CRATE

Cyber Range And Training Environment

Nyhetsbrev Informationssäkerhet nr 2, 2026

Välkommen till vårt nyhetsbrev från enheterna *Cybersäkerhet*, *Förmågor i cyberdomänen* och *Cyberanläggningsteknik* som ingår i verksamhetsområde Cyber. Vi har försökt samla ihop de utskick vi gör i olika sammanhang från vårt verksamhetsområde till ett gemensamt nyhetsbrev som planeras att komma ut några gånger per år. Vi hoppas att du hittar något intressant att fördjupa dig i här, men skulle du känna att det här var helt fel så finns det en länk längst ner på sidan där du kan avregistrera dig från framtida utskick.

I det här nyhetsbrevet skriver vi om:

- Publika data som riskfaktor - En förstudie
- Försvarbarhet i cyberdomänen - litteratur- och intervjustudie
- CEMA - koncept för cyber- och elektromagnetiska aktiviteter
- Cyberrymd på riktigt - två domäner i ett
- Mythos - Är ryktena om cybersäkerhetens död överdrivna?
- Civila tekniktrender med relevans för cyberförsvar
- Stärkt nationellt cyberförsvar genom gemensamma övningar
- Crate-CTF - En tävling i cybersäkerhet - anmälan öppnar 1 september!
- *Save the date* - IT-försvarsdagen genomförs den 3 december
- "FOI ger stöd till att förbättra Sveriges cyberförsvar, **foi.se/cyber**
- FOI växer och söker nya kollegor! **FOI:s lediga tjänster!**
- Rapportsamling - för er som är speciellt intresserade av Informationssäkerhet

Kontakta oss

Har du frågor om vårt nyhetsbrev - kontakta:
Gunilla Friberg

gunilla.friberg@foi.se

Publikationer

FOI publicerar rapporter där de flesta är tillgängliga i elektronisk form via

www.foi.se

Våra kurser 2026

Elektronisk säkerhet:
Följande kurstillfälle är nu öppna för anmälan:
v40 2026 fullbokat
v20 och v40 2027
Vi erbjuder även anpassade kurser och utbildningar baserade på vår breda kompetens.

Kurser och utbildningar
Här finner du kursbeskrivningar och anmälningsformulär till vårt övriga kursutbud.

Publika data som riskfaktor - En förstudie om påverkan på informationssäkerhet och säkerhetsskydd

Rapport av Daniel Eidenskog och Christian Vestlund

Med ökad generell hotbild mot Sverige blir även underrättelsehotet mer påtagligt. Den stora mängden publikt tillgängliga data kan om de kombineras potentiellt leda till information som påverkar skyddet av säkerhetskänslig verksamhet. Genom moderna analysmetoder kan stora mängder data av olika typ kombineras för att dra slutsatser som inte explicit uttrycks i ursprungliga data. Detta ger problem med exempelvis sekretess- och riskbedömningar inför publicering av öppna data eller offentliga handlingar. Denna rapport presenterar en förstudie med ett första steg mot att förstå vilka risker för sekretess och säkerhetsskydd som kan uppstå ur antagonisters möjligheter att nyttja publika data i underrättelsesammanhang. Det långsiktiga målet är att bidra med kunskap som behövs för att kunna göra genomarbetade och välförankrade sekretess- och riskbedömningar, som även hanterar de problem som uppstår genom publika data. Förstudien är av explorativ natur och ger en översikt över underrättelsearbete, källor till publika data samt metoder för bearbetning och analys av insamlade data. Rapporten diskuterar även ett antal ytterligare områden och perspektiv som behöver hanteras i framtida forskning, såsom datamängdernas omfattning,

tekniker för komplexa analyser, riskbedömningsmetodik, kompetensbehov, etik och juridik.
Läs hela rapporten

Försvarbarhet i cyberdomänen - En litteraturstudie

Rapport av Henrik Karlzén, Hannes Holm och Martin Karresand
Den här rapporten sammanställer forskningslitteratur om skydds- och försvarslösningar som kan påverka förutsättningarna för försvar (försvarbarheten) i cyberdomänen. Rapporten ger en första inblick i det relativt nya begreppet försvarbarhet, genom att bedöma hur forskarnas lösningar förhåller sig till försvarbarhet. Eftersom det finns extremt stora mängder skydds- och försvarslösningar görs här en begränsning till lösningar som använder terminologin i Mitres D3fendramverk. Den allra mesta inkluderade forskningslitteraturen fokuserar på ramverkets taktik benämnd detektion. Den forskningen rör främst nätverkstrafikanalys (77 % av artiklarna), men också användarbeteendeanalys (7 %), filanalys (6 %) med flera. De allra flesta artiklarna (85 %) presenterar lösningar som bedömds underlätta försvarbarheten. Även de flesta av dessa är fokuserade på detektion. De lösningar som tvärtom försvårar försvarbarheten rör mestadels isolering men också härdning, kompletterat med detektion och vilseledning. Försvarbarhet verkar alltså underlättas av främst detektion, men försvåras av flera olika taktiker. Det talar också för att detektion i huvudsak ökar försvarbarheten, medan arkitektoniska förändringar som härdning och isolering mer troligt minskar försvarbarheten. Artiklarna själva diskuterar inte lösningarnas påverkan på försvarbarheten. Anledningen till de uteblivna diskussionerna tyder på att de som föreslår tekniska lösningar inte brukar beakta försvararens roll. En del av artiklarna nämner dock människan och främst då hur lösningarna kan ge visualisering av loggar. För att bedöma hur applicerbara forskarnas lösningar är i praktiken gör rapporten också bedömningar av lösningarnas mognad och kvalitet samt vilken typ av indata de använder för utvärdering och framförallt om det är data från verkligheten. De allra flesta lösningar som forskningen producerat är på sin höjd prototyper i labbmiljö (TRL 3-4). Enbart 16 % av alla artiklar bedömdes vara av hög kvalitet. Av de studerade 198 artiklarna bedriver 192 någon typ av datainsamling. Det finns bara 29 artiklar (15 %) som använder publika dataset med data från riktiga system.
Läs hela rapporten

Försvarbarhet i cyberdomänen - En intervjustudie

Rapport av Martin Karresand, William De Brun Mangs, Ralf Alvarsson och Frankie Johansson
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.
Läs hela rapporten

CEMA - ett koncept för cyber- och elektromagnetiska aktiviteter

Memo av Henrik Karlzén
Projektet Omvärldsanalys av koncept och teknik för cyberförsvar kartlägger kunskap som kan ha relevans för cyberförsvaret. Här görs en preliminär analys av konceptet cyber- och elektromagnetiska aktiviteter (CEMA).
Läs Memo här

Cyberrymd på riktigt - två domäner i ett

Memo av Henrik Karlzén och Viktor Bergström
Projektet Omvärldsanalys av koncept och teknik för cyberförsvar kartlägger civil kunskap som kan ha relevans för cyberförsvaret. Detta memo ger en preliminär analys av rymdens förhållande till cyberförsvar.
Läs Memo här

Mythos - Är ryktena om cybersäkerhetens död överdrivna?

Memo av Viktor Bergström och John Ziegenbein
Anthropic beskriver sin nya språkmodell Mythos som så kapabel att hitta sårbarheter att den inte bör släppas fritt till allmänheten. Detta memo granskar publicerad information om Mythos i syfte att skilja fakta från marknadsföring. Slutsatsen är att Mythos i sig inte är avgörande för cyberförsvaret, men att språkmodellers förmågor att hitta sårbarheter utvecklas snabbt just nu och lär utgöra ett allt kraftfullare verktyg med tiden.
Läs Memo här

Civila tekniktrender med relevans för cyberförsvar - Explorativ analys av trender 2026

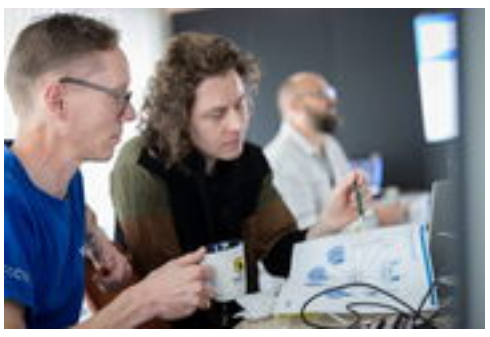
Rapport av John Ziegenbein, Henrik Karlzén, Viktor Bergström och Christoffer Lauri

Rapporten analyserar de tekniktrender som fem inflytelserika analysföretag identifierat som särskilt relevanta för 2026.
Rapportförfattarna har bedömt trenderna utifrån relevansen för Försvarsmakten och specifikt för cyberförsvaret. Nio trender tas upp i rapporten: - multiagenta system - tillgång till AI-modeller och AI-beräkningskapacitet - molntjänsters utmaningar - AI-baserad mjukvaruutveckling - AI för cyberförsvar - digitalt ursprung - postkvantkryptering - säkerhet för stora språkmodeller - fysisk AI.

Varje trend analyseras utifrån forskning gjord av FOI och andra. Analyserna mynnar ut i praktiska rekommendationer till cyberförsvaret. Eftersom de flesta trender berör AI har flera av rekommendationerna gemensamma drag: skydd och försvar mot och med AI, organisatoriska förändringar samt aspekter kring digital suveränitet. Bland organisatoriska förändringar ingår även rekommendationer som rör postkvantkryptering.
Läs hela rapporten

Stärkt nationellt cyberförsvar genom gemensamma övningar

Av Fredrik Johansson



För att möta ett alltmer komplext hotlandskap har FOI under våren lett en serie cyberövningar åt Nationellt cybersäkerhetscenter (NCSC). I fokus har plattformen MISP stått, ett kraftfullt verktyg för att dela information om cyberhot.
Under tre intensiva övningstillfällen har deltagare från både myndigheter och kommuner arbetat med praktisk incidenthantering. Genom att agera i en simulerad miljö har deltagarna tvingats samarbeta kring informationsdelning; för att skydda sin egen miljö krävdes det att man snabbt kunde tolka och applicera den hotinformation som kom från andra aktörer.
Detta samarbete är en del i lanseringen av MISP-SE – Sveriges nya nationella plattform för hotdelning. Plattformen, som drivs av CERT-SE, gör det möjligt för svenska organisationer att dela kritiska hotindikatorer, såsom skadliga IP-adresser och domäner, vilket skapar ett kollektivt skydd mot cyberattacker. Genom att öva på dessa processer idag säkerställer vi att Sverige är bättre förberett för morgondagens digitala hot.

Crate-CTF - En tävling i cybersäkerhet

Crate-CTF är en årligt återkommande cybersäkerhetstävling som anordnas av FOI i samarbete med Försvarsmakten.

Årets tävling kommer genomföras **21 november 2026**.

En CTF (Capture the Flag) är ett tävlingsinriktat övningsformat där deltagarna ges uppgifter inom cybersäkerhet och hantering av it-system som ska lösas inom en viss tid. Crate-CTF bygger på det så kallade Jeopardy-formatet, där varje uppgift innehåller en egen flagga i form av en krypterad eller på annat sätt dold textsträng. Det gäller för deltagarna att med hjälp av den information som tillhandahålls, och med en god portion list och klurighet, hitta flaggan och därmed få poäng.
I Crate-CTF utmanar vi både nybörjare och avancerade tävlare. Uppgifterna är fördelade över olika kategorier. Deltagandet sker över

internet, enskilt eller i grupp.
Anmälan till Crate-CTF 2026 öppnar 1 september.

IT-försvarsdagen den 3 december - Save the date!

IT-försvarsdagen är en digital heldag om problemställningar, inriktningar och resultat från aktuell forskning inom Cyberförsvar. Förra årets event lockade drygt 800 anmälda deltagare och handlade bl.a om Kvantdatorers påverkan på cybersäkerhet, AI för taktiskt planering, cyberövningar på distans och vad cyberkrigföring egentligen kostar samhället. Medverkande kom från FOI, Försvarshögskolan, Netnod NCSC och Linköpings universitet.

En inbjudan med länk till anmälan för årets evenemang kommer senare under hösten.
Har du frågor är du välkommen att skicka dem till
itforsvarsdagen@foi.se

Kurs i Elektronisk säkerhet

Elektroniska system är en integrerad del av vardagen. Nästan alla verksamheter är beroende av elektroniska system som måste fungera om verksamheten ska fungera normalt, eller om den ska fungera alls. Säkerhetsfrågor i sådana system är verksamhetskritiska i de flesta branscher. FOI erbjuder därför en skräddarsydd kurs i elektronisk säkerhet där FOI på ett unikt sätt bjuder på sin speciella kompetens.

Säkerhet handlar dock inte bara om att system ska vara tillgängliga, utan också om att de inte ska läcka information till obehöriga, och att informationen i dem ska vara korrekt. För att kunna hantera och bedöma frågor som rör säkerhet i elektroniska system krävs en omfattande kunskap om systemen och de hot de är utsatta för. Den här kursen erbjuder en bred genomgång av dagens elektroniska system, både vad gäller normal funktion och säkerhetsproblematik. Vissa delar av kursen berör områden där FOI är ensamma i Sverige om att ha forskningsverksamhet, till exempel radiostörning, radiopejling och IT-vapen.

Målgruppen för kursen är personer som har säkerhet inom sitt ansvarsområde men som inte nödvändigtvis själva är tekniskt verksamma, t.ex. chefer, beslutsfattare, projektledare och tjänstemän.
Följande kurstillfälle är nu öppna för anmälan:
v40 2026, kurstillfället är fullbokat.
v20 och v40 2027.

Är du intresserad och vill få mer information går det bra att ringa eller mejla till kursansvarig, Fredrik Söderström, 08-555 030 00
Hkes@foi.se
En mer detaljerad kursbeskrivning och anmälan hittar du här:
Kurser och utbildningar

Brinner du för cybersäkerhet?

Vi söker nya kollegor som brinner för cybersäkerhet och vill bidra till att stärka Sveriges totalförsvar, bland annat med hjälp av den **nationella cyberanläggningen Crate.**

På FOI:s hemsida **Jobba hos oss** finns att läsa om de tjänster som annonseras ut nu.
Sidan uppdateras kontinuerligt med nya jobbtillfällen.

Just nu söker vi
Drivna ledare som vill utveckla Sveriges cyberförmåga i totalförsvaret

Varmt välkommen med din intresseanmälan.
Är du intresserad och vill få mer information ring eller mejla
Foteini Papiri, verksamhetsområdeschef Cyber, 08-555 030 00
foteini.papiri@foi.se
Jonas Hallberg, enhetschef Cybersäkerhet, 08-555 030 00
jonas.hallberg@foi.se
Jonas Hallberg, tf enhetschef Förmågor i Cyberdomänen**,** 08-555 030 00**,** **jonas.hallberg@foi.se**
Jonas Wiman, tf enhetschef Cyberanläggningsteknik, 08-555 030 00**,** **jonas.wiman@foi.se**

Rapportsamling

Du vet väl om att de flesta rapporter som FOI publicerar är tillgängliga i elektronisk form från vår webplats? För att underlätta för er som är speciellt intresserade av informationssäkerhet så har vi samlat just dessa rapporter i en speciell lista. Listan uppdateras kontinuerligt.
Rapportsamling Informationssäkerhet

Kurser 2027

Vi erbjuder utbildningar, kurser och seminarier inom våra kompetensområden. Vi kan även skräddarsy kurser utifrån din organisations behov

Kontakta oss för mer information.
Kurser och utbildningar

Crate City

OM NYHETSBREVET

FOI, Totalförsvarets forskningsinstitut, *är ett av Europas ledande forskningsinstitut inom försvar och säkerhet. Hos oss arbetar cirka 1700 medarbetare med varierande bakgrunder. FOI:s kärnverksamhet är forskning, metod- och teknikutveckling samt analyser och studier. Myndigheten är uppdragsfinansierad och ligger under Försvarsdepartementet.*

Vid synpunkter på innehållet i detta nyhetsbrev kontakta Gunilla Friberg, ***gunilla.friberg@foi.se***
FOI ansvarar inte för länkar som leder till andra webbplatser.

Hantering av personuppgifter
FOI:s nyhetsbrev skickas ut via ett webbverktyg där dina personuppgifter sparas. Du samtycker till behandlingen av dina personuppgifter genom att ange din e-postadress, och i förekommande fall för- och efternamn. Endast de som administrerar verktyget och leverantören av verktyget har tillgång till personuppgifterna. Dina personuppgifter sparas så länge du prenumererar på nyhetsbrevet. Vill du avsluta din prenumeration på FOI:s nyhetsbrev kan du avanmäla dig genom att klicka på den avprenumerationslänk som finns längst ned i varje nyhetsbrev.
Om du väljer att avanmäla dig raderar vi manuellt dina personuppgifter den första arbetsdagen nästkommande månad. Om du vill att raderingen ska ske snabbare än så, kontakta FOI.

Läs mer om dataskyddsförordningen, dina rättigheter och kontaktuppgifter till FOI.

Följ oss gärna i sociala medier

För att avbeställa nyhetsbrevet klicka här.