Samverkande IoT-system och lägesbild

Ronnie Johansson (redaktör),
Pontus Hörling, Farzad Kamrani

FOI-R--5029--SE

Februari 2021

FOI

Ronnie Johansson (redaktör),
Pontus Hörling, Farzad Kamrani

Samverkande IoT-system och lägesbild

Titel	Samverkande IoT-system och lägesbild
Title	Collaborative IoT Systems and Common Operational Picture
Rapportnr/Report no	FOI-R--5029--SE
Månad/Month	Februari
Utgivningsår/Year Antal sidor/Pages	2021 43
ISSN	1650-1942
Kund/Customer	Försvarets materielverk
Forskningsområde FoT-område	Ledningsteknologi Inget FoT-område
Projektnr/Project no	E64177
Godkänd av/Approved by	Lars Höstbeck
Ansvarig avdelning	Försvarsteknik

Bild/Cover: shutterstock / Sergey Nivens

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 tekniska utvecklingen, bland annat i form av telekommunikation med hög bandbredd och miniatyriserad energisnål elektronik, stimulerar investeringar i IoT-system (Internet of things/”Sakernas internet”) och framväxten av fenomen som ”smarta städer” och ”smarta bilar.” Förväntningen är att en ökad tillgång på (relevant) data skall möjliggöra uppföljning och effektivisering av existerande verksamhet och skapandet av helt nya tjänster. Samtidigt finns det en potential i att IoT-system som primärt är utvecklat för ett visst syfte kan komma till användning i en helt annan verksamhet, exempelvis för samverkan vid samhällskriser. Särskilt myndigheter kan tänkas vara benägna att samverka kring IoT-system.

I föregående arbete fokuserades på framväxande civila IoT-system, men i det här arbetet tas ett steg närmare nyttan för Försvarsmakten genom att undersöka hur FM skulle kunna förstärka sin lägesbild med hjälp av offentliga IoT-system. MSB:s modell för lägesbildsarbete och hur den har tillämpats i Stockholmsregionen studeras, samt dess relevans för Försvarsmakten diskuteras. De tekniska lösningar en arbetsgrupp inom Nato har använt för att förstärka den militära lägesbilden i samverkan med en smart stad studeras också och nyttan med dessa lösningar för att möjliggöra IoT-samverkan i syfte att förstärka Försvarsmaktens lägesbild diskuteras.

Nyckelord: Internet of Things, IoT, Lägesbild, Nato

Summary

Technological developments, including in the form of high-bandwidth telecommunications and miniaturized energy-efficient electronics, stimulate investment in IoT (Internet of Things) systems and the emergence of phenomena such as "smart cities" and "smart cars." The expectation is that an increased access to (relevant) data will enable monitoring and optimization of existing activities and the creation of completely new services. At the same time, there is potential in IoT systems that have been designed for a specific purpose to be used for other purposes than the originally intended, for example for collaboration in societal crises. Authorities, in particular, may be inclined to collaborate on IoT systems.

In previous work, the focus was on the emerging public IoT systems, but in this work, the benefits for the Swedish Armed Forces (SwAF) are approached by examining how SwAF could strengthen its position with the help of public IoT systems.

A proposed model for collaboratively developing situation pictures and how it has been applied to crisis management in the Stockholm region is studied, and its relevance to SwAF is discussed. The technical solutions of a working group within NATO has been used for utilizing smart cities to strengthen the military situation pictures is studied and the benefits of these solutions to enable IoT collaboration to strengthen the SwAF's situation picture are discussed.

Keywords: Internet of Things, IoT, Common Operational Picture, NATO

Innehållsförteckning

1 Inledning

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

Den här typen av teknik och tillämpning kallas ofta *sakernas internet* (eng. Internet of things, IoT) och har många tillämpningar (kap. 3, Johansson, 2018) exempelvis i hem (för övervakning och energieffektivitet), på den mänskliga kroppen (för att mäta hälsa), i industriprocesser (för optimering av process och underhåll), och offentlig stadsmiljö/”smart stad” (för mätning av luftföroreningar, trafikoptimering, med mera). Intresset för IoT väntas dessutom öka i och med 5G-teknikens introduktion under början av 2020-talet vilken möjliggör större och snabbare dataflöden samt fler uppkopplade sensorer.

Ett användningsfall som är relevant för Försvarsmakten (FM) presenteras av den Nato-arbetsgrupp som återkommande hänvisas till i den här rapporten (Johnsen, o.a., 2018). Användningsfallet omfattar en militär styrka som gör en insats i en smart IoT-uppkopplad stad och erhåller bland annat uppgifter om fordonstrafikförhållanden för att förbättra styrkans lägesinformation.[1] Det föreslagna systemet skapar samverkan med IoT-system i en smart stad, och är implementerat och demonstrerat i Helsingfors år 2017 med visserligen simulerade militära styrkor men med åtkomst till faktiska IoT-system bland annat för trafikinformation. En generell princip som arbetsgruppen framhåller är att den smarta stadens IoT-system erbjuder en annars ej tillgänglig inblick i läget på insatsplatsen och en förbättrad lägesbild för den militära styrkan när den smarta stadens lokala information fusioneras med militär data (Pradhan, o.a., 2018).

I detta arbete undersöks möjligheterna att på liknande sätt som Nato-arbetsgruppen nyttja externa IoT-system, men i ett svenskt sammanhang. I tidigare projekt (Johansson, o.a., 2019; Johansson, 2018) studerades 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). I det här projektet tas arbetet vidare genom att undersöka hur svenska myndigheter kan samverka om lägesinformation samt genom vad som kan läras av den nämnda Nato-arbetsgruppens omfattande arbete.

[1] Annan information av intresse skulle kunna röra pågående kriser som eldsvådor och andra risker.

1.1 Bakgrund

Internet of things (IoT), eller sakernas internet på svenska, handlar i korta drag om att koppla upp saker (*IoT-enheter*) i den fysiska världen och förankra dem i cybervärlden, i ”molnet”, med information om exempelvis sakernas placering, status och sensormätvärden. Därigenom finns möjlighet att dels få en överblick över resurser och den mätta delen av den fysiska världen, dels få ett kvantifierbart beslutsunderlag.

Det finns just nu ett stort intresse både hos kommersiella och offentliga aktörer att införskaffa *IoT-system* (innehållandes IoT-enheter, nödvändig kommunikationsutrustning, eventuellt databaser för loggar och databuffrar, edge-enheter, säkerhetslösningar, med mera) en utveckling som förväntas öka i och med lanseringen av den femte generationens mobiltelefoninät (5G) som bland annat tillåter snabbare dataöverföring och mer tillförlitlig uppkoppling. Resultatet blir en gradvis växande *IoT-miljö* bestående av olika privata och offentliga IoT-system för olika tillämpningsområden.
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.[2]

Avancerade övervakningssystem finns redan idag, men är oftast inte att karaktärisera såsom hörande till IoT-världen. De är ofta stuprörsformade och har informationshanterings- och presentationssystem som är specialutformade, ofta från samma leverantör, även om internet mycket väl kan användas för datatransporten.[3] Det är troligt att sådana system kommer att hänga med länge än för mer fasta övervakningsinstallationer, men den flexibilitet som IoT innebär för övervakning som behöver skapas snabbt, ad-hoc, och situationsanpassat gör att IoT-anpassade system kan vara att föredra. Tidskritisk information kan även behöva överföras trådlöst direkt till personal ute på fältet i ett krisområde utan att behöva gå via en ledningscentral.

IoT-enheter och andra källor levererar i dessa system information om en händelse eller situation av intresse som efter eventuell bearbetning och sammanställning utgör den tillgängliga *lägesinformationen* om en situation. Lägesinformationen kan sedan presenteras på ett operatörsanpassat sätt beroende på operatörens ansvarsområde och rättigheter. Lägesinformationen uttryckt med

[2] https://iotsverige.se/projekt/lunds-kommun-malmo-stad (besökt 2020-11-30)

[3] Det handlar då snarare om ett Intranet of Things där IoT-idén används internt i en organisation eller industri. En analys av IoT:s framtid, framför allt för styrsystem, görs i (Hedtjärn Swaling & Malmberg Andersson, 2018) där man skiljer mellan en framtid där IoT-system främst nyttjas i ”Silos” (inom ett intranet) där kommunikation mellan Silos sker på internet enligt reglerade överenskommelser resp. IoT som nyttjas i ett öppet ”Mesh” (idealt ett obegränsat nätverk på internet).

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 den närmast underliggande informationen.

Totalförsvaret har behov av aktuell information från olika områden eller situationer för effektivt beslutsfattande, vare sig 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 man avser göra detta i kan vara mer eller mindre svårarbetat. Det kan bero på en naturkatastrof som försvårat framkomligheten och skadat byggnader, eller en civil eller militär konflikt som gjort området farligt att beträda.

Begreppet *IoT-samverkan* används precis som i den föregående rapporten (Johansson, o.a., 2019). *Samverkan* definieras som följer i (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 ställdon.[4]

1.2 Syfte och avgränsningar

Det övergripande syftet med projektet är att på sikt öka *FM:s förmåga att dra nytta av den framväxande civila IoT-miljön för att förstärka den militära lägesbilden* (det är projektets 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 FM i totalförsvaret för att förbättra lägesbilden*.

[4] 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.

Arbetet består av två delmål:

1. Omvärld: Studie av befintliga arbeten på området IoT-samverkan

2. Lägesbild: Utredning av hur IoT-samverkan påverkar lägesbilden

Del 1, benämnd Omvärld, omfattar främst tekniska lösningar från ett Nato-projekt vars rapporter studerats under projektets gång.[5] Arbetet innefattade att identifiera vilka problem inom området som är lösta och vilka som kan vara av intresse att undersöka vidare för att realisera måltillämpningen.

I del 2, benämnd Lägesbild, utreddes hur IoT-samverkan kan påverka arbetet med att skapa och underhålla en lägesbild. Ett relevant sätt att beskriva lägesbild eftersöktes och hur arbetet idag sker med den. MSB:s modell för att arbeta med lägesbild användes och konkretiseras med hjälp av erfarenheterna från Stockholmsregionen där FM är en deltagare.

IoT-system, och särskilt när det handlar om system av samverkande system, är i sin helhet mycket komplext och bara delar av problemområdet behandlas i den här rapporten. Fokus ligger på tekniska frågor kring uppkoppling och interoperabilitet mellan IoT-system, men etiska och juridiska frågor, exempelvis, behandlas inte.

1.3 Metod

Det utförda arbetet har en *explorativ* ansats,[6] både vad det gäller delmålen Omvärld och Lägesbild. Tid har exempelvis inte avsatts för en uttömmande sökning efter relevant litteratur och en fullständig beskrivning av området eftersträvas inte. Arbetet är istället fokuserat på intressanta uppslag som framkommit i de föregående projekten för att i detta projekt bilda en fördjupad uppfattning om utsikterna att skapa en förbättrad lägesbild med hjälp av civila IoT-system.

Avseende studien av tidigare arbeten (delmål Omvärld) så finns sedan föregående projekt (Johansson, o.a., 2019) kännedom om ett par starkt relaterade och till synes heltäckande arbeten (en EU- och en Nato-arbetsgrupp) om IoT-samverkan. I slutändan kom fokus att hamna på Nato-projektet (resultatet redovisas i kapitel 2). Baserat på studien lyftes de tekniska lösningarna av intresse från Nato-arbetsgruppen (avsnitt 4.2) fram.

Gällande delmål Lägesbild så användes MSB:s modell för arbete med lägesbilder, som Stockholmsregionen realiserat (detta presenteras i kapitel 2 och diskuteras i avsnitt 4.1).

[5] En större undersökning av tillgänglig forskningslitteratur skedde redan i det föregående projektet (Johansson, o.a., 2019) där intresse för Nato-projektet väcktes.

[6] https://www.formpl.us/blog/exploratory-research (besökt 2020-11-29)

En kompletterande del av omvärldsbevakningen har, i likhet med det föregående projektet under 2019, varit att följa IoT-utvecklingen (och relaterade faktorer som 5G-introduktionen och myndigheternas digitalisering) i samhället och världen. DIGG[7] och Länsstyrelsen i Stockholm har kontaktats och projektet har deltagit i ”Arbetsgrupp Standarder och teknisk plattform” inom ramen för det Vinnova-sponsrade strategiska innovationsprogrammet IoT Sverige.[8] 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 det offentliga (exempelvis Sveriges kommuner och regioner, RISE, samt Post- och telestyrelsen) och industrin (exempelvis Microsoft). Projektet har även, av ett annat projekt, engagerats som expertstöd åt FHS angående så kallad *edge-teknik* i arbetet med ”Teknisk prognos 2020”.

Projektet deltog i en konferens, 3rd-annual Baltic Sea Region 5G ecosystem forum.[9] Intressant att notera från konferensen är föredrag om 5G-användning både för norska och lettiska försvaret.

1.4 Relaterat arbete

Det nu rapporterade arbetet föregås av ett par andra studier vid FOI, (Johansson, 2018) och (Johansson, o.a., 2019), och är en direkt fortsättning på dessa. Andra FOI-arbeten relaterade till IoT-system har fokuserat på IT-säkerhet (Kamrani, Wedlin, & Rodhe, 2016) samt elektromagnetisk kompabilitet (Wiklundh & Stenumgaard, 2018).

FOI deltog under åren 2014-2016 i det FMV-stödda Eda-projektet IN-4-STARS2.0 som handlade om militär IoT i internationella insatser (Horndahl, o.a., 2016).

FOI genomförde en studie kallad TOppS[10] inom ett snarlikt område redan 2007-2009 (Garcia Lozano, Sigray, o.a., 2009; Garcia Lozano, o.a., 2009) kring hur små sensorer skulle kunna placeras ut i ett krisområde eller krigszon och spontant koppla upp sig mot varandra och gentemot en ledningscentral för att snabbt kunna etablera en tillfällig infrastruktur för informationsinsamling. Studien var inspirerad av den satsning LedSystT som då under närmare åtta år genomförts av

[7] Myndigheten för digital förvaltning, https://www.digg.se

[8] IoT Sverige (https://iotsverige.se) startade 2014 och är ett av ett tiotal så kallade strategiska innovationsprogram gemensamt finansierade av Vinnova, Energimyndigheten och Formas. ”IoT Sverige finansierar innovationsprojekt som sker i samverkan mellan offentlig sektor, som är programmets huvudsakliga behovsägare, och företag, akademi/institut och civilsamhället.”

[9] Konferensen var uppkopplad och organiserades från Lettlands huvudstad Riga och hölls 11 och 12 november 2020. https://www.5gtechritory.com (besökt 2020-11-29)

[10] Tjänstebaserat Opportunistiskt Sensornätverk

FM och FMV inom konceptet NBF[11] och dess fokus på tjänsteorienterade arkitekturer SOA.[12] Resultatet av denna satsning lades därefter till stor del i malpåse (Arnoldsson, 2010), men TOppS studerade åtskilliga koncept som sedermera dök upp inom IoT-världen. Erfarenheterna från TOppS, bland annat tjänstekonceptet och opportunistisk samverkan, kan bli användbara vid framtida studier av tjänster för IoT-system.

1.5 Läsanvisningar

I kapitel 2 diskuteras begreppet lägesbild och där redovisas MSB:s syn på detta ämne och hur MSB:s modell tillämpas i praktiken i Stockholmsregionen.

Nato-arbetsgruppen NATO STO IST-147-RTG har i en serie arbeten redovisat sina resultat rörande militär användning av IoT-system. Gruppens arbete och resultat sammanfattas i kapitel 3.

I kapitel 4 diskuteras relevansen av det lägesbildsarbete som beskrivs i kapitel 2 och några av de teknikerna som presenteras i kapitel 3, och i kapitel 5 lyfts de viktigaste slutsatserna fram och vidare arbete föreslås.

Rapporten innehåller många förkortningar och en lättillgänglig ordlista finns i bilaga 1. Bilaga 2, slutligen, erbjuder en fördjupad diskussion om lägesbilder.

Notera den flitiga användningen av fotnoter i den här rapporten för att erbjuda förtydliganden och hänvisning av den intresserade läsaren till fördjupad läsning.

1.6 Tackord

FOI-kollegorna Peter Hammar och Lars-Åke Hansson tackas, samt företrädarna för de externa organisationer som stöttat arbetet med rapporten.

[11] NätverksBaserat Försvar

[12] Service Oriented Architecture, https://en.wikipedia.org/wiki/Service-oriented_architecture (besökt 2020-12-06)

2 Lägesbild

Ett syfte med denna rapport är att diskutera hur IoT-system kan bidra med information till uppbyggnad av en lägesbild över det område där IoT-enheterna redan är befintliga eller efter att en aktör placerat ut dem till följd av exempelvis en krissituation.

Först behandlas begreppet *lägesbild*. Därefter refereras kort innehållet i ett par svenska studier kring lägesbild. Begreppet saknar en entydig definition, sannolikt för att det används inom så många olika branscher där man sinsemellan har helt väsensskilda ”lägen” man anser viktigt att ha en ”bild” över. Begreppen *lägesuppfattning* och *lägesförståelse* finns även, men är snarast psykologiska; den bild den mänskliga operatören mentalt skapar sig över ett visst läge i den fysiska omgivningen. Nedan avses dock främst den lägesbild som kan skapas i IT-system genom sammanställning och presentation av insamlad och bearbetad information om en fysisk händelseutveckling. En fördjupad diskussion om lägesbild finns i bilaga 2.

I detta kapitel diskuteras inte nyttjande av IoT för skapandet av lägesbild, det anstår till en separat diskussion i kapitel 4.

2.1 Aktörer och roller

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 en organisation, för viss infrastruktur, för utvecklingen inom ett visst geografiskt område etc. behöver löpande information om läget (tillståndet) inom sitt ansvarsområde för fortlöpande justeringar och för att kunna agera och ta beslut i tid och på rätt sätt om, exempelvis, utvecklingen tar en oönskad riktning.

Vilken typ av lägesinformation aktören behöver varierar naturligtvis helt med uppgiften. Informationen kan vara genererad av sensorer, av mänskliga iakttagare, av simulerings- och prognostiseringsverktyg m.m. Sättet att presentera informationen varierar likaså; geografisk (eller rumslig i fallet infrastruktur) information presenteras gärna på en karta över området eller en, ibland starkt förenklad, ritning eller skiss över en övervakad infrastruktur. Relationsinformation (sociala relationer, orsak-verkanssamband etc.) kan presenteras i form av relationsnätverk med länkar och noder.

I det offentliga (på kommun-, region- och riksnivå) finns många aktörer i form av organisationer (ofta myndigheter), som ansvarar för sina egna områden, såsom

polis, brandförsvar, energiproducenter, sjukvård, trafiköverväkning till luft, sjöss och på land med mera. Dessa har sina specifika, ofta väsensskilda, men ibland överlappande, informationsbehov till sina respektive lägesbilder. Vid samhällskriser kan flera av dem behöva samarbeta, och övningar av sådant samarbete genomförs i MSB:s övningsserie ”samverkansövningar” (SAMÖ).

2.2 Svenska studier kring lägesbild för krisberedskap

Med de aspekter på lägesbildsarbete som behandlas i avsnitt 2.1, i bakgrunden, kan ett par svenska studier relaterade till myndigheters krishantering, och därmed relaterad informationshantering och skapande av lägesbild, närmare studeras (Landgren & Borglund, 2016; Totalförsvarsstiftelsen, 2019). Den första studien av Landgren och Borglund (2016) och utgiven av MSB är en välskriven, ganska djuplodande men också mera teoretisk utredning av begreppet lägesbild och därmed associerade områden. Den andra studien (Totalförsvarsstiftelsen, 2019) är snarast en statusrapport i ett pågående arbete som studerar konceptet ”Distribuerad realtidslägesbild” och hur det nyttjas eller planerar att nyttjas inom några organisationer med övervaknings- och utryckningsansvar i Stockholmsområdet.

I (Landgren & Borglund, 2016) diskuteras vad som typiskt ingår i en lägesbild vid samhällsstörningar, nämligen information om:

- inträffad händelse
- händelseutveckling
- resursanvändning
- åtgärder och beslut
- prognos.

Vid mer omfattande händelser, som involverar flera aktörer, behövs även information om:

- andra aktörer
- uppgifter och ansvar.

Det sätt en lägesbild kan skapas på utifrån den här diskussionen är inte entydigt då själva begreppet ”lägesbild” som nämnts ännu saknar en entydig definition. I (Landgren & Borglund, 2016) blir man här mer teoretisk och berör två tydliga synsätt på begreppet: Det ena synsättet fokuserar på att erbjuda aktörerna välfungerande källor till sin lägesinformation (Wolbers & Boersma, 2013) från vilken de kan erhålla den information de finner viktigast. Det andra synsättet fokuserar på att utifrån den åtkomliga informationen uppnå förståelse för situationen ur aktörernas respektive perspektiv (Comfort, 2007). Detta innebär bland annat att aktörerna måste inse vilka möjligheter och även begränsningar som samarbete dem emellan innebär. Syntesen av de bägge synsätten blir då att

det även går att, förutsatt att aktörerna har möjlighet att dela information, med hjälp av lägesbilden som ”handelsplats” och diskussionsforum etablera ett ”kollaborativt meningsskapande” (Comfort, 2007). Utifrån sina respektive kontexter tolkar aktörerna informationen och erhåller lägesuppfattning samt förstår sammanhanget, i den situationsutveckling man gemensamt har att hantera och därmed erhåller lägesförståelse. Mycket av detta handlar om gruppdynamik och andra psykologiska faktorer, men förutsättningen är tillgången till information samt möjligheten att gemensamt analysera denna.

I (Landgren & Borglund, 2016) skiljer författarna mellan ”Lägesbild” och ”Samlad lägesbild”, där det förstnämnda är den aktörsspecifika lägesbilden, och den senare erhålls då den organisationsspecifika lägesinformationen som är relevant för flera aktörer sammanförs för att erhålla en mer sammansatt bild över situationsutvecklingen. Den samlade lägesbilden kan antas ha en lägre grad av upplösning men sammanfattar hela situationen och ger möjlighet till snabbare överblick för alla aktörer för att i högre gemensamma beslutsnivåer, virtuellt eller i fysisk ledningscentral, förbättra samordning och resursutnyttjande. Man vill skilja mellan ”Samlad lägesbild” och något som ibland kallas ”Gemensam lägesbild” då det förra inte innebär att alla aktörer har samma lägesuppfattning då de har fokus på olika delar av situationen och det senare snarast innebär att alla istället har tillgång till samma jämkade lägesbild.

Att dra nytta av delad information innebär även att, då en potentiellt mycket större informationsmängd blir tillgänglig, ha förmåga att sovra fram det för den egna aktören mest relevanta, samt även att till andra aktörer delge, eller peka ut, det för dem mest relevanta. Detta för att undvika informationsstress och risken att missa viktiga detaljer detta innebär.

Avgörande för att få till god samverkan mellan aktörer är förstås att dessa ges möjlighet att kommunicera, vilket kan ske i så kallade ”operatörskluster”, där företrädare för de olika aktörerna samlas för att samverka. Dessa operatörskluster är samlokaliserade eller samlänkade via IT-lösningar såsom delade virtuella whiteboards, videokonferens och tillgång till egna eller gemensamma informationskällor och dataanalysverktyg. Kommunikationen sker verbalt, eller eventuellt asynkront via meddelanden, och man måste snabbt kunna göra varandra uppmärksamma på nyinkommen information som berör flera aktörer och besluta om åtgärd. Mobila lösningar är nödvändiga för att stå i kontakt med de olika aktörernas personal på fältet som har att hantera den uppkomna situationen och direktrapportera från denna samt motta direktiv.

I situationer, där lägesbilden ännu är för oklar för att ge tillräcklig förståelse för bakgrunden till det uppkomna läget och trolig vidareutveckling av detsamma, kan uppställandet av ett antal möjliga hypoteser om vad som hänt underlätta samsynen. Hypoteserna ställs mot tillgänglig information och får genom diskussion mellan aktörerna mer eller mindre trovärdighet, och kan då hjälpa till att avgränsa antalet troliga händelseutvecklingar och lämpliga åtgärder.

I (Landgren & Borglund, 2016) beskrivs tre olika varianter av lägesbilder, eller snarare arbetssätt, för att etablera och upprätthålla en aktuell lägesbild från olika typer av informationskällor:

- Sensororienterad: Informationen som skapar lägesbilden kommer från fysiska sensorer i geografin och presenteras därför gärna geografiskt på en karta.
- Informationsorienterad: Även här väljs gärna en geografisk presentation, men informationen kommer i större utsträckning från människor i form av underrättelser.
- Kommunikationsorienterad: Är mer fokuserad mot att i en mer komplex situation, med flera ingående aktörer, producera en ”metalägesbild”. Här försöker man, förutom en eller bägge ovanstående punkter, med hjälp av de ingående aktörernas kompetensområden resonera sig fram till ett gemensamt sätt att förstå och hantera situationsutvecklingen och parallellt även skapa en ”lägesbild” över de ingående aktörernas ansvarsområden och förmågor.

I sitt sjätte kapitel för Landgren & Borglund vidare en ingående diskussion kring vad som är viktigt att beakta i aktörernas samarbete för att bygga en samlad lägesbild. Man hänvisar[13] till MSB:s publikation MSB777 ”Gemensamma grunder för samverkan och ledning vid samhällsstörningar” (MSB, 2018) och beskriver stegen Rapportering, Strukturering, Reflektiv analys, Förhandling som viktiga för att från de enskilda aktörernas lägesbilder skapa en samlad sådan. Detta refereras inte närmare här utan hänvisning sker till publikationerna från MSB.

Den andra studien, (Totalförsvarsstiftelsen, 2019), är en delstudie inom ”Fördjupningsstudie Ledning - Ledningsstudien” vilken är en delmängd av ”Totalförsvarsstudien”. Här har man bland annat studerat avtalsorganisationen ”Samverkan Stockholmsregionen”[14] som skapades 2015 och vars syfte är att underlätta och främja samverkan både vid normalläge och vid akuta och omfattande situationer, där samarbetet mellan olika aktörer behöver komma till stånd snabbt och resurserna kan utnyttjas mer effektivt. Här har man bl.a. testat koncept som ”Gemensam samverkansstab” samt nämnda ”operatörskluster”. Vid normalläge, i vad man kallar ”ordinarie läge”, arbetar en planerande nivå, en

[13] Landgren & Borglund hänvisar till 2015 års utgåva av MSB777. I den nu aktuella (MSB, 2018) återfinns diskussionen på s. 127 ff i kapitel 15, men hela kapitlet är läsvärt.

[14] En aktörsgemensam avtalsorganisation som utgår från MSB:s nationella koncept ”Gemensamma grunder för samverkan och ledning vid samhällsstörningar”, se http://www.msb.se. En avtalsorganisation är en samarbetsform som inte utgör en juridisk person och därmed inte kan anställa egen personal eller ingå avtal, men som ger de samarbetande aktörerna gemensamma strukturer och resurser för att stödja samordning.

”regional samordningsgrupp”, med löpande ärenden kring samordning av gemensamma projekt med mera. Då en kris uppstår vilket kallas ”aktiverat läge” sker kommunikation över telefon eller Rakel-systemet men man kan även samlas fysiskt i en gemensam samverkansstab. Vid aktiverat läge finns en realiserats verkställande nivå vilka kan samlas i operatörskluster för att effektivt samarbeta kring det uppkomna läget. Den samlade lägesbilden omfattar, förutom uppgifter om operationssituationen, även uppgifter om de samverkande aktörernas antaganden, vad de har gjort, och vad de avser att vidta för åtgärder.

Följande kapitel beskriver en studie kring ett sådant informationsutbyte som gjorts inom Natos forskningsorganisation STO. Kapitlet är tekniskt orienterat mot IoT-teknik och adresserar i stor utsträckning olika teknologier som studien använt.

3 Omvärldsstudie: Arbetsgruppen NATO STO IST-147-RTG

3.1 Bakgrund

Utvecklingen av IoT har främst drivits av civila behov och civil teknologi-utveckling. Inom organisationer för civil säkerhet såväl som inom militären (exempelvis inom Nato och Eda) har man fått upp ögonen för IoT, främst som möjlig bidragsgivare till omvärldsuppfattning i geografiska områden där nyttjande av IoT-teknologi är realistiskt. Pålitliga försvars- och säkerhets-tillämpningar av IoT ställer dock i allmänhet större krav än civila tillämpningar på (Fraga-Lamas, o.a., 2016):

- Fysiskt tålig IoT-utrustning
- Strategier för hantering av osäker energiförsörjning
- Störtålig kommunikation med andra IoT-system och mot gateways (sv. nätsluss) utåt där även bandbredden kan komma att variera kraftigt
- Säker kommunikation (avser alla aspekter av cybersäkerhet).

Då militär eller civilmilitär personal når ett operationsområde måste även följande egenskaper beaktas avseende egna medtagna IoT- system:

- De skall kunna medtagas och utplaceras i operationsområdet och självkonfigurera sig mot varandra och gateways.
- De skall kunna placeras rörligt på egen personal och fordon (även autonoma sådana) för att övervaka dessa och omgivningen.
- De skall idealt på ett säkert sätt kunna kommunicera med lokala IoT-system (avser främst vid operationer i så kallade *Smarta städer*[15] där sådana redan finns på plats).
- Vid en koalitionsoperation skall de kunna nyttja gemensamma standarder för dataåtkomst och styrning.

Den produktiva NATO STO IST (NATO Science and Technology Organization, Information Systems Technology) Panel arbetsgrupp 147[16] *Military Applications of Internet of Things* som arbetade under perioden 2016-2019[17] adresserade på

[15] Populär benämning på en stad med bl.a. en sedan tidigare utbyggd IoT-infrastruktur

[16] Nato-arbetsgrupp IST-147-RTG. Den är för sitt arbete belönad med ett 2020 ”IST Panel Team Excellence Award”.

[17] Gruppen arbetar idag delvis vidare som IST-176-RTG ”Federated Interoperability of Military C2 and IoT Systems” till och med år 2022.

ett tämligen uttömmande sätt ovanstående egenskaper och åtskilliga andra. Man försökte även åtgärda bristen på standarder inom det mycket snabbt utvecklande IoT-området, samt hur detta skulle kunna hanteras av den militära domänen, exempelvis genom nyttjandet av Nato-standarder såsom NISP,[18] som beskriver både militära och civila standarder, samt NGVA.[19] Åtskilliga publikationer har kommit ut från arbetsgruppen[20] (Johnsen, o.a., 2018; Pradhan, Fuchs, & Johnsen, 2018; Pradhan, Suri, o.a., 2018; Pradhan, Manas, o.a., 2019), och en omfattande slutrapport planeras i Springer Open Access såsom en bok med samma titel som arbetsgruppen. Den finns för närvarande endast som utkast och är ännu inte publicerad, men det antas ske kort efter denna FOI-rapports publicering. I kapitel 3.2 till 3.4 följer en teknisk sammanfattning av Nato-arbetsgruppens resultat.[21]

3.2 Tekniker

Arbetsgruppen IST-147-RTG har brett studerat ett användningsfall om hur IoT-system skulle kunna användas militärt för att uppnå bättre lägesförståelse, och specifikt hur system som medförts till en drabbad (av krig, naturkatastrofer etc.) region skulle kunna samverka med en smart stads befintliga IoT-system.

Det typiska sättet IoT ansluts gentemot nätverk (internet eller intranät) är via routrar och gateways där olika former av protokollöversättning från IoT-systems proprietära protokoll, men även viss databearbetning, sker. I (Johnsen, o.a., 2018) beskrivs ett antal intressanta militära användningsfall för IoT-system med nära samverkan med civila system. När en extern användare via nätverket ansluter sig till miljöer med ännu okända IoT-system vill denne få reda på vilka som alls finns och är tillgängliga, det vill säga *service discovery* (sv. *tjänsteupptäckt*). Ett sätt som inte nämns i (Johnsen, o.a., 2018) men i ett utkast av arbetsgruppens kommande rapport är det som föreslås av NATO TIDE[22] är

[18] *NATO Interoperability Standards and Profiles (ADatP-34(K)).* Hämtat från https://nhqc3s.hq.nato.int/Apps/Architecture/NISP (besökt 2020-12-03)

[19] NATO Generic Vehicle Architecture (STANAG 4754).

[20] Noteras skall att dessa NATO-STO arbetsgrupper inte finansieras av Nato, så mycket av arbetet som här hänvisas till såsom kommande från denna arbetsgrupp har utförts i andra projekt där de medverkande varit verksamma i sina vanliga forskarroller, och där resultaten från dessa sammanförts inom ramen för Nato-arbetsgruppen.

[21] I de refererade publikationerna finns åtskilliga illustrationer som avses förtydliga resonemangen som där förs och som sammanfattas nedan. Illustrationerna har dock varierande förmåga att klarlägga det de avser. Då de är behäftade med copyright kan de ej publiceras här, utan betraktas säkrast i originalpublikationerna.

[22] Think-tank for Information, Decision and Execution superiority

mDNS.[23] Tillvägagångssättet, som även kan integreras med andra metoder för tjänsteupptäckt, beskrivs närmare på NATO Tidepedia.[24]

På samma sätt är det viktigt att dessa IoT-system vid förfrågan om tillgänglighet kan beskriva sina förmågor (*service description*). SensorML[25] är ett sätt för sensorer att göra detta via metadata vilket kan vara mycket användbart för att hitta lämpliga sensorer som kan leverera önskvärd data. SensorML skulle även kunna nyttjas av gateways för att beskriva både förmågorna de enskilda IoT-systemen besitter som är anslutna till dem, såväl som att beskriva aggregerade förmågor. SensorML måste dock kompletteras med en lämplig ontologi för att kunna utnyttjas fullt ut. Detta arbete kvarstår även om man diskuterar ett av andra forskare framfört förslag (Wang, o.a., 2012).

SensorML ger ingen möjlighet att beskriva vilken standard för informations-överföring som används, såsom för diskreta meddelanden (exempelvis JSON[26]) eller strömmande (exempelvis H.264[27]) information. Lämpligen används någon standard i nämnda NISP. För diskret överföring finns ett antal olika API-specifikationer, varav man lyfter fram OpenAPI Specifikation (OAS[28]). Ramverket Swagger[29] implementerar OAS och erbjuder ett RESTful metadata API som beskriver de tjänster och resurser (i detta fall vilka IoT-enheter) som finns tillgängliga. I brist på en lämplig överenskommen ontologi att använda valde man istället att i arbetsgruppen att implementera identifieringen av lämpliga IoT-tjänster utifrån de MQTT[30]-ämnen (MQTT-protokollet beskrivs på nästa sida) dessa kunde publicera vilket dock inte är långsiktigt hållbart då dessa ämnen inte är standardiserade.

I (Johnsen, o.a., 2018) beskrivs även hur man i Helsingfors kan få tillgång från information (väder och vind, väglag, sikt etc.) från en stor mängd trafikrelaterade IoT-tjänster genom ett API kallat Digitraffic[31] vars API beskrivs med nämnda OAS. Informationsutbytet avseende enstaka textmeddelanden sker i form av JSON-meddelanden över MQTT-protokollet. Som videoformat används istället lämpligen H.264 formatet. Vid konferensen ICMCIS 2017 i Uleåborg

---

[23] Multicast DNS är ett protokoll som kan användas i små isolerade nätverk där en Domain name system saknas. http://www.multicastdns.org (besökt 2021-01-26)

[24] https://tide.act.nato.int/tidepedia/index.php (besökt 2020-12-16), tillgänglig för registrerade användare

[25] https://www.ogc.org/standards/sensorml (besökt 2020-12-16)

[26] https://www.json.org (besökt 2020-12-16)

[27] https://sv.wikipedia.org/wiki/H.264 (besökt 2020-12-16)

[28] https://www.openapis.org (besökt 2020-12-16)

[29] https://swagger.io/specification (besökt 2020-12-16)

[30] https://www.mqtt.org (besökt 2020-12-16)

[31] https://www.digitraffic.fi/en (besökt 2020-12-16)

demonstrerade arbetsgruppen hur Digitraffics API kunde användas för att en simulerad expeditionär styrka kunde tillgodogöra sig IoT-information därifrån på en lägeskarta i verktyget ATAK.[32]

Ett problem för IoT-system, som ofta har begränsade minnes- och kommunikationsresurser, är hur information från dem skall kunna förmedlas på ett effektivt sätt. MQTT-protokollet valdes av arbetsgruppen efter att ha gjort jämförelser mellan detta protokoll och två andra (AMQP[33] och WSNotification[34]) avseende tidsåtgång för meddelandeöverföring, overhead etc.

MQTT är ett dubbelriktat protokoll och en OASIS-standard optimerad för smala bandbredder och därmed passande för IoT-system. Den förutsätter en meddelandemäklare och ett antal klienter (publicerande IoT-tjänst å ena sidan och prenumererande klienter å andra sidan). Mäklaren distribuerar meddelanden taggade med ett *topic* (ämne) i meddelanderubriken. Varje IoT-tjänst kan märka sina meddelanden med lämpligt ämne beroende på vilken typ av information den publicerar. Olika tillförlitlighetsnivåer för meddelandeutbyte kan väljas beroende på tillgänglig bandbredd och bedömt informationsvärde:

- "At most once" – Meddelandet sänds endast en gång och vare sig klienter eller mäklare vidtar några åtgärder att försäkra sig om att överföringen lyckades; "fire and forget"
- "At least once" – Meddelandet sänds flera gånger till dess att mottagningsbekräftelse erhålls; "acknowledged delivery"
- "Exactly once" – Sändare och mottagare utför handskakning för att försäkra sig om att en och endast en kopia av meddelandet gick fram; "assured delivery"

Vidare beskrivs i (Johnsen, o.a., 2018) hur man demonstrerat hur data från IoT-system burna av UAV:er och UGV:er såväl som soldater kan levereras till en mobil militär ledningscentral, en Mobile Tactical Operations Center (MTOC). UxV:erna bär sensorer, såsom videokameror, som mäter ljud, rörelser, avstånd och riktning till fenomen, CBRN kontaminering med mera, vilka står i kontakt med MTOC via WiFi. Soldaterna i sin tur bär hälsosensorer som mäter fysisk status respektive RFID som regelbundet känner av att de inte tappat viktig personlig utrustning. Soldaterna bär var sin smartphone som via Bluetooth kommunicerar med likaså burna mikrokontroller som sköter kommunikationen mot de burna sensorerna. Soldatgruppens smartphones kommunicerar via ett

[32] Android Tactical Assault Kit är ett verktyg som utvecklats av US Army för att presentera lägesinformation på en display buren av person, eller på en presentationsyta inne i ett fordon.

[33] https://www.amqp.org (besökt 2020-12-16)

[34] https://www.oasis-open.org/committees/wsn (besökt 2020-12-16)

MANET[35] ovanpå varje individuell Bluetooth, och på så sätt erhåller gruppledaren och MTOC information om gruppens status. Denna information kan presenteras i MTOC exempelvis genom NGVA. Via NGVA kan informationen även delges andra fordon som implementerar denna.

I (Pradhan, Fuchs, & Johnsen, 2018) beskrivs en vidareutveckling av nämnda idéer om hur de militära och civila (smart stad-) domänerna mest effektivt skulle kunna samarbeta avseende vilken bearbetningsnivå man önskar på den information som önskas utbytas. Finkornig information kan utbytas via gateways på bearbetningsnivå 1, medan mer övergripande information, som redan aggregerats på den ena eller andra sidan kan utbytas på bearbetningsnivå 4:

1. Nivå 1 Gateway: Via denna kan rådata föras över till den militära domänen. Förslaget är att nämnda NGVA nyttjas från den militära sidan. NGVA nyttjar OMG:s Data Distribution Service Middleware (DDS[36]) vilken använder ett publish-subscribe-förfarande liksom MQTT baserat på ämnen av intresse för prenumeranten vilket skulle kunna användas för att efterfråga önskad information från en smart stad / IoT-sidan. NGVA inkluderar i sin arkitektur möjligheten att ansluta gentemot en sådan sidas externa gateways. De data som förs över behöver inte alltid vara ”rå” utan kan i förekommande fall vara redan förbehandlad / aggregerad genom edge-teknik (se nedan).

2. Nivå 2 Gateway: *finns inte* då ingen information på denna nivå överförs. Här bearbetas data från IoT i en smart stads egna servrar och i molnprocesser.

3. Nivå 3 Gateway: Här har bearbetade data från nivå 2 även semantiskt annoterats med metadata avseende innehåll, ursprung etc. Den militära domänen är genom nivå 3 tänkt att kunna efterfråga dessa annoterade data från den smarta staden genom att nyttja vissa ontologier. Förslaget (Wang, o.a., 2012) är att nyttja Semantic Sensor Network[37] Ontology och Semantic Web tekniker. På denna nivå kan man potentiellt nyttja nämnda SensorML med lämpliga ontologier för att beskriva tillgängliga sensorer. Som nämnts i (Johnsen, o.a., 2018) kan inte SensorML beskriva format på data som levereras, exempelvis strömmande eller diskret. Man rekommenderar här format från NISP.

[35] Mobile Ad hoc NETwork (https://en.wikipedia.org/wiki/Wireless_ad_hoc_network, besökt 2020-12-03)

[36] https://www.dds-foundation.org/what-is-dds-3 (besökt 2020-12-16)

[37] https://www.w3.org/TR/vocab-ssn (besökt 2020-12-16)

4. Nivå 4 Gateway: På denna nivå skulle processade rapporter från den smarta staden-sidan kunna utbytas via den militära MIP4 IES (Multilateral Interoperability Programme 4 Information Exchange Specification).[38] Denna är huvudsakligen avsedd för informationsutbyte på högre semantisk nivå mellan ledningssystem. Detta förutsätter att informationen från den smarta staden kan representeras av lämplig(a) så kallade MIP BSOs (Battle Space Objects) vilka utbyts i form av XML-meddelanden via, främst, publish / subscribe eller vid behov request / response för att exempelvis från en MTOC begära mer detaljerad info om en viss BSO. Man skulle även i MIP4 IES kunna prenumerera på vissa specifika händelser från IoT-tjänster och presentera dessa hos den militära prenumeranten som ”alerts” i valfritt ledningssystem som implementerar MIP4 IES; i en MTOC eller högre ledningscentral.

Vid militära operationer då IoT-system är tänkta att nyttjas måste man utgå från att miljön för att överföra information från (och till) IoT inte är den optimala beroende på allt från cyberkrigföring till effektbrist hos IoT-system, räckviddsproblem eller frekvenskonflikter för nyttjad trådlös kommunikation etc. Allt detta innebär begränsad bandbredd och intermittent uppkoppling. Dessutom finns många aktörer som vill ha olika typer av information från IoT-tjänster varför informationen bör filtreras med avseende på prenumeranternas specifikt uttryckta behov. Det enklaste sättet är att endast prenumerera på vissa ämnen som IoT-tjänster publicerar, men det går att göra prenumerationen mer nyanserad. Den under senare år alltmer studerade principen om *edge-teknik,*[39] d.v.s. att flytta mycket av tyngre beräkningar och dataaggregering närmare källorna till data passar mycket bra för hantering av IoT-tjänster. Arbetsgruppen har även ingående studerat sådana idéer vilket presenteras närmare i avsnitt 3.3.

Johnsen o.a. (2018) föreslår fem tillvägagångssätt baserade på olika tekniker för att hantera informationssäkerhetsproblem som kan uppstå i det användningsfall som studeras i Nato IST-147 arbetet. Nedan beskrivs lösningarna kortfattat:

---

[38] För kort beskrivning se https://public.mip-interop.org/Public%20Document%20Library/10-Programme-Mgmt/Information-Sheets/MIP4IES_Information_Sheet_ver21.0.0.pdf (besökt 2020-05-18)

[39] Även kallat *edge computing* eller *fog computing*. Edge avser ”änden” på informationshanteringen där data genereras (här IoT och deras gateways) till skillnad från en central bearbetningsplats dit allt skickas (större servrar eller ”molnet”). Analogin ligger i att molnet (cloud) finns högt uppe, dimman (fog) nära marken som s.a.s. är änden där data samlas in. Då dock dessa benämningar ännu inte fått fullständig konsensus kan fog computing ibland även avse kombinationen av edge- och cloud computing. Målet är dock i bägge fallen att sprida beräkningskapaciteten närmare datagenereringen för att få snabbare lokala lägesuppdateringar samt reducera belastningen på nätverk och centrala beräkningsresurser. En bra sammanfattning av edge computing, finns i (Ruhlig, 2019).

1) End-to-end kryptering: Detta är en metod för att skydda information i ett nätverk genom att kryptera data från sensor till slutanvändare. För att bemöta de problem som kan uppstå i en federerad nätverksmiljö föreslår Johnsen o.a. (2018) *end-to-end* kryptering med *attributbaserad kryptering* som går ut på att man krypterar med nycklar som är definierade över en kombination av attribut (t.ex. roll, resurser, mål, miljöförhållanden) istället för användare. Den användare vars attribut matchar rätt kan dekryptera meddelandet.
2) Omkryptering och aggregering i Edge: Om man har sensorer med mer begränsade resurser är end-to-end-kryptering inte möjligt. I sådana fall kan en säker kanal skapas mellan sensorn och edge-noden som efter eventuell aggregering av data omkrypterar dessa med hjälp av en hybrid attributbaserad kryptering.
3) Säker lagring och bearbetning i en publik molntjänst: Att använda tredjeparts molntjänster för lagring och beräkning erbjuder ett kostnadseffektivt alternativ till användning av egna infrastrukturer. De flesta molntjänster tillhandahåller någon optimerad plattform för bearbetning av IoT-data. Medan man kan nå en säker överföring och lagring av data med end-to-end-kryptering, krävs för säkra beräkningar med data att tekniker som *partiell homomorfisk kryptering* nyttjas. Denna teknik är en form av kryptering som tillåter att man kan utföra programmeringsoperationer på krypterade data utan att behöva dekryptera den först. Nato IST-147 har demonstrerat enklare former av sådana beräkningar, t.ex. att beräkna medelvärdet av ingående data.
4) Säkerhet och förtroende mellan noder: Ett av de större problemen med säkerhet och hantering av förtroende mellan noder i en federation av IoT-system är att säkerställa att olika enheter / objekt som är okända för varandra ska kunna kommunicera med varandra på ett säkert sätt. Ett effektivt sätt att hantera detta och bekräfta identiteten av objekt i IoT-system är hårdvarubaserade tekniker som använder sig av *Trusted Platform Modules* (TPM). (Johnsen, o.a., 2018) utnyttjar TPM för att möjliggöra autentisering inom vissa grupper av enheter / noder genom att skapa säkerhetsdomäner med hjälp av COTS IoT-enheter utrustade med TPM. Dataöverföring inom den säkra domänen är skyddade genom kryptering.
5) Säkerhet i det fysiska skiktet med riktad modulering: Anpassade IoT-enheter kan också utnyttja säkerhet med hjälp av riktad modulering (eng. *Directional Modulation*) som är en teknik för säker kommunikation implementerad i det fysiska skiktet. Riktad modulering (DM) är en teknik på sändarsidan som riktar digitalt modulerade signaler i en förutbestämd säker kommunikationsriktning samtidigt som

konstruktionen förvränger samma signaler i alla andra riktningar på ett sådant sätt att enheter belägna där inte kan avlyssna kommunikationen. DM-antennsystemet möjliggör fokusering på områden där relevant kommunikation kan förväntas. Medan DM-systemet för närvarande har tillämpats på 802.11ac, kan det lika gärna användas på andra vågformer som LoRa.[40] En sådan krypteringsfunktion som är riktningsbaserad kan komma till nytta inom användningsfall som diskuteras i (Johnsen, o.a., 2018) genom att den kan avvisa signaler och data från sensorer som har flyttats (av misstag eller avsiktligt) från sina avsedda platser och därmed kan påverka IoT-system med icke relevanta / skadliga data. Dessutom, i ett mycket ”tätbefolkat” IoT-scenario där många noder konkurrerar om radioåtkomst och nätverkskapacitet, kommer den riktade filtrerings-förmågan som är inneboende hos DM att vara till hjälp för att avvisa oönskade data redan i det fysiska skiktet och inte tillåta felaktiga data att levereras vidare i systemet.

3.3 Inspiration från SDN och edge-teknik: ”PIG”

Tortonesi o.a. (2016) presenterar ett centralt koncept vidareutvecklat i (Pradhan, Poltronieri, & Tortonesi, 2019) för att förverkliga IoT-tjänster med edge-teknik i form av *Programmable Internet Gateways* (PIG). Dessa PIG:ar administrerar ett antal IoT-system eller gateways mot dessa IoT och utgör en middleware (i dessa tillämpningar ibland kallad *cloudlet* eller *fog node*) för edge-teknik. Idén är inspirerad av arkitekturen för *Software Defined Networking*[41] (SDN) (Open networking foundation, 2016) vilken man här har utvidgat. Mjukvaran för en PIG kan installeras direkt på gatewaynoderna, som upprätthåller anslutningen till IoT, eller på någon annan nod i nära anslutning till dessa gateways. PIG:en har till uppgift att via gateways mottaga, aggregera, samt vidareförmedla de data IoT-system samlat in. De kan programmeras för att bearbeta och delge insamlad data på de sätt prenumeranter och andra mottagare av bearbetad data önskar. För att associera den typ av data som kan levereras av de IoT-system som är anslutna mot en viss PIG till de informationstjänster (services) en prenumerant kan begära

[40] https://en.wikipedia.org/wiki/LoRa (besökt 2020-12-15)

[41] SDN är en nätverksarkitektur som syftar till att göra nätverken lättare att administrera centralt via en så kallad SDN Controller istället för att hantera enskilda switchar i nätverket. Detta underlättar bl.a. konfigurering av underordnad nätverkshårdvara och adaptiv dirigering av trafikflöden.

tillgång till i sin prenumerations-profil,[42] så finns i varje PIG en Service Component Manager (SCM) som startar lämpliga databearbetningssteg (pipelines) som bearbetar IoT-data till den information som informations-tjänsterna erbjuder.

Exempelvis kan bildsekvenser kodade med en viss videokompressionsstandard från en IoT med videokamera av SCM associeras med en pipeline med uppgift att packa upp och analysera videoströmmen för att exempelvis hitta och följa objekt, det vill säga leverera informationstjänsten ”Följ mål i videosekvens”. Om en prenumerant önskar en mer kvalificerad informationstjänst i form av ”Följ mål mellan kameror” kan SCM ansluta ännu en pipeline med uppgift att vidare-bearbeta målspår från flera videokameror genom lämplig sensorfusionsmetod för att följa objekt som rör sig från kamera till kamera. En illustration finns i Figur 1.

Vidare är det SCM:s uppgift att via PIG:ens gränssnitt direkt mot IoT, eller motsvarande gateway, kommunicera med anslutna IoT-system för att vid behov ge styrkommandon. Detta ger även styrmöjligheter av de IoT-system som innehåller styrbara sensorer eller enbart utgörs av ställdon. En PIG kan kommunicera med en IoT-enhet på två sätt: antingen genom att regelbundet begära (”polla”) data från den - typiskt genom REST-anrop (om den har ett sådant API) - eller genom att ge IoT-tjänsten kommando att publicera data i form av MQTT-ämnen, regelbundet eller då vissa villkor uppfyllts. Exakt vilka styrkommandon som kan ges varierar förstås beroende av respektive IoT-systems API och funktionssätt.

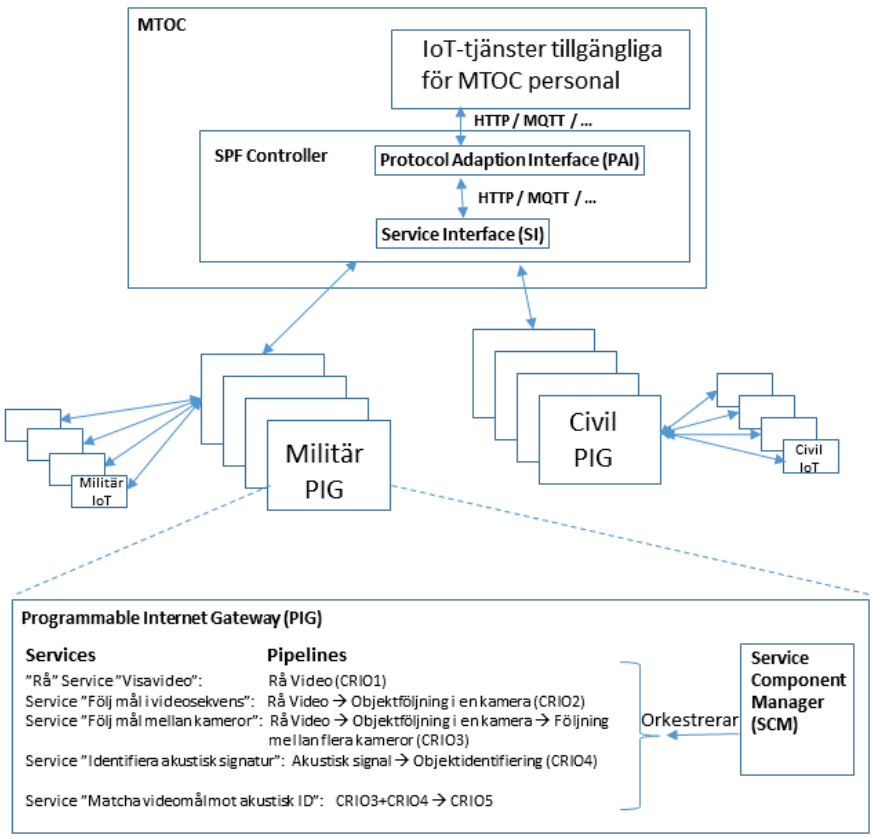
Ett antal PIG som var och en ansvarar för en grupp IoT-enheter orkestreras vidare från (typiskt) en server på en mer central plats, såsom en MTOC eller fast ledningscentral, som kör en mjukvara kallad *SPF Controller*. På så sätt erhålls i princip en tre- eller fyranivåers hierarki ”IoT-gateway / PIG-SPF Controller” eller ”IoT-gateway-PIG-SPF Controller” beroende på om PIG körs i en gateway nära IoT-enheten eller i en egen nod ovanför en eller flera gateways. Mer om SPF Controller nedan.

I en PIG utförs en procedur med faserna *Sieve, Process, Forward* (SPF) (Tortonesi, o.a., 2016) vilken beskrivs som en ”Adaptive, Information-centric and Value-based” informationsmodell (Poltronieri, o.a., 2018).

Den första fasen, *Sieve* (sv. *sålla*), motsvaras av att ett visst antal rådata-meddelanden från IoT-systemet sparas i minnet hos den pipeline det förts till och endast nya meddelanden, som ger tillräcklig uppdatering informationsmässigt i förhållande till aktuellt meddelandeminne, förs vidare till processteget. Om

[42] En prenumerationsprofil kan exempelvis omfatta typ av information som önskas, från vilket geografiskt område, med vilken uppdateringstakt, samt förädlingsnivå (för en bildalstrande sensor kan det exempelvis vara rådata eller ur bildsekvensen extraherade objekt).

uppdateringen underskrider en viss tröskelnivå sker inte detta, utan meddelandet ignoreras helt eller läggs eventuellt till i minnet som senast erhållna meddelande.



Figur 1. En illustration av hur de olika teknikerna för PIG-SPF Controller hänger ihop. Services är informationstjänster som kan efterfrågas, pipelines är processteg i förädlingen till dessa (pilarna i den förstorade PIG ovan) där varje pipeline stegvis producerar var sitt IO. Ett IO analyseras avseende sin VoI. Om den inte är tillräcklig avvaktas till nästa IO kommer. Om det har tillräcklig VoI (eventuellt i kombination med tidigare IO) går den vidare i processkedjan med slutprodukten CRIO. En viss Pipeline kan instansieras av flera Services, såsom den första pilen mellan ”Rå Video” och ” Objektföljning i en kamera” som används både i Service ”Följ mål i videosekvens” och ”Följ mål mellan kameror” (samt även indirekt för sensorfusion i Service ”Matcha videomål mot akustisk ID”).

Process-fasen följer härefter och bearbetar de meddelanden som gått vidare efter sållningsfasen. Detta sker i en viss pipeline med eventuell tillhörande fusions-metod som för denna informationstjänst tidigare startats i PIG:en av SCM i sållningsfasen. Denna fas producerar så kallade *Information Objects* (IO), såsom

ett målspår från en videokamera. I processfasen värderas därefter varje IO enligt det *Value-of-Information* (VoI) det beräknas ha vilket påverkar om det skall sändas vidare, allt för att minimera nätverksbelastningen samt informationsbelastning på högre nivåer. IO:er som inte har tillräcklig VoI för att levereras omedelbart kan sparas i denna fas för att i samma pipeline eller i en efterföljande pipeline fusioneras med andra IO:er för att förbättra VoI. VoI är ett mått som en middleware (sv. mellanprogramvara) i varje PIG kallad *Proactive Dissemination Service* (DSPro) beräknar utifrån både de informationstjänster prenumeranterna anger samt exempelvis det geografiska avståndet mellan prenumeranterna och fenomenet informationen beskriver samt hur gammal informationen är då den kan delges prenumeranterna. Slutligen skapas så kallade *Consumer Ready Information Objects* (CRIO) baserat på IO:er som då är förberedda på att delges prenumeranterna. Om en prenumerant anmält intresse för en informationstjänst som presenterar information av en lägre förädlingsnivå (exempelvis målspår från en kamera) är dessa målspår CRIO för denne prenumerant, medan det är IO till nästa pipeline som producerar CRIO i form av följda mål över flera kameror, för den prenumerant som efterfrågar en sådan informationstjänst.

Forward-fasen, slutligen, sköts av DSPro och skapar en ”matchmaking” mellan de profiler prenumeranterna angivit och de CRIO som PIG:en kan producera för att preliminärt beräkna vilka VoI som ett visst CRIO kan ha för en viss prenumerant. Detta påverkar vilka CRIO som dirigeras till vilka prenumeranter. Om en prenumerant ”anmäler” en annan profil utförs en ny matchmaking. Eventuellt kvarvarande CRIO som finns sparade i PIG som tidigare inte passade en prenumerants profil, men då den nya profilen anmälts gör det, kan då sändas till prenumeranten som således direkt kan få en uppfattning om det senaste läget inom sitt intresseområde. Baserat på detta orkestrerar DSPro distributionen av CRIO till prenumeranterna. Detta görs i arbetsgruppen med ett proprietärt protokoll baserat på UDP Unicast, men för att passa bättre in i militära standarder föreslår Pradhan o.a. (2019) en övergång till MQTT- protokollet med möjlighet att märka meddelandet med ämne. Dock finns även fortsättningsvis möjlighet att direkt prenumerera på endast lätt behandlad, eller obehandlad, rådata såsom en videosekvens.

Övergången till MQTT skulle också göra det lättare att uppfylla kommunikationskraven inom *Federated Mission Networking* (FMN) mellan koalitionspartners som på taktisk nivå vill utbyta IoT-information (Pradhan, Suri, o.a., 2018).[43] En NATO STO IST arbetsgrupp IST-150-RTG *NATO Core Services profiling for Hybrid Tactical Networks* (som arbetar till och med 2020[44])

[43] Hantering av IoT inom ramen för FMN är planerat att ske under den så kallade ”FMN spiral 6” år 2028-2029.

[44] Denna arbetsgrupp är inte fokuserad på utbyte av IoT information men har gjort experiment med att utbyta Friendly Force Information (NFFI), även kallad Blue Force Tracking, information. Den föregicks

undersöker hur publish / subscribe på taktisk nivå kan underlättas genom att nyttja MQTT-protokollet och det kompaktare JSON-meddelandeformatet för kommunikation mellan partners snarare än det mer tungrodda SOAP / XML-baserade WS-Notification-protokollet som rekommenderas av FMN.[45]

Interoperabilitet mellan system som behåller WS-Notification och MQTT-kompatibla system kan uppnås med en överbryggande gateway. MQTT stödjer dock inte egenskapen att automatiskt upptäcka vilka ämnen som är tillgängliga för prenumeration från en mäklare. Detta innebär att det redan från början måste finnas en överenskommen hierarkisk struktur på de ämnen som kan finnas tillgängliga.

Alla PIG:ar står under befäl av en nämnd SPF Controller. Denna mjukvara körs lämpligen i någon form av ledningscentral, i Unix-miljö, och kan nyttja sådan mjukvara som finns i operativsystemet. Den består av två delar: en *Protocol Adaption Interface* (PAI) samt *Service Interface* (SI). PAI agerar brygga mellan ledningscentralens system och SPF Controller. Denna förmedlar operatörers kommandon från ledningscentralen till SPF Controller, och returnerar meddelanden som kommer från de PIG:ar som sorterar under SFP Controller. En operatörsförfrågan i ledningscentralen om att prenumerera på en viss typ av information går genom PAI och når SI. SI har en lista över vilka PIG:ar som sorterar under denna SFP Controller, och vilka typer av IO och CRIO dessa kan producera, från vilka geografiska områden dessa har sitt ursprung etc.

En SFP Controller kan, utan att tvinga PIG:en att starta om, i runtime ladda upp nya tjänsteapplikationer till denna. Detta föreslås exempelvis kunna ske i form av OSGi bundles (OSGI, u.d.).

3.4 SDN:s påverkan på FMN

Det kan slutligen i detta avsnitt nämnas att arbetsgruppen NATO STO IST-142-RTG *Software Defined Network Architectures for the Federated Mission Networks,* som avslutas under 2020, under några år har studerat i avsnitt 3.3 nämnda SDN och hur det kan nyttjas i FMN. Resultat från denna grupp kan eventuellt komma att påverka eventuell realisering av de delarna av den nämnda arkitekturen. Arbetsgruppens slutrapport beräknas utkomma i nära anslutning till den här rapporten.

av en arbetsgrupp IST-118-RTG *SOA recommendations for disadvantaged grids in the tactical domain*, se exempelvis (Johnsen F. T., o.a., 2017).

[45] Presentation vid NATO STO IST Panel Business Meeting, oktober 2019

4 Diskussion

I det här kapitlet diskuteras relevansen för FM av den form av samverkande lägesbildsarbete som beskrivs i kapitel 2 och användbarheten av utvalda tekniska lösningar för IoT-samverkan som utvecklats inom ramen för Nato-arbetsgruppen (kapitel 3).

4.1 Lägesbildsarbete och samverkande IoT

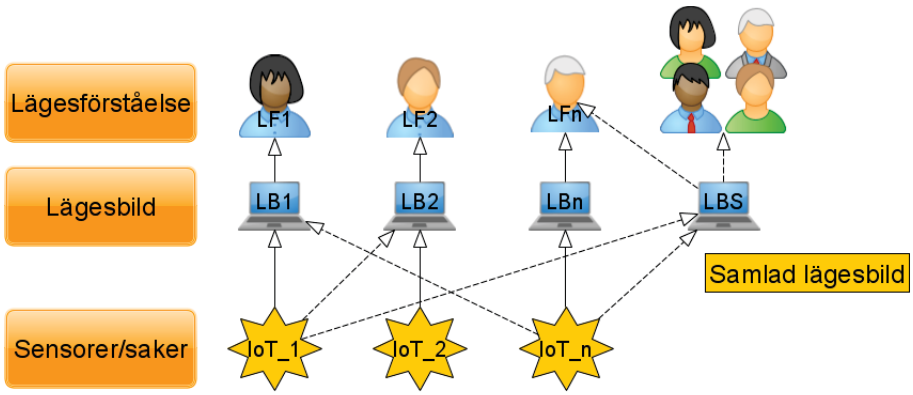
Arbetet har kommit att fokuseras på MSB:s syn på lägesbildsarbete och hur den har implementerats i Stockholmsregionen (se avsnitt 2.2). Att Stockholms-regionens samverkansmodell är relevant ur ett samverkansperspektiv med FM understryks av att den aktuella militärregionen redan idag är en integrerad del av samverkan. Däremot har projektets studie av samverkansmodellen inte lett till ökad förståelse för de krav som kan ställas på system som underhåller och upp-daterar lägesbilder i samverkan.

Efter samtal med personal på Länsstyrelsen Stockholm och FOI dras slutsatsen att det primärt finns två sätt för FM att delta i samverkansmodellen: i fredstid och höjd beredskap. I fredstid, det vill säga det normala tillståndet, har FM en observ-erande roll där man mest hämtar in information från aktörerna i samverkan. Däremot i händelse av höjd beredskap, då FM behöver en med högre takt upp-daterad lägesbild, bör FM kunna gå in som en aktiv part jämte exempelvis Polisen och Brandförsvaret. Det är också i detta läge som nyttan med IoT-samverkan för FM är som störst.

Länsstyrelsen i Stockholms samverkansmodell påminner om den som eftersträvas i den här rapporten, en samverkansmodell för en situation där IoT i större omfattning och fördelat över en mängd samverkande aktörer bidrar med lägesinformation. Av intresse är framför allt en situation där information från olika aktörers IoT-system direkt kan distribueras till personal och operatörer på lägre nivåer, ända ned till de som agerar på ”fältet”, och där bidra till deras specifika lägesbild. Om dessa kan få tillgång till lägesuppdateringar från såväl egna som andra aktörers IoT-system skapas ett nätverkande som kan öka takten i insatsen och eliminera risken för att viktig information inte delges de som bäst behöver den för sin lägesbild.

Stockholmsregionens samverkansmodell illustreras från ett IoT-samverkans-perspektiv i Figur 2. Figuren visar tre generiska aktörer som var och en har en mängd informationskällor (”sensorer / saker”) och lägesbild och lägesförståelse som är anpassade efter aktörens individuella uppdrag, kunskaper och resurser. Heldragna pilar visar på information från det egna IoT-systemet och streckade visar information från en annan aktörs system (som man normalt har begränsat inflytande över). Längst till höger i bilden finns den samlade lägesbilden, som är

helt försörjd med extern information och kan delges en variabel skara beslutsfattare.



Figur 2. 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.

Hanteringen av den samlade lägesbilden kan säkerligen utgöra en intressant domän för att vidare utforska problemdomänen samverkande IoT-system. Hanteringen behöver kunna bearbeta inkommande information och anpassa den samlade lägesbilden på olika sätt för att passa de beslutsfattare som nyttjar den, exempelvis genom att jämka mellan motstridig information eller information med olika tidsstämplar, samt aggregera, fusionera och presentera den.

Trots att dessa är intressanta och nödvändiga forskningsuppgifter är den än mer intressanta tekniska och vetenskapliga uppgiften antagligen att utforska den direkta uppkopplingen mellan IoT-system (en uppgift som även omfattar de utmaningar som listas för den samlade lägesbilden). All information bör inte göras tillgänglig för alla aktörer via den samlade lägesbilden. I Figur 2 illustreras denna situation exempelvis genom att den individuella aktörslägesbilden LB2 är beroende av både den interna informationen från IoT-system IoT_2 men även från det externa IoT_1. Denna typ av anslutning är fördelaktig när lägesbilden behöver uppdateras i realtid. Den tekniska integrationen av multipla IoT-system möjliggör också en förutsägbar uppdatering av lägesbilden, jämfört med muntlig informationsspridning i ledningscentralen (vilket kan påverkas av den ”mänskliga faktorn”). Det kan också vara så att viss information av intresse inte delas via en samlad lägesbild utan behöver tillgängliggöras genom direkt anslutning till det aktuella systemet (exempelvis temperatursensorer i en fabriksbyggnad som intas av militär personal).

Direktkoppling av externt IoT-system och dess eventuellt förädlade information innebär ett behov av att en praxis utvecklas för hur man vill fusionera den externa informationen med den interna lägesinformationen för att få en god behovsanpassad sammanställning över läget. Då det vid IoT-samverkan även nyttjas extern information är det viktigt att på samma sätt som för icke-fusionerad information i förväg (innan skarpt samarbetsläge uppstår) analysera hur fusionering med extern information lämpligen kan göras för att ge bästa mervärde till lägesbilden. Då fusionering kan ske redan i sensorerna eller i edge-noder (beskrivet i avsnitt 3.3), såsom då ett rörligt objekt följs från en video-kamera till en annan, avses här dock även fusion som sker högre upp, på ledningscentralens nivå. Man bör dock vara beredd på situationer där en organisation efterfrågar mer obearbetad rådata från en annan organisation som normalt fusionerar information innan den presenteras för sina operatörer, men som i detta fall även skulle behöva vidareförmedla obearbetad data till den efterfrågande organisationen. Juridiska hänsyn måste troligen tas avseende vilken information som får delas. Att dela aggregerad eller fusionerad data kan vara lämpligare än obearbetad rådata vilken kan innehålla sekretessbelagda detaljer. Det kan även vara mindre känsligt att dela anonymiserad data, men det kan förstås sänka värdet för mottagaren.

4.2 Tekniker

I kapitel 3 beskrivs hur en arbetsgrupp inom Nato arbetat med tekniska lösningar rörande samverkande IoT-system för användning inom militära operationer. I följande avsnitt diskuteras dessa tekniska lösningar med avseende på IoT-samverkan för FM.

Följande aspekter av samverkande IoT som Nato-arbetet hanterar och som passar att diskutera i det här projektet identifieras:

- Standarder
- Öppen mjukvara
- Tjänstehantering
- Edge-teknik
- Informationssäkerhet.

4.2.1 Standarder

Nato-arbetsgruppen menar att en av utmaningarna med IoT-samverkan är att det fortfarande saknas allmänt antagna standarder för kommunikation, data-överföring och tjänster (Johnsen, o.a., 2018). Arbetsgruppen rekommenderar, vilket beskrivs i kapitel 3, användning av öppna dataformat såsom JSON, dataöverföringsformat såsom MQTT samt standarder såsom Sensor ML och OpenAPI Specification (OAS). Detta underlättar naturligtvis utvecklingen av samverkande IoT-system då beskrivningen av standarderna, och hur de är tänkta

att användas, är öppet tillgängliga. Sådana standarder underhålls och utvecklas vanligtvis inom internationella standardiseringsorganisationer med många medlemmar snarare än av ett enda kommersiellt företag. Det förefaller därför vara lämpligt att projektet har deltagit i den svenska IoT-standardiseringsgruppen ”Standarder och teknisk plattform” (läs mer i avsnitt 1.3).

4.2.2 Öppen mjukvara

IoT-konceptet uppmuntrar nyttjandet av öppen mjukvara för informationsutbyte med, och orkestrering av, IoT-system och en stor mängd sådana mjukvaror finns att tillgå på internet. Användandet av olika öppna programmeringsgränssnitt och prenumerationsförfaranden, som utvecklats inom IoT-världen för att göra IoT-informationen lättare åtkomlig underlättar skapandet av situationsanpassad presentation av information för personal på fältet eller i ledningscentral.

Nato-arbetsgruppen har som nämnts i kapitel 3 till synes framgångsrikt valt en del öppen mjukvara såsom Swagger (som implementerar OpenAPI Specification) för beskrivning och generering av tjänstegränssnitt och meddelandemäklaren Eclipse Mosquitto[46] som implementerar MQTT-protokollet. Man menar inte oväntat att användandet av öppen mjukvara underlättar interoperabilitet. Ibland annat (Johnsen, Bloebaum, o.a., 2018) finns en bred genomgång av mjukvaror och API:er man studerat och funnit lämpliga för uppbyggnad av interoperabla IoT-system i smarta städer.

4.2.3 Tjänstehantering

Ett paradigm för att dynamiskt koppla ihop separata system fokuserar på begreppet tjänster. Nato-arbetsgruppen har (som redovisas i avsnitt 2.2) undersökt tekniker för att realisera (beskriva och upptäcka) IoT-tjänster. Emedan vissa tekniker och standarder som sensorbeskrivningsspråket SensorML och kommunikationsprotokollet MQTT redovisas, är det mindre klart hur sökfrågor rörande tillgängliga informationstjänster formuleras. En nytillkommen aktör i en ledningscentral vill snabbt kunna få reda på vilken för denne relevant information som finns tillgänglig.

Beroende på hur kvalificerade de nyttjade IoT-tjänsterna är kan förädlingsnivån från dem variera. Istället för att leverera en råvideoström med valbart antal bilder per sekund finns alternativet att leverera en förädlad ström av olika objekt (personer, fordon etc.), positioner och rörelser i bilderna, från en viss videokameras synfält eller från flera kameror där objekten kan fortsätta följas då de övergår från ett synfält till ett annat. Detta innebär en kraftig besparing i bandbreddskrav. Andra IoT-tjänster kanske endast mäter endimensionella tidsserier av temperatur, fuktighet, ljudnivå, vibrationer etc. Vissa kanske endast ger larm

[46] https://mosquitto.org/ (besökt 2020-12-17)

med aktuell lägesinformation då en viss tröskelnivå överskrids, eller annars endast lagrar information från ett glidande tidsfönster en viss tid bakåt som kan efterfrågas vid behov. För att realisera IoT-samverkan för FM:s lägesbild kan alternativa sätt att formulera sökfrågor kring tillgängligheten av denna typ av information behöva undersökas. Detta gäller i synnerhet förädlad information då grundläggande information om tillgängliga IoT-enheter kan erhållas via exempelvis Swagger.

Att hitta och tillgodogöra sig lägesinformation som har sitt ursprung i en annan organisations IoT-system torde även underlätta för en organisations datainhämtning, förutsatt att lägesinformationen alls är juridiskt delgivningsbar. När väl informationen finns tillgänglig kan den sedan filtreras och presenteras anpassat på det sätt som den mottagande organisationen finner bäst, gärna utnyttjandes de användargränssnitt dess medarbetare redan är vana vid.

4.2.4 Edge-teknik

Att förädla uppmätta data kan göras antingen centralt (i ledningscentral eller ”i molnet”) om hög bandbredd finns tillgänglig, men för IoT-enheter som kan producera stora datavolymer görs analys och förädling helst så tidigt i kedjan som möjligt, nära eller i själva IoT-enheten. Det är grundkonceptet för edge-tekniken.

Edge-teknik i kombination med förmåga att lagra information kan även innebära en större robusthet mot tillfälliga kommunikationsavbrott gentemot operatören då analys och lagring av bearbetad information kan fortgå nära enheterna under avbrottet. Senare, då kommunikationen återetablerats, kan den information som lagrats under kommunikationsavbrottet direkt förmedlas till operatören. Edge-teknik innebär också på flera sätt en möjlighet att göra information snabbare tillgänglig. Dels kan sensordataberäkningar göras närmare IoT-enheten och dels behöver informationen inte gå omvägen via en ledningscentral eller ”moln”.

För att uppnå IoT-samverkan med hjälp av tjänster använder Nato-arbetsgruppen edge-teknik-konceptet IoT-PIG-SPF Controller. Nato-arbetsgruppens bedömning att edge-tekniken är viktig och kan utgöra ett bärande fundament för samverkande IoT.

Edge-enheten utgör ett naturligt gränssnitt mellan IoT-system som ägs av olika organisationer. Edge-enheten erbjuder också en lämplig beräkningsresurs för att hantera mer eller mindre nödvändiga funktioner som kryptering, anonymisering, fusion, aggregering, samt resursallokering och schemaläggning av underliggande IoT-enheter.

4.2.5 Informationssäkerhet

Informationssäkerheten är IoT-teknikens akilleshäl, inte minst i militära sammanhang där man varken kan tolerera att en fientlig part stjäl känslig information eller att fienden nästlar sig in i systemet och sprider felaktig information.

I kapitel 3 redovisas olika metoder som Nato-arbetsgruppen betraktat. Eftersom det i föregående avsnitt uttrycks intresse för nyttan med edge-tekniken så lyfts särskilt den säkerhetslösning som bygger på edge-teknik fram. Här får edge-enheten ta ansvar för att hantera kryptering av informationen från de IoT-enheter som edge-enheten ansvarar för, och därmed slipper externa system upprätta säker kommunikation med samtliga IoT-enheter.

5 Slutsatser

I avsnitt 1.2 uttrycks syftet med projektet nämligen att undersöka hur Försvarsmakten skall kunna dra nytta av den framväxande civila IoT-miljön för att förstärka den militära lägesbilden (projektets måltillämpning), främst genom att lära från existerande relaterat arbete.

I ett föregående projekt undersöktes förutsättningarna för IoT-samverkan hos svenska myndigheter. I detta projekt undersöks hur FM kan samverka med svenska myndigheter om skapande och underhåll av lägesbild. Ett konstaterande är att FM redan idag är en integrerad del av den samverkansmodell som tillämpas i Stockholmsregionen, vilken är baserad på MSB:s utförliga modell för lägesbildsarbete. Den samlade lägesbilden, som är en central del av samverkansmodellen, är intressant ur ett IoT-samverkansperspektiv men än mer intressant är IoT-samverkans möjliga direkta stöd till FM:s lägesbild.

De tekniker som föreslagits av en Nato-arbetsgrupp, vilken har ett tillämpningsområde som liknar projektets, undersöktes. Av särskild relevans för måltillämpningen är tjänstehanteringen och edge-tekniken. Dessa erbjuder dock endast ett partiellt svar och svar skulle även behövas på exempelvis hur data från externa IoT-system skall kunna integreras effektivt i FM:s lägesbild.

Den sammanfattande slutsatsen är att *FM:s lägesbildsarbete i samverkan med civila myndigheter* är organisatoriskt och i viss mån tekniskt möjligt redan idag. Trots att detaljerna kring uppdatering av FM:s lägesbild, baserat på extern IoT-information, inte har kunnat undersökas ännu så har existerande teknik och teknik under utveckling identifierats som förväntas bidra till det.

Baserat på slutsatsen identifieras följande intressanta möjligheter för vidare studier:

- Organisatoriskt är, som konstaterarats, FM redan väl integrerad i den samverkansmodell som Stockholmsregionen tillämpar. Däremot skulle man behöva se närmare på hur de olika lägesbildernas innehåll (både de samverkande organisationernas individuella och den samlade) beskrivs, uppdateras och förmedlas. Det är viktig kunskap för att kunna skapa ett relevant flöde av information för att förstärka FM:s lägesbild.
- Edge-tekniken (och det av Natoarbetsgruppen föreslagna IoT-PIG-SPF controller-systemet) är en intressant teknisk plattform för att implementera tjänster för IoT-samverkan, samt för att hantera olika funktioner som interoperabilitet, kryptering, aggregering, fusion, med mera. Bedömningen är att det här är en nyckelteknik för att skapa ett gränssnitt mellan olika svenska myndigheters IoT-system för att bland annat hantera datasäkerhetsfrågor (som kryptering och anonymisering) samtidigt som det beskriver vilken typ av information som respektive myndighet kan erbjuda.

- Eftersom IoT-samverkan är ett framväxande område (som dels vilar på äldre resultat från området sensornätverk) behöver bevakning av omvärldsutvecklingen även i fortsättningen genomföras, både nationellt (rörande exempelvis lagar, regler och myndighetsdigitalisering) och internationellt (rörande exempelvis teknikutveckling och forskning).

Litteraturförteckning

Arnoldsson, E. (2010). *LedsystT Historia en resumé av 4 faser.* FMV.

Comfort, L. K. (2007). Crisis management in hindsight: cognition, communication, coordination, and control. *Public Administration Review, 67*(1), 189-197.

Fraga-Lamas, P., Fernández-Caramés, T. M., Suárez-Albela, M., Castedo, L., & González-López, M. (2016). A Review on Internet of Things for Defense and Public Safety. *Sensors, 16*(10). doi:10.3390/s16101644

Garcia Lozano, M., Hörling, P., Moradi, F., & Tjörnhammar, E. (2009). Supporting C2 with a Service Oriented Framework for Opportunistic Sensors and Sensor Networks. *Proc. ICCRTS 2009.*

Garcia Lozano, M., Hörling, P., Moradi, F., Sigray, P., & Tjörnhammar, E. (2009). *Dynamiskt Tjänstebaserat Ramverk för Opportunistiska Sensorer och Sensornätverk (TOppS).* FOI-R--2860--SE.

Hammond, G. T. (2018). Appendix - The OODA loop. i *A discourse on winning and losing.* Maxwell AFB, Alabama: Air University Press. Hämtat från https://www.airuniversity.af.edu/Portals/10/AUPress/Books/B_0151_Boyd_Discourse_Winning_Losing.PDF den 9 november 2020

Hedtjärn Swaling, V., & Malmberg Andersson, F. (2018). *NCS3 Förstudie - Bortom sakernas internet.* FOI.

Horndahl, A., Johansson, F., Johansson, R., Mårtenson, C., Rosell, M., Pavlin, G., & Preden, J.-S. (2016). *D5.4 - Design of tools for automatic processing of heterogeneous intelligence information.* FOI-S--5538--SE.

Johansson, R. (2018). *Försvarsmakten i den civila IoT-miljön.* FOI Memo 6641.

Johansson, R., Andersson, M., Hörling, P., & Kamrani, F. (2019). *Samverkande IoT-system och databearbetning.* FOI-R--4884--SE.

Johnsen, F. T., Bloebaum, T. H., Brannsten, M. R., & Lund, K. (2018). Using open standards for utilizing IoT sensor in a smart city scenario. *International command and control research and technology symposium (ICCRTS).* Pensacola, FL, USA.

Johnsen, F. T., Bloebaum, T. H., Calero, J. M., Wang, Q., Nightingale, J., Manso, M., & Jansen, N. (2017). WS-Notification case study and experiment. *International Conference on Military Communications and Information Systems (ICMCIS).*

Johnsen, F. T., Zieliński, Z., Wrona, K., Suri, N., Fuchs, C., Pradhan, M., & Furtak, J. (2018). Application of IoT in Military Operations in a Smart

City. *International Conference on Military Communications and Information Systems (ICMCIS)*, *maj.*

Kamrani, F., Wedlin, M., & Rodhe, I. (2016). *Internet of Things: Security and Privacy Issues.* FOI-R--4362--SE.

Landgren, J., & Borglund, E. (2016). *Lägesbilder - Att skapa och analysera lägesbilder vid samhällsstörningar.* MSB.

Lindgren, D., Andersson, M., Berglund, Å., Nilsson, P., Krona, M., Svenonius, O., . . . Trnka, J. (2018). *BEViS 2018.* FOI MEMO 6613.

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

Open networking foundation. (2016). *SDN Architecture.* ONF TR-521. Hämtat från http://www.opennetworking.org

OSGI. (u.d.). Hämtat från https://www.osgi.org/developer/architecture/ den 18 maj 2020

Poltronieri, F., Stefanelli, C., Suri, N., & Tortonesi, M. (2018). Phileas: A Simulation-based Approach for the Evaluation of Value-based Fog Services. *IEEE 23rd International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD).*

Pradhan, M., Fuchs, C., & Johnsen, F. T. (februari 2018). A Survey of Applicability of Military Data Model Architectures for Smart City Data Consumption and Integration. *IEEE 4th World Forum on Internet of Things*.

Pradhan, M., Poltronieri, F., & Tortonesi, M. (2019). Generic Architecture for Edge Computing Based on SPF for Military HADR Operations. *IEEE 5th World Forum on Internet of Things (WF-IoT).*

Pradhan, M., Suri, N., Fuchs, C., Bloebaum, T. H., & Marks, M. (oktober 2018). Toward an Architecture and Data Model to Enable Interoperability between Federated Mission Networks and IoT-Enabled Smart City Environments. *IEEE Communications Magazine*.

Ruhlig, K. (2019). *Edge Computing.* Fraunhofer Institute for Technological Trend Analysis INT. Fraunhofer institute.

Tortonesi, M., Michaelis, J., Morelli, A., Suri, N., & Baker, M. A. (2016). SPF: An SDN-based Middleware Solution to Mitigate the IoT Information Explosion. *IEEE Symposium on Computers and Communications (ISCC).*

Totalförsvarsstiftelsen. (2019). *Ledningsstudien - regional virtuell samverkan och distribuerad lägesbild.* ISBN nr 4 978-91-983358-3-5.

Wang, W., De, S., Toenjes, R., Reetz, E., & Moessner, K. (2012). A Comprehensive Ontology for Knowledge Representation in the Internet of Things. *IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications.*

Wiklundh, K., & Stenumgaard, P. (2018). *Internet of Things - framtida EMC-utmaningar.* FOI-R--4550--SE.

Wolbers, J., & Boersma, K. (2013). The common operational picture as collective sensemaking. *Journal of Contingencies and Crisis Management, 21*(4), 186-199.

Bilaga 1 – Ordlista

Förkortning	Förklaring
CBRN	Omfattar kemiska, biologiska, radiologiska, och nukleära ämnen
CRIO	Consumer-Ready Information Object
DSPro	Proactive Dissemination Service
FM	Försvarsmakten
FMN	Federated Mission Networking
IO	Information Object
IoT	Internet of things – sakernas internet
JSON	JavaScript Object Notation – datalagrings och -överföringsformat
MANET	Mobile Ad hoc NETwork
MQTT	Message Queuing Telemetry Transport
MTOC	Mobile Tactical Operations Center
NGVA	NATO Generic Vehicle Architecture
OODA	Observe, Orient, Decide, Act
PIG	Programmable IoT Gateway
RFID	Radio-frequency identification
SCM	Service Component Manager
SDN	Software Defined Networking
SPF	Sieve, Process, Forward
UAV	Unmanned aerial vehicle – Obemannat luftfartyg, drönare
UGV	Unmanned ground vehicle – Obemannat markfordon
UxV	Ospecificerad form av obemannad farkost
VoI	Value of Information

Tabell 1. Lista över förkortningar

Bilaga 2 – Kompletterande aspekter på lägesbild

En regelbundet uppdaterad lägesbild kan naturligtvis genereras som en del i en kontinuerligt pågående övervakning. Den kan då ofta sättas i jämförelse med en genomsnittlig ”normalbild”, där beredskapsnivån att agera på förändringar i förhållande till denna i vissa mindre kritiska fall kan vara låg om sådana inte förväntas, men där man skall kunna gå upp till kortare reaktionstid efter att förvarningar erhållits. På mer sårbara platser eller arenor som kärnkraftverk, flygplatser, militära ledningscentraler i gråzonstid, seismiska övervakningscentraler krävs att man ständigt har högre beredskapsläge och snabbare kan reagera på erhållen information. Den lägesbild denna information försörjer måste då också uppdateras med högre takt. Inom vilka numeriska ramar ”takt” skall sättas beror på hur snabbt tillståndet kan ändras mellan normalt, avvikelseindikering, allvarligt, och katastrofalt och kan beroende på tillämpning variera från sekunder till veckor. Detta påverkar naturligtvis vilken längsta responstid som kan accepteras för informationsinsamlande funktioner och reglerande funktioner, det vill säga de åtgärder man kan vidta för att styra händelseutvecklingen.

Då mycket snabb responstid krävs finns ofta automatiserade reglersystem som reagerar snabbare än människan. De är ofta regelbaserade även om system baserade på mer sofistikerad Artificiell Intelligens är på frammarsch. Man brukar tala om den så kallade OODA-loopen (Hammond, 2018) Observe, Orient, Decide, Act, där det avgörande för en gynnsam händelseutveckling är att man kan observera och förstå utvecklingen samt ta beslut och agera tillräckligt snabbt för att kunna påverka den. Om händelseutvecklingen accelererar tar den överhanden och man blir så att säga ”frånsprungen” av denna och möjligheten att effektivt agera begränsas. När man till sist försöker hindra en viss händelse från att inträffa har den redan hänt och man kan i bästa fall försöka lindra dess negativa effekter.

Beroende på krisens karaktär kan olika sammansättningar av flera organisationer behöva göras, vilket också påverkar organisationernas lägesbilder. Organisationerna måste lära sig att gå från normalläge med det informationsflöde och arbetssätt och -takt medarbetarna är vana vid, till att samarbeta med medarbetarna i de andra organisationerna. Då informationsbehov och arbetsprocesser skiljer sig åt måste sådant övas i förväg för att fungera i skarpt läge så man förstår varandras behov, hur man kan hjälpa men även dra nytta av övriga aktörer, deras kunskap och information. Det säger sig självt att det är svårt, eller snarast omöjligt, att få många heterogena aktörer att oövade, utan erfarenhet av samarbete med varandra, direkt sätta sig tillsammans (fysiskt, eller virtuellt) och bli perfekt samspelta med ett gemensamt fokus att föra en plötsligt uppkommen kris

till lösning. Om förövning inte skett blir det lätt kaotiskt och man får samtidigt som krisen fortlöper försöka förstå varandra och finna samarbetsformer ad-hoc.

Det är viktigt att man i förväg klarat ut vilken information som kan, eller alls får (juridiskt) delas, hur man skall kunna förstå information man kan erhålla från andra (både semantiskt och hur den skall kunna mottas och presenteras av egna tekniska informationssystem). Det kan underlätta att i förväg komma överens om vem som ”prenumererar” på vilken typ av information från andra organisationer. Man måste kunna förstå denna information och hur man kan dra nytta av den i sin egen kontext. En mer djuplodande studie i dessa problemområden redovisas i Lindgren (2018).

Det är troligtvis av juridiska skäl lättare att dela med sig av ett informationsflöde från egna sensorer där mottagaren inte lagrar informationen annat än en kort tid. Om information alls får lagras en längre tid för att nyttjas till uppföljning och ”lessons learnt” så är det sannolikt att ansvaret för detta faller på den part som ursprungligen samlade in informationen. Här kan man även hamna i en gråzon om information ägd av olika organisationer fusioneras till en aggregerad lägesbild, vem äger den lägesbilden? Får denna då alls sparas?

ISSN 1650-1942

www.foi.se