringen av försvarbarhet utredas ytterligare. Detta bör dock ses i ljuset av att försvarbarhet i cyberdomänen är ett relativt outforskat koncept, vilket medför att denna brist vanligtvis påträffas inom verksamheter i domänen, även i den privata sektorn.

Tabell 1 beskriver systemegenskaper som under intervjuerna frekvent nämndes som förmågehöjande vid DCO. Bland dessa egenskaper finns *passiv inhämtning*, vars effekter inkluderar förhöjd detektionsförmåga. Vikten av att detektera angripare styrks ytterligare av *Försvarbarhet i cyberdomänen – En litteraturstudie*, där detektionshöjande egenskaper framträder som de mest gynnsamma för försvarbarheten [5, s. 36]. Tabell 6 visar att detta är i linje med respondenternas rangordning av MITRE D3FEND-ramverkets kategorier, där *detect* värderades högst. Den här enigheten visar tydligt på en väg framåt, vilket är ett ljus i mörkret på systemutvecklingssidan. Dock kvarstår det faktum att en angripare kan dölja sig

på en mängd olika sätt, medan försvararna måste känna till och ständigt beakta samtliga strategier.

Ytterligare stöd för vikten av detektionsförmågor ges av arbetsuppgifterna som NICE-ramverket presenterar inom defensiv cybersäkerhet, incidenthantering och digital forensik. Dessa uppgifter omfattar bland annat identifiering av avvikande nätverkstrafik [7, 10, 11], vilket innebär att det bör finnas tekniska förutsättningar för att höja detektionsförmågan.

Passiv inhämtning i form av nätverksövervakning och detektion identifierades även i ”Defining, Measuring, and Analyzing Defensibility in The Defensive Cyber Operations Context” som en nödvändig förutsättning för system och plattformars försvarbarhet [4, s. 53, 71]. Det här visar på behovet och vikten av ett informationsövertag genom god kännedom om de egna systemen och en eventuell angripares förehavanden där.

Utan adekvata detektionsegenskaper ökar risken att angripare lyckas åstadkomma signifikant skada på systemet eller plattformen, vilket kan innebära katastrofala konsekvenser för verksamhetens konfidentialitet, integritet eller tillgänglighet. Verksamheter bör därför rikta sitt fokus på att implementera utökad funktionalitet för detektion av angripare i sina system och plattformar i cyberdomänen. Utan spaning, ingen aning, som devisen lyder.

4.2.2 Terrängkännedom som förutsättning för aktivt försvar

Genom temat *terrängkännedom som förutsättning för aktivt försvar* tydliggörs behovet av att operatörer bistås med tillräcklig terrängkännedom för att kunna genomföra effektiva defensiva cyberoperationer. Detta då en hög terrängkännedom ökar operatörernas insyn i de blå terrängområdena. Avsaknad av sådan insyn skulle innebära att de i praktiken famlar i blindo, vilket kan medföra att spår av angripare förbises eller tillgängliga verktyg inte nyttjas fullt ut. Detta kan vidare resultera i att angriparen kan röra sig fritt i systemet eller plattformen och orsaka ytterligare skada. Även här kommer informationsövertaget in som en viktig beståndsdel i försvarbarhetskonceptet.

Det bör noteras att terrängkännedom är tätt sammankopplat med insyn, men att egenskaperna trots allt skiljer sig åt. Det förra avser kunskap om systemets konfiguration och uppbyggnad, på samma sätt som en planritning av en medeltida borg eller en karta ger viktig kunskap om stridens omgivning. Terrängen är relativt statisk i sin utformning, även om moderna digitala system kan konfigureras om på ett ögonblick. Insyn däremot är mer dynamisk till sin natur och möjliggör kontinuerlig uppdatering av lägesbilden, vilket kan liknas vid att ha god sikt i strid, utan skylande rök och dimma.

Behovet av insyn i och kunskap om terrängen stärks ytterligare av resultaten i tabell 6 där MITRE D3FEND kategorin *model* tillskrivs en framträdande betydelse ur ett DCO-perspektiv. Model har en tydlig koppling till terrängkännedom och insyn, vilket innebär att vikten av informationsövertag ännu en gång har påvisats.

Studiens analys pekar på att verksamheter ska förbereda information om terrängen på ett sådant sätt att DCO-operatörer har möjligheten att få en överblick av hur terrängen är uppbyggd och konfigurerad, vilka segment som är prioriterade och hur systemens funktion kan tänkas bli påverkat av ändringar i terrängen. I synnerhet bör verksamheter säkerställa tillgång till maskinläslig systemdokumentation och -konfiguration samt kommunikationsvägar mellan operatörer och systemkunnig personal vid defensiva cyberoperationer. Det här är dock inte lätt och ställer stora krav på att systemdokumentationen är korrekt och uppdaterad, ett arbete som förmodligen många gånger ses som mindre viktigt jämfört med det operativa arbetet. Nyttan av bra förberedelser brukar dock visa sig när läget blir skarpt.

4.2.3 Beredning av defensiva cyberoperationer genom organisatorisk förståelse av försvarbarhet

Den begränsade forskningen om försvarbarhet i cyberdomänen medför att kunskapen om begreppets innebörd ännu inte har utvecklats i någon större utsträckning utanför DCO-sfären. Denna kunskapsbrist hindrar verksamheter från att förbereda sina system och plattformar i tillräcklig utsträckning för att underlätta defensiva cyberoperationer. Även bristen på en generellt accepterad definition av försvarbarhet utgör ett hinder i utvecklingen genom att inte tillåta de

inblandade parterna att ha en gemensam måttstock för vad som behövs och ska uppnås i form av förmåga och funktion i systemen som ska försvaras. Det är därför viktigt att snabbt formulera en definition som kan accepteras av alla berörda inom försvarbarhetsområdet.

I det analytiska arbetet identifierades temat *beredning av defensiva cyberoperationer genom organisatorisk förståelse av försvarbarhet* som tydliggör behovet av grundläggande kunskap om DCO i samtliga led inom organisationer. Exempelvis kan en defensiv cyberoperation bli effektiviserad av grundläggande förståelse av försvarbarhet inom verksamheten som ska skyddas. Detta då verksamheten kan förbereda tydligare information om terrängen samt vid behov utföra inledande basala steg i operationen.

Det insamlade materialet indikerar att kunskapsnivån om försvarbarhet ofta är låg inom verksamheterna som operationen avser att skydda. Operatörerna tvingas således spendera omfattande arbetsinsatser åt att beskriva situationen för verksamheten i stället för att rikta uppmärksamhet på försvar av verksamheten, vilket i sin tur medför ytterligare möjligheter för angriparen att röra sig fritt i terrängen. Det är därmed nödvändigt att organisationer säkerställer en adekvat kunskapsnivå om försvarbarhet i cyberdomänen för att underlätta, eller åtminstone inte hindra defensiva cyberoperationer.

4.2.4 Anpassning av den militära kontexten för integrering av försvarbarhet i cyberdomänen

Att den militära kontexten behöver anpassas för att integrera försvarbarhet i cyberdomänen exemplifieras av att Försvarsmaktens processer för ackreditering och kravställning av system och plattformar i cyberdomänen inte beaktar försvarbarheten på ett adekvat sätt. Detta kan hindra försvarsoperatörerna från att påföra nödvändiga ändringar då ett systems ackreditering riskerar att brytas. Vidare kan operatörerna tvingas söka efter alternativa strategier för att uppnå önskat resultat då de inte alltid har mandat att påföra en ändring som bryter ett systems ackreditering. Detta kan öka kostnaden (arbetsinsatsen) för DCO och ge angripare tid att orsaka ytterligare skada i terrängen. Behovet att anpassa kravställning och ackrediteringsprocesser i syfte att integrera försvarbarhet i

cyberdomänen påverkar samtliga aktörer i domänen och är en direkt konsekvens av att försvarbarhet i cyberdomänen är ett relativt nytt koncept.

För att tillgodose nödvändiga förutsättningar för aktivt försvar i cyberdomänen behöver den militära kontexten anpassas på ett sådant sätt att cyberförsvarets adaptiva förmåga inte hindras av tidskrävande beslutskedjor. Även KSF:en bör uppdateras med försvarbarhetskrav, för att säkerställa tillgången till nödvändiga försvarsåtgärder vid defensiva cyberoperationer. Förflyttningar och andra åtgärder går i många fall blixtsnabbt i cyberdomänen, vilket ställer mycket högre krav på snabb ordergång. I motsats till den fysiska världen finns det sällan tid för användning av traditionella beslutskedjor, utan beslut måste fattas omedelbart.

4.2.5 Samverkan mellan statiskt skydd och aktivt försvar

Temat *samverkan mellan statiskt skydd och aktivt försvar* belyser vikten av att statiskt skydd och aktivt försvar tillsammans bygger upp säkerheten hos system och plattformar. Det är därmed nödvändigt att kravställare förstår den ömsesidiga påverkan som skydds- och försvarsåtgärder utövar på varandra för att uppnå en god balans. Resultaten i avsnitt 3.5 beskriver respondenternas upplevelser med kravställningsprocesser, vilka visar visar att nödvändiga försvarbarhetsaspekter inte beaktas i tillräcklig utsträckning. Detta pekar tydligt på att förmågan att genomföra defensiva cyberoperationer påverkas negativt av att kravställningsprocesser i dagsläget saknar ett försvarbarhetsperspektiv. Det bristande fokuset på försvarbarhet i kravställningsprocesser genomsyrar aktörer över hela cyberdomänen, både i den privata och offentliga sektorn. Detta behöver åtgärdas snarast i och med att de system som utvecklas nu kommer att användas i årtionden framåt.

Ett starkt fokus på statiska skyddsåtgärder på bekostnad av försvarbarheten kan i förlängning orsaka överdrivet härdade system och plattformar, vilket i sin tur kan resultera i att försvaret riskerar att bli oförmögna att hantera angriparen på ett adekvat sätt. Av liknande skäl bör inte försvarbarheten prioriteras på ett sätt som leder till betydande brister i det statiska skyddet. Den ömsesidiga negativa påverkan mellan försvarbarheten och det statiska skyddet tydliggörs ytterligare av resultaten i *Försvarbarhet i cyberdomänen – En litteraturstudie*, vilka visar att

åtgärder som härdning och isolering kan orsaka en minskning av försvarbarheten [5, s. 36]. För att säkerställa system och plattformars säkerhet och motståndskraft i cyberdomänen behöver statiskt skydd samverka med aktivt försvar utan att de i någon större utsträckning hindrar varandra. Det är därmed nödvändigt att vidare forskning bedrivs i syfte att konkretisera hur och av vad försvarbarheten hos system och plattformar i cyberdomänen påverkas. Detta för att möjliggöra integrering av konkreta försvarbarhetshöjande egenskaper, snarare än att huvudsakligen fokusera på statiskt skydd. Det är därför viktigt att närmare studera balansen mellan skydd och försvarbarhet, med målet att kunna optimera de båda egenskapernas inverkan på systemets totala säkerhet.

4.3 Studiens begränsningar

Under intervjuerna visade sig fråga 9 vara öppen för feltolkningar[5]. I och med att frågan tolkades likartat fel av respondenterna korrigerades den inte, utan behölls i sin ursprungliga utformning vartefter intervjuerna fortskred. Den efterföljande analysen av frågan visade trots det på intressanta resultat, men feltolkningarna var begränsande och resulterade i att eftersökta svar uteblev.

Försvarbarhet hos system och plattformar i cyberdomänen är ett relativt outforskat område, vilket medför att stöd för studiens resultat är begränsade. Därmed bör denna studie och dess resultat ses som en ansats till att undersöka vilka organisatoriska och tekniska egenskaper som har positiv respektive negativ inverkan på system och plattformars försvarbarhet inom cyberdomänen.

[5] Den feltolkade frågan lyder: Hur kan de två översta kategorierna i MITRE D3FEND-ramverket anpassas till DCO-konceptet?

5 Slutsats

Denna studie utgör en inledande ansats till att undersöka vilka organisatoriska och tekniska egenskaper som påverkar försvarbarheten hos system och plattformar i cyberdomänen. Studiens slutsatser bör därför betraktas som ett underlag för framtida forskning.

Syftet med denna studie var att undersöka hur försvarbarheten hos system och plattformar i cyberdomänen kan påverkas. Genom en tematisk analysprocess har fem centrala teman identifierats och anpassats till studiens frågeställningar. I detta kapitel sammanfattas studiens resultat i relation till forskningsfrågorna, där varje frågeställning presenteras i ett separat avsnitt. Avslutningsvis presenteras förslag på framtida forskning inom området försvarbarhet i cyberdomänen.

5.1 Vilka egenskaper i ett system eller en plattform i cyberdomänen är viktiga för att uppnå försvarbarhet?

Analysen av det insamlade intervjumaterialet identifierade egenskaper som bidrar till ökad detektion- och övervakningsförmåga som mest framstående för att uppnå en hög försvarbarhetsnivå i system och plattformar i cyberdomänen. Av dessa egenskaper åsyftas främst passiv inhämtning av data, där respondenternas utsagor var synnerligt fokuserade på logghanteringssystem och analys av nätverkstrafik. Detta stämmer väl överens med *Försvarbarhet i cyberdomänen – En litteraturstudie* [5], där författarna beskriver skydds- och försvarslösningar inom detektionsområdet som egenskaper som ökar försvarbarheten.

Materialet beskriver även möjligheten att aktivt inhämta data genom exempelvis nätverksskanning som en viktig egenskap för att uppnå försvarbarhet. Vidare beskrivs tillgång till förberedda konton och anslutningspunkter som förstärkande egenskaper.

5.2 Vad hindrar eller minskar försvarbarheten för ett system eller en plattform i cyberdomänen?

Förmågan att utföra aktivt försvar av system och plattformar begränsas främst till följd av att försvarsåtgärder inte ges tillräcklig prioritet. Istället tilldelas statiska skyddsåtgärder ofta en högre prioritet vid kravställningar av system och plattformar, i synnerhet i den militära kontexten. Respondenternas beskrivningar av KSF:en och Försvarsmaktens ackrediteringsprocess visar att endast skyddsåtgärder beaktas. Huruvida aktivt försvar hindras av dessa skyddsåtgärder beaktas alltså inte vid kravställning av system och plattformar inom Försvarsmakten. Sammantaget indikerar detta att den militära kontexten behöver anpassas för att ge det aktiva försvaret rätt förutsättningar. Vidare bör statiska skydd och försvarsförberedande åtgärder ställas mot varandra för att hitta en balans mellan statisk säkerhet och förmågan att utföra aktivt försvar.

5.3 Vad möjliggör eller förstärker försvarbarheten för ett system eller en plattform i cyberdomänen?

Operatörers möjlighet att försvara system och plattformar i cyberdomänen är i hög grad beroende på de förutsättningar som tillhandahålls inför operationen.

En kritisk förutsättning vid defensiva cyberoperationer är kunskap om terrängen där operationen ska genomföras. Därmed kan faktorer som underlättar terränganalys betraktas som möjliggörande för system och plattformars ökade försvarbarhet. Resultaten indikerar att tillgång till dokumentation och aktiv konfiguration av systemet eller plattformen är två framstående faktorer som bidrar till en effektiv terränganalys. Vidare kan etablerade kommunikationsvägar till kunnig personal som kan beskriva terrängen och dess komponenter betraktas som en förstärkande faktor då terrängkännedom anskaffas. Möjligheten att tillhandahålla denna information och säkerställa gynnsamma förutsättningar är beroende av kunskap om defensiva cyberoperationer och försvarbarhet på

organisationsnivå. Exempelvis kan relevant kunskap hos beslutsfattande chefer bidra med tydligare operationsplaner och effektivare processer för anskaffning av mandat. Samtidigt kan höjd kunskap om defensiva cyberoperationer och försvarbarhet hos personal inom verksamheten som ska försvaras skapa starkare lokala förmågor som kan tillföra systemdokumentation av högre kvalitet samt tillåta genomförande av enklare inledande steg i operationen.

Sammanfattningsvis kan organisatorisk förståelse av försvarbarhet skapa förmågor som kan tillhandahålla gynnsamma förutsättningar vid defensiva cyberoperationer och bidra till ökad försvarbarhet hos system och plattformar i cyberdomänen.

5.4 Framtida forskning

Försvarbarhet hos system och plattformar i cyberdomänen är ett relativt nytt begrepp som ännu inte fått en tydlig definition. Framtida studier bör därmed fokusera på att beskriva en global definition av begreppet i syfte att möjliggöra mätning av försvarbarheten.

En möjlig väg för att vidare undersöka mätning av försvarbarhet är att genomföra praktiska övningar där förutsättningarna varierar. Dessa förutsättningar kan inkludera olika systemegenskaper och organisatoriska förmågor, vilka med fördel kan utformas från de parametrar som Ekstorm beskriver i ”Defining, Measuring, and Analyzing Defensibility in The Defensive Cyber Operations Context” [4].

Referenser

[1] F. Hickey, B. Magurno, S. Pastor, N. Rodrigues och D. Štrucl, utg. *Cyber Commanders' Handbook 2*. NATO Cooperative Cyber Defence Centre of Excellence, 2025.

[2] Försvarsmakten. *Doktrinansats Cyberförsvar*. 1.1. 2024.

[3] D. Cloud. "Integrated Cyber Defenses: Towards Cyber Defense Doctrine". Masteruppsats. Naval Postgraduate School, Monterey, Kalifornien, USA, 2007.

[4] B. Ekstorm. "Defining, Measuring, and Analyzing Defensibility in The Defensive Cyber Operations Context". Masteruppsats. Naval Postgraduate School, Monterey, Kalifornien, USA, 2022-06.

[5] H. Karlzén, H. Holm och M. Karresand. *Försvarbarhet i cyberdomänen – En litteraturstudie*. FOI-R--5850--SE. Totalförsvarets forskningsinstitut (FOI), 2025.

[6] MITRE. *About the D3FEND Knowledge Graph Project*. URL: `https://d3fend.mitre.org/about/` (hämtad 2025-12-05).

[7] NICCS. *Digital Forensics*. URL: `https://niccs.cisa.gov/tools/nice-framework/work-role/digital-forensics` (hämtad 2025-12-05).

[8] Försvarsmakten. *KSF - Krav på IT-säkerhetsförmågor hos IT-system*. 3.1. FM2014-5302:1. 2014. (Hämtad 2025-11-19).

[9] V. Braun och V. Clarke. *Thematic Analysis – A Practical Guide*. SAGE Publication Ltd, 2022.

[10] NICCS. *Defensive Cybersecurity*. URL: `https://niccs.cisa.gov/tools/nice-framework/work-role/defensive-cybersecurity` (hämtad 2025-12-05).

[11] NICCS. *Incident Response*. URL: `https://niccs.cisa.gov/tools/nice-framework/work-role/incident-response` (hämtad 2025-12-05).

A Intervjuguide

1. Berätta kort om din erfarenhet av defensiva cyberoperationer?
2. Hur många år har du arbetat med defensiva cyberoperationer?
3. Beskriv de generella mönster vad gäller nödvändiga variabler (attribut) du uppmärksammat i de defensiva cyberoperationerna du utfört?
    a) Kan du beskriva en typisk defensiv cyberoperation?
4. Hur vet du om en DCO-insats varit framgångsrik eller inte?
    a) Vilka är de tydligaste/bästa markörerna?
    b) Varför valde du dessa? Redogör gärna för var och en?
5. Vilka variabler (attribut) påverkar förmågan till DCO i system?
    a) Rangordna dem om möjligt.
    b) Hur kom du fram till rangordningen?
    c) Vilka av de nämnda egenskaperna är möjliggörande (skall finnas), respektive förstärkande (bör finnas)?
    d) Vilka kompetenser/roller är möjliggörande (skall finnas), respektive förstärkande (bör finnas) hos den personal du interagerar med vid DCO?
    e) Är det skillnad på kraven vad gäller nära kollegor (intern personal) och övrig (extern) personal?
6. Vilka cybersäkerhetsåtgärder/funktioner påverkar förmågan till DCO negativt respektive positivt vid:
    a) SA? Går de att rangordna?
    b) UV? Går de att rangordna?
    c) IH? Går de att rangordna?
    d) MÅ? Går de att rangordna?

7. Vilka behov av försvarsåtgärder och systemstöd finns vid DCO för:
    a) SA? Går de att rangordna?
    b) UV? Går de att rangordna?
    c) IH? Går de att rangordna?
    d) MÅ? Går de att rangordna?
8. Vilka avtal/regelverk/policyer påverkar förmågan till DCO negativt respektive positivt?
    a) Vilka specifika delar är mest relevanta i ditt tidigare svar?
9. Hur kan de två översta kategorierna i MITRE D3FEND-ramverket (https://d3fend.mitre.org/) anpassas till DCO-konceptet?
    a) Rangordna kategorierna på båda nivåerna om möjligt.
    b) Hur kom du fram till rangordningen?
10. Vilka artefakter har störst påverkan på förmågan att utföra effektiva defensiva cyberoperationer?
    a) Varför valde du dessa?
11. Vilken typ av hotaktör tänkte du på när du svarade på dessa frågor?
12. På vilka sätt påverkar hotaktören insatsen/operationen?
13. Vad behöver göras på en hög nivå för att öka förmågan att utföra framgångsrika DCO-insatser på kort och lång sikt (*t ex tydligare krav, uppgraderade system, en standardiserad verktygslåda, nya (AI) verktyg*)?
    a) Vad bör FOI fokusera på av detta?
14. Vad ska en övning för att öka förmågan till DCO innehålla?
    a) Vad ska terrängen/cybermiljön ha för egenskaper/utseende?
    b) Ska övningen vara styrd, eller öppen (t ex två lag mot varandra)?
    c) Om du tänker helt fritt, hur skulle en övning i DCO se ut?

FOI

ISSN 1650-1942

www.foi.se