Analys av koncept och teknik för cyberförsvar och informationssäkerhet

Slutrapport

Jerry Falkcrona

FOI-R--5834--SE

December 2025

Jerry Falkcrona

Analys av koncept och teknik för cyberförsvar och informationssäkerhet

Slutrapport

Titel	Analys av koncept och teknik för cyberförsvar och informationssäkerhet – Slutrapport
Title	Analysis of concepts and technology for cyber defence and information security – Final report
Rapportnr/Report no	FOI-R--5834--SE
Månad/Month	December
Utgivningsår/Year	2025
Antal sidor/Pages	20
ISSN	1650-1942
Uppdragsgivare/Client	Försvarsmakten
Forskningsområde	Cyberförsvar och cybersäkerhet
FoT-område	Operationer i cyberdomänen
Projektnr/Project no	E38556
Godkänd av/Approved by	Emil Hjalmarson
Ansvarig avdelning	Cyberförsvar och ledningsteknik

Bild/Cover: Shutterstock

Sammanfattning

Denna rapport beskriver det arbete som genomförts inom ramen för FoT-projektet *Analys av koncept och teknik för cyberförsvar och informationssäkerhet*, åren 2021–2025. Projektet har bedrivits som ett antal fristående studier och har utvärderat tekniker och metoder för att stärka säkerheten i it-system. Rapporten sammanfattar resultatet från dessa studier och beskriver den övriga verksamhet som genomförts inom projektet.

Nyckelord: cybersäkerhet, informationssäkerhet, mjukvarusäkerhet

Summary

This report describes the work that has been done within the FoT project *Analys av koncept och teknik för cyberförsvar och informationssäkerhet* (Analysis of concepts and technology for cyber defence and information security) during 2021–2025. The project has been conducted as a number of separate studies and has evaluated technologies and methods for strenghtening the security in IT systems. The report summarizes the results of these studies and describes the other activities performed within the project.

Keywords: cybersecurity, information security, software security

Innehållsförteckning

1 Inledning

Försvarsmakten använder en stor mängd olika it-system. Att upprätthålla säkerheten i it-systemen, som kan se väldigt olika ut, är en stor utmaning.

Denna rapport ger en övergripande beskrivning av de studier och annan verksamhet som genomförts inom projektet *Analys av koncept och teknik för cyberförsvar och informationssäkerhet* som ingår i Försvarsmaktens samlingsbeställning inom forskning och teknikutveckling (FoT). Projektet har utvärderat tekniker och metoder för att stärka säkerheten i IT-system. De tekniker och metoder som studerats omfattar såväl tekniska lösningar som tekniknära sociotekniska aspekter, däribland hantering av IT-system. Därtill har projektet utvärderat hur de studerade teknikerna och metoderna kan nyttjas inom Försvarsmakten. FoT-planen beskriver följande frågeställningar för projektet:

- Vilka nya cyberförsvarsrelaterade koncept och tekniker har bäring på Försvarsmaktens förmåga att genomföra myndighetsförvaltning och operationer?
- Hur kan identifierade koncept och tekniker nyttjas inom Försvarsmakten?

Projektet har bedrivits under fem år (2021–2025) och har genomförts som ett antal fristående studier. Projektet har inte fokuserat på ett specifikt område, vilket innebär att det inte alltid finns en tydlig röd tråd mellan studierna. I stället har projektet omfattat studier inom en större bredd av områden.

Denna rapport inleder med en beskrivning av de studier som genomförts inom projektet (kapitel 2). Därefter beskrivs det arbete som projektet bedrivit för kunskapsspridning i form av en årlig seminariedag (kapitel 3). Rapporten fortsätter sedan med att beskriva det arbete som genomförts inom en Nato-arbetsgrupp (kapitel 4). Sedan följer en diskussion kring projektets arbete (kapitel 5). Avslutningsvis presenteras förslag på framtida forskning (kapitel 6). Bilaga A listar de rapporter, memon och akademiska forskningsartiklar som projektet producerat.

2 Studieverksamhet

Detta kapitel beskriver den studieverksamhet som genomförts inom projektet. Studierna är grupperade i ett antal områden som beskrivs i separata avsnitt.

2.1 Hantering av cyberintrång

Detta avsnitt beskriver de studier som relaterar till att upptäcka eller hantera intrång i datornätverk. De ämnen som behandlas inom området är honungsfällor (eng. honeypots) och dataexfiltration.

Rapporten *Honungsfällor - Att vilseleda och studera cyberangripare* (Karlzén, 2021) beskriver en introduktion till honungsfällor och definierar honungsfällor enligt följande:

”En honungsfälla är en cybersäkerhetsfunktion som med hjälp av vilseledning lockar till sig angripare och får dem att stanna kvar, varpå ägarens IT-system förskonas från angrepp samtidigt som lärdomar för framtiden kan dras om angreppen.” (Karlzén, 2021).

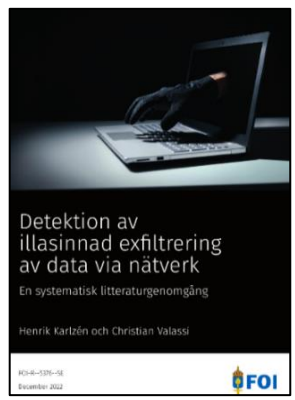
Studien är en genomgång av främst akademiska forskningsartiklar och undersöker de typer och taxonomier som används för att beskriva honungsfällor. Studien finner att det inte finns en vedertagen kategorisering av honungsfällor för att sedan presentera ett försök till en sammanställning och gruppering av de olika kategorierna av honungsfällor som identifierats.

Rapporten beskriver att honungsfällor kan nyttjas för att studera angripare och de tekniker som angripare använder. På detta sätt skulle honungsfällor kunna användas av Försvarsmakten för att vilseleda motståndare, eller potentiellt för underrättelseinhämtning.

Rapporten *Dynamiska honungsnätverk – Utmaningar och teknik för sömlös överflyttning av angrepp* (Bildsten m.fl., 2021) beskriver hur honungsfällor kan efterlikna en produktionsmiljö genom att samordna flera honungsfällor i ett honungsnätverk. Studien fokuserar på hur en angripare kan flyttas sömlöst från en produktionsmiljö till en honungsfälla utan att angriparen upptäcker det.

Inom studien tas en konceptlösning fram, där en virtuell maskin i drift kopieras och en aktiv TCP-anslutning förflyttas till den nya kopian av maskinen (läs: honungsfällan). Den anslutning som förflyttas simulerar en angripare som fått fotfäste i en server. Konceptlösningen utvärderas sedan genom att mäta den tid som anslutningen inte kan användas för att skicka eller ta emot trafik på grund av förflyttningen till honungsfällan. Mätningarna genomförs för ett antal olika fall med varierande mängd primärminne för den virtuella maskinen, vilket är den huvudsakliga faktorn som avgör hur lång tid kopieringen tar.

Mer information om ett angrepp kan potentiellt samlas in genom att förflytta aktiva angrepp till en honungsfälla istället för att direkt stänga ute angriparen vid upptäckt.



Rapporten *Detektion av illasinnad exfiltrering av data via nätverk – En systematisk litteraturgenomgång* (Karlzén & Valassi, 2022) beskriver en litteraturstudie över artiklar som publicerats under perioden 2012–2022. Studien identifierar 42 artiklar som beskriver olika tekniker för att upptäcka när en angripare överför information via nätverk från ett målsystem till ett system kontrollerat av angriparen.

Studien beskriver hur angripare kan använda olika tekniker för att dölja att exfiltration av data sker. Vanliga sätt att dölja exfiltrationen är att gömma information i protokoll som vanligtvis inte används för överföring av information, till exempel protokollet DNS som syftar till att översätta domännamn till IP-adresser. Studien beskriver att vanliga tekniker för att upptäcka exfiltration är att studera entropi, trafikflöden eller tidsaspekter hos nätverkstrafiken. Rapportens resultat visar att mycket av forskningen genomförs i nätverk som inte nödvändigtvis överensstämmer med verkligheten, så som universitetsnät och labbmiljöer. Rapporten menar även att det saknas diversitet i

vilka typer av nätverksprotokoll som studeras och efterfrågar mer detaljer i hur detektionsmetoderna realiserats.

Detektion av exfiltrering skulle potentiellt kunna användas som en indikator för att initiera en förflyttning av en angripare till en honungsfälla.

2.2 Mjukvarusäkerhet

Mjukvarusäkerhet är ett stort område och projektet valde att fokusera på mjukvarusårbarheter och hur de kan förebyggas. Mjukvarusårbarheter förekommer i stort sett i all mjukvara, trots att det bedrivits forskning inom området i årtionden. Målet med projektets arbete inom området var att undersöka vanliga orsaker till att mjukvarusårbarheter uppstår som ett steg i att kunna identifiera lämpliga åtgärder för att undvika dem.

Rapporten *Varför har mjukvaror sårbarheter?* (Karlzén m.fl., 2023) beskriver en litteraturstudie som fokuserar på vad forskningen identifierat som orsaker till att mjukvarusårbarheter uppstår och varför de inte upptäcks av testare och mjukvaruutvecklare. Studien visar att det finns många bakomliggande aspekter kopplat till detta: osäkra programmeringsspråk, bristande säkerhetskompetens och motivation hos mjukvaruutvecklare, organisatoriska faktorer och bristfälliga verktyg.

Resultatet av studien visar att det behövs fortsatt forskning inom området och pekar på ett antal relevanta områden: organisation och utvecklare, programmeringsspråk och verktyg samt sårbarhetsupptäckt.

Projektet valde att gå vidare inom området organisation och utvecklare i efterföljande studie, viken beskrivs nedan.

Rapporten *Mjukvarors säkerhet beror på utvecklarnas motivationer och hinder – En enkätundersökning* (Karlzén m.fl., 2024) beskriver en enkätundersökning som skickades ut till mjukvaruutvecklare verksamma på myndigheter och företag. Enkätdeltagarna arbetade med mjukvara inom samhällskritisk verksamhet och fick svara på frågor om motivationsfaktorer och vad som ansågs vara främjande eller hindrande kopplat till arbete med mjukvarusäkerhet.

Resultatet av studien visar på att utvecklarnas egen motivation, som i förlängningen beror av individens ansvarstagande och medvetenhet, är det som är viktigast för att prioritera arbete med mjukvarusäkerhet. Studien identifierar även att karriärrelaterade faktorer och monetära belöningar inte främjar utvecklares motivation och inställningar kopplat till arbete med mjukvarusäkerhet. De största hindren som identifierades i studien var brist på konsekvenser för utvecklare när mjukvarusårbarheter identifierats samt bristande konkurrens, vilket leder till att organisationen inte behöver lägga energi på mjukvarusäkerhet eftersom kunderna inte har några, eller få, alternativ.

Rapporten *Mjukvarusårbarheter och skyddstekniker – Analys av Pythonmjukvara* (Jensen m.fl., 2025) beskriver en studie som undersöker de vanligaste sårbarheterna och skyddsteknikerna för programmeringsspråket Python och Pythonmjukvara. Studien har valt att undersöka programmeringsspråket Python för att det är ett populärt språk bland utvecklare. Studien presenterar även en taxonomi för skyddstekniker och undersöker hur skyddsteknikerna relaterar till olika typer av sårbarheter.

Resultatet visar på att de vanligast förekommande sårbarheterna är olika typer av bristande hantering av indata. Även sårbarheter kopplade till otillräcklig hantering av autentisering och åtkomstkontroll är vanligt förekommande. Studiens resultat beskriver att indatavalidering är den vanligast förekommande skyddstekniken, vilket kan anses rimligt då den används för att hantera sårbarheter kopplade till hantering av indata.

2.3 Säkerhetsevidens

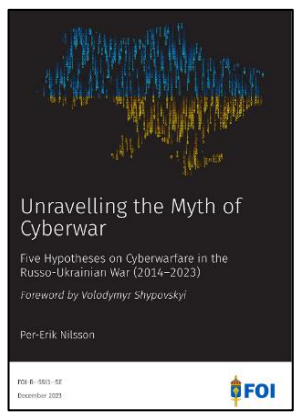
Projektet genomförde en initial studie inom området säkerhetsevidens. Säkerhetsevidens är en del av det arbete som genomförs för att kunna utveckla system som kan godkännas för att hantera säkerhetsskyddsklassad information.

Rapporten *Säkerhetsevidens för IT-system – En inledande studie om bevisföring för systematisk säkerhet* (Eidenskog & Vestlund, 2024) beskriver en studie som undersöker hur evidens används i olika säkerhetsstandarder och processer. Evidens är den bevisföring som används för att påvisa att ett system uppfyller de säkerhetskrav som ställs på systemet och att det således uppnår en tillräcklig säkerhetsnivå. Tilltron till att ett system uppnår en tillräcklig säkerhetsnivå brukar även kallas assurans.

Studien visar att de standarder och processer som undersökts är generellt beskrivna och saknar detaljer om vilka uppgifter som egentligen behöver genomföras. Studien identifierar även att underlaget bara ytligt beskriver hur evidens skall värderas och hanteras. Därtill föreslår rapporten att vidare forskning behövs inom området.

2.4 Säkerhetspolitik

Under 2023 genomförde projektet en studie inom forskningsområdet säkerhetspolitik. Vidare arbete inom området säkerhetspolitik följde sedan under ett eget FoT-projekt.



Rapporten *Unravelling the Myth of Cyberwar – Five Hypotheses on Cyberwarfare in the Russo-Ukrainian War (2014–2023)* (Nilsson, 2023) beskriver en studie som undersöker de bakomliggande anledningarna till att Rysslands cyberkrigföring mot Ukraina inte åstadkommit den effekt som många befarade. Studien har genomförts som en litteraturstudie och har inkluderat publikationer från bland annat akademiska databaser, nyhetsmedier och olika forskningsinstitut. Resultatet av studien presenterar ett antal tänkbara orsaker till den bristande effekten av cyberangreppen. Nedan följer några av de potentiella orsakerna som beskrivs:

- Ukraina har lärt sig att försvara sig, då de under många år behövt värja sig mot cyberangrepp från Ryssland.

- Ukrainas motoffensiv i cyberdomänen mot Ryssland kan ha påverkat Rysslands förmåga till cyberangrepp.
- Internationellt stöd kan ha hjälpt Ukraina att förbereda sig samt skydda sig mot cyberangrepp.

Vidare konstaterar studien att kriget mellan Ryssland och Ukraina visar på hur viktig cyberkrigföring är i moderna konflikter.

3 Seminarieverksamhet

Projektet har tillsammans med Försvarsmakten årligen planerat och genomfört seminariedagen IT-försvarsdagen. Syftet med IT-försvarsdagen är att sprida kunskap inom området cybersäkerhet och cyberförsvar till målgruppen myndigheter och samhällsviktiga verksamheter. IT-försvarsdagen har under de senaste åren anordnats digitalt och åhörarna har deltagit via strömmad video. Genom att strömma innehållet har det varit möjligt att låta fler åhörare delta. Till IT-försvarsdagen 2024 var det över 800 anmälda, vilket är mångdubbelt fler än vid de fysiska evenemang som anordnades till och med 2019. Alla deltagare har under presentationerna haft möjlighet att via en chatt kunna ställa frågor till talarna.

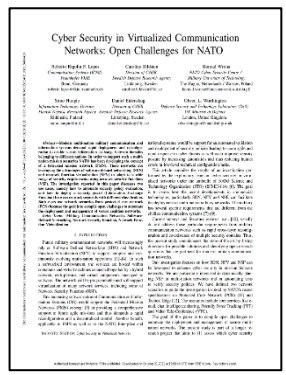
IT-försvarsdagen har under projektets gång haft talare från en rad olika myndigheter och organisationer:

- Cybercampus Sverige
- Försvarets materielverk (FMV)
- Försvarshögskolan (FHS)
- Försvarsmakten
- Kungliga Tekniska högskolan (KTH)
- Linköpings universitet
- Netnod
- Nationellt cybersäkerhetscenter (NCSC)
- Nationellt samordningscenter för forskning och innovation inom cybersäkerhet (NCC-SE)
- Nato Cooperative Cyber Defence Centre of Excellence (CCDCOE)
- Totalförsvarets forskningsinstitut (FOI).

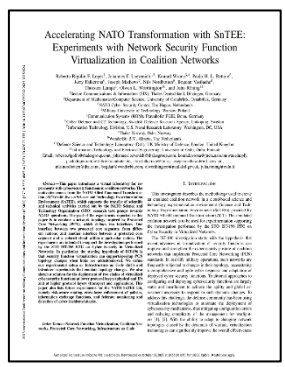
Projektet har under de senaste två åren även tillgängliggjort flera av de strömmade föredragen på FOI:s Youtube-kanal för att främja en vidare spridning av kunskap.

4 Arbete inom Nato-forskningsgrupp

Projektet deltar i Nato-forskningsgruppen IST-196 som behandlar säkerhet i virtualiserade miljöer. Huvudsyftet med deltagandet är att utbyta erfarenhet inom området. Arbetet inom forskningsgruppen sker genom regelbundna möten där deltagarna kommer överens om vilka arbetsuppgifter som skall genomföras inför kommande mötestillfällen. Nato-gruppen har publicerat tre forskningsartiklar som inkluderar författare från projektet. Forskningsartiklarna presenteras kort nedan.

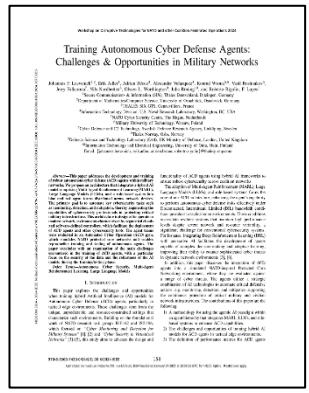

Cyber Security in Virtualized Communication Networks: Open Challenges for NATO

Artikeln *Cyber Security in Virtualized Communication Networks: Open Challenges for NATO* (Lopes m.fl., 2022) undersöker hur mjukvarubaserade tekniker kan användas för att realisera säkerhetsfunktioner i koalitionsnätverk. Ett koalitionsnätverk består av nätverk från flera olika nationer som kopplas samman för att utbyta information. Teknikerna mjukvarudefinierade nätverk (eng. software defined networking, SDN) och virtualiserade nätverksfunktioner (eng. network function virtualization, NFV) används för att kunna driftsätta nätverksbaserade säkerhetsfunktioner (eng. network security functions, NSF) dynamiskt i ett nätverk. Genom att använda mjukvarubaserade tekniker kan nätverket anpassas dynamiskt efter de förändringar som ofta sker i militära nätverk. Artikeln publicerades i samband med konferensen 2021 International Conference on Military Communication and Information Systems (ICMCIS).


Accelerating NATO Transformation with SnTEE: Experiments with Network Security Function Virtualization in Coalition Networks

Artikeln *Accelerating NATO Transformation with SnTEE: Experiments with Network Security Function Virtualization in Coalition Networks* (Lopes m.fl., 2023) beskriver hur ett emulerat koalitionsnätverk kan realiseras med hjälp av molnteknik. Ett koalitionsnätverk består av nätverk från flera olika nationer som kopplas samman för att utbyta information. Artikeln beskriver hur ett nätverk av typen *protected core networking* (PCN) kan emuleras. PCN är en nätverkstopologi som används inom Nato. Syftet med det emulerade koalitionsnätverket är att kunna experimentera med virtuella nätverksfunktioner i en PCN-miljö. Artikeln publicerades i samband med konferensen 2023 International Conference on Military Communications and Information Systems (ICMCIS).

Artikeln *Training Autonomous Cyber Defense Agents: Challenges & Opportunities in Military Networks* (Loevenich, m.fl. 2024) undersöker vilka utmaningar som finns för att utveckla och träna automatiserade agenter för cyberförsvar i militära nätverk. Agenterna syftar till att automatisera delar av monitorering och detektion av cyberattacker, samt att genomföra viss mitigering. Artikeln beskriver en arkitektur för agenterna som bygger på multi-agent reinforcement learning, anpassad för att realiseras i mjukvarudefinierade nätverk. Artikeln publicerades i samband med konferensen 2024 IEEE Military Communications Conference (MILCOM).



Training Autonomous Cyber Defense Agents:
Challenges & Opportunities in Military Networks

5 Diskussion

Detta kapitel sammanfattar hur det arbete som projektet genomfört relaterar till projektets frågeställningar beskrivna i FoT-planen.

De två övergripande frågorna som tas upp i FoT-planen är följande (se även kapitel 1):

- Vilka nya cyberförsvarsrelaterade koncept och tekniker har bäring på Försvarsmaktens förmåga att genomföra myndighetsförvaltning och operationer?
- Hur kan identifierade koncept och tekniker nyttjas inom Försvarsmakten?

Även om projektet inte fullständigt har utforskat den första frågans potentiella översikt över nya koncept och tekniker av intresse för Försvarsmakten, så har projektet studerat ett antal relevanta områden. Dessa utgör ett brett spektrum av olika tekniker och metoder för att höja säkerhetsnivån i it-system och mjukvara. De tekniknära undersökningarna inkluderar tekniker för att skapa honungsfällor, att upptäcka exfiltrering av data och att skapa säkerhet i virtualiserade miljöer. Därtill har projektet undersökt de mer mjuka aspekterna kring varför mjukvara får sårbarheter samt vilka drivkrafter utvecklarna har för arbete med mjukvarusäkerhet. Dessutom har projektet genomfört en första studie inom evidens för mjukvarusäkerhet, det vill säga hur bevisföring för säkerhetsnivån i systemen kan byggas upp. Projektet har också genomfört en säkerhetspolitisk undersökning kring cyberangreppens (och därmed mjukvarusäkerhetens) roll i en krigssituation. Alla dessa områden har relevans för Försvarsmaktens förmåga att upprätthålla pålitliga och säkra it-system. I den utsträckning det går har också frågan om hur resultaten kan nyttjas inom Försvarsmakten besvarats i respektive rapport. Tabell 1 beskriver de områden som studerats under projektets gång och som bedömts vara viktigast för Försvarsmakten.

Tabell 1 De viktigaste områdena för Försvarsmakten: urval från studieverksamhet.

Område	**Varför är det viktigt för Försvarsmakten?**
Mjukvarusäkerhet	Det finns idag ingen lösning för att helt undvika mjukvarusårbarheter. Genom att bättre förstå varför, och hur, sårbarheter uppstår kan framtida system göras säkrare.
Säkerhetsevidens	Säkerhetsevidens kan bidra till en bättre förståelse av och högre tilltro till ett systems säkerhetsegenskaper.

Ett sätt som resultaten redan nyttjats är genom de presentationer som getts i samband med de IT-försvarsdagar som genomförts under projektet. I detta forum har resultaten kunnat delges brett till såväl deltagare från Försvarsmakten som deltagare från de många andra aktörer som sett sändningarna.

6 Framtida forskning

Mjukvarusårbarheter har förekommit i princip lika länge som mjukvara har funnits och det finns idag ingen lösning för att helt undvika dem. Det är ett stort forskningsområde som har många olika aspekter; från faktorer såsom motivation, utvecklingsmetoder och processer, till verktyg och programmeringsspråk. De senaste årens utveckling inom maskininlärning gör att det finns stora möjligheter att utforska hur maskininlärning kan användas för att förbättra verktyg och programmeringsspråk ur ett mjukvarusårbarhetsperspektiv. Vidare finns det inom mjukvaruutveckling vedertagna bäst praxis, vilka om de följs, sägs ge upphov till bättre mjukvarusäkerhet. Det är dock i många fall oklart hur dessa bäst praxis uppstått och evidensen är bristande för huruvida de är korrekta, eller vilken effekt de egentligen har. Ett framtida forskningsprojekt som undersöker bäst praxis kan ge insikt i hur de bör användas.

Säkerhetsevidens är en viktig del i den bevisföring som krävs för att säkerställa att de säkerhetsmål som är uppsatta för ett system uppfylls. De processer och standarder som finns inom området saknar detaljer om vilka uppgifter som behöver tas fram och hur de ska värderas. Vidare studier kan ge en bättre förståelse för hur arbetet med säkerhetsevidens kan göras tydligare och effektivare. Det finns även inom området säkerhetsevidens möjligheter att undersöka hur maskininlärning kan användas för att underlätta arbetet med att påvisa assurans.

Bilaga A. Publikationslista

Rapporter

Bildsten, C., Falkcrona, J., & Eidenskog, D. (2021). *Dynamiska honungsnätverk – Utmaningar och teknik för sömlös överflyttning av angrepp*. FOI-R--5216--SE. Totalförsvarets forskningsinstitut.

Eidenskog, D., & Vestlund, C. (2024). *Säkerhetsevidens för IT-system – En inledande studie om bevisföring för systematisk säkerhet*. FOI-R--5686--SE. Totalförsvarets forskningsinstitut.

Jensen, C., Ekman, D., Karlzén, H., Eidenskog, D., & Falkcrona, J. (2025). *Mjukvarusårbarheter och skyddstekniker – Analys av Pythonmjukvara*. FOI-R--5829--SE. Totalförsvarets forskningsinstitut.

Karlzén, H. (2021). *Honungsfällor – Att vilseleda och studera cyberangripare*. FOI-R--5217--SE. Totalförsvarets forskningsinstitut.

Karlzén, H., Eidenskog, D., Falkcrona, J., & Valassi, C. (2023). *Varför har mjukvaror sårbarheter?* FOI-R--5550--SE. Totalförsvarets forskningsinstitut.

Karlzén, H., Falkcrona, J., Eidenskog, D., & Karresand, M. (2024). *Mjukvarors säkerhet beror på utvecklarnas motivationer och hinder – En enkätundersökning*. FOI-R--5691--SE. Totalförsvarets forskningsinstitut.

Karlzén, H., & Valassi, C. (2022). *Detektion av illasinnad exfiltrering av data via nätverk – En systematisk litteraturgenomgång*. FOI-R--5376--SE. Totalförsvarets forskningsinstitut.

Nilsson, P.E. (2023). *Unravelling the Myth of Cyberwar – Five Hypotheses on Cyberwarfare in the Russo-Ukrainian War (2014-2023)*. FOI-R--5513--SE. Totalförsvarets forskningsinstitut.

Memon

Bildsten, C. (2021). *Planerade studier AKTCI 2021*. FOI Memo 7543. Totalförsvarets forskningsinstitut.

Bildsten, C. (2021). *Analys av koncept och teknik för cyberförsvar och informationssäkerhet – verksamhetsår 2021*. FOI Memo 7714. Totalförsvarets forskningsinstitut.

Falkcrona, J. (2022). *Analys av koncept och teknik för cyberförsvar och informationssäkerhet – Planerade studier för 2022*. FOI Memo 7886. Totalförsvarets forskningsinstitut.

Falkcrona, J. (2022). *Analys av koncept och teknik för cyberförsvar och informationssäkerhet verksamhetsår 2022*. FOI Memo 7992. Totalförsvarets forskningsinstitut.

Falkcrona, J. (2024). *Analys av koncept och teknik för cyberförsvar och informationssäkerhet verksamhetsår 2024*. FOI Memo 8667. Totalförsvarets forskningsinstitut.

Falkcrona, J. (2025). *Analys av koncept och teknik för cyberförsvar och informationssäkerhet – Planerade studier för 2025*. FOI Memo 8816. Totalförsvarets forskningsinstitut.

Falkcrona, J. (2025). *Analys av koncept och teknik för cyberförsvar och informationssäkerhet verksamhetsår 2025*. FOI Memo 9021. Totalförsvarets forskningsinstitut.

Falkcrona, J., & Vendil Pallin, C. (2023). *Analys av koncept och teknik för cyberförsvar och informationssäkerhet – Planerade studier för 2023*. FOI Memo 8113. Totalförsvarets forskningsinstitut.

Falkcrona, J., & Vendil Pallin, C. (2023). *Analys av koncept och teknik för cyberförsvar och informationssäkerhet verksamhetsår 2023*. FOI Memo 8346. Totalförsvarets forskningsinstitut.

Falkcrona, J., & Vendil Pallin, C. (2024). *Analys av koncept och teknik för cyberförsvar och informationssäkerhet – Planerade studier för 2024*. FOI Memo 8453. Totalförsvarets forskningsinstitut.

Vetenskapliga publikationer

Loevenich, J. F., Adler, E., Bécue, A., Velazquez, A., Wrona, K., Boshnakov, V., Falkcrona, J., Nordbotten, N., Worthington, O. L., Röning, J., & Lopes, R. R. F. (2024). *Training Autonomous Cyber Defense Agents: Challenges & Opportunities in Military Networks*. MILCOM 2024 - 2024 IEEE Military Communications Conference (MILCOM). (FOI-S--6936--SE).

Lopes, R. R. F., Bildsten, C., Wrona, K., Huopio, S., Eidenskog, D., & Worthington, O. L. (2021). *Cyber Security in Virtualized Communication Networks: Open Challenges for NATO*. 2021 International Conference on Military Communication and Information Systems (ICMCIS). (FOI-S--6413--SE).

Lopes, R. R. F., Loevenich, J. F., Wrona, K., Rettore, P. H. L., Falkcrona, J., Mathews, J., Nordbotten, N., Vasilache, B., Worthington, O. L., & Röning, J. (2023). *Accelerating NATO Transformation with SnTEE: Experiments with Network Security Function Virtualization in Coalition Networks*. 2023 International Conference on Military Communications and Information Systems (ICMCIS). (FOI-S--6682--SE).

ISSN 1650-1942