

RONNIE JOHANSSON OCH PONTUS HÖRLING



Ronnie Johansson och Pontus Hörling

IoT-samverkan

Uppföljning 2021

Titel	IoT-samverkan – Uppföljning 2021
Title	IoT collaboration – Follow-up 2021
Rapportnr/Report no	FOI-R--5258--SE
Månad/Month	Februari
Utgivningsår/Year	2022
Antal sidor/Pages	29
ISSN	1650-1942
Uppdragsgivare/Client	Försvarets materielverk
Forskningsområde	Ledningsteknologi
FoT-område	Inget FoT-område
Projektnr/Project no	E86218
Godkänd av/Approved by	Cecilia Dahlgren
Ansvarig avdelning	Förvarsteknik

Bild/Cover: Shutterstock/Alexandra Lande

Detta verk är skyddat enligt lagen (1960:729) om upphovsrätt till litterära och konstnärliga verk, vilket bl.a. innebär att citering är tillåten i enlighet med vad som anges i 22 § i nämnd lag. För att använda verket på ett sätt som inte medges direkt av svensk lag krävs särskild överenskommelse.

This work is protected by the Swedish Act on Copyright in Literary and Artistic Works (1960:729). Citation is permitted in accordance with article 22 in said act. Any form of use that goes beyond what is permitted by Swedish copyright law, requires the written permission of FOI.

Sammanfattning

Den övergripande frågan i det här arbetet, liksom i ett föregående arbete, är hur Försvarsmakten och totalförsvaret kan dra nytta av civila IoT-system (så kallad IoT-samverkan). Den föregående rapporten från 2020 betonade dels betydelsen av så kallad randteknik (eng. edge technology), dels en existerande krissamverkansgrupp, vilken förefaller vara en lämplig miljö för att studera IoT-samverkan operativt.

Det aktuella uppföljande arbetet har två delmål: I) bevakning av förutsättningarna för IoT-samverkan och II) undersökning av hur lägesbilsarbetet går till i Stockholmsregionens operatörskluster. Bevakningen omfattar samtal med svenska myndigheter, deltagande i konferenser, en utblick till situationen i andra länder, samt en översikt över relaterade aktiviteter inom Nato. Vad gäller stöd för lägesbild har organisatörerna av krissamverkansgruppen rådfrågats om hur samarbete kring lägesbilder sker för närvarande.

Rapporten behandlar följande aspekter av IoT-samverkan: Tekniskt diskuteras bland annat nyttan av Kubernetes-teknologier för randteknik, uppdateringen av Rakel, samt offentliga IoT-plattformar. Organisatoriskt förstärks bilden av att Stockholmsregionens operatörskluster med dess IT-stöd är en lämplig miljö för att experimentera med och demonstrera IoT-samverkan.

För vidare arbete rekommenderas samarbete med aktörerna i operatörsklustret för att bland annat undersöka aktörernas acceptans för och nyttan med IoT-samverkan, samt fortsatt undersökning av hur randteknik kan realisera delade IoT-tjänster.

Nyckelord: Internet of Things, IoT, IoT-samverkan, lägesbild, edge, randteknik

Summary

The overarching question in this work is how the Swedish Armed Forces and the total defence can benefit from civilian IoT systems (so-called IoT collaboration). The previous report from 2020 emphasized the importance of edge technology, as well as an existing crisis collaboration group, which seems to be a suitable environment for studying IoT collaboration operationally.

The current work has two sub-goals: I) to monitor the conditions for IoT collaboration and II) investigate how the work on situational pictures is conducted in the Stockholm region crisis management cluster. The monitoring includes communication with Swedish authorities, participation in conferences, an overview of the situation in other countries, as well as an overview of related activities within NATO. With regard to goal II), i.e. support for situational pictures, the project has consulted the organizers of a crisis collaboration group on how it currently collaborate on situational pictures.

The present report addresses various aspects of IoT collaboration: the benefits of Kubernetes technologies for edge computing, the update of Rakel, and public IoT platforms are discussed. Organizationally, the comprehension is strengthened that the Stockholm region's operator cluster with its IT support is a suitable environment for experimenting with and demonstrating IoT collaboration.

Keywords: Internet of Things, IoT, IoT collaboration, situation picture, edge technology

Innehållsförteckning

1	Inledning	7
1.1	Bakgrund	7
1.2	Syfte.....	12
1.3	Metod	12
1.4	Läsanvisning.....	13
2	Omvärldsbevakning.....	14
2.1	Nato	14
2.2	Sverige.....	15
2.2.1	Försäkringskassan.....	15
2.2.2	Ericsson	16
2.2.3	AI Sweden och Edge Learning Lab.....	17
2.2.4	Rakeldagen.....	18
2.2.5	Stockholms stad.....	18
2.3	Utblick till övriga världen.....	20
2.3.1	Finland	20
2.3.2	Estland	21
2.4	Kubernetes – teknik för randen	22
3	Lägesbilsarbete	24
3.1	Länsstyrelsen om operatörsklustret	24
4	Slutsatser och vidare arbete.....	27
4.1	Omvärldsbevakning.....	27
4.2	Lägesbilsarbete	27
4.3	Förslag på vidare arbete.....	28
	Litteraturförteckning	29

1 Inledning

Sedan senaste sekelskiftet har den tekniska utvecklingen resulterat i strömsnål, billig, och allt småskaligare elektronik. En bekant och samhällsomvälvande konsekvens av detta är den globalt spridda mobiltelefonitekniken som idag är en integrerad del av allmänhetens vardag. En annan konsekvens är trådlösa sensor-nätverk och möjligheten att koppla upp sensorer mot internet för att inhämta sensordata i syfte att övervaka eller analysera en process i den fysiska världen.

Den här typen av nätverksanslutna sensorer, ofta kallat *sakernas internet* (eng. *Internet of things*, IoT), har många tillämpningar, exempelvis i privata hem (för övervakning och energieffektivitet), på den mänskliga kroppen (för att mäta hälsa), i industriprocesser (för optimering av process och underhåll), och offentlig stadsmiljö (för mätning av luftföroreningar, trafikoptimering, med mera, så kallad ”smart stad”¹). Genom 5G-teknikens successiva införande och integration med IoT-system möjliggörs dessutom större och snabbare dataflöden samt fler uppkopplade sensorer.

I de projekt som föregått det nuvarande (Johansson & Hörling, 2021; Johansson, o.a., 2019; Johansson, 2018) har bland annat förutsättningarna (främst i termer av infrastruktur) för IoT-samverkan mellan svenska myndigheter och olika tekniska metoder (exempelvis artificiell intelligens för IoT och databehandling av strömmande data) studerats. Särskilt intresse riktades mot en Natoarbetsgrupp² och dess arbete med *randteknik* (eng. *edge computing*) för att möjliggöra åtkomst av IoT-tjänster från externa organisationer. Projektet har också identifierat ett så kallat operatörskluster i Stockholmsregionen. Operatörsklustret utgör en miljö för utbyte av information mellan olika offentliga organisationer i krislägen, en miljö som även skulle kunna hysa en plattform för utbyte av IoT-information.

I det här uppföljande projektet tas arbetet vidare genom dels I) omvärldsbevakning (se kapitel 2) och II) lägesbilsarbete (se kapitel 3). Omvärldsbevakningen omfattar aktiviteter som sker i Sverige och som har bäring på IoT-samverkan. Omvärldsbevakningen omfattar dessutom en kortfattad utblick mot andra delar av världen. Slutligen följs också relaterade verksamheter inom Nato upp. Intresset för lägesbilsarbete fokuseras på det operatörskluster tillhörande Stockholmsregionen som beskrivs i Johansson och Hörling (2021).

1.1 Bakgrund

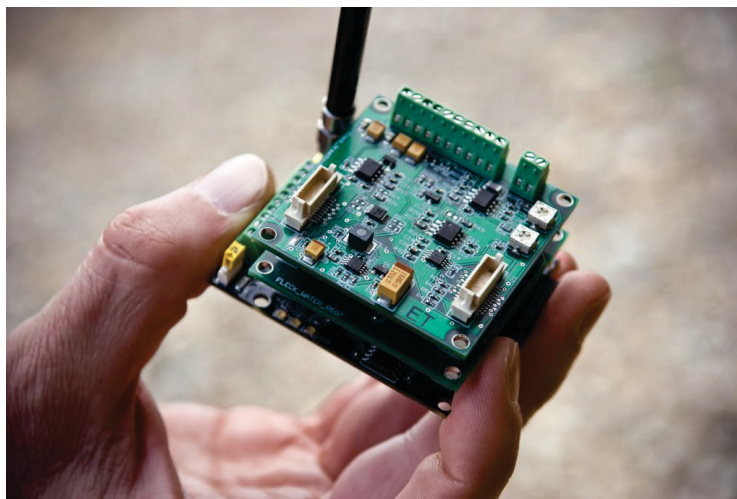
IoT handlar i korta drag om att förankra internet i den fysiska världen genom att tillgängliggöra (realtids-) information om *saker* i världen (dvs. utanför

¹ En fördjupad diskussion om smarta städer finns i en rapport av Bengtsson och Mickelsson (2021).

² Nato-arbetsgruppen NATO STO IST-147-RTG

cyberrymden) för databearbetning.^{3,4} Information om saker kan omfatta exempelvis sakernas position, status och sensormätvärden och tillgängliggörs med hjälp av särskilt utvecklad elektronik, *IoT-enheter*. Sådana IoT-enheter (se Figur 1 för ett exempel) erbjuder förmåga att känna (omvärlden med sensorer), bearbeta (insamlad data med mikroprocessor), lagra (på minneskrets), kommunicera (trådbundet eller trådlöst med antenn och radioteknik), samt även i vissa fall styra (sensorer, lampor, dörrar, termostater, eller andra funktioner).

IoT-enheter som är uppkopplade på det här sättet kallas ”smarta” då de ger möjlighet att få dels en överblick över tillgängliga resurser och den inmätta delen av den fysiska världen, dels ett kvantifierbart beslutsunderlag. Utöver att insamla information om en sak är det tänkbart med tillämpningar där även saker eller deras miljö kan styras. Styrbara enheter brukar i sådana här sammanhang kallas *ställdon* (eng. *actuator*).⁵



Figur 1. Ett exempel på en IoT-enhet. Det här exemplet är batteridrivet (möjliggör mobilitet och flexibel placering), trådlöst (kommunicera), och bestyckat med sensorer (känna). Med tillstånd av CSIRO (<https://www.scienceimage.csiro.au/>)

³ En längre diskussion om definitionen av IoT, och mer specialiserade begrepp som Internet of battle things, finns i den föregående rapporten av Johansson m.fl. (2019, s. 62).

⁴ Notera att även om IoT i sin helhet möjliggjorts av modern teknik så kan vissa delar av ett IoT-system bestå av förvisso föråldrad men ändå användbar teknik (exempelvis pålitliga sensorer som använts förtjänstfullt för någon tillämpning, men vars information görs tillgänglig genom integrering i ett IoT-system).

⁵ Med fjärrmanövrerade ställdon avses i denna utvidgade mening IoT-enheter som har förmåga att agera *på* sin omgivning såsom att öppna/stänga en dörr eller lucka, röra en hydraulkolv, ändra motorvarv, men även icke-mekaniska förmågor såsom att elektroniskt utlösa ett larm eller slå på en lampa. System av sensorer och styrbara enheter kallas ibland också *cyber physical systems*.

Det finns just nu ett stort intresse både hos kommersiella och offentliga aktörer att införskaffa *IoT-system* (innehållandes IoT-enheter bestående av nödvändig kommunikationsutrustning, eventuellt databaser för loggar och databuffrar, säkerhetslösningar, med mera) en utveckling som förväntas öka i och med införandet av den femte generationens mobiltelefoni (5G) som bland annat tillåter snabbare dataöverföring och mer tillförlitlig uppkoppling. Resultatet blir en gradvis växande och diversifierad *IoT-miljö* bestående av olika privata och offentliga IoT-system för olika tillämpningsområden.

Ordet ”internet” i IoT antyder att IoT-enheter är anslutna till internet eller åtminstone till någon form av avgränsat nätverk⁶ som möjliggör spridning, bearbetning och lagring av information. IT-tjänster, exempelvis fillagring, som erbjuds på Internet eller i ett avgränsat nät brukar kallas *molntjänster*, eller lite förenklat bara *moln*. I vissa tillämpningar, exempelvis ”smarta fordon”, är direktkoppling mellan IoT-enheter nödvändig (exempelvis vid överföring av trafikinformation mellan två fordon). Även i andra tillämpningar är beroendet av uppkoppling till ett moln problematiskt, såsom om molnet är otillgängligt, dess kapacitet för datatrafik är begränsad samtidigt som en snabb respons krävs hos ställdon. För att hantera sådana situationer finns så kallade *randenheter* (eng. *edge devices*) som fysiskt skall ligga nära relaterade IoT-enheter och därför kan utföra vissa databehandlingsuppgifter (exempelvis detektion, lära från insamlad data, buffring och loggning,⁷ fusion, aggregering, filtrering, anonymisering, kryptering, och schemaläggning av resurser).

För Försvarsmakten kan kunskap om IoT-teknik vara viktigt ur åtminstone tre olika perspektiv:

- 1) för eget utnyttjande av IoT-teknik för exempelvis underhåll av fordon, logistik, lägesbild över slagfält och uppfattning av egna resursers tillstånd (dvs den delmängd av IoT som kallas *Internet of Battlefield Things*, IoBT, illustrerat i Figur 2)
- 2) för att uppskatta och bemöta en motståndares IoT-förmågor
- 3) för att kunna dra nytta av civilsamhällets IoT-system (både privata och offentliga) för att exempelvis förstärka den egna lägesbilden, koordinera med andra totalförsvarsaktörer, samt dela och nyttja andra aktörers sensorer och resurser

Den här rapporten behandlar primärt det tredje perspektivet.

⁶ Med ”avgränsat” avses inte nödvändigtvis en geografisk avgränsning utan den kan istället vara logisk som ett virtuellt privat nät.

⁷ Loggning av sensordata och enhetsparametrar kan utföras exempelvis för att underlätta felsökning, automatisk rapportgenerering och datainsamling för lägesbildsuppdatering.



Figur 2. En illustration av ett IoT-uppkopplat militärt scenario (IoBT) med uppkopplade drönare och soldater i samverkan. (CCDC Army Research Laboratory, Public domain, via [Wikimedia Commons](#))

Försvarmakten och totalförsvaret har behov av aktuell information från olika områden och situationer för effektivt beslutsfattande, oavsett om uppdraget gäller daglig övervakning eller en eskalerande krissituation. I krissituationer kan det vara bråttom att etablera en *lägesbild* över ett händelseförlopp samtidigt som det område om avses kan vara mer eller mindre svårarbetat. Det skulle till exempel kunna bero på en naturkatastrof som försvårat framkomligheten och skadat byggnader, eller en konflikt (civil eller militär) som gjort området farligt att beträda.

IoT-enheter och andra källor (exempelvis sociala medier och databaser) kan leverera information om en händelse eller situation av intresse till IT-system för krishantering. Efter eventuell bearbetning och sammanställning bidrar systemet till den tillgängliga *lägesinformationen* om en situation. Lägesinformationen kan sedan presenteras på ett operatörsanpassat sätt beroende på operatörens ansvarsområde och rättigheter. Lägesinformationen uttryckt med lämpliga operatörsanpassade modaliteter (det vill säga bild, ljud, med mera) utgör lägesbilden. Operatörens mentala bild av vad lägesbilden förmedlar kallas *lägesförståelse*. I den här rapporten görs ingen skarp distinktion mellan lägesbild och lägesinformation då presentationsgränssnitt inte är ett projektfokus utan snarare den närmast underliggande informationen är det.

Lägesbild är ett brett begrepp vars uttryck är aktörs- eller rollberoende. Med *aktör* menas en person, grupp, eller organisation som har en uppgift med behov av en viss lägesbild för effektivt agerande. Med *operatör* menas en viss fysisk person (en aktör eller del av en aktör) i den *roll* denne har i sin interaktion med det system som presenterar lägesbilden.

En aktör som har ansvar för hanteringen av händelseutvecklingen inom den egna organisationen, för viss infrastruktur, för utvecklingen inom ett visst geografiskt område etc. behöver löpande information om läget inom sitt ansvarsområde för fortlöpande justeringar och för att kunna agera och ta beslut i tid och på rätt sätt om, exempelvis, utvecklingen för en uppkommen situation tar en oönskad riktning.

Vilken typ av lägesinformation aktören behöver är naturligtvis beroende på uppgiften. Informationen kan vara genererad av sensorer, av mänskliga iakttagare, av simulerings- och prognostiseringsverktyg med mera. Sättet att presentera informationen kan också variera; geografisk (eller rumslig i fallet med infrastruktur) information kan presenteras på en karta över området, eller en mer eller mindre förenklad ritning eller skiss över en övervakad infrastruktur.

I offentlig verksamhet (på kommun-, region- och riksnivå) finns många aktörer i form av organisationer (ofta myndigheter) som ansvarar för sina egna respektive områden, såsom polis, brandförsvaret, energiproducenter, sjukvård och trafikövervakning. Dessa har sina specifika, ofta väsensskilda, men ibland överlappande, informationsbehov för sina respektive lägesbilder.

För att aktörerna skall kunna agera effektivt tillsammans krävs *samverkan*, vilket definieras enligt följande i en rapport från MSB (2018, s. 20): ”Samverkan är den funktion som, genom att aktörer kommer överens, åstadkommer inriktning och samordning av tillgängliga resurser.”

Samordning i definitionen ovan betyder vidare ”[...] anpassning av aktiviteter och delmål så att tillgängliga resurser kommer till största möjliga nytta.” och att ”Samordning handlar om att aktörer inte ska vara i vägen för varandra, och hjälpa varandra där det går.”

Med IoT-samverkan menas då att IoT-system har förmågan att dela med sig av sina insamlade data till godtyckliga (men behöriga) användare (mänskliga individer eller andra tekniska system). Ett samverkande IoT-system kan eventuellt även erbjuda ett gränssnitt för styrning av dess datainsamling och ställidon.

Vinnovas strategiska innovationsprogram IoT Sverige stöttar och följer upp en del av de IoT-satsningar som utförs i Sverige. Ett konkret exempel på offentliga IoT-system finns hos de skånska grannkommunerna Malmö och Lund vilka bland annat har IoT-tillämpningar för övervakning av energiförsörjning och avfallshantering.⁸

⁸ <https://iotsverige.se/projekt/lunds-kommun-malmo-stad> (besökt 2021-11-26)

1.2 Syfte

Det övergripande syftet med projektet⁹ är att på sikt öka Försvarsmaktens förmåga att dra nytta av den framväxande civila IoT-miljön för att förstärka den militära lägesbilden (det är projektets primära måltillämpning), främst genom att lära från existerande relaterat arbete.

Det nuvarande projektet tar ett steg mot att skapa denna förmåga genom att undersöka hur den civila IoT-miljön skall kunna nyttjas av Försvarsmakten i totalförsvaret för att förbättra den militära lägesbilden.

Det aktuella arbetet har dessa två delmål:

I. Omvärldsbevakning: Följa utvecklingen av teknik för IoT-samverkan och förutsättningarna för svenska myndigheter att delta i och bidra till IoT-samverkan

II. Lägesbildsarbete: Undersöka vidare hur arbetet med lägesbild går till i Stockholmsregionens operatörskluster

Omvärldsbevakningen omfattar delvis tekniska lösningar från relaterade Nato-projekt. Det Natoprojekt som följts tidigare år har nu avslutats, men liknande verksamhet bedrivs av Nato i nya projekt. Omvärldsbevakningen omfattar dessutom samhällsfunktioners beredskap att delta i IoT-samverkan, exempelvis därtill stödjande offentlig infrastruktur.

Lägesbildsarbete omfattar hur IoT-samverkan kan påverka arbetet med att skapa och underhålla en lägesbild. Lärdomar kan dras från Stockholmsregionens operatörskluster där samverkan om lägesbild rutinmässigt sker (dock för närvarande inte någon IoT-samverkan) och där dessutom representanter för Försvarsmakten (FM) finns med.

IoT-system, särskilt system av samverkande system, är i sin helhet mycket komplexa, varför bara delar av problemområdet kan beaktas i den här rapporten. Fokus ligger på tekniska frågor kring sammankoppling och interoperabilitet mellan IoT-system, medan exempelvis etiska och juridiska frågor inte behandlas.

1.3 Metod

I föregående rapport redogjordes för det arbete om militär IoT och samverkan som sker inom Nato (Johansson & Hörling, 2021). Det Natoprojekt som tidigare studerats är nu avslutat men dess slutrapport, som skulle granskats i det här projektet, och utgöra teknikdelen av delmål 1) Omvärld, har ännu inte publicerats. Istället har projektet tagit del av rapporteringen av en studie om

⁹ På de platser i rapporten där ordet "projektet" används är det just det här projektet som avses.

nerskalad Kubernetes för randteknik som ett efterföljande Natoprojekt har genomfört (Fogli, o.a., 2021).

I övrigt har projektet följt utvecklingen i omvärlden genom att delta i (virtuella) konferenser och samtala med olika myndigheter och organisationer.

Konferenserna omfattar 5G Techritory 2021¹⁰ (2021-11-24), Rakeldagen (2021-05-05), IoT-Sverige årskonferens¹¹ (2021-11-18), samt Tamsec¹² (2021-11-09). De organisationer projektet haft kontakt med omfattar Försäkringskassan (möte 2021-09-30), Ericsson (möte 2021-09-20), AI Sweden (möte 2021-10-15), och Rise projektavslutning "City as a platform" (2021-09-30). Projektet har också samlat in information om utvecklingen i Finland och Estland genom öppna nätkällor och experter verksamma i de två länderna.

För att ytterligare följa IoT-utvecklingen har projektet deltagit i "Arbetsgrupp Standarder och teknisk plattform" inom ramen för det Vinnova-sponsrade strategiska innovationsprogrammet IoT Sverige.¹³ Arbetsgruppen har bland annat till syfte att "... arbeta med standarder för att öka förutsättningarna för interoperabilitet mellan och inom offentliga verksamheter." och har medlemsorganisationer från både offentlig (exempelvis Sveriges kommuner och regioner, Rise, samt Post- och telestyrelsen) och privat (exempelvis Microsoft) sektor.

Vad det gäller delmål 2) Lägesbilsarbete har projektet samtalat med representanter för Stockholmsregionens länsstyrelse, som arbetar med regionens operatörskluster kring möjligheten att integrera IoT-samverkan i dess miljö. Projektet har dessutom i sitt slutskede etablerat kontakt med FM:s deltagare i operatörsklustret, men ett möte har inte kommit till stånd under projektets gång.

1.4 Läsanvisning

I kapitel 2 redovisas resultatet av delmål 1 (omvärldsbevakning) som bland annat diskuterar förutsättningarna för IoT-samverkan i Sverige och internationellt. I kapitel 3 diskuteras vidare möjligheterna att införa IoT-samverkan i Stockholmsregionens operatörskluster. Kapitel 4 omfattar slutsatser och förslag på vidare arbete.

¹⁰ Konferensen var uppkopplad och organiserades från Lettlands huvudstad Riga och hölls 22-24 november 2021. <https://www.5gtechritory.com> (besökt 2021-11-24)

¹¹ <https://iotsverige.se/events/arskonferens-2021> (besökt 2022-02-09)

¹² <https://linkopingsciencepark.se/events/tamsec> (besökt 2022-02-09)

¹³ IoT Sverige (<https://iotsverige.se>) startade 2014 och är ett av ett tiotal så kallade strategiska innovationsprogram gemensamt finansierade av Vinnova, Energimyndigheten och Formas.

2 Omvärldsbevakning

Vad det gäller nyttjande av IoT-system i samhället konstaterades i Computer Sweden i augusti 2019 (Malmqvist, 2019) att de största användningsområdena globalt av IoT (räknat i "flest ändpunkter") under början av 2020-talet skulle komma att vara energibolag (smarta elmätare), därefter intrångsdetektering/övervakning, därefter fordonsindustri, hälso- och sjukvård.

Förutsättningarna för samverkande IoT förändras snabbt i takt med nya tekniska landvinningar, politiska beslut och anammande av IoT-tjänster.

I de följande avsnitten redovisas projektets bevakning av utvecklingen inom IoT-området, med betoning på IoT-samverkan. Inom Natos arbetsgrupper (avsnitt 2.1) sker arbete som beaktar IoT-samverkan och militära förutsättningar. I Sverige arbetar myndigheter, institut, och företag med digitalisering och andra frågor som kan påverka möjligheten till IoT-samverkan (avsnitt 2.2). Utvecklingen sker inte bara i Sverige utan även i andra länder där det kan finnas intressanta initiativ. Som jämförelse diskuteras förutsättningarna för IoT-samverkan i några andra länder i avsnitt 2.3. I avsnitt 2.4 beskrivs en teknologi, Kubernetes, som studeras inom Nato som kandidat för att implementera randteknik för IoT-samverkan.

2.1 Nato

Arbetsgrupper inom Natos Science and Technology Organization (STO) arbetar sedan en tid med militär IoT och randteknik för IoT-samverkan. Arbetsgrupp IST-147:s tidigare arbete behandlas i (Johansson & Hörning, 2021, s. 18).

Slutrapporten från IST-147, som bland annat väntas omfatta FMN¹⁴ som är av intresse för militära tillämpningar av IoT, har ännu inte kommit ut (2022-01-27) och kan därför inte kommenteras på i den här rapporten.

Efterföljande arbetsgrupp, IST-176-RTG "Federated Interoperability of Military C2 and IoT Systems" (maj 2019 – maj 2022), hade tänkt leverera slutpresentation redan vid förra IST panelmöte (PBM) i oktober 2021, men det är uppskjutet till vårens PBM i Italien (49th PBM) i maj 2022. Det är värt att nämna att IST-176 har ett större fokus på hur införandet av FMN kan påverka hanteringen av IoT-system.

Några deltagare i arbetsgrupperna har studerat tillämpningen av Kubernetes-teknologin. Ett referat av deras utvärdering av denna följer i avsnitt 2.4.

¹⁴ Federated Mission Networking, ett initiativ för interoperabilitet mellan Natomedlemmar.

2.2 Sverige

Projektet har diskuterat med Försäkringskassan om några av de IT-tjänster som denna myndighet erbjuder och huruvida IoT-samverkan kan dra nytta av dem (avsnitt 2.2.1). Projektet har också haft en dialog med Ericsson om randteknik och interoperabilitet (avsnitt 2.2.2). Centret AI Sweden har ett labb för randteknik och detta avhandlas i avsnitt 2.2.3. Projektet har deltagit i Rakeldagen 2021 och nyheter om Rakel G2 beskrivs i avsnitt 2.2.4. I avsnitt 2.2.5 presenteras IoT Stockholm som är Stockholm stads IoT-initiativ.

2.2.1 Försäkringskassan

Sedan 2017 har Försäkringskassan haft i uppdrag regeringen att erbjuda samordnad och säker IT-drift och i dag använder sig sex myndigheter av den möjligheten och ett antal till är intresserade. 2019 tog regeringen nästa steg och gjorde klart att den också ville ha en statlig molntjänst för myndigheter på plats (Lindström, 2019). Eftersom ett datormoln är en naturlig del av IoT-system (som yta för datalagring, informationsdelning, och hantering) kan ett myndighetsmoln utgöra en viktig del i en infrastruktur för IoT-samverkan i totalförsvaret.

2019 beslutade den svenska regeringen att tillsätta en särskild utredning, IT-driftsutredningen (SOU 2021:1).¹⁵ Dess syfte är enligt hemsidan ”att skapa bättre förutsättningar för den offentliga förvaltningen att få tillgång till säker och kostnadseffektiv IT-drift genom antingen samordnad statlig IT-drift eller tydligare rättsliga förutsättningar för att kunna anlita privata leverantörer av IT-drift.”¹⁶ Ett delbetänkande med ställningstaganden i mer juridiska frågor kom i januari 2021 och slutbetänkandet i december 2021.¹⁷ Det är omfattande och fokuserar på förutsättningar och förslag på samordnad statlig IT-drift. Betänkandet redovisar bland annat en utvärdering av Försäkringskassans ovan nämnda regeringsuppdrag om samordnad och säker statlig IT-drift. Betänkandet föreslår att regeringen skall inrätta varaktiga former för samordnad statlig IT-drift samt att regeringen skall skapa mer varaktiga former för ett samordnat statligt tjänsteutbud. Målet för en samordnad statlig IT-drift skall vara ökad säkerhet och kostnadseffektivitet i statliga myndigheters IT-drift, vägen dit blir ett stegvis införande och IT-driften skall organiseras genom en samordnande myndighet och flera leverantörsmyndigheter.

¹⁵ <https://www.regeringen.se/rattsliga-dokument/statens-offentliga-utredningar/2021/01/sou-20211/> (besökt 2022-02-09)

¹⁶ <https://www.regeringen.se/pressmeddelanden/2021/12/regeringen-tar-emot-it-driftsutredningens-slutbetankande/> (besökt 2022-03-15)

¹⁷ https://www.regeringen.se/4af21e/contentassets/7dfb476c7990499f8bf194954ba460b5/sou-2021_97_webb.pdf (besökt 2022-02-09)

Betänkandet utvecklar på sidan 58 tankarna kring en statlig molntjänst: ”En statlig molntjänst skulle [...] ses som en skalbar, elastisk pool som delas mellan organisationer inom statsförvaltningen. Molntjänsten skulle kunna ägas och administreras av en eller flera av dessa myndigheter eller av en extern part, t.ex. ett privat företag. I slutbetänkandet ser vi att statliga molntjänster ingår som en del av den totala leveransen av ett samordnat statligt tjänsteutbud.” Vissa molntjänster finns redan idag och hanteras av Försäkringskassan.

Projektet hade möte med Försäkringskassan den 30 september 2021. En del av myndighetsmolnet går under namnet SAFOS (Samarbetsplattform För Offentlig sektor). SAFOS bygger på en teknologi som heter Nextcloud (som möjliggör delning av filer).¹⁸ För närvarande används SAFOS mest för fillagring men kommer under 2022 erbjuda anslutna myndigheter både chattrum och videokonferens.

Det är idag inte tekniskt möjligt för myndighetsmolnet att agera datormoln för samverkande IoT-system, men tekniken är inte låst utan möjliggör utveckling av ett sådant stöd. Myndighetsmolnet kan även komma att sammankopplas eller integreras med det myndighetsgemensamma intranätet SGSI (Swedish Government Secure Intranet, som förvaltas och utvecklas av MSB), som beskrivs i den tidigare rapporten (Johansson, Andersson, Hörning, & Kamrani, 2019, s. 19).

2.2.2 Ericsson

Relaterat till utvecklingen inom 5G har Ericsson utvecklat ett intresse för IoT och randteknik.¹⁹ Projektet hade möte med Ericsson den 20 september 2021. Intrycket är att Ericsson har identifierat flera av de utmaningar och möjligheter som även gäller IoT-samverkan. Det handlar bland annat om interoperabilitet mellan disparata system med olika ägare, inklusive möjligheten att smidigt utbyta och förstå information, sammanväga extern och intern information, samt spårbarhet (eng. provenance) av information. Ericsson lyfter också, inte oväntat, upp frågan om IT-säkerhet som viktig. Standardisering av informationsmodeller är viktigt för att nå vidare framgång och den europeiska standardiseringsorganisationen ETSI är en viktig aktör i det avseendet.²⁰

¹⁸ <https://nextcloud.com/> (besökt 2022-02-01)

¹⁹ <https://www.ericsson.com/en/edge-computing/> (besökt 2022-02-02)

²⁰ <https://www.etsi.org/> (besökt 2022-02-02)

2.2.3 AI Sweden och Edge Learning Lab

AI Sweden²¹ är ett nationellt center för tillämpad artificiell intelligens, finansierat av den svenska staten och deltagande medlemsorganisationer (i skrivande stund 117 medlemmar). Syftet med centret är att accelerera användningen av AI till nytta för det svenska samhället och näringslivets konkurrenskraft. AI Sweden har inga egna forskningspengar att dela ut men Vinnova, som är en huvudfinansiär av centret, kan tänkas finansiera relaterad forskning.

AI Sweden har en testbädd som kallas Edge Learning Lab²² (ELL). Den 15 oktober 2021 hade projektet möte med Mats Nordlund, som är grundare av centret, för att avgöra om ELL kan vara en resurs för forskning kring randteknik för IoT-samverkan. Mats Nordlund är också ledare för ”the data factory”²³ vilket är en del av AI Sweden som omfattar olika samarbetsmöjligheter för medlemmarna. En sådan möjlighet är just ELL, andra är analys av egen data, test av hårdvara, samarbete kring forskning och examensarbeten.

Under mötet framkom att ELL har utrustning för att bedriva experiment och forskning med randteknik, men att fokus ligger på en viss form av AI, nämligen ”federated learning on the edge”. Fördelen med distribuerad maskininlärning i randen är bland annat att minska datatrafik och undvika att sprida känslig data.

Även om federated learning har en plats i utvecklingen av IoT-samverkan (typiskt när fokus ligger på tolkning av sensordata och effektivt utbyte av IoT-data) är projektets nuvarande fokus att skapa en randinfrastruktur för IoT-samverkan, omfattandes bland annat formulering av IoT-tjänster och utbyte av realtidsdata. Eftersom nyttjande av ELL endast är öppet för AI Swedens medlemmar är bedömningen att vidare arbete om IoT-samverkan i dagsläget inte direkt och kostnadseffektivt kan dra nytta av de möjligheter som ELL erbjuder.

Det är dock intressant att notera att några av AI Swedens medlemmar kommer från fordonsindustrin där vehicle-to-vehicle-samverkan²⁴ (dvs. system där IoT-enheter kommunicerar direkt utan moln) är av intresse. Även för IoT-samverkan är den typen av kommunikation viktig och det kan därför bli intressant att studera relaterade resultat från AI Sweden i framtiden.

²¹ <https://ai.se/> (besökt 2022-02-07)

²² <https://www.ai.se/en/data-factory/edge-lab/> (besökt 2022-02-08)

²³ <https://ai.se/en/data-factory/> (besökt 2022-02-07)

²⁴ <https://en.wikipedia.org/wiki/Vehicle-to-everything/> (besökt 2022-02-07)

2.2.4 Rakeldagen

Rakel²⁵ står för *RA*dio*K*ommunikation för *E*ffektiv *L*edning och ”används av aktörer inom allmän säkerhet, hälsa och försvar” för säker och effektiv radiokommunikation. MSB ansvarar för drift, förvaltning och utveckling.

I en tidigare rapport (Johansson, Andersson, Hörling, & Kamrani, 2019, s. 18) diskuteras den potentiella nyttan med Rakel för IoT-samverkan genom möjligheten att säkert och trådlöst överföra IoT-data.

Rakeldagen är ett årligt arrangemang för användarna av Rakel som bland annat omfattar nyheter och användningsexempel. Rakeldagen 2021²⁶ hölls online den 5 maj.

Den stora tekniknyheten som presenterades under Rakeldagen var nästa generations Rakel, kallat Rakel G2.²⁷ Ett viktigt bidrag med Rakel G2 är utökad dataöverföringskapacitet (samma nivå som modern mobiltelefonidata), något som är en förutsättning för IoT-samverkan. Utbyggnaden av Rakel G2 påbörjas år 2023 och byggs successivt ut. Mobildatakommunikation planeras dock att finnas tillgängligt redan från den 1 september 2022. Det gamla Rakelnätet planeras att stängas ner fullständigt år 2028.

2.2.5 Stockholms stad

I april 2017 antog Stockholm stads kommunfullmäktige ”Strategi för Stockholm som smart och uppkopplad stad”.²⁸ Strategin uttrycker en vision om Stockholm som världens smartaste och mest uppkopplade stad. Mellan 2018 och 2020 drevs ett program, ”Smart och uppkopplad stad”, fokuserat bl.a. på kravställning på en central IoT-plattform. I december 2020 framlades ett utkast över en arkitektur för IoT-system i dokumentet ”Målarkitektur för IoT och dataplattform”.²⁹ Projektet

²⁵ <https://www.msb.se/sv/verktyg--tjanster/rakel/> (besökt 2022-02-09)

²⁶ <https://www.msb.se/rakeldagen2021/> (besökt 2022-02-09)

²⁷ <https://www.msb.se/sv/verktyg--tjanster/rakel/regeringsuppdrag-om-nasta-generations-rakel/> (besökt 2022-02-09)

²⁸ <https://smartstad.stockholm/wp-content/uploads/sites/10/2019/09/Bilaga-1-Strategi-for-en-smart-och-uppkopplad-stad-Stockholms-stad.pdf> (besökt 2022-02-15)

²⁹ <https://smartstad.stockholm/wp-content/uploads/sites/10/2021/05/M%C3%A5larkitektur-f%C3%B6r-IoT-och-dataplattform.pdf> (besökt 2022-02-15)

”IoT Stockholm”,³⁰ som tog över efter programmet avslutats, har därefter arbetat vidare bl.a. med en då redan inledd upphandling och etablering av plattformen.³¹

Begreppet ”plattform” används här inte i bemärkelsen fysisk plattform, utan det avser den centrala IT-infrastruktur som krävs för att hantera alla anslutna IoT-system, och data därifrån. Plattformskonceptet tar även hänsyn till att randteknik skall kunna användas för att nyttja beräkningskapacitet nära IoT-enheterna och därmed minska latensen (dvs. fördröjningen) i återkopplingsloopen från datainsamlingen i dem till reaktion på dess levererade data, samt kunna buffra och bearbeta data inför vidareförmedling av den upp till ”plattformen” där den även kan göras bredare tillgänglig.

Arkitekturen adresserar fyra områden. Den skall vara:

- en IoT- och dataarkitektur för interaktion med IoT-enheter i staden eller andra datakällor med strömmande data
- en arkitektur för delning av information från staden både inom och utanför stadens verksamheter
- en tjänsteorienterad arkitektur för att hantera förfrågningar från medborgare, företag eller mellan förvaltningar i staden och andra samhällsfunktioner för påverkan av sakerna inom staden
- erbjuda platser för interaktion mellan människor och den Smarta staden. Det kan vara portaler, appar eller likande platser för åtkomst till ovanstående förmågor på ett samlat sätt.

Projektet ”Uppkopplade Norra Djurgårdsstaden”,³² vilket är en av IoT Sweden:s ”hubbar”, har drivits sedan slutet av 2018, bl.a. tillsammans med Rise, för att till att börja med testa olika tekniska IoT-koncept, och därefter även se på organisatoriska krav för systemägare och användare. IoT-systemen som testats har varit inriktade mot resursanvändning i bostäder, övervakning av växtlighet på grönytor, användning av offentliga platser samt resvanor. Projektet var under slutrapportering i slutet av 2021.

För totalförsvarets del är troligen det intressantaste att ta del av hur arkitekturen utformas för att externa aktörer (såsom FM) skall kunna ta del av informationen, adresserat i andra och tredje punkterna ovan.

³⁰ <https://smartstad.stockholm/IoT-stockholm/> (besökt 2022-02-15)

³¹ Endast 2 av 33 ansökande parter lämnade dock anbud vid upphandlingen, men denna avbröts i november 2021 p.g.a. ett överklagande av den förlorande anbudsgivaren. Arbetet fortsätter enligt IoT Stockholms hemsida under 2022 ”med målet att ha både tekniska förutsättningar och kompetenser på plats för att påbörja etablering av IoT-tillämpningar.”

³² <https://iotsverige.se/projekt/stockholms-stad-exploateringskontoret/> (besökt 2022-02-15)

2.3 Utblick till övriga världen

Föregående projekt har fokuserat på de svenska förutsättningarna för IoT-samverkan. Det kan dock vara lärorikt att studera hur dessa frågor hanteras i andra länder. I ett begränsat försök att skapa en bättre uppfattning om vad som sker utomlands har projektet tagit hjälp av öppna informationskällor och välinformerade personliga kontakter. Resultatet är alltså knappast fullständigt, men ger ändå en viss initierad inblick i situationen. Nedan följer resultatet för Finland (avsnitt 2.3.1) och Estland (avsnitt 2.3.2).

2.3.1 Finland

I en tidigare rapport (Johansson & Hörning, 2021, s. 7) diskuteras ett Nato-experiment med IoT-samverkan som utförts i Helsingfors år 2017 då en simulerad Natostyrka inhämtade verklig data om Helsingfors trafik (genom en tjänst som heter Digitraffic³³). En sakkunnig kontaktperson hos Finnish Defence Research Agency (FDRA), som deltagit i ovan nämnda experiment, bistår med informationen nedan.

6Aika³⁴ är en portal för att stödja stadsutvecklingen i Finlands sex största städer (Helsinki/Helsingfors, Espoo/Esbo, Vantaa/Vanda, Tampere/Tammerfors, Turku/Åbo, och Oulu/Uleåborg). Inom portalen ryms beskrivningar av olika stadsutvecklingsprojekt och även projekt rörande smarta städer. Ett projekt, "The open data and interfaces spearhead project",³⁵ som avslutades 31 december 2017, utvecklade teknik för att kunna utbyta data mellan de samarbetande städerna, genom utveckling av gemensamma datamodeller, API:er och dataportaler.

Ett annat projekt, "The CityIoT project",³⁶ fokuserade på problemet med samverkan mellan separata IoT-system i en smart stad. Projektet avslutades 2020 och resulterade bland annat i en integrationsplattform för IoT-data med syfte att möjliggöra tillämpningar baserade på information från flera IoT-system. Plattformen är baserad på FIWARE³⁷ och *international data spaces*,³⁸ det sistnämnda är en referensarkitektur som stöder säkert utbyte av data.

Dessutom finns *Helsinki region infoshare* som är den finska huvudstadsregionens dataportal.³⁹ Ett hastigt besök på dataportalen tydde på att de flesta av

³³ <https://www.digitraffic.fi/en/> (besökt 2022-02-08)

³⁴ <http://6aikia.fi/en/> (besökt 2022-02-08)

³⁵ <https://6aika.fi/en/project/open-data-and-interfaces/> (besökt 2022-02-08)

³⁶ <https://www.cityiot.fi/english/> (besökt 2022-02-08)

³⁷ <https://www.fiware.org/developers/catalogue/> (besökt 2022-02-09)

³⁸ <https://internationaldataspaces.org/use/reference-architecture/> (besökt 2022-02-09)

³⁹ <https://hri.fi/sv> (besökt 2022-02-09)

de sökbara datamängderna är statiska (precis som i Stockholms dataportal). Ett undantag är dock en datamängd som gäller mätning av luftkvalitet på tretton olika platser i Helsingforsregionen. Luftmätningarna uppdateras en gång i timmen.

Slutsatsen, efter denna hastiga blick på situationen i Finland, är att landet har tagit ett tydligt steg mot en infrastruktur som stödjer IoT-samverkan.

2.3.2 Estland

Estland började tidigt, runt år 2000, bygga upp en digital infrastruktur för myndighetssamarbete och myndighetskontakter, kallat e-Estonia.⁴⁰ Estland har en liten befolkning vilket gjorde det svårt att besätta alla nödvändiga myndighetsuppgifter med personal varför landet tidigt valde att försöka automatisera mycket av offentlig verksamhet.

e-Estonia baseras på X-Road,⁴¹ vilken utvecklats i Estland och är en plattform för säkert datautbyte. Ur X-Road har X-tee⁴² utvecklats, som är ryggraden i e-Estonia, vilket sköter datatransaktioner, sökningar etc., allt med hög säkerhet (kryptering, autentisering m.m.). Finland använder också en implementation baserad på X-Road, kallad ”Finnish National Data Exchange Layer”, och det går att få dess system att samarbeta i en federation, vilket görs mellan Estland och Finland sedan 2018 vilket kraftigt underlättar datautbyte. Den estniska delen ingår i ”Estonian Government Cloud”⁴³ där bl.a. Telia (operations, cloud related products and services) och Ericsson (project management, hardware and software) ingår som parter i det konsortium som byggt upp infrastrukturen.

För att öka säkerheten i sina datalager replikeras dem, förutom till en plats utanför Tallinn, även till datacenter hos ”dataambassader”⁴⁴ i andra vänligt sinnade länder (Luxemburg i detta fall; det verkar kunna bli flera länder). Datan ägs dock fortfarande av Estland. Dataambassaderna är under diplomatisk immunitet, lyder under Wienkonventionen och har samma skydd som en fysisk ambassad, vilket är ett helt nytt koncept.

Bland annat som konsekvens av IT-attackerna 2007 mot Estland anlades ”NATO Cooperative Cyber Defence Centre of Excellence” (CCDCoE) och ”the

⁴⁰ <https://e-estonia.com/> (besökt 2022-02-09)

⁴¹ <https://x-road.global/> (besökt 2022-02-09)

⁴² <https://www.ria.ee/en/state-information-system/x-tee.html> (besökt 2022-02-09)

⁴³ <https://e-estonia.com/solutions/e-governance/government-cloud/> (besökt 2022-03-15)

⁴⁴ <https://e-estonia.com/solutions/e-governance/data-embassy/> (besökt 2022-02-09)

European IT agency” i Estland. KSI⁴⁵ (utvecklat i Estland) blockkedjor används för att upprätthålla säkerhet inom molnet och vid transaktioner mot det.

Världsbanksgruppen har bland annat 2017 skrivit om ett antal länders, inklusive Estlands, IoT-satsningar (World Bank Group, 2017). Bland annat hänvisas till ett estniskt regeringsdokument (Estonian Ministry of Economic Affairs and Communications, 2018). Om IoT skriver gruppen dock på sid. 53 att IoT-användningen stött på flera hinder, även om det här främst är den privata sektorn som adresseras snarare än myndigheter:

“The adoption of digital solutions including IoT-based solutions within the private sector continues to be low. Issues such as lack of knowledge and awareness, inadequate government support and incentives, and infrastructure availability despite the presence of new solutions (for example, LPWANs) are seen as barriers for industry participation. The value chain of IoT provisioning is also seen as very complicated, with very few clear business models around them. The part of the value chain that has the highest entry barrier is network availability. Estonian telecom operators currently seem to favour closed value chains.”

Den brokiga floran av IoT-system (vid dokumentets tillkomst 2017) underlättar alltså inte heller större satsningar på IoT i Estland.

2.4 Kubernetes – teknik för randen

Kubernetes⁴⁶ är ett av flera öppna ramverk för att samordna exekverande applikationer som körs paketerade i så kallade ”containrar”,⁴⁷ såsom Docker.⁴⁸ Containrar är typiskt ”lightweight” och delar den maskins operativsystem (OS) och kärna de kör på vilket ökar effektiviteten, till skillnad från virtuella maskiner som var och en har ett eget OS som dess applikationer körs på. Detta gör att flera instanser av samma (eller olika) OS körs på samma fysiska maskin. Container-lösningar kan sägas vara det tredje utvecklingssteget efter 1) fysiska servrar och 2) flera virtuella miljöer i samma server. Varje steg innebär att serverns resurser kan utnyttjas än bättre. De enskilda applikationerna som paketeras i containrarna kan i Kubernetes köras isolerade från varandra, med egna logiska filsystem, enkelt startas upp, övervakas, och stängas ned (Kubernetes kan även identifiera

⁴⁵ <https://e-estonia.com/solutions/security-and-safety/ksi-blockchain/> (besökt 2022-02-09)

⁴⁶ <https://kubernetes.io/docs/concepts/overview/what-is-kubernetes/> (besökt 2022-02-09)

⁴⁷ En container är ett programvarupaket som inkapslar koden för en applikation tillsammans med nödvändiga konfigurationsfiler och programbibliotek med mera som krävs för att köra applikationen. Fördelen med detta är att containern/applikationen lätt kan överföras till och köras hos olika mottagare utan installationsproblem.

⁴⁸ <https://www.docker.com/> (besökt 2022-02-09)

dåligt responderande containrar och starta om dem) samt är portabla till andra containerlösningar. De kan köras lokalt, i ”randen”,⁴⁹ eller högre upp i molnmiljön. De kan kommunicera via sina tilldelade DNS-namn eller IP-adresser. Det som skapas är ett lokaliserat eller distribuerat kluster av fysiska (eller virtuella) maskiner, ”noder”, med containrarna som arbetsprocesser. En, eller flera grupper av, containrar körs i sin tur på en nod i form av en så kallad Kubernetes ”pod” som är Kubernetes sätt att, enligt en speciell tillhörande beskrivning i markupspråket `yaml`,⁵⁰ styra en container eller en grupp av containrar som kör applikationer i nära samarbete i en pod.

Kubernetes – ofta förkortat k8s – är främst avsett för större kluster eller molnlösningar där hög och pålitlig bandbredd råder mellan ingående noder. I fallet med randteknik råder ofta inte detta förhållande, varför andra implementationer av Kuberneteskonceptet finns, såsom k3s^{51,52} (”Lightweight Kubernetes”), KubeEdge⁵³ och OpenShift.⁵⁴ Här har en del icke nödvändig kod, anpassad för större Kuberneteskluster, skalats bort för att den bantade versionen skall kunna exekvera även i randen, och kommunicera med varandra och även med ett mer centraliserat moln. En intressant jämförelse mellan några av de olika implementationerna vad gäller förmåga vid låg eller opålitlig bandbredd mellan noder, som ju ofta råder vid randen presenteras i ett arbete benämnt ”Adaptive information processing and distribution to support Command and Control” från arbetsgrupp NATO STO IST-168 (Fogli, o.a., 2021).

Då dessa nerskalade Kubernetesmodeller är avsedda att kunna samordna exekveringen av applikationer vid randen, där IoT-enheter oftast befinner sig, är detta ett tilltalande koncept för att sköta hanteringen av applikationerna. Då kan dataanalys och fusion utföras mellan IoT-enheter, maskininlärning etc. för att möjliggöra randens fördelar i form av snabb återkoppling utan att behöva gå via molnet, något som vara försvårat vid låg eller opålitlig bandbredd.

⁴⁹ Randen eller ”edge” förklaras i avsnitt 1.1.

⁵⁰ Yet Another Markup Language

⁵¹ <https://k3s.io/> (besökt 2022-02-09)

⁵² <https://more.suse.com/rs/937-DCH-261/images/ARM-White-Paper-V3.pdf> (besökt 2022-02-09)

⁵³ <https://kubedge.io/> (besökt 2022-02-09)

⁵⁴ <https://www.redhat.com/en/technologies/cloud-computing/openshift/edge-computing/> (besökt 2022-02-09)

3 Lägesbilsarbete

En potentiell nytta med IoT-samverkan är som stöd till deltagande aktörers respektive egna lägesbilder och eventuell gemensam eller samlad lägesbild.⁵⁵ I en tidigare rapport (Johansson & Hörling, 2021) diskuterades Stockholmsregionens operatörskluster, vilket är en operativ verksamhet, och dess lämplighet för att kunna illustrera och vidare undersöka IoT-samverkan i praktiken. För att vidare undersöka denna möjlighet har projektet haft möte med Länsstyrelsen i Stockholmsregionen. På grund av den då rådande viruspandemin (Covid-19) har dock operatörsklustret varit stängt under projektperioden och det har därför inte gått att besöka klustret.

3.1 Länsstyrelsen om operatörsklustret

Ett möte med Länsstyrelsen genomfördes den 24 november 2021. Vid mötet framkom följande fakta och slutsatser:

Ett antal myndigheter och kommuner i Stockholmsregionen samarbetar sedan 2015 inom ett forum kallat ”Samverkan Stockholmsregionen”. I slutet av 2021 deltog 37 aktörer (exempelvis Trafikverket, Kustbevakningen, Brandförsvaret, Försvarsmakten, och länets kommuner) för att erhålla en ökad gemensam förmåga att hantera samhällsstörningar och kriser i Stockholmsregionen. Förmågan skall upprätthållas genom bland annat gemensam målbild, arbetssätt, finansiering, och ändamålsenliga samverkanslokaler.

Vid upplevt behov av aktiverad regional samverkan kontaktas Länsstyrelsens ”tjänsteman i beredskap” som kallar till regional samverkanskonferens (via telefon, Rakel och/eller fysiskt möte i en så kallad samverkansstab) och är mötesvärd.

Konferenserna inriktas av en regional samverkanskoordinator och följer en överenskommen agenda. Mötet sammanställs i en regional lägesbild som distribueras i MSB:s webbaserade informationssystem⁵⁶ (WIS) för krishantering.

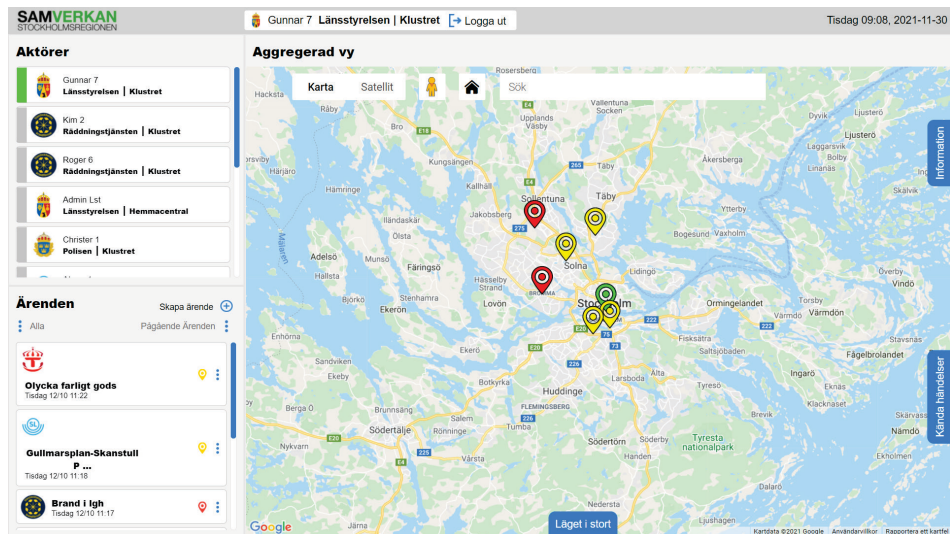
Arbete sker i två beredskapslägen; ”ordinarie läge” och ”aktiverat läge”. Vid aktiverat läge deltar bland annat en representant från Försvarsmakten.

Fysiskt samverkar aktörernas representanter i en samverkanslokal, ”Operatörsklustret”, där närvarande aktörer har tillgång till sin egen lägesbild, samt verbal kontakt med varandra. Stöd för den samlade lägesbilden finns i form av IT-verktyget ”Virtuell SamverkansPlattform” (VSP) där olika ärenden med olika prioritet kan läggas in på en karta som visar en aggregerad vy över ärenden

⁵⁵ Samlad respektive gemensam lägesbild diskuteras av Johansson och Hörling (2021, s. 15).

⁵⁶ WIS beskrivs i en tidigare rapport (Johansson, Andersson, Hörling, & Kamrani, 2019, s. 19).

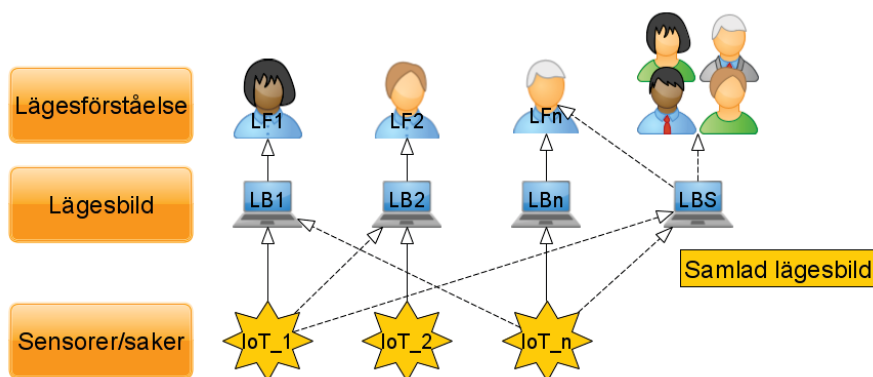
(Figur 3).



Figur 3. Den virtuella samverkansplattformen har ett grafiskt gränssnitt som möjliggör att operatörsklustrets deltagande aktörer kan registrera ärenden i en aggregerad vy som är tillgänglig för alla myndigheter. Bilden är publicerad med tillåtelse av Länsstyrelsen i Stockholmsregionen.

I VSP:n finns en lista över anslutna aktörer (i övre vänstra hörnet i figuren) och en lista över de aktuella ärenden som aktörerna registrerat för att informera (i nedre vänstra hörnet). Användargränssnittet domineras av kartbilden, den ”aggregerade vyn”, där ärendenas fysiska position och prioritet (i färgkod) framgår för samtliga aktörers representanter.

I det tidigare arbetet illustrerades på en översiktlig nivå hur IoT-samverkan skulle kunna realiseras i operatörsklustret (Johansson & Hörling, 2021, s. 30); enkelt uttryckt att aktörerna har åtkomst till varandras IoT-system samt att samtliga IoT-system kan bidra till den samlade lägesbilden. Idén visualiseras i Figur 4.



Figur 4. I samverkansmodellen har varje aktör sin egen lägesbild (exempelvis LB1) och lägesförståelse (exempelvis LF1). Varje aktör har också en egen uppsättning med nätverkande informationskällor (exempelvis IoT_1). Av effektivitetsskäl kan en aktör vilja ha direkt tillgång till information från sensorer som tillhör andra aktörer. Det skulle säkerligen kunna finnas fler informationsflödespilar i bilden, men det skulle innebära att figuren förlorar i läsförståelse. Bilden kommer ursprungligen från den föregående rapporten (Johansson & Hörling, 2021).

Länsstyrelsens representanter såg inte några direkta hinder för upplägget i Figur 4, men nödvändiga tekniska lösningar, berörda aktörers acceptans, och inte minst juridiska frågor behöver också övervägas och dessa diskuterades inte under det genomförda mötet.

VSP:n förefaller erbjuda en naturlig miljö för IoT-samverkan. I operatörsklustret är aktörernas lägesbilder dock inte direkt sammankopplade, utan kunskap om de individuella lägesbilderna överförs manuellt av representanterna, vilket möjliggör stor kontroll ("human in the loop") över den information som förs in i VSP:n men försvårar IoT-samverkan, då IoT-samverkan kräver tillgång till IoT-data i ett tempo och omfattning som en mänsklig operatör inte kan hantera.

VSP-mjukvaran i sig verkar dock tillåta att inhämtad IoT-data och delbara IoT-tjänster⁵⁷ automatiskt registreras i VSP:n. Detta skulle potentiellt möjliggöra för en aktör att, förutom de aktiva ärendena, se vilka IoT-tjänster (exempelvis en kamerabestyckad UAV) som erbjuds av andra aktörer och vilken information de kan erbjuda (exempelvis fotografier över ett visst område). Varje aktör måste dock acceptera att dela IoT-data på detta sätt, utan ständig inblandning av aktörens representant i operatörsklustret.

⁵⁷ I tidigare arbete (Johansson & Hörling, 2021, s. 20) diskuteras möjligheten att aktörers IoT-system erbjuder "tjänster" till andra aktörer (dvs. möjligheten att inhämta data med hjälp av andra aktörers IoT-system) som en central del av IoT-samverkan.

4 Slutsatser och vidare arbete

Projektets två övergripande mål (avsnitt 1.2) är att ”Följa den tekniska och samhälleliga utvecklingen (främst i Sverige) rörande samverkande IoT-system” (Delmål 1: omvärldsbevakning) och ”Undersöka vidare hur arbetet med lägesbild går till i Stockholmsregionens operatörskluster” (Delmål 2: lägesbilsarbete). Slutsatser för Delmål 1 återfinns i avsnitt 4.1 och för Delmål 2 i avsnitt 4.2. I avsnitt 4.3 erbjuds förslag på vidare arbete.

4.1 Omvärldsbevakning

Kubernetes är ett open-source ramverk för att samordna exekverande applikationer. Flera varianter inriktade mot att användas för randteknik finns, exempelvis KubeEdge. Natogruppen IST-168 har studerat dessa med avseende på nyttan inom militära koalitioner. Dessa teknologier förefaller ha potential att realisera även IoT-tjänster i IoT-samverkan.

Det är intressant att notera att Stockholm stads projekt, IoT Stockholm, ämnar realisera en plattform för att tillgängliggöra IoT-data. En sådan plattform har potential att bli en resurs i exempelvis operatörsklustret. I Helsingfors verkar dessutom arbetet med en IoT-plattform ha kommit ännu längre och lärorika konkreta tillämpningar kan tänkas uppstå med tiden.

Standardmodellen för IoT-system omfattar en molnlösning som lagrar och förädlar data. För att IoT-samverkan för FM och totalförsvaret skall kunna realiseras behöver den använda molnlösningen vara säker. En kandidat för en sådan molnlösning är det så kallade ”Myndighetsmolnet” som är en IT-tjänstplattform under utveckling och som hittills drivits av Försäkringskassan. Myndighetsmolnet stödjer inte strömmande IoT-data idag, men skulle kunna göra det i framtiden enligt Försäkringskassan.

IoT-samverkan för totalförsvaret innebär i de flesta konkreta fall ett behov av att samverka med trådlös kommunikation. Det är naturligt att överväga att nyttja Rakel för att bära den trådlösa kommunikationen för IoT-samverkan. Den nuvarande Rakeltekniken har dock en bandbredd som är otillräcklig för IoT-tillämpningar, men kommer under 2022 få utökad dataöverföringskapacitet till samma nivå som modern mobiltelefonidata.

4.2 Lägesbilsarbete

Projektet har samtalat med Länsstyrelsen såsom representanter för Stockholmsregionens operatörskluster. Tyvärr har operatörsklustrets verksamhet haft uppehåll under pandemin och projektet har varken kunnat besöka klustret eller få till stånd möten med andra deltagande aktörer än Länsstyrelsen (dvs. inte heller

Försvarmakten). Därför har inga nya insikter om aktörsspecifika lägesbilda-behov kunnat erhållas under projektets gång.

Av samtalen med Länsstyrelsen framgår att det digitala verktyget VSP (Virtuell SamverkansPlattform, se Figur 3) är av central betydelse för samverkan i operatörsklustret. VSP:n innehåller och visualiserar de ärenden som de deltagande aktörerna matat in och utgör operatörsklustrets samlade lägesbild. Projektets bedömning är att operatörsklustret och VSP:n utgör en lämplig miljö för att experimentera med och demonstrera IoT-samverkan. Ett steg i riktningen att konkretisera IoT-samverkan är att dra nytta av IoT Stockholms plattform (se avsnitt 2.2.5) när den blir tillgänglig.

4.3 Förslag på vidare arbete

Några förslag på vidare arbete baserat på de resultat och slutsatser som presenteras här (och i tidigare rapporter) är:

1. **Försvarmaktens lägesbild:** Intervjua FM:s representant i Stockholms-regionens operatörskluster om vilken information (primärt från IoT-system) som kan stödja FM:s lägesbild, och eventuellt vilka externa resurser FM vill kunna styra.
2. **Försvarmaktens lägesbild (fördjupning):** Hur hanteras lämpligen extern IoT-data i den militära lägesbilden? Hur hanteras osäker information? Krävs en intern lägesbild och en separat lägesbild som påbyggs med extern IoT-data?
3. **Tekniska experiment:** Införskaffa IoT-utrustning för att experimentera med en enkel IoT-tjänst i randen. Experimenten skall erbjuda djupare insikt om möjligheter och begränsningar med utrustningen.
4. **Metodutveckling i IoT-samverkan:** Hur vill aktörerna i operatörsklustret använda egen och extern IoT-data, och i vilken utsträckning ska andra aktörers tillgång till den interna datan begränsas?
5. **Följa utvecklingen av förutsättningarna för IoT-samverkan:** Hur kan exempelvis Stockholm IoT:s plattform, Rakel, Myndighetsmolnet och SGSI användas för IoT-samverkan?
6. **Samarbete med Ericsson:** Kontakter har inletts med Ericsson och många gemensamma frågor kring utbyte av IoT-data finns, exempelvis rörande interoperabilitet och hantering av extern information.

Litteraturförteckning

- Bengtsson, J., & Mickelsson, L. (2021). *Svenska smarta städer - en explorativ studie om förväntad nytta och potentiella sårbarheter*. FOI-R--5117--SE.
- Estonian Ministry of Economic Affairs and Communications. (2018). *Digital Agenda 2020 for Estonia*. Hämtat från https://wp.itl.ee/files/DigitalAgenda2020_Estonia_ENG.pdf den 15 maj 2022
- Fogli, M., Kudla, T., Musters, B., Pingen, G., van den Broek, C., Bastiaansen, H., . . . Webb, S. (2021). Performance evaluation of Kubernetes distributions (K8s, K3s, KubeEdge) in an adaptive and federated cloud infrastructure for disadvantaged technical networks. *Proceedings of the 2021 international conference on military communication and information systems (ICMCIS)*.
- Johansson, R. (2018). *Försvarsmakten i den civila IoT-miljön*. FOI Memo 6641.
- Johansson, R., & Hörling, P. (2021). *Samverkande IoT-system och lägesbild*. FOI-R--5029--SE.
- Johansson, R., Andersson, M., Hörling, P., & Kamrani, F. (2019). *Samverkande IoT-system och databearbetning*. FOI-R--4884--SE.
- Lindström, K. (den 30 september 2019). Regeringen har bestämt sig – Sverige ska ha ett statligt moln. *Computer Sweden*. Hämtat från <https://computersweden.idg.se/2.2683/1.724249/regeringen-sverige-statligt-moln/> den 16 mars 2022
- Malmqvist, M. (den 30 augusti 2019). Smarta elmätare och uppkopplade bilar lyfter IoT-marknaden. *Computer Sweden*. Hämtat från <https://computersweden.idg.se/2.2683/1.722749/smarta-elmatare-bilar-boostar-iot> den 16 mars 2022
- MSB. (2018). *Gemensamma grunder för samverkan och ledning vid samhällsstörningar*. MSB777. Hämtat från <https://rib.msb.se/filer/pdf/28738.pdf> den 10 januari 2021
- World Bank Group. (2017). *Internet of Things – The New Government to Business Platform – A Review of Opportunities, Practices and Challenges*. Hämtat från <https://documents1.worldbank.org/curated/en/610081509689089303/pdf/120876-REVISED-WP-PUBLIC-Internet-of-Things-Report.pdf> den 9 februari 2022

FOI är en huvudsakligen uppdragsfinansierad myndighet under Försvarsdepartementet. Kärnverksamheten är forskning, metod- och teknikutveckling till nytta för försvar och säkerhet. Organisationen har cirka 1000 anställda varav ungefär 800 är forskare. Detta gör organisationen till Sveriges största forskningsinstitut. FOI ger kunderna tillgång till ledande expertis inom ett stort antal tillämpningsområden såsom säkerhetspolitiska studier och analyser inom försvar och säkerhet, bedömning av olika typer av hot, system för ledning och hantering av kriser, skydd mot och hantering av farliga ämnen, IT-säkerhet och nya sensorers möjligheter.



FOI
Totalförsvarets forskningsinstitut
164 90 Stockholm

Tel: 08-55 50 30 00
Fax: 08-55 50 31 00

www.foi.se