

IT-försvarsdagen Program 3/12 2026

(hålltider kan komma att justeras)

08.30-09.00	<i>Digitala rummet öppnar, vi släpper in 30 minuter innan konferensen startar.</i>
09.00-09.10 <i>Foteini Papiri FOI, Cyberförsvar och ledningsteknik</i>	Inledning
09.10-09.30 <i>John Ziegenbein FOI, Cyberförsvar och ledningsteknik</i>	Civila tekniktrender 2026 <i>Presentation av nio civila tekniktrender 2026. Trenderna berör områden såsom AI-baserad mjukvaruutveckling, postkvantkryptering, tillgång till AI-modeller, fysisk AI, säkerhet för stora språkmodeller och multiagenta system.</i>
09.35-10.05 <i>Martin Karresand FOI, Cyberförsvar och ledningsteknik</i>	Försvarbara system <i>Efter att fokus i många år legat på att bygga säkra IT-system, ökar nu intresset för att göra dem försvarbara. Men vad innebär det och hur ser forskning och verklighet ut i dagsläget?</i>
10.05-10:20	Fikapaus
10.20-10.50 <i>Christoffer Flygare NCSC</i>	Nationellt cybersäkerhetscenter <i>NCSC har tagit över den civila cyberverksamheten, inklusive CERT-SE, och ska samordna arbetet med AI-relaterad cybersäkerhet. Vi går igenom vad som har hänt, hur samarbetet med myndigheter och näringsliv fungerar i praktiken och vad som prioriteras härnäst.</i>
10.55-11.25 <i>Hannes Holm FOI, Cyberförsvar och ledningsteknik</i>	Automatisk sårbarhetsanalys med Lore <i>Lore kombinerar regelbaserade metoder med stora språkmodeller för att automatisera sårbarhetsanalyser av nätverk. Presentationen introducerar Lore och dess arbetssätt samt belyser hur stora språkmodeller har påverkat forskningen om automatiserad sårbarhetsanalys.</i>
11.30-12.00 <i>Lena Strömbäck FOI, Cyberförsvar och ledningsteknik</i>	Digitala tvillingar för bättre cybersäkerhet <i>Digitala tvillingar är en intressant teknik för att modellera, övervaka eller bättre förstå dagens komplexa IT-system. Men vad är det egentligen och kan digitala tvillingar användas för förbättrad cybersäkerhet?</i>
12.00-13.00	Lunch

13.00-13.30

*Generalmajor Mattias Hanson
Försvarsstaben Cyber*

Ökad resiliens genom kunskap och handlingskraft

Cyberhoten utvecklas i takt med tekniken och ett förändrat säkerhetsläge. Samtidigt ökar beroendet mellan militära och civila system och samhällsviktig infrastruktur. Hur möter vi dagens och morgondagens hot, och hur kan gemensam förståelse, ansvarstagande och samverkan bidra till ökad motståndskraft?

13.35-14.05

*Erika Holmquist
FOI, Försvarsanalys*

Irans cyberstrategi

Irans säkerhetspolitiska utveckling under 2026 är den mest turbulenta sedan Iran-Irakkriget, och har synliggjort vikten av cyberrymden som arena för konflikter med både interna och externa fiender.

14.10-14.40

*Fredrik Ruuda
FMV*

Demonstratorer – Projekt i agil anda

FMV genomför tre demonstratorprojekt tillsammans med FOI och andra intressenter. Tekniken ska testas och demonstreras i en så realistisk operationell miljö som möjligt, utan att röja möjliga existerande förmågor och genom att nyttja forskning och marknadens möjligheter.

14.40-14.55

Fikapaus

14.55-15.25

*Mikael Asplund
Department of Computer and
Information Science
Linköpings Universitet*

Cybersäkerhet i AI-eran

AI-agenter utvecklas snabbt och mjukvaruutveckling är ett av de områden som påverkas kraftigt av de nya modellerna. Modellerna har också visat sig vara allt bättre på att hitta och utnyttja sårbarheter i programvara. Kommer AI också kunna lösa framtidens cybersäkerhetsutmaningar, eller står vi snarare inför vad som populärt kallas för cybergeddon?

15.30-16.00

*Fredrik Johansson
FOI, Cyberförsvar och ledningsteknik*

Säkra AI-modeller

För nyttjande av AI-modeller i försvars- och säkerhetskritisk verksamhet blir det viktigt att kunna utvärdera modeller på domänrelevant data och att säkerställa att modellerna kan tas in och nyttjas i känsliga IT-miljöer på ett säkert sätt.

16.00-16.10

*Matyas Barocsai
FOI, Cyberförsvar och ledningsteknik*

Avslutning