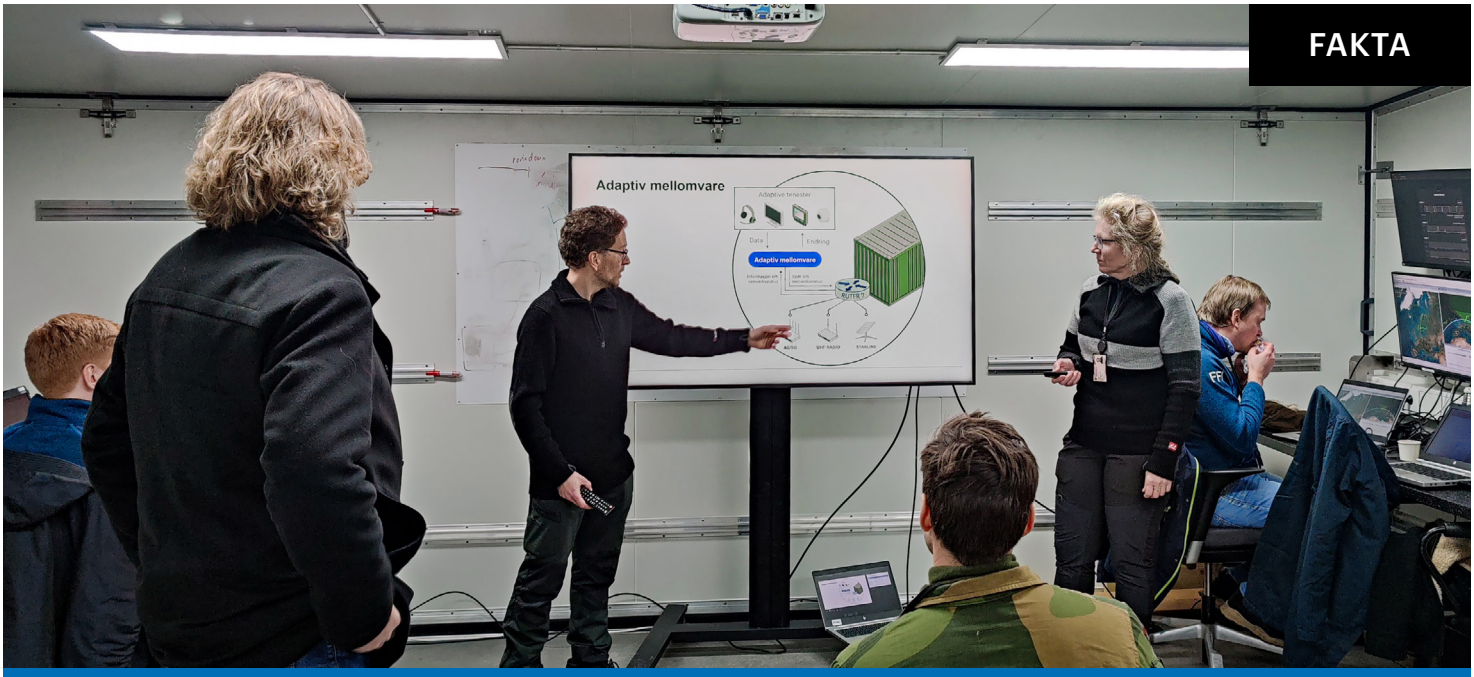
FFI Forsvarets forskningsinstitutt



FAKTA

September 2023 – Design/produksjon: FFI, Foto: FFI

FIST skal sikre informasjonsdeling

FIST er et flernasjonalt forskningssamarbeid mellom Norge, Tyskland og USA. Formålet er å utvikle, teste og demonstrere teknologier og metoder som gjør det mulig å dele informasjon sikkert og effektivt mellom militære styrker.

Moderne IKT er nødvendig for å understøtte Forsvarets operative evne. Forsvarets kampkraft sikres i stor grad gjennom interoperabilitet med våre allierte. Det er derfor avgjørende at norske styrker kan virke effektivt sammen med allierte styrker.

Federated Information Sharing for Tactical Networks (FIST) handler om å finne løsninger som gjør det mulig å dele informasjon i militære koalisjoner. FFI har deltatt i FIST siden 2019, i samarbeid med norske industripartnere. Hovedtemaer har vært kommunikasjonsnettverk, tjenester og sikkerhet. FFI har samarbeidet med tre virksomheter: med Kongsberg Defence & Aerospace AS (KDA) om løsninger for effektiv sammenkobling av ulike militære kommunikasjonsbærere, med Sysint AS om hvordan IKT-tjenestene Forsvaret bruker kan fungere effektivt også når kommunikasjonsresurssene er begrensede, og med Thales Norway AS om sikkerhet.

Nyttig for Mime

Forsvarets IKT for taktisk ledelse er under modernisering. Det skjer gjennom programmet Mime. Kunnskapen som er bygget gjennom å delta i FIST vil særlig være nyttig for dette programmet. Mime skal sikre Forsvaret relevante og tidsriktige leveranser av løsninger som understøtter operative behov og krav. Når Mime avsluttes i 2030 skal norske styrker ha en taktisk informasjonsinfrastruktur med funksjonalitet som sikrer vesentlig økt handlingsrom, sammenholdt med situasjonen før 2018.

Tjenester søker ressurser

De digitale tjenestene som Forsvaret bruker er avhengige av et nettverk for å virke.

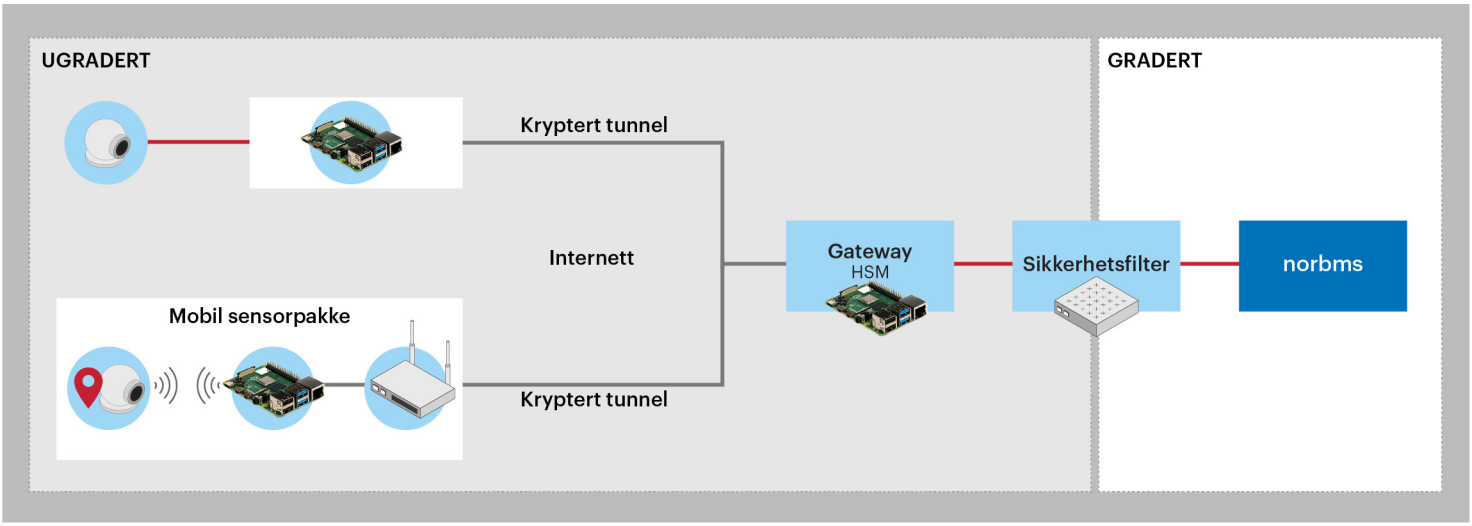
FIST: Federated Information Sharing for Tactical Networks

Bygger på forskningssamarbeider mellom Norge og sentrale allierte:

- CONSIS – Coalition Networks for Secure Information Sharing
- INSC – Interoperable Networks for Secure Communications
- CSNI – Communications Systems Network Interoperability

Arbeidsgrupper etter temaene:

- Kommunikasjonsnettverk (Communication and Network Infrastructure)
- Tjenester (Information Services)
- Sikkerhet (Cyber Security)



Informasjon samlet inn med et utvalg av billig hyllevare ute i felt kan krypteres på en tilfredsstillende måte, og sendes til graderte systemer. Sensorene kan styres fra innsiden av det graderte nettverket, men slik at vi er sikre på at gradert informasjon ikke kommer på avveie.

I militære nettverk kan de tilgjengelige ressursene variere over tid. Tjenestene kan i perioder måtte kommunisere ved hjelp av nettverk med begrensede ressurser. Begrensningene kan være i form av for eksempel lav datarate eller lange forsinkelser. Det minsker mengden informasjon som kan deles. I slike situasjoner trenger Forsvaret tjenester som fungerer godt, med et minimum av informasjon. Samtidig bør tjenestene kunne fungere bedre når ytterligere nettverksressurser er tilgjengelige. For at slike adaptive tjenester skal fungere best mulig, trenger tjenestene informasjon om ressurssituasjonen i nettverket.

Deling mellom enheter

Forsvarets enheter, for eksempel ulike typer kjøretøy, har typisk flere kommunikasjonsbærere. Disse har ulike egenskaper for å dekke enhetenes behov for å sende og motta data. Enheter kan ha både såkalte smalbåndsbærere og bredbåndsbærere. Smalbånd gir lang rekkevidde, men liten dataoverføringskapasitet. Bredbånd gir høy kapasitet, men kort rekkevidde. Ved å bruke en taktisk ruter kan en bygge et felles nettverk som utnytter de ulike bærerne effektivt. Ruteren kan rekonfigurere nettverket automatisk når enheter beveger seg og mister forbindelser. Det samme skjer dersom forbindelser faller bort som en følge av elektronisk krigføring.

I FIST har vi vært med på å videreutvikle en rutingprotokoll som kan lete etter ruter i et nettverk som oppfyller et sett med valgte krav, såkalt policy-ruting. I tillegg har vi utviklet og testet en mekanisme for deling av informasjon mellom tjenestene og nettverk. Til sammen gjør disse det mulig for tjenestene å tilpasse egen ressursbruk til den kapasiteten nettverket til enhver tid har. Vi har sett på flere ulike måter å dele informasjon om tilgjengelige ressurser mellom nettverket og tjenestene.

Strenge sikkerhetskrav

Forsvaret er vant med at graderte data som skal overføres må krypteres, ved hjelp av dedikerte komponenter. Disse komponentene er produsert ut fra krav fra Nasjonal sikkerhetsmyndighet og Nato. De må som regel behandles som gradering «konfidensielt» eller

Forsvaret fikk se at tjenestene tilpasser seg nettverket under program Mimes IDA (Innovasjons- og demonstrasjonsarena) i desember 2022

høyere. Både å kjøpe og behandle slike komponenter er kostbart. Det er uforenlig med bruk på enheter som en må forvente at kan gå tapt, som ubemannede enheter. Det er likevel behov for å beskytte data herfra. Sensordata som samles inn kan ha stor verdi for motstandere: De forteller noe om hva våre styrker vet og ikke vet, og de kan røpe egne plasseringer.

Integriteten av data er ofte vel så viktig som konfidensialiteten. En motstander kan sende forfalskede styringssignaler, eller returnere gale sensordata og få en ubemannet plattform til å forårsake skade på operasjonen. I FIST er det tatt fram løsninger som gjør det mulig å bruke sterk kryptografi sammen med vilkårlig hyllevare. Det er gjort på en slik måte at vi selv kontrollerer implementasjon og nøkler.

Kontaktpersoner:
trude-hafsoe.bloebaum@ffi.no
jan-erik.voldhaug@ffi.no