Slutrapport Verktyg för informationshantering och analys (VIA)

CHRISTIAN MÅRTENSON, PONTUS SVENSON

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

FOI-R--3533--SE
ISSN 1650-1942

December 2012

Christian Mårtenson, Pontus Svenson

Slutrapport Verktyg för informationshantering och analys (VIA)

Titel	Slutrapport Verktyg för informations-hantering och analys (VIA)
Title	Final report Tools for Information Management and Analysis
Rapportnr/Report no	FOI-R--3533--SE
Månad/Month	December
Utgivningsår/Year	2012
Antal sidor/Pages	52 p
ISSN	1650-1942
Kund/Customer	FM
FoT område	Ledning och MSI
Projektnr/Project no	E36701
Godkänd av/Approved by	Lars Höstbeck
Ansvarig avdelning	Informations- och aerosystem

Sammanfattning

Den här rapporten sammanfattar verksamheten och resultaten från FoT-projektet Verktyg för informationshantering och analys (VIA). Projektet har under tre års tid, 2010-2012, bedrivit forskning för att ta fram nya algoritmer, metoder och verktyg för informationsfusion och underrättelseanalys.

För att säkerställa relevansen av forskningen har VIA-projektet genomfört ett flertal domänkompetenshöjande aktiviteter parallellt med att en kontinuerlig dialog hållits med intressenter och slutanvändare från FM. En viktig insats har varit en användarstudie där ett antal fiktiva men representativa användarprofiler, så kallade personas, tagits fram baserat på intervjuer med underrättelseanalytiker.

Forskningen i projektet kan delas in i tre temaområden. Det första handlar om effektiv hypoteshantering och hur man kan utveckla verktyg som stödjer den analytiska processen. Det andra temaområdet är riktat mot taktisk underrättelsehantering och handlar om hur information bör struktureras för att effektivisera inhämtning och möjliggöra heterogen fusion. Det sista området behandlar text- och nätverksanalys med syftet att snabbare kunna kartlägga trender och hot på internet. Temaområdena hänger nära samman och alla aktiviteter har arbetat med en gemensam teknisk plattform för att möjliggöra enkel integration och återanvändning av implementerade algoritmer och verktyg.

Forskningsresultaten består bland annat av ett verktyg för multihypoteshantering, ett verktyg för inmatning av strukturerad information, metoder för fusion av heterogen information, en metod för att identifiera hotaktörer på webben, samt algoritmer för att utföra analys av sociala nätverk baserade på osäker data.

Utöver forskningsresultaten har projektet levererat nytta till FM genom kunskapsöverföring i form av rapporter och seminarier, samt genom direktstöd i form av teknisk expertis vid olika arbetsgrupper och företagspresentationer.

Under 2013 och framåt kommer flera av metoderna och verktygen att fortsätta att utvecklas, dels inom VIA:s många samarbetsprojekt, dels inom ett nytt FoT-projekt, Stödverktyg för informationsfusion och analys (SIA).

Nyckelord: informationshantering, informationsfusion, underrättelseanalys

Summary

This report summarizes the activities and results of the project Tools for Information Management and Analysis. The project started 2010 and ended 2012. Throughout these years research has been conducted with the end goal of developing new algorithms, methods and tools for information fusion and intelligence analysis.

To ensure relevance of the research the project has kept a close dialogue with stakeholders and end users from the Swedish Armed Forces. Additionally, a user study was performed in which a number of fictitious but representative user profiles were developed based on interviews with intelligence analysts.

The project's research can be divided into three areas: hypothesis management, heterogeneous fusion, and web based trend and threat analysis. The research resulted in an analysis tool for multi-hypothesis management, a reporting tool for input of structured information, a method for fusion of heterogeneous information, a method to identify potential terrorists on the web, and algorithms for social network analysis on networks with uncertain data.

Research will continue in a follow-up project as well as in a number of closely related on-going projects.

Keywords: information management, information fusion, intelligence analysis

Innehållsförteckning

1 Inledning

Inom flera av Försvarsmaktens (FM) inhämtningsdiscipliner ökar mängden tillgänglig information, vilket gör det allt svårare för människan att tillgodogöra sig den och upprätthålla sin situationsförståelse. Ökad tillgång till bättre och billigare sensorer, ett ökat informationsutbyte med allierade, samt en ökad användning av ny teknik och nya media hos både motståndare och allmänhet gör också att man måste kombinera olika informationskällor och format. Det är av stor vikt för FM att kunna dra nytta av denna splittrade och växande informationsbild för att inte hamna i informationsunderläge. För detta krävs inte bara kraftfull bearbetningsförmåga inom respektive inhämtningsdisciplin, utan också förmågan att hantera, fusionera och analysera den bearbetade informationen.

Den här rapporten utgör slutrapporten för FoT-projektet Verktyg för informationshantering och analys (VIA). Projektet har pågått mellan 2009 och 2012 under vilket forskning har bedrivits kring nya verktyg för att inhämta, fusionera, analysera och presentera underrättelseinformation. Målbilden har varit inspirerad av Popp och Poindexters försök från 2005, som visade att en uppsättning datorbaserade verktyg för bland annat sökning, automatöversättning och hypotesnedbrytning ökade produktiviteten hos analytiker och frigjorde tid för analysfasen, den fas i underrättelsearbetet där människans kognitiva förmågor är mest värdefulla.[1]

1.1 Bakgrund

VIA-projektet har varit en del i Försvarsmaktens samlingsbeställning till FOI. Utpekade huvudmottagare har varit MUST UTV, FMKE Knowledge Support och UndSäkC, med en mängd övriga intressenter både inom FM och andra myndigheter. Ett ingångsvärde var att bygga vidare på den kunskap och de resultat som tagits fram inom föregående FoT-projekt Situations och hotanalys för BG 2011[2]. Ett av dessa resultat var hypotesvärderingsverktyget Impactorium, som under 2009-2010 vidareutvecklats inom ramen för FM:s transferprogram. VIA-projektet och Impactorium-transferprojektet har haft ett nära samarbete, framför allt kring den tekniska plattform som byggts upp kring Impactorium och som fungerat som en integrationsplattform för nya forskningsresultat.

[1] Popp och Poindexter, *Countering Terrorism through Information and Privacy Protection*, IEEE

[2] Se FOI-R--2859--SE, 2009

Projektbeskrivning
Följande text utgör beskrivning av frågeställningar och syfte från projektbeställningen:

> *Nuvarande och framtida insatsförband har att hantera en stor mängd heterogen information från olika källor, från sensorinformation till skriven text. Projektet ska utveckla och testa verktyg som hjälper analytiker och beslutsfattare att kvalitetsmärka, hantera och analysera denna information, t ex för att besvara underrättelsefrågor eller planera framtida handlingar. Syftet med projektet är att utveckla fusionsalgoritmer samt beslutsstödsverktyg och -metodik som bidrar till ökad lägesförståelse för insatsförbanden. Verktygen ska kunna hantera såväl information från sensorer som und-information och annan text. Projektet ska ta fram en gemensam arkitektur för samtliga beslutsstödsverktyg, och anpassa denna så att det är möjligt att utnyttja verktyg som tagits fram i tidigare projekt (Impactorium). Projektet ska undersöka hur de verktyg som utvecklas kan anpassas för användning i internationella insatser där andra länder än Sverige har ansvar för ledningssystemen.*
>
> *Exempel på frågeställningar som projektet skall försöka besvara:*
>
> - *Inom informationsanalys: Hur ska verktyg för analys av heterogen information (inkl. textinformation och sensorfusionsresultat) användas, utformas och utvecklas?*
> - *Inom informationshantering: Hur ska heterogen information från olika källor (sensorer, text, und-analyser, bakgrundskunskap) märkas och hanteras för att säkerställa att den blir sökbar och att osäkerheter i den hanteras rätt?*
> - *Inom informationspresentation: Hur ska visualisering och interaktion med människan användas för att förbättra informationsanalysen?*
>
> *Projektmål är att ha utvecklat nya algoritmer, verktyg och metoder för underrättelseanalys. Effektmål är att implementationer av dessa resultat leder till ökad lägesförståelse och förmåga till informationshantering hos FM.*

1.2 Genomförande

Fokus under projektets första år låg på att bygga upp en fördjupad domän- och behovsförståelse kring underrättelseanalys samt att göra en omvärldsanalys för att identifiera viktiga forskningsfrågor inom ramarna för beställningen. Omvärldsanalysen genomfördes i form av en litteraturstudie med fokus på viktig forskning inom området informationsfusion under 2009-2010 och finns utgiven

som en FOI-rapport [1]. En del forskningsfrågor ärvdes även från det tidigare FoT-projektet, vilket bidrog till att forskningen inte behövde avstanna i väntan på resultat från behovsarbetet. Under andra och tredje året har fokus flyttats till ren forskningsverksamhet samt implementation av demonstrationsverktyg. Omvärldsbevakningen har dock fortsatt, främst genom deltagande i för området centrala akademiska konferenser såsom Fusion och EISIC. Dessa konferenser har också spelat en roll i projektets kvalitetssäkringsarbete där publicering i konferenser och tidsskrifter med granskningsförfarande har varit centralt. Projektets vetenskapliga publikationer finns listade i avsnitt 6.2.

Projektarbetet har till största del bedrivits av medlemmar från FOI:s kompetensområde Beslutsstöd, kunskapshantering och informationsfusion (BKI), men har kompletterats med forskare från enheterna Sensorinformatik och Människa teknik organisation, samt med operationsanalytiker med kopplingar till FM:s underrättelsefunktion. Under 2010 leddes projektet av Pontus Svenson och under 2011-2012 av Christian Mårtenson.

En viktig komponent i projektarbetet har varit att knyta kontakter och samverka med andra forskare i syfte att stimulera till nya idéer och öka effekten av satsade medel. Utöver Impactorium-transferprojektet har VIA framför allt haft nära samarbete med ett antal EU-projekt som projektet medfinansierat. Samarbete har även skett i hög grad med svenska universitet och högskolor till vilka projektgruppen har många kopplingar. Projektet har även finansierat deltagande i en NATO-grupp. En mer ingående redogörelse för projektets samarbeten ges i kapitel 4.

För att säkerställa att framforskade algoritmer och verktyg ska kunna återanvändas i olika projekt, har ett ramverk för integration tagits fram baserat på den kod som utvecklats för Impactorium i tidigare projekt. Ramverket består av en plattform för lagring av information, fusions- och analysresultat, samt olika tjänster (algoritmer och verktyg) för informationshantering, fusion och analys.

För att säkra framtida samarbeten och nuvarande forskningsvolym har projektet deltagit i ett antal forskningsutlysningar, framförallt inom EU:s säkerhets-forskningsprogram. Bland de ansökningar som lämnats in och där utvärderingen är klar har fyra stycken beviljats. Två av dessa behandlar informationshantering och riskanalys för post (SAFEPOST) respektive flygfrakt (EUROSKY) och hänger tematiskt ihop med tidigare EU-projekt inom transportsäkerhet som FOI bedriver. FOI deltar i båda projekten med metoder för riskvärdering och hypoteshantering som är direkt överförbara till VIA:s intressen. Förutom den verksamhet som medfinansieras från VIA deltar FOI också med utveckling av förbättrade system för detektion av farliga ämnen i projekten. SAFEPOST startade i april 2012 och avslutas i mars 2016, medan EUROSKY förväntas börja i januari eller februari 2013 och avslutas fyra år senare. Projektet FIDELITY, som handlar om förbättrad hantering av biometrisk information i pass, startade i februari 2012 och avslutas januari 2016. VIA medfinansierar här utveckling av

arkitektur och metoder för distribuerad analys i databaser med olika behörighetsrättigheter; större delen av FOI:s medverkan handlar om IT-säkerhetsaspekter. Slutligen pågår startförhandlingarna med EU om D-BOX, ett projekt om förbättrade minröjningssystem. VIA medfinansierar här forskning om fusion av text och sensordata.

I säkerhetsforskningsutlysningen 2012 deltar FOI i några ansökningar med forskning relaterad till VIA och dess efterföljande projekt.

1.3 Nytta för Försvarsmakten

Nyttan för FM av VIA-projektet kan delas in i tre kategorier: forskningsresultat, kunskapsöverföring och direktstöd.

Forskningsresultaten svarar mot VIA:s projektmål, att ha tagit fram nya verktyg, algoritmer och metoder för underrättelseanalys. Tabell 1 nedan listar de konkreta resultaten och var information om respektive resultat finns publicerat. Kapitel 3 ger en översikt över bedriven forskning och sätter resultaten i ett sammanhang.

Tabell 1. Projektets forskningsresultat.

Forskningsresultat	**Referenser**
Verktyg för multihypoteshantering	[3,10]
Verktyg för inmatning av strukturerad information	[28,41]
Verktyg/algoritmer för inhämtningsstyrning	[13,18,19,32]
Verktyg för trendanalys på webben	[9,21,26,30,35,38]
Metod för fusion av heterogen information	[7,16,27]
Metod för samverkan mellan fusionssystem på olika ledningsnivåer	[23,45]
Metod för att identifiera hotaktörer på webben	[8,9,25,29,39,40,48]
Metod för användarprofilering i hemliga organisationer resp. av motståndarorganisationer	[46,47,49]
Algoritmer för att beräkna SNA-mått på osäker data	[9,20,24,31]
Algoritmer för abstraktion av nätverk	[15,36]
Algoritmer för planigenkänning	[12,42]

Kunskapsöverföringen har inneburit att med rapporter och presentationer överföra den kunskap som byggts upp genom forskningen till huvudmottagarna inom FM och andra intressenter.

Målet med rapporterna har varit att skapa lättillgängliga och icke-tekniska beskrivningar av de adresserade forskningsfrågorna för att belysa dessa för en relativt bred läsekrets inom försvarsfamiljen. Rapporterna finns listade med korta sammanfattningar i avsnitt 6.1.

Projektet har presenterat sin verksamhet vid ett stort antal informella möten med olika representanter för bland annat MUST, FMKE, PROD LEDUND, Underrättelsebataljonen, ITF, Psyops-förbandet och FMV. En mer officiell presentation av resultatet av den användarprofileringsstudie som genomförts har anordnats på HKV i formen av en vernissage. Projektet har också hållit presentationer vid FMV:s sensorsymposium 2012, FMV:s workshop om Team Situation Awareness, samt anordnat och hållit presentationer vid en polisforskningskonferens där flera representanter från FM deltog. Medarbetare i projektet har även blivit inbjudna och hållit presentationer på FRA, Polisen, Riksdagen och AFCEA.

FoT-projektens direktstöd till FM utgör en viktig komponent i forskningens nyttiggörande. FM har vid behov möjlighet att åberopa stöd i form av till exempel särskilda rapporter, expertgranskning av programvaror eller studiedeltagande. VIA-projektet har lämnat expertstöd i ett flertal sammanhang:

- Projektet har gett stöd till FM:s verksamhet för skydd mot improviserade sprängladdningar (C-IED). Under 2010 deltog medarbetare i projektet vid flera möten i C-IED-arbetsgruppen där de stöttade med råd om informationshantering. I projektets årsrapport för 2010 [2] finns en kort redogörelse för detta.
- Under 2011-2012 har projektet medverkat i FM:s förstudie Exploatering mot irreguljära aktörer och den därpå följande utredningen om Verkan mot illegala aktörers nätverk (Attack the Networks) för att diskutera hur FOI:s och projektets kompetens kan nyttiggöras. Som en följd av detta har även en projektmedarbetare bjudits in till att bidra med undervisning om nätverksanalys i en kurs på temat Attack the Networks som anordnades av FHS hösten 2012.
- Under 2008-2009 genomförde EDA (European Defence Agency) ett projekt med namnet CSUI (Common Standardised User Interface). Det har bekostats av medlemsländer, och haft som mål att undersöka möjligheterna i ett gemensamt användargränssnitt för underrättelsetjänst. VIA-projektet blev inbjudet av FM att bevista en demonstration i Bryssel av CSUI i egenskap av teknisk expertis. I projektets årsrapport för 2010 [2] finns en kort redogörelse för detta.
- Projektet har som oberoende tekniska experter blivit inbjudna av FM att delta vid en stor mängd företagspresentationer. FOI har även hjälpt till att anordna flera av dessa.

- Projektet har stöttat MUST med expertkompetens vid tre interna workshopar för analytiker, inom kritiskt tänkande, morfologisk analys och analys av konkurrerande hypoteser.
- Medarbetare i VIA-projektet har bidragit till FOI:s underlag till regeringskansliet inför nästa försvarspolitiska inriktningsbeslut. Bidraget bestod av ett kapitel om möjligheter och hot i informationssamhället i huvudbilagan, samt ett kapitel i den bifogade rapporten Strategic Outlook 2012[3] om möjligheterna att med hjälp av analys av svaga signaler hitta ensamagerande terrorister.
- Projektet har kontinuerligt haft informationsutbyte med MUST och vid ett flertal tillfällen agerat diskussionspart vid kravställningsarbete.

1.4 Rapportstruktur

Resterande del av den här rapporten är upplagd enligt följande. Kapitel 2 ger en översikt över projektets arbete med att bygga upp kompetens kring underrättelsedomänen. Kapitel 3 beskriver den forskning som bedrivits och sätter forskningsresultaten i sitt sammanhang. Därefter följer i kapitel 4 en redogörelse för de samarbeten som projektet har haft med andra projekt och organisationer. Kapitel 5 återger planen för fortsatt forskning och slutligen listas projektets publikationer i kapitel 6.

[3] Emma Skeppström, Stefan Olsson och Åke Wiss (red.), *Strategic Outlook 2012*, FOI-R--3449--SE, 2012

2 Domänförståelse

VIA-projektet har bidragit kontinuerligt till att förbättra projektdeltagarnas kännedom om underrättelsedomänen för att bättre kunna fånga forskningsbehov och därigenom öka relevansen i forskningen. Ett flertal domänkompetenshöjande aktiviteter har genomförts parallellt med att en dialog hållits med intressenter och slutanvändare från FM. Den största insatsen har varit den användarprofilering som påbörjades under 2010 och slutfördes och levererades under tidig vår 2011. Nedan redovisas denna profileringsstudie liksom ett antal övriga aktiviteter med användaranknytning.

2.1 Användarstudie personas

Personas är beskrivningar av fiktiva användare som syftar till att fånga de verkliga användarnas beteendemönster, mål och behov. Dessa beskrivningar kan till exempel skapas utifrån användarstudier och tjänstebeskrivningar. Personas används för att utvecklare ska kunna skapa anpassade hjälpmedel och stödverktyg.

Personas-metoden har potential att skapa en gemensam beskrivning och uppfattning om användarna av ett specifikt system. Denna beskrivning kan ge ett systemutvecklingsteam en gemensam uppfattning om vilka användarna är, vilket kan utnyttjas i utvecklingen av system genom att vara en del av beställarprocessen samt att ge utvecklarna en konkret bild att arbeta utifrån. Personas kan också användas som ett designverktyg för att kommunicera användarbehov och krav kontinuerligt under hela systemutvecklingsprocessen.

Personas används för att möjliggöra en starkare koppling mellan den forskning som bedrivs och relevanta användare. Metoden är relativt vanlig inom industriella utvecklingsprojekt, medan VIA:s användning av den för att hjälpa till att inrikta forskning är mer innovativ.

Arbetet med personas började under våren 2010 då hypotetiska personas baserade på inläsning av tidigare FOI- och FHS-material skapades och reviderades efter diskussion med MUST UTV. En säkerhetsanalys av arbetet genomfördes också. Intervjuer genomfördes sedan hösten 2010, följt av analysarbete och skapande av slutgiltiga personas. Förutom själva personas togs också en önskelista över framtida informationshanteringssystem fram under intervjuarbetet. Arbetet redovisades för FM under första kvartalet 2011 genom en användardag på HKV den 21 januari. Dagen hade två delar: På förmiddagen genomfördes föreläsningar om personas/användarprofiler och visualisering. Denna del var öppen för all personal på HKV. Ca 30 personer bevistade föreläsningarna. Under eftermiddagen genomfördes en ”vernissage” av de personas som tagits fram, där också forskarna som genomfört arbetet deltog.

Vernissagen var av drop in-format och besöktes av totalt ca 40 personer från MUST, inklusive chefspersoner. Möjlighet gavs att ge feedback på personas. Ett fåtal förtydligande och rättelser inkom, men det generella intrycket var att användarprofilerna var väl underbyggda och trovärdiga. Ytterligare redovisning av personasarbetet har levererats direkt till FM. Figur 1 illustrerar principen för hur en persona kan se ut.

För att befästa personas-arbetet i projektet och koppla resultaten till övriga forskningsaktiviteter har två projektinterna workshops anordnats. Målet var att lära känna de olika användarprofilerna, förstå deras respektive behov och koppla dessa till projektets pågående tekniska forskning och bistå i inriktningen av nya aktiviteter. En persona har valts ut som ”huvudpersona” för projektet. Denna persona är en analytiker på MUST med ansvar över ett visst geografiskt område. För att identifiera vilka möjliga verktyg som skulle kunna vara till bra stöd har ett mer detaljerat scenario tagits fram med en händelsekedja och frågeställningar som måste hanteras. I en version av scenariot antar vi att analytikern har tillgång till ett antal framtida stödverktyg och spekulerar i hur detta kan hjälpa analysarbetet. Dessa verktyg består av avancerade text- och nätverks-analysverktyg som kan stödja analytikern att snabbt skaffa sig en grov uppfattning om vilka entiteter i scenariot som är av vikt och hur de är relaterade. Denna analysmodell ligger sedan till grund för förfinad manuell analys och generering och prövning av hypoteser. Scenariot har stämts av med en erfaren underrättelseanalytiker från MUST.

En grundlig utvärdering av nyttan av personas för styrning av forskningsverksamheten har ännu inte genomförts. En preliminär sammanfattning av erfarenheterna är dock att personaarbetet har bidragit stort till den allmänna domänförståelsen inom projektet. Av särskild vikt har den ökade förståelsen för vissa arbetsflöden inom MUST varit. Dessa har konkretiserats i ovan nämnda scenario och därigenom ökat förståelsen för i vilka situationer som de olika forskningsverktygen kan komma till nytta. För den konkreta verktygsdesignen har de framtagna personas haft mindre betydelse, främst på grund av att mognaden hos de framforskade verktygen inte uppnått en sådan nivå att de verkliga användningssituationerna spelar stor roll.

Kim Granath 35 år **Ledord:** *”Analysen ger förståelse för uppdraget”*	
Roll:	Kim gör huvudsakligen analyser åt UD. Han har arbetat i sju år och kom dit efter sin magisterexamen i idehistoria. Det långsiktiga uppdraget är att ”*ha koll på*” XX och organisationer där. Detta innebär att han alltid läser dagstidningar samt även gräver i landets historia för att alltid kunna vara förberedd på frågor som berör området…[..]
Arbetsmiljö:	Kim arbetar på Högkvarteret. Han har ett eget kontorsrum där han arbetar när han läser och skriver. En stor del av tiden går åt att vara i kontakt med kollegor både inom sektionen och på andra delar av …[..]
Verktyg:	PC, papper & penna, tidningar, …
Scenario:	Kim kommer till arbetet kl 0600. Redan på bussen har han läst de svenska dagstidningarna. Direkt på kontoret läser han sedan Internettidningar för att gå på ett enhetsmöte kl 0900. Efter ska han författa en dagrapport till YY. På enhetsmötet får han ett nytt uppdrag att snabbt sammanställa en rapport om en familjefejd…[..]
Mål:	• Ha ett stimulerande uppdrag med stor frihet • Göra en rapport som gör skillnad
Behov:	• Videokonferenssystem, öppet Internet

Figur 1. Exempel som illustrerar principen för hur en persona kan se ut. Exemplet har av sekretesskäl ingen koppling till de personas som togs fram baserat på intervjuerna.

2.2 Övriga aktiviteter

Utöver personastudien kan de aktiviteter som genomförts i projektet för att bygga kunskap kring underrättelsedomänen delas in i kurser, övningar, företags-presentationer och användarmöten.

Kurser

- VIA:s projektmedarbetare har deltagit i kurser om Försvarmaktens informationshanteringssystem.
- Kurs i underrättelseanalys. En 3-dagars kurs i underrättelseanalys hölls i maj 2011 för projektet i UndSäkC:s regi. Kursen innehöll en övergripande del samt fördjupningar inom bearbetning respektive teknik. Upplägget erbjöd även många tillfällen för diskussioner om problem och frågeställningar relevanta för projektets forskning.

Övningar

- Viking 11. Fyra projektmedarbetare besökte den stora distribuerade stabsövningen Viking 11 vid LedR och Stenvreten i Enköping ett antal dagar vecka 14 och 15, 2011. Något som är speciellt för vikingövningen är samverkan mellan militära och civila organisationer. Totalt medverkade personal från 26 nationer. Det välkända så kallade Bogalandscenariot användes. Uppgiften för VIA:s räkning var att undersöka hur övningsdeltagarna såg på de verktyg de använde för underrättelsehantering, både under övningen och i verkligheten. Iakttagelser, huvudsakligen från NBG:s J2-funktion, blandat med idéer om hur forskningen i VIA och relaterade projekt skulle kunna förbättra verksamheten, finns redovisade i kvartalsrapport 2, 2011[4].
- Workshopar med analytiker. Medarbetare i projektet har observerat och på olika sätt deltagit i en serie workshopar som MUST anordnat för analytiker.

Företagspresentationer

- För att skapa en överblick av vad marknaden har att erbjuda inom system för informationsfusion och underrättelseanalys, har en stor mängd kommersiella aktörer bjudits in till FOI för att presentera sina produkter, till exempel Autonomy, Basis Technology, Columba, Detica, Gavagai, i2, Palantir, Recorded Future och Silobreaker. Några av dessa kontakter har följts upp med nya möten, vilket bland annat resulterat i ett samarbete med Recorded Future om trendspaning på webben, vilket finns beskrivet i avsnitt 3.3.1.

[4] FOI Memo 5120.2, Christian Mårtenson, *Kvartalsrapport 2 2011 för VIA - Verktyg för informationshantering och analys*, 2011

Användarmöten

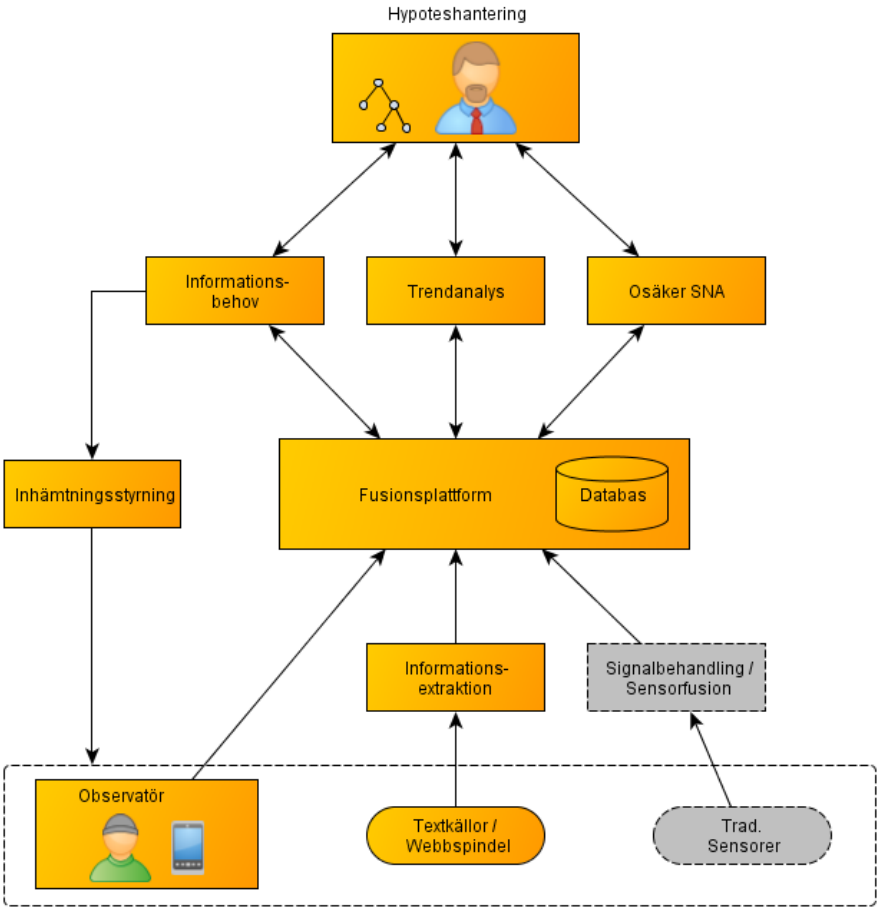
- Möte FMKE 2009. Innan projektstart, på hösten 2009, genomfördes en brainstorming kring behov och forskningsfrågor med representanter från FMKE Knowledge Support. Dessa har fungerat som en god startpunkt för hela behovsarbetet.
- Några projektmedarbetare har i mars 2010 fått en förevisning av OSINET, FM:s verktyg för inhämtning av öppen information på internet.
- Möte FMKE 2011. I maj 2011 besökte projektet åter FMKE Knowledge Support i Enköping för en heldag med informations- och erfarenhetsutbyte.
- Möte med underrättelseanalytiker. I november 2011 genomfördes en användardag på FOI i Kista, där VIA-projektet diskuterade scenarion, underrättelsemetodik och forskningsidéer med en erfaren underrättelseanalytiker från MUST. Syftet var att värdera realismen av framtagna scenarion och stämma av hur projektets verktygsförslag matchar underrättelsefunktionens behov.
- Besök hos UndBat. I juni 2012 åkte fem projektmedarbetare till Karlsborg på studiebesök hos underrättelsebataljonen. Nya behov inom informationshantering och analys fångades upp och projektet fick värdefull återkoppling på sin verksamhet.
- Polisen. FOI har inom ramen för projektet vid ett flertal tillfällen haft informationsutbyte med olika delar av RKP och SÄPO.
- Löpande dialog med MUST UTV. En central intressent för projektet har varit MUST UTV. Tack vare den täta dialog som projektet har haft med sin kontaktperson där har många dörrar öppnats vilket inneburit bättre och snabbare tillgång till domänkunskap och användare.

3 Bedriven forskning

De övergripande forskningsfrågorna som formulerats i projektbeställningen, har under projektets gång konkretiserats och exemplifierats i takt med att domänförståelsen ökat och dialogen med FM fortskridit. Forskningsfrågorna har adresserat olika aspekter av informationshanteringsprocessen men bidragit till samma övergripande systembild.

Figur 2 ger en översikt av hur komponenterna som projektet forskar kring hänger ihop. Längst ned finns ett antal inhämtningsresurser i form av människor, traditionella sensorer och system för inhämtning av textbaserad information. I lagret ovanför finns olika typer av moduler för signalbehandling med syftet att extrahera informationselement och strukturera den för vidare fusion och analys. Den strukturerade informationen lagras i fusionsplattformen som fungerar som en så kallad ”blackboard”, där olika tjänster kan publicera information som sedan kan utnyttjas för vidare bearbetning av andra tjänster. Dessa tjänster kan sen i sin tur publicera mer förädlad information till samma plattform. I den övre delen av bilden finns analytikern med en mängd stödverktyg för hypoteshantering och analys. Vid analysen uppkommer osäkerheter som genererar behov för inhämtning av ny information. Stöd för hur dessa ska prioriteras sköts av inhämtningsstyrningen. Inhämtning, signalbehandling och fusion av traditionell sensorinformation har inte gjorts inom VIA-projektet, men behandlad sensordata har i vissa fall tillhandahållits av andra aktörer inom de medfinansierade EU-projekten.

I nedanstående beskrivning har forskningen delats in i tre temaområden. Det första handlar om hypoteshantering och hur man kan utveckla verktyg som stödjer den analytiska processen. Det andra temaområdet är riktat mot taktisk underrättelsehantering och handlar om hur information bör struktureras för att effektivisera inhämtning och möjliggöra heterogen fusion. Det sista området behandlar text- och nätverksanalys i syfte att snabbare kunna kartlägga trender och hot på internet, en tillämpning som berör mer eller mindre samtliga delar av det uppskissade systemet.



Figur 2. Övergripande bild över de komponenter som VIA bedrivit forskning kring. Pilarna representerar informationsflöden. Inom de grå komponenterna har VIA inte utfört någon egen forskning, men kopplingarna har ändå kunnat studeras tack vare samarbete med andra projekt.

3.1 Hypoteshantering

De uppgifter som underrättelseanalytiker måste hantera är komplexa. Förenklat kan dessa bland annat sägas bestå av att i stora mängder av inkomplett och osäker data, insamlad från en rad olika källor med varierande tillförlitlighet, kunna urskilja relevanta bitar av information och utifrån dessa formulera hypoteser. Troligheten hos dessa hypoteser kan sedan analyseras genom insamling av ytterligare evidens som talar för eller emot de uppställda hypoteserna. Redan med 3-4 aktiva hypoteser blir det svårt för en människa att

hålla all relevant information i minnet. En starkt bidragande orsak till detta är att antalet kopplingar mellan hypoteser och evidens ökar snabbt med varje nytt evidens som blir tillgängligt. För att en mänsklig analytiker ska klara av att samtidigt hantera många alternativa hypoteser krävs ett strukturerat arbetssätt. En komplicerande faktor är att detta arbete också ofta görs under tidspress.

VIA-projektet har undersökt hur datorstöd skulle kunna användas för att underlätta analytikers hypoteshanteringsarbete. I dialog med MUST UTV har följande forskningsfråga tagits fram.

Hur bör ett hypoteshanteringsverktyg utformas för att:

1. *stödja en analytiker vid skapandet av nya hypoteser,*
2. *öka en analytikers förmåga att hantera flera alternativa hypoteser, samt att*
3. *hjälpa en analytiker att hitta för hypotesarbetet relevant information, såsom relaterade hypoteser, underlag och kompetenser?*

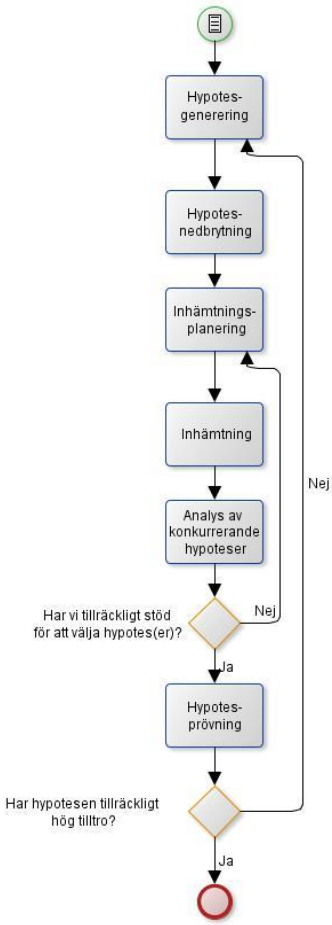
Arbetet med forskningsfrågan har gjorts i tre steg. Först har ett konceptuellt arbete gjorts för att kartlägga var och hur datorstöd kan tänkas spela en roll i hypoteshanteringsarbetet. Det andra steget har varit att göra en inventering av befintliga analytiska verktyg i form av metoder och modeller som kan utgöra pusselbitar vid konkretiseringen av det konceptuella arbetet. I det tredje steget har ett nytt datorverktyg för multihypoteshantering tagits fram och implementerats i en första version.

3.1.1 Datorstöd för hypoteshantering

Det konceptuella forsknings- och utvecklingsarbetet kring generellt datorstöd för hypoteshantering har sammanfattats i en FOI-rapport [3]. Rapporten beskriver ett koncept för ett hypoteshanteringsverktyg som är tänkt att stödja underrättelseanalytiker i deras arbete med att skapa och pröva olika hypoteser. Det föreslagna verktyget bygger på ett agentbaserat tänkesätt i vilket analytikern bidrar med den rena analysverksamheten och datorverktyget bidrar med funktionalitet för att strukturera arbetet, söka och rekommendera relaterad information och öka spårbarheten i analysen. Vidare erbjuder förslaget till hypoteshanteringsverktyg stöd för ett kollaborativt arbetssätt, dels genom att möjliggöra att sökningar görs efter relaterade hypoteser som är skapade av andra analytiker, dels genom att uppmuntra till interaktion och samarbete. Rapporten är en vision om hur denna typ av verktyg ska kunna fungera i framtiden, och beskriver var och hur tekniken bäst kommer till nytta och hur arbetsprocessen kan anpassas. Några av idéerna som presenteras kan implementeras med en relativt liten arbetsinsats medan andra ligger längre fram i tiden. De idéer som lyfts fram rörande hur analysprocessen kan göras mer strukturerad och hur vissa

delar av arbetet kan automatiseras syftar alla till att skapa ökat utrymme för den mänsklige analytikern att fokusera på den avancerade analysen och på så sätt uppnå högre kvalitet i sitt arbete.

Figur 3 visar den övergripande hypoteshanteringsprocessens delar: hypotesgenerering, hypotesnedbrytning, inhämtningsplanering, inhämtning, analys av konkurrerande hypoteser (eng. Analysis of Competing Hypotheses, ACH), samt hypotesprövning. I rapporten har respektive del brutits ned i ytterligare processdiagram där det framgår var och hur ett datorstöd kan hjälpa analytikern.



Figur 3. Det övergripande arbetsflödet för hypoteshantering.

3.1.2 Befintliga analytiska verktyg

Arbetet med att kartlägga befintliga analytiska verktyg finns sammanfattat i FOI-rapporten ”Analytiska verktyg - en översikt av metoder och modeller för underrättelseanalys” [5]. Det huvudsakliga syftet med rapporten var att samla den kunskap om analytiska verktyg i form av metoder och modeller för underrättelseanalys som finns på FOI och att göra den tillgänglig i en lättförståelig och översiktlig form. Även om rapporten inte är heltäckande är förhoppningen att den dels ska ge läsaren en uppfattning om vilken sorts analytiska verktyg som finns, dels ska kunna användas i det praktiska underrättelsearbetet som ett stöd för att avgöra hur och när man ska använda de verktyg som presenteras i rapporten. Tabell 2 ger en översikt över de verktyg som beskrivs och kategoriserar dem också enligt ett antal viktiga egenskaper.

Tabell 2. En översikt av ett antal analytiska verktyg och deras egenskaper.

Metod	Datadriven/ Modelldriven	Kvalitativ/ Kvantitativ	Hypotesskapande/ Hypotestestande
Morfologisk analys	Modelldriven	Kvalitativ	Hypotesskapande
Grundad teori	Datadriven	Kvalitativ	Hypotesskapande
Attackträd	Modelldriven	Kvalitativ	Hypotesskapande/ hypotestestande
Wigmoreanska nätverk	Modelldriven	Delvis kvantitativ	Hypotestestande
Bayesianska nätverk	Modelldriven (finns även som datadriven variant där modellen lärs in från data)	Kvantitativ	Hypotestestande
Analys av konkurrerande hypoteser	Modelldriven (till viss del datadriven)	Kvalitativ	Hypotestestande
Orsak-verkandiagram	Modelldriven	Kvalitativ	-
Bow-Tie-diagram	Modelldriven	Kvalitativ	-

3.1.3 Verktyg för multihypoteshantering

Baserat på kunskapen om befintliga verktyg och det konceptuella arbetet har projektet utvecklat ett datorverktyg som stödjer multihypoteshantering med syftet att hjälpa analytiker att jobba strukturerat, med utgångspunkt i beprövade analytiska metoder, och att samtidigt underlätta analysarbetet genom att erbjuda ett metodanpassat stöd för att kunna spara, strukturera, organisera och visualisera information. Grundidén bakom analysverktyget är att man inte ska behöva begränsa sig till att titta endast på ett fåtal hypoteser, utan man ska kunna ha ett större antal hypoteser aktiva samtidigt. När ny information läggs in i systemet ska denna användas för att automatiskt uppdatera status för alla hypoteser, även om man bara jobbar aktivt med ett mindre antal av dessa.

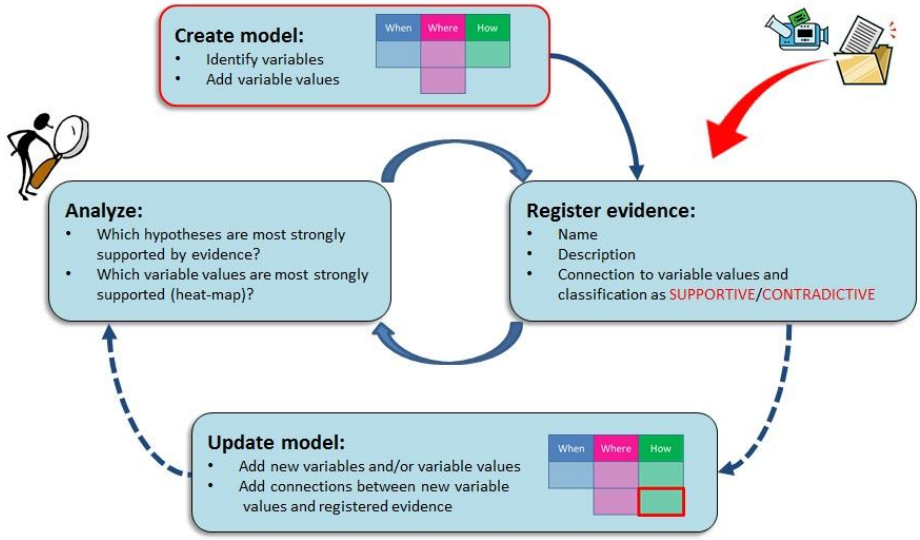
I det nyutvecklade hypoteshanteringsverktyget finns tre grundfunktionaliteter:

- Stöd för hypotesgenerering
- Stöd för hantering av evidens
- Grundläggande analysstöd

Analytikern börjar med att skapa en modell av sitt problem för att utifrån den på ett strukturerat sätt kunna generera nya hypoteser. Man tänker sig sedan ett iterativt arbetssätt, där varje nytt evidens som blir tillgängligt registreras och kopplas till den befintliga modellen, varefter analytikern kan använda sig av de tillgängliga analysfunktionerna för att skapa sig en överblick över det aktuella läget. I vissa fall leder ny evidens till att man måste uppdatera modellen. Uppdateringen av modellen kommer då in som ett ytterligare steg i iterationen. Iterationerna fortsätter så länge man får in nya evidens, eller så länge det bedöms vara meningsfullt. Den tänkta arbetsgången illustreras i Figur 4. Verktygets grundfunktionaliteter beskrivs i kommande stycken.

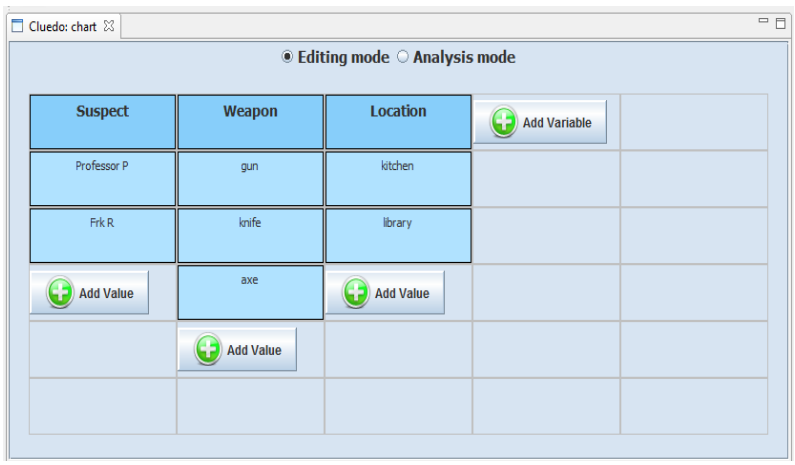
Hypotesgenerering

Hypotesgenereringen i verktyget bygger på morfologisk analys, ett av de analytiska verktyg som beskrivits i [5]. Morfologisk analys är en etablerad metod som används av analytiker för att spänna upp ”hypotesrum” som innehåller både mer och mindre troliga hypoteser för givna scenarion. Genom att använda metoden minskar man risken att helt missa hypoteser som i ett senare skede kan visa sig vara relevanta. I morfologisk analys kännetecknas en hypotes av ett antal variabler som representerar de viktigaste delarna av hypotesen. Variablerna identifieras för varje enskilt problem av en analytiker. I en mordutredning kan man till exempel tänka sig att ha med variablerna Gärningsman, Plats och Vapen.



Figur 4. Arbetsgång för multihypoteshantering

Genom att lista olika tänkbara värden som de identifierade variablerna kan anta och sedan kombinera dessa värden på alla möjliga tänkbara sätt får man fram ett stort antal hypoteser som man sedan på ett systematiskt sätt kan gå igenom och utvärdera. Själva modellen som används för att generera hypoteser tar i det här fallet formen av en tabell (se Figur 5), där kolumnerna motsvarar variabler och elementen i kolumnerna utgörs av variabelvärdena.



Figur 5. Modell för hypotesgenerering i form av en morfologisk tabell.

Evidenshantering

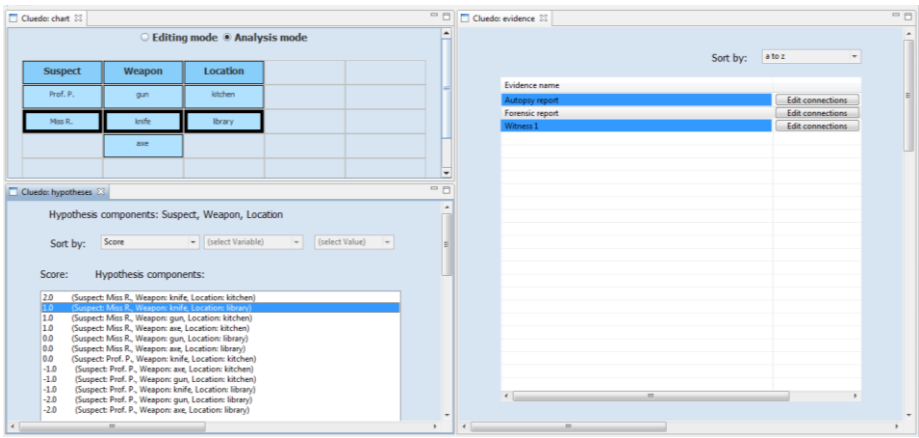
I verktyget finns stöd för att registrera evidens och för att koppla dessa till variabelvärden i modellen – och därmed också till alla hypoteser som inkluderar det/de aktuella variabelvärdena. Kopplingen kan antingen vara positiv eller negativ beroende på om evidenset stödjer eller motsäger värdet.

Analysstöd

Förutom möjlighet att lagra och söka i inlagd information finns grundläggande analysfunktioner i programmet. Dessa inkluderar:

- rangordning av hypoteser,
- överblick av inlagda kopplingar mellan hypoteser/variabelvärden och evidens (Figur 6), samt
- HeatMap-vy som ger en visuell överblick över vilka variabelvärden som har mycket/lite stöd av evidens.

Ovanstående funktioner är avsedda att ge en lättförståelig överblick över den aktuella situationen och att åskådliggöra de fakta (evidens, antaganden, etc.) som ligger bakom ett analysresultat. Verktyget finns för närvarande i en första stabil version, nästa steg blir att göra användartester. I sin nuvarande form är verktyget endast avsett som ett stödverktyg och resultaten av analysen måste alltid tolkas av en expert. Ambitionen är att i framtida versioner av verktyget också erbjuda ett bättre stöd för utforskande analys, där man undersöker den aktuella situationen utgående från frågan ”vad händer om…?”.



Figur 6. Evidens som är kopplade till den valda hypotesen (listan till vänster) markeras i evidensvyn till höger i bild.

3.2 Inhämtning och fusion av heterogen information

För Försvarsmakten innebär dagens konflikter och IT-intensiva miljö hantering av en stor mängd olika informationskällor av vitt skilda typer och ursprung. Den heterogena information som strömmar in har i skiftande grad olika syntaktiskt format, olika terminologi, använder olika sätt för att uttrycka osäkerhet, är olika noggrann med metadata, och är olika pålitlig. Att skapa situationsförståelse ur sådan information är utmanande, samtidigt som belöningen om man lyckas kan vara stor. Heterogena källor är oftast oberoende och bidrar med information som kompletterar varandra, vilket kan skapa mer heltäckande och robusta system. I takt med att sensor- och kommunikationssystem blir kraftfullare och mer allmänt tillgängliga ökar också mängden information som ska hanteras. Detta innebär att datorstöd för fusion av information från heterogena källor blir en viktig komponent i bearbetningssystemet.

VIA-projektet har tagit fram en rapport om den allmänna problematiken och forskningsläget kring fusion av information från heterogena källor [7]. Rapporten riktar sig till personer inom försvarsmyndigheter och industrin med intresse för informationshantering och systemintegration inom underrättelsedomänen. Syftet är att ge läsaren en förståelse för de fördelar och utmaningar som fusion av information från heterogena källor innebär. Rapporten ger en översiktlig introduktion till begreppen situationsförståelse och informationsfusion, för att sedan fördjupa sig i de speciella utmaningar som det innebär att koppla samman och fusionera information från heterogena källor. Dessa utmaningar handlar till stor del om olika aspekter av dataensning (eng. data alignment): hur man ensar information som beskrivs med olika begreppsapparater och hur man ensar information som använder olika osäkerhetsformalismer. Rapporten behandlar också hantering av spårbarhet och så kallad härkomstmetadata (eng. pedigree metadata), en viktig källa när trovärdigheten av ett fusionsresultat ska värderas.

De generella problemställningarna kring heterogen fusion som belysts i rapporten har konkretiserats i en tillämpningssituation som tillhandahållits av det medfinansierade hamnsäkerhetsprojektet SUPPORT [16,27]. FOI:s del har här handlat om att integrera och fusionera data från olika typer av sensorer, administrativa system och underrättelseinformation, samt att utveckla ett verktygsstöd för situationsövervakning i en hamn. Verktygsstödet bygger på FOI:s Impactorium-system där tänkbara hot mot hamnen kan modelleras och prövas kvantitativt genom att inkommande information från olika källor matchas mot modellens olika komponenter.

Integrationen av informationskällorna har gjorts med så kallade semantiska tekniker, en uppsättning standardiserade modelleringsspråk och -verktyg som kan användas för att på ett flexibelt sätt strukturera den information som ska utbytas. VIA-projektet har bedrivit forskning kring hur de semantiska teknikerna

kan utnyttjas för att formalisera informationsbehov för att koppla inkommande information till hotmodellerna. Projektet har också utvecklat algoritmer och stödverktyg för hur dessa informationsbehov kan prioriteras och kopplas till olika inhämtningsresurser. Slutligen har arbete utförts kring ett manuellt rapporteringssystem som automatiskt genererar information på ett strukturerat format och därför direkt kan kopplas mot informationsbehoven. I den tidigare presenterade översiktbilden, Figur 2, syns hur dessa komponenter hänger ihop ur ett informationsflödesperspektiv.

3.2.1 Formalisering av informationsbehov

En grundläggande metod inom underrättelseanalys är att formulera och bryta ner hypoteser till delhypoteser och indikatorer. För att avgöra sanningshalten för en eller flera hypoteser krävs underlag i form av evidens. För hypoteser och dess indikatorer kan man formulera ett antal frågor vars svar ger tillräcklig information för att avgöra om hypotesen är sann eller inte. Dessa frågor definierar ett informationsbehov.

I ett övervakningsscenario där man har för avsikt att tidigt upptäcka hot kan förmågan att formulera informationsbehovet spela en avgörande roll. Sensordata och observationsrapporter utgör indata mot vilken man vill ställa frågor. Väldefinierade frågor, som besvaras så fort information som matchar frågorna finns tillgänglig, skapar ett bra underlag med minimal fördröjning vilket möjliggör proaktiva åtgärder.

Det finns en rad öppna frågor inom ramen för formalisering av informationsbehov. En sådan fråga som projektet har adresserat är hur man på bästa sätt uttrycker sitt informationsbehov och hur en informationsmodell bör konstrueras för att stödja detta. En öppen fråga för framtiden är hur osäker information skall hanteras vid inmatning och hur man tar hänsyn till detta då inhämtningsfrågorna formuleras. Ett formellt och entydigt formulerat informationsbehov är önskvärt men kanske inte möjligt på grund av tekniska och kognitiva begränsningar.

En automatiserad informationsinhämtning ställer krav på både konsument och producent av informationen samt på den informationsmodell som används. Informationskonsumenten behöver uttrycka sitt behov på ett precist sätt vilket medför att informationsmodellen måste täcka de begrepp som behövs för att formulera frågor kring konsumentens specifika intressen. Informations-producenten å sin sida måste kunna relatera till samma informationsmodell för att generera information som är märkt på ett adekvat sätt.

3.2.2 Inhämtningsstyrning

De situations- och hotmodeller som används för underrättelseanalys måste kopplas till inkommande information, från sensorer, webben eller mänskliga källor, för att kunna svara mot organisationens informationsbehov. För att vara säker på att inhämtningsresurser används optimalt behöver de styras så att de levererar den data och information som efterfrågas mest.

Projektets arbete om inhämtningsstyrning har fokuserat på automatisk behandling av en hothypotes modellerad som ett så kallat bayesianskt nätverk (BN). Modellen speglar hur hotet som man försöker analysera relaterar till ett antal hotindikatorer som man med hjälp av inhämtning kan observera. Med hjälp av modellen och en beskrivning av tillgängliga inhämtningsresurser och deras förmågor uppskattas en mest lämplig användning av inhämtningsresurserna [13,18,19].

Algoritmutvecklingen har varit inriktad på maximering av ett godhetsmått som uttrycker förväntad förändring av osäkerhet kring den underrättelsefråga som en hotmodell beskriver. Ett högt värde på den förväntade osäkerhetsförändringen motsvarar en inhämtning av information som kan leda till en stor förändring av situationsförståelsen (och visar därmed på information som är extra känslig och intressant).

I ett samarbete med Högskolan i Skövde har arbetet utökats med att tydligare föra in den mänskliga expertens kunskaper om nyttjandet av inhämtnings-resurserna. Det ursprungliga arbetet fokuserade på inhämtning enbart baserad på formaliserad (statistisk) kunskap om relationer mellan indikatorer i hotmodeller. I samarbetet med Skövde användes metoder från "Multi-Attribute Decision Making" (MADM) för att även beakta analytikerns kunskaper om exempelvis resursanvändningens påverkan på den övergripande planen och risken för att resurser förstörs eller misslyckas med inhämtningen [32].

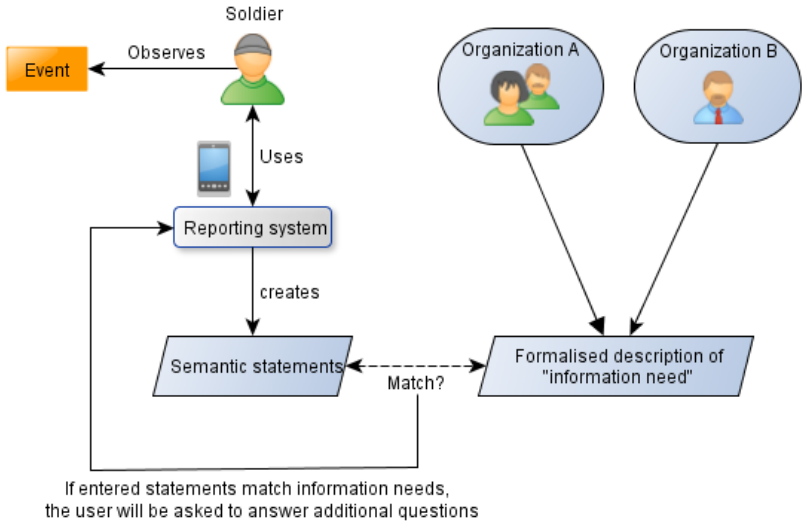
Viktiga frågor för fortsatt arbete om informationsinhämtning är att identifiera under vilka förutsättningar metoden är särskilt lämplig samt en anpassning av metoden till problem då inhämtningsresurserna inte är tillgängliga för analytikern utan där denne enbart kan uttrycka sitt informationsbehov. Här är det också viktigt att komma ihåg att de inhämtningsresurser som styrs inte behöver vara traditionella sensorplattformar (till exempel UAV:er), utan kan också vara till exempel riktad inhämtning från webbplatser.

3.2.3 Verktyg för manuell inmatning av strukturerad information

Projektet har utarbetat ett verktygskoncept för inmatning av strukturerad information. Den grundläggande frågeställningen har varit hur man kan erhålla maskinbearbetningsbar information från en mänsklig observatör utan att behöva gå omvägen att först tolka naturligt språk genom Natural Language Processing (NLP). Huvudargumentet för att man vill undvika NLP vid underrättelse-rapportering är att det idag mycket sällan går att göra helt korrekta automatiska tolkningar. Projektet har utvecklat ett inmatningsverktyg där användaren istället arbetar med att uttrycka sig direkt i en ontologi (en logikbaserad semantisk informationsmodell) som tillåter maskinell bearbetning [28]. Inmatnings-verktyget utnyttjar strukturen i ontologin för att anpassa användargränssnittet efter vad användaren matar in. Om användaren till exempel vill rapportera in en händelse där en grupp upprorsmän hotat en byäldste, kan denne ange händelsetypen ”hot” (förutsatt att den finns definierad i ontologin). Verktyget ser i ontologin att ett hot normalt sett innefattar två aktörer, någon som uttalar hotet (gärningsmannen) och någon som blir hotad (offret), och frågar användaren efter dessa.

En ytterligare funktion som verktyget erbjuder är möjligheten att ta hänsyn till externa informationsbehov i en rapporteringssituation [41]. Låt säga att användaren i hotexemplet ovan anger gärningsmannen som en grupp talibaner. Antag också att det i en annan del av organisationen finns en analytiker som har ett behov av information kring vilka vapentyper som talibanerna besitter. Om analytikern uttrycker sitt informationsbehov i samma ontologi som rapportören kan en matchning av det som rapporteras och de informationsbehov som finns göras. I det här fallet görs en matchning av ”taliban”, och verktyget ber rapportören att ta reda på och rapportera eventuella vapen som observerades vid hotsituationen. Flödet för funktionen illustreras av Figur 7.

Möjligheten att direkt från rapporteringsverktyget få strukturerad information möjliggör omedelbar fusion med information från andra typer av källor, exempelvis sensorer, förutsatt att de har ensade informationsmodeller.



Figur 7. Användaren rapporterar observationer i verktyget som formaterar dem på rätt sätt enligt ontologin. Informationen kan sedan matchas mot informationsbehov som finns på andra ställen i organisationen (eller utanför). Om det blir match presenteras behovet för rapportören.

3.3 Analys av webbdata

Det tredje temat för VIA-projektet har varit analys av sociala nätverk och textanalys tillämpat på webbdata. Textanalysen har använts dels för att undersöka möjligheten att upptäcka trender i händelserapportering i media, dels för att monitorera känsloläget i sociala media vid krishantering. Nätverksanalysen har gått ut på att utveckla metoder för att ta hänsyn till osäkerhet i data, vilket är vanligt förekommande om man automatiskt extraherar nätverksdata från webben. Slutligen har projektet utfört arbete på temat analys av svaga signaler för att upptäcka ensamagerande terrorister. Här har en metod utvecklats som kombinerar det mesta som projektet har forskat kring: hypotesnedbrytning, heterogen fusion, text- och nätverksanalys. Forskningen som beskrivs i det här avsnittet finns mer utförligt beskrivet i FOI-rapporterna [4], [8] och [9], samt i flera vetenskapliga publikationer.

3.3.1 Trendanalys

Nya konflikter eller krissituationer uppstår ofta runt om i världen och alla möjligheter till tidigare förvarning skulle vara av stort värde, i syfte dels att möjliggöra bättre planering och anpassad träning innan nya humanitära eller

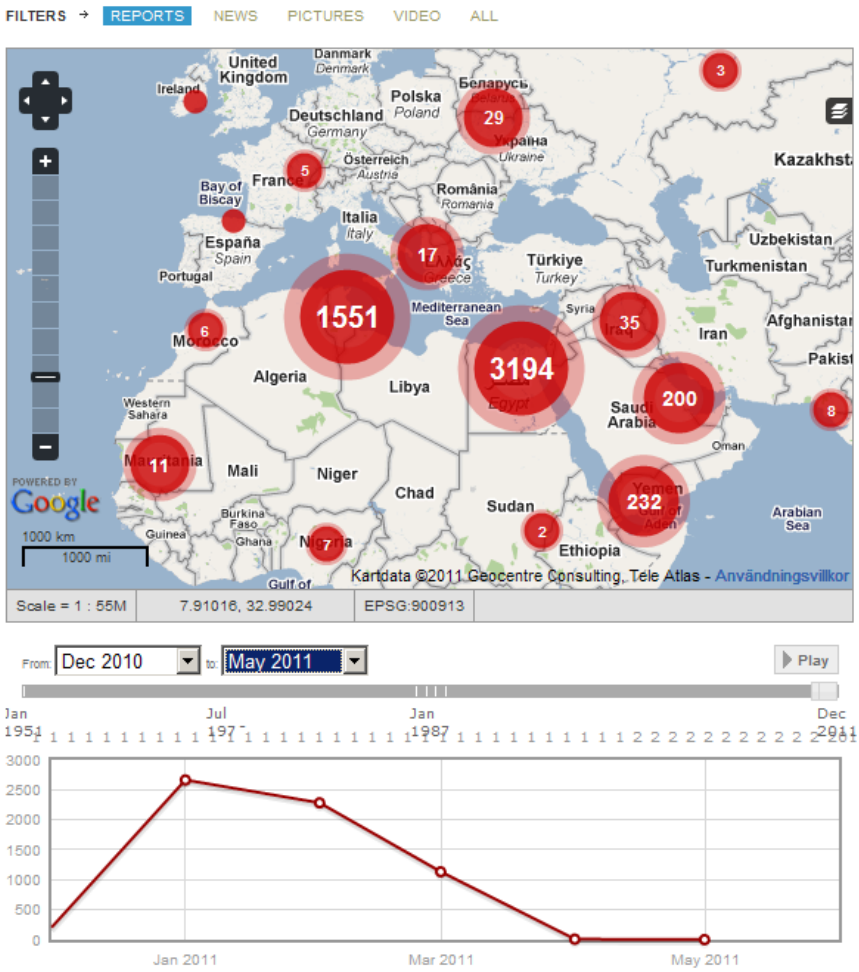
militära insatser görs, dels att skapa bättre underlag för säkerhetspolitiska analyser. Med detta som utgångspunkt har VIA och ett mindre projekt, ”Teknikstöd till FM UtvC”[5] tillsammans tagit fram ett prototypsystem för trendanalys. Systemet kombinerar en produkt från det svenska företaget Recorded Future för insamling och analys av öppna datakällor med den öppna mjukvaran Ushahidi [26,30]. Ushahidi har använts i olika krissituationer för geospatial visualisering av insamlade ögonvittnesskildringar i syfte att ge en bättre lägesförståelse. Genom att integrera dessa system blir det möjligt att extrahera händelser som en analytiker är intresserad av (exempelvis händelser som har att göra med terrorism, hungersnöd eller demonstrationer) och att visualisera dem med Ushahidi i syfte att se uppkommande trender. Systemet har använts för att samla in och analysera RSS-flöden från människorätts-organisationen Human Rights Watch och diverse nyhetsbyråer. Insamlingen gjordes huvudsakligen under första kvartalet 2011 och de rapporter som klassificerats som att handla om protesthändelser filtrerades ut. Dessa händelser visualiserades med hjälp av Ushahidi, vilket gav användaren en möjlighet att se hur protesthändelserna spridde sig under början på den Arabiska våren (se Figur 8).

Ett problem kopplat till trendanalys av detta slag är att nyhetsmedia snabbt byter fokus, så att det som ena dagen får stor uppmärksamhet i nyhetsflödena nästa dag inte uppmärksammas alls. Ett sätt att komma tillrätta med detta är att inte ta med rapporterna från nyhetsmedier i inhämtningen utan bara fokusera på rapporter från mer nischade hjälp- och människorättsorganisationer. Ett alternativ kan dock vara att i områden där användningen av sociala medier är utbredd även väga in användargenererat innehåll.

Analys av sociala medier för förbättrad kriskommunikation

Sociala medier har använts för kommunikation och informationsinhämtning vid en rad olika kriser, däribland Fukushima-krisen och terrorattentaten i Norge. I det av VIA medfinansierade EU-projektet Alert4All pågår forskning kring hur man kan hämta in och analysera data som relaterar till pågående kriser från sociala medier. Analysen går ut på att skapa en överblick över hur människor reagerar på krisen och på utkommunicerade krismeddelanden. Genom användning av algoritmer för så kallad sentiment- och affektanalys kan man få en uppfattning om människors känslostämningar, vilket kan användas som underlag när beslut ska fattas om huruvida ny krisinformation ska skickas ut till befolkningen och hur den i så fall ska utformas [21,35,38].

[5] Se ”Översiktlig beskrivning av Trendanalysverktyg”, FOI Memo 3589.



Figur 8. Överst: Karta med händelsetypen "protest", där händelser aggregerats baserat på geografisk närhet. Underst: Histogram över antal inträffade protesthändelser i Egypten under första kvartalet 2011.

3.3.2 Kartläggning och analys av sociala nätverk

Sociala nätverk finns överallt i vår omgivning, från våra egna nätverk av arbetskamrater och vänner till större nätverk som kan beskriva exempelvis FOI som organisation eller en bostadsrättsförening. Allmänt beskrivs ett socialt nätverk av en mängd individer eller aktörer som är sammankopplade med någon form av relation. Dessa relationer kan beskriva allt från vilka som kommunicerar med varandra till vilka som exempelvis har publicerat en vetenskaplig artikel

tillsammans. Under den senare delen av 1900-talet har sociologer, psykologer, epidemiologer och naturvetare studerat olika typer av nätverk och skapat metoder för att analysera dessa kvantitativt.

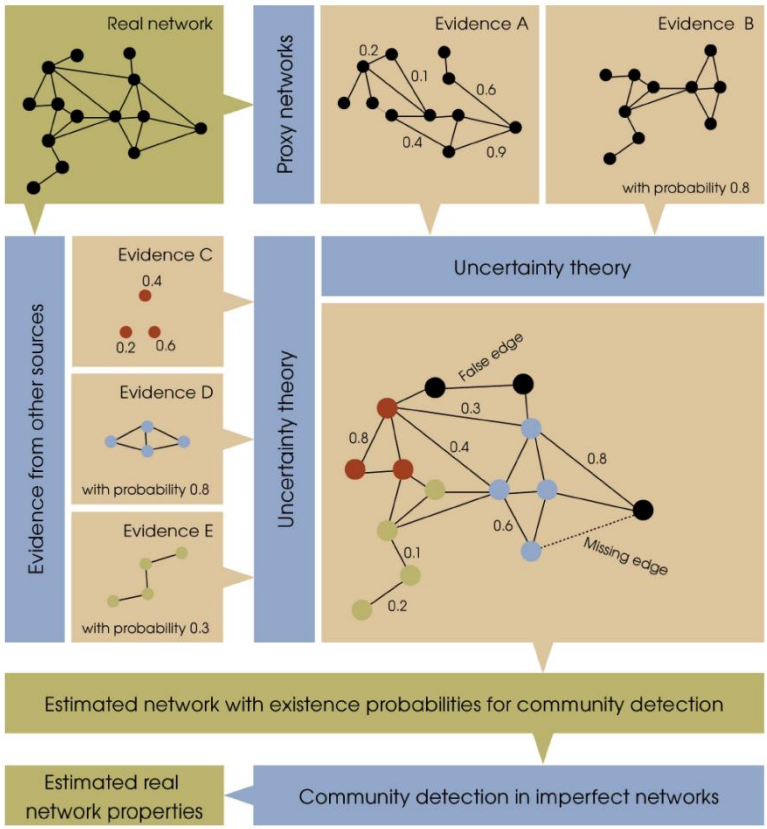
Webben är en rik källa till information om sociala nätverk. Sociala medier bygger mycket av sin struktur på länkar mellan olika individer och man kan även extrahera nätverk med hjälp av textanalys. Beroende på inhämtningsmetod blir dessa nätverk dock behäftade med osäkerhet, något som sällan hanteras av de verktyg för analys av nätverk som finns idag.

Metod för analys av osäker data

För att komma till rätta med problemen och begränsningarna med att tillämpa analys av nätverk för webbdata i allmänhet och underrättelsedomänen i synnerhet så har VIA-projektet utvecklat en metod för att hantera osäkerhet i nätverket [20,22,24,31]. Denna osäkerhet kan gälla olika fenomen som huruvida två alias relaterar till en och samma individ eller huruvida det ska finnas en relation mellan två eller flera aktörer.

Utgångspunkten i metoden är att det verkliga (underliggande) sociala nätverket inte är direkt observerbart utan att olika så kallade proxy-nätverk istället är det som observeras och får användas som approximation av det verkliga nätverket. Ett exempel på ett sådant proxy-nätverk är när kommunikation mellan aktörer (där sådan kommunikation exempelvis kan identifieras via loggning av mailkonversationer) används som proxy för olika typer av mer abstrakta relationer av intresse. Utöver denna typ av proxy-nätverk går det även att få in annan typ av evidens från olika källor, så som att ett en källa säger sig ha sett två aktörer kommunicera med varandra (där utsagan från källan alltså gäller små delar av nätverket snarare än hela nätverket, vilket är fallet för proxy-nätverk). Skillnaden mellan evidens i form av proxy-nätverk och andra typer av evidens illustreras i Figur 9.

I korthet går metoden ut på att genom stickprov extrahera ett stort antal (säkra) nätverk från det osäkra nätverket (där dessa stickprov är konsistenta med informationen i det osäkra nätverket), göra en traditionell nätverksanalys av de samplade nätverken och sedan slå samman resultaten från de samplade nätverken. Denna metod har testats på så väl verkliga och syntetiska nätverk med genererade osäkerheter och brister. Möjligheten att på detta sätt hantera osäkerhet vid analys av sociala nätverk är något som inte finns i kommersiella programvaror utan bara i forskningsprototyper.



Figur 9. Illustration av den allmänna metoden för att analysera nätverk med osäker data.

Automatisk extraktion av nätverk

Projektet har även arbetat med att automatiskt skapa osäkra nätverk från ostrukturerade textdokument. Entiteter (personer, platser, organisationer m.m.) extraheras automatiskt från textdokument (exempelvis underrättelserapporter eller information inhämtad från webben). För varje par av entiteter som återfinns i samma mening skapas en relation, där vikten på relationen bland annat bestäms av antalet ord mellan entiteterna. Vidare så vägs antalet meningar som två entiteter förekommer tillsammans i in när styrkan på deras relation bestäms. Utifrån de utvunna entiteterna och relationerna skapas med automatik ett osäkert nätverk, i vilket analytikern kan välja att fokusera på de delar som är av intresse för dennes analys [49].

En av de nämnda osäkerheter som kan uppträda i sociala nätverk är om två alias refererar till samma person. Tekniker för att avgöra detta kallas aliasmatchning och är ett specialfall av entitetsmatchning, en komponent inom informations-extraktion. Entitetsmatchning används för att avgöra om två olika entiteter i till

exempel en text eller en databas egentligen är en och samma. Projektet har tagit fram en rapport [4] som innehåller en genomgång och diskussion av tidigare arbeten inom entitetsmatchning samt aktuella implementationer av dessa i form av olika programvaror.

Abstraktion av sociala nätverk

Social nätverksanalys är ett grundläggande verktyg inom underrättelseanalys. Det är dock svårt att visualisera och analysera stora nätverk. Ett sätt att lösa detta är att försöka hitta mindre, enklare nätverk som fångar de mest viktiga särdragen hos det stora nätverket. Det mindre nätverket kallar vi en abstraktion av det större. Ett enkelt exempel på nätverksabstraktion är så kallade blockmodeller, där man i ett stort nätverk slår samman noder som till exempel tillhör samma organisation. Genom att endast visa organisationer och deras förbindelser får man en mer lättförståelig bild än om alla enskilda personer som tillhör organisationerna och deras länkar visas. Ett annat exempel på abstraktion är community clustering, där man skapar grupper i nätverket genom att hitta delmängder av noder som har tätare förbindelser inbördes än utanför gruppen.

VIA-projektet har studerat hur mer avancerade abstraktioner kan skapas genom att utnyttja algoritmer från området automatateori inom datalogi [15,36]. Metoden används för att identifiera sociala roller i nätverk, till exempel kan man i ett nätverk över ett företag hitta alla chefer, sekreterare och projektledare. Det mindre nätverk som bildas genom att slå samman alla noder som har samma sociala roll kan användas som en abstraktion av originalnätverket. Genom att studera de ekvivalensklasser av sociala roller som algoritmen ger ifrån sig kan man också hitta sårbarheter och styrkor i nätverket.

Forskningen inom området är förhållandevis omogen och mer forskning krävs innan användbara och relevanta abstraktionsalgoritmer kan förväntas dyka upp.

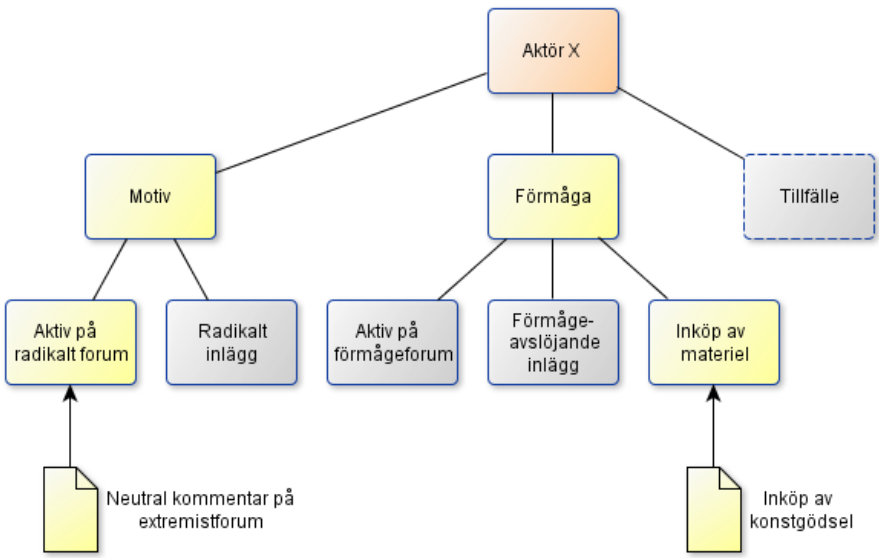
3.3.3 Analys av svaga signaler för att fånga ensamagerande terrorister

Våra liv tar i större och större utsträckning plats på internet och detta gäller även mer ljusskygga delar av samhället. Därför är internet en viktig plats för att leta efter kriminell verksamhet, terrorister och andra typer av hot mot samhällets säkerhet. Ett påtagligt och aktuellt hot är ensamagerande terrorister vilket uppmärksammades på ett tragiskt sätt den 22 juli 2011 i Norge då Anders Behring Breivik utförde två terrorattentat som resulterade i 77 döda. Eftersom ensamagerande terrorister arbetar på egen hand kan man inte samla information om dem genom traditionellt polisarbete som exempelvis infiltrering och avlyssning av kända extremistgrupper. Ett sätt att försöka upptäcka dem i tid är att analysera data från internet i jakt på digitala spår. Det har visat sig att ett flertal terrorister har använt sig av internet för att uttrycka radikala åsikter och i vissa fall även berättat om sina planer innan sina attacker. Om dessa digitala spår

skulle upptäckas och tas på allvar i tid finns alltså i varje fall en teoretisk möjlighet att förhindra terrordåd. Dessvärre är det inte lätt att upptäcka och analysera dessa digitala spår eftersom det ofta handlar om uttalanden som i sig inte är speciellt anmärkningsvärda men i kombination med annan typ av information kan ge en indikation på att de kan vara värda att analysera vidare. Digitala spår i form av uttryck för extrema åsikter eller planer på framtida terrorbrott kan liknas vid svaga signaler. Med en svag signal menar vi något som i sig själv inte betyder någonting men som kan bli starkare genom att kombineras med andra signaler.

Problemet med att spana efter potentiella ensamagerande terrorister är att det på många sätt är som att leta efter en nål i en höstack. Internet rymmer en överväldigande mängd information. Att manuellt scanna igenom alla nätforum som skulle kunna vara platser som exempelvis inbjuder till ”självradikalisering” är en omöjlig uppgift.

VIA-projektet har utarbetat en metodansats som syftar till att automatisera delar av arbetet för att upptäcka och kombinera svaga signaler [25,29,39,40]. Metoden utgår från den hypotesnedbrytningsprocess som stöds av det tidigare utvecklade Impactorium-verktyget som också användes vid områdesövervakningen i avsnitt 3.2. Ett exempel på hur man kan använda sig av nedbrytning finns i Figur 10.



Figur 10. Exempel på nedbrytning av hothypotesen att Aktör X kommer att begå en terrorhandling. I exemplet finns en uppsättning indikatorer som kan upptäckas genom spaning på internet, men även en indikator ”Inköp av materiel” som skulle kunna upptäckas via andra informationskanaler. Här blir förmågan till heterogen fusion återigen central.

I figuren är det grundläggande problemet huruvida aktör X planerar att begå ett terrorbrott. Problemet bryts ner i beståndsdelarna motiv (intention), förmåga och tillfälle. Nästa nivå i nedbrytningen exemplifierar ett antal indikatorer. En indikator är en så kallad observerbar faktor, d.v.s. en händelse, företeelse, beteende eller dylikt, och kan jämföras med en svag signal.

Istället för att bara använda sig av en sökmotor (och således missa de delar av webben som inte är indexerade) kan man göra en kartläggning av de delar av webben som anses vara intressanta och använda sig av en riktad inhämtning. Detta ökar chansen att man letar på rätt ställe. Tanken är att man utgår från en mängd identifierade webbsidor och sedan använder sig av en webbspindel för att undersöka vilka sidor som är länkade från dessa sidor. Genom att använda sig av textanalys och identifierade nyckelord (d.v.s. ord som man anser att sidor med potentiellt intressant innehåll ska innehålla) kan man automatiskt skapa ett nätverk av potentiellt intressanta webbplatser. Inhämtningen av information kan sedan riktas till dessa webbplatser.

När man har hämtat in den information som man tror kan vara av intresse inleds analysarbetet. I den föreslagna metoden plockas alla alias ut från den inhämtade datamängden. Varje alias kopplas till en modell liknande den i Figur 6, med syftet att beräkna troligheten att personen bakom aliaset är benägen att begå ett våldsbrott. För att kunna beräkna detta mått analyseras texterna som respektive alias skrivit med hjälp av olika former av textanalys. De indikatorer som man kan leta efter på internet är framför allt indikatorer som tyder på att ett alias har utryckt motiv för att begå ett terrorbrott. Projektet har anlitat en psykolog-studerande för att göra ett arbete om vilka varningsbeteenden som skulle kunna ge upphov till indikatorer som är möjliga att upptäcka med hjälp av automatisk textanalys. Arbetet har lett både till en extern publikation [48] och en FOI-rapport [8].

Nästa steg i metoden är att väga samman de indikatorer som eventuellt har upptäckts. Sammanvägningen kan göras med ett flertal olika beräkningar som exempelvis Dempster-Shafer, Bayesianska metoder eller olika typer av medelvärdesberäkningar. Varje alias får en rankning som beskriver hur pass intressant det är att göra ytterligare analyser av aliaset. Det är dock vanligt att en användare har ett flertal olika alias och därför är det viktigt att göra en bedömning huruvida samma användare har flera olika alias. Projektet har inlett forskning kring tekniker för aliasmatchning. Bland annat har det doktorandarbete på Umeå universitet som projektet delfinansierar inriktats mot tekniker för författarigenkänning vilket är en viktig komponent för aliasmatchning.

Det finns en mängd integritetsaspekter som aktualiseras när man spanar efter potentiella ensamagerande terrorister eftersom spaningen sällan kan ske på grundval av misstanke om brott. Ett forskningsområde som FOI inlett arbete kring är så kallad integritetsbevarande data mining, vilket kan användas för att

skydda den personliga integriteten då man vill samköra data från exempelvis internet med känsliga register [9].

Ytterligare en relaterad aktivitet inom projektet har varit att undersöka alternativa modeller till den enkla trädnedbrytning som presenterats här. Målet har varit att kunna representera mer komplexa samband mellan olika indikatorer eller mellan olika aktiviteter i en plan. För detta har metoder från teoretisk datalogi används för att skapa mer avancerade modeller som till exempel innehåller temporala operatorer [12,42].

4 Samarbeten

VIA-projektet har haft en förhållandevis stor mängd samarbeten, framförallt med transferprojektet Impactorium och de EU-projekt som projektet medfinansierat, men också med ett antal universitet och högskolor. Syftet med samarbetena har dels varit att öka volymen på och effektivisera forskningen genom att utnyttja synergieffekter, dels att genom kunskapsutbyte stimulera till nya och bättre idéer.

4.1 Impactorium

FM FoT-transferprojekt ”Impactorium”, 2010-2011, är ett resultat av det föregående FoT-projektet Situations- och hotanalys för BG 2011. Impactorium som idé började utvecklas 2006 efter observationer av hur hotanalyser bedrevs under övningen Demo 06 Vår i Enköping. Avsikten var att visa hur man i ett datorbaserat beslutsstödssystem kan sammanställa inkomna underrättelser för att från dem, med hjälp av hotmodeller utvecklade av ämnesexpertis, bedöma sannolikheten för att olika tänkbara hotscenarier kan komma att realiseras. Server- och klientmjukvara har utvecklats inom projektet för att stödja denna funktion och för att demonstrera en systemidé som skulle kunna implementeras i kommande versioner av skarpa ledningssystem såsom SWECCIS, eller i lämpligt system för hantering av rena underrättelser. VIA och Impactorium-transferprojektet har samordnats avseende utveckling och implementation av IT-infrastruktur (den så kallade fusionsplattformen), samt avseende ett samarbete med Singapore.

4.2 Singapore

FOI har inom VIA och Impactorium-transferprojektet haft ett samarbete med RAHS Experimentation Centre i Singapore, kallat S2ESA (Singapore-Sweden Experiment on Situation Awareness). Samarbetet ligger under ett avtal inom ledningsområdet som skrevs 2006-2007. Första fasen av samarbetet genomfördes under vintern 2010-2011 och omfattade användartester av Impactorium i Singapore med singaporianska analytiker. Resultaten finns dokumenterade i FOI Memo 4201. Den andra fasen är under förberedelse och kommer att handla om kvalitetsbedömning av information insamlad från webben.

4.3 EU:s sjunde ramprogram

VIA-projektet har medfinansierat FOI:s medverkan i ett antal EU-projekt där forskningsverksamheten överlappat med VIA:s verksamhet. En gemensam målsättning för EU-projekten och VIA är att implementerade algoritmer och verktyg ska integreras via fusionsplattformen. Syftet är att underlätta

återanvändningen av resultaten för olika ändamål och projekt, och säkerställa den hävstångseffekt som medfinansieringen syftar till.

Samtliga rapporter som FOI har bidragit till i EU-projekten finns tillgängliga för FM och FMV efter begäran till FOI, men får i många fall inte spridas allmänt. En lista på dessa rapporter kommer att levereras i ett särskilt memo.

Alert4All

Alert4All handlar om att lägga grunden för en europeisk standard för kommunikation med allmänheten vid kriser. Kommunikationen ska nyttja flera olika kanaler, och omfattar även att förstå allmänhetens reaktioner på det kommunicerade budskapet. Att få sådan återkoppling avseende ett krismeddelandes inverkan syftar i sin tur till att kunna följa upp och vid behov skicka ut nya förtydligande meddelanden. EU-projektet pågår 2011–2013, involverar 12 partners och har som övergripande mål att ta fram ett sammanhållet system för kriskommunikation. FOI:s medverkan är speciellt fokuserad på att hjälpa analytiker förstå allmänhetens reaktioner och känslor genom inhämtning och semi-automatisk analys av användargenererad text från sociala media.

Nyttan av att medfinansiera EU-projektet Alert4All är att FOI får utveckla och ta del av teknik och metoder som möjliggör för analytiker och staber att uppnå en ökad situationsförståelse avseende uppfattningar, medvetenhet och känsloyttringar utifrån vad som skrivs på webben. Från Alert4All kommer FM kunna tillgodogöra sig kunskap, system och träningsprinciper som kan ligga till grund för ett framtida eget införande av samma typ av lingvistiska analysmetoder.

SUPPORT

Målet för SUPPORT är att visa på lösningar som kan höja säkerhetsnivån för hamnar genom att integrera befintliga hamnsystem med nya bevaknings- och informationshanteringssystem. Projektkonsortiet består av 19 partners och leds av brittiska BMT. Utöver FOI är Securitas och STENA svenska deltagare. VIA-projektet har ett stort intresse av flera delar av SUPPORT och medfinansierar därför ett antal arbetspaket i syfte att genom samarbetet få ut mer forskning för samma ekonomiska insats.

SUPPORT har bland annat arbetat med att sätta ihop en "Port Security Threat Taxonomy". Intressant för VIA är här bland annat en listning av olika sensorer som kan användas för övervakning samt vilken sorts information man kan utvinna från respektive sensor. Taxonomin håller på att vidareutvecklas till en ontologi som ska ligga till grund för heterogen fusion och hotvärderingsverktyg.

SUPPORT arbetar även med att producera ett antal hotscenarier där det bl.a. beskrivs hur input från olika sensorer kan användas för att producera en enhetlig lägesbild för en operatör som övervakar systemet. Scenarierna har med viss modifiering återanvänts inom VIA i arbetet med situationsövervakning på taktisk nivå.

CONTAIN och SAFEPOST

CONTAIN handlar om att förbättra informationshanteringen inom transportsäkerhetsområdet. FOI koordinerar projektet, som har totalt 20 partners från 8 olika europeiska länder. Projektet ska visa hur förbättrade positionerings- och andra sensorer tillsammans med system för säkert utbyte av information kan leda till snabbare upptäckt av farliga ämnen. Den del av projektet som är relevant för VIA och kommande FoT-projekt handlar om riskvärdering av containrar baserat på information om avsändare, mottagare, transportör med mera. CONTAIN ska ta fram stödverktyg för att möjliggöra för tullverk i olika länder att förbättra sina processer för riskvärderingen för att välja ut vilka containrar som ska inspekteras. FOI deltar också i projektet med hypoteshanteringssystem som baseras på det verktyg som utvecklats i VIA.

SAFEPOST är ett systerprojekt till CONTAIN som berör samma forskningsfrågor men fokuserar på riskvärdering för brev och postpaket. I både CONTAIN och SAFEPOST medverkar FOI även med annan forskning, som inte medfinansierats av VIA. I SAFEPOST vidareutvecklas till exempel FOI:s raman-baserade explosivämnesdetektor. Som nämndes i avsnitt 1.2 är ytterligare ett projekt med likartad forskningsinriktning, EUROSKY, beviljat och förväntas starta tidigt 2013.

FIDELITY

FIDELITY är ett projekt som går ut på att ta fram säkerhetsförbättringar kring hanteringen av elektroniska pass. Den del av projektet som är relevant för VIA (och efterföljande projekt SIA) är tekniker för att hantera distribuerade databaser med komplexa och kraftigt begränsade accessmöjligheter. Speciellt gäller detta sökning i personregister med känslig information där många olika organisationer vill dela information men samtidigt skydda personlig integritet och inte avslöja mer än precis det som behövs för att genomföra en överenskommen undersökning. Algoritmer behöver konstrueras så att de flexibelt anpassar sig till hårda (juridiska, etiska och policydrivna) begränsningar samtidigt som effektiviten optimeras givet begränsningarna. Den här typen av algoritmer kan vara intressant för FM i samband med analys av sekretessbelagd information.

4.4 Universitet och högskolor

VIA har haft en naturlig koppling till flera svenska universitet och högskolor tack vare att många av projektets medarbetare har eller har haft uppdrag där. Detta har utnyttjats genom diverse samarbeten, vilka kortfattat beskrivs nedan.

Umeå universitet

VIA-projektet har haft ett samarbete kring analys av sociala nätverk och planigenkänning med en forskargrupp i Umeå. Detta har resulterat i gemensamma publikationer [12,15,42] samt en samfinansiering av en doktorand

inom planigenkänning. Doktoranden heter Niklas Zechner och påbörjade sin doktorandtjänst under sommaren 2012, efter att ha varit anställd som forskningsassistent under en tid. Till att börja med har Niklas läst in sig på tekniker för författarigenkänning, vilket bland annat utgör en komponent i aliasmatchning.

Uppsala universitet

På Uppsala Universitet finns ett nyetablerat centrum för polisforskning som jobbar med frågeställningar som delvis överlappar med VIA:s. Detta har utnyttjats genom informationsutbyte och en gemensamt anordnad konferens på temat sociala medier och brottslighet som hölls i november 2011 i FOI:s lokaler i Kista. Även ett VIA-relaterat examensarbete om analys av terroristnätverk har utförts vid universitet med Lisa Kaati från projektet som handledare. Arbetet har också lett till en konferensartikel [43].

FHS

Projektet har samarbetat med professor Martin Holmberg vid avdelningen för Ledningsvetenskap kring frågor om hur fusionssystem på olika ledningsnivåer kan stödja varandra [23,45].

Högskolan i Skövde

Flera projektmedarbetare har haft engagemang på Högskolan i Skövde. Ronnie Johansson och Fredrik Johansson har undervisat på högskolans kurs i informationsfusion. Det examensarbete om Multi-Attribute Decision Making som beskrevs i avsnitt 3.2.2 har utförts vid högskolan med Ronnie Johansson som examinator. Problemställningen är hämtad från VIA-projektet och arbetet har lett till en publikation [32]. Pontus Svenson är med i referensgruppen för NFFP-projektet om informationsfusion för piloter som drivs i samverkan mellan SAAB och Högskolan i Skövde.

KTH

Projektet har gjort en satsning på kompetensuppbyggnad kring området ”visual analytics” som handlar om hur man kan stödja analys genom olika typer av informationspresentation och -interaktion. FOI har genom VIA-projektets försorg gått med i VIC-Sthlm, en organisation med koppling till KTH som samordnar verksamhet kring visualisering i Stockholmsregionen. VIC-Sthlm har ordnat en endagskurs i visualisering på FOI som kompletterats med en FOI-intern studiecirkel i ämnet.

Joel Brynielsson och Henrik Artman från projektet är båda deltidsanställda vid KTH. Där har de tillsammans med en doktorand utvecklat personametoden med syftet att modellera en typisk motståndarorganisation. Detta har lett till publikationer om hur persona kan användas för att fånga typiska motiv inom organiserad cyberbrottslighet [46,47].

Under våren 2012 engagerade VIA tio studenter från KTH:s civilingenjörsutbildning i Datateknik genom den projektkurs på fyra veckor som de läser under sitt sista år vid KTH. Syftet var att ta fram en tidig prototyp för domänspecifik textanalys av Twitter-flöden, i linje med det mer långsiktiga arbetet som gjorts för VIA:s räkning inom ramen för det medfinansierade EU-projektet Alert4All. Studenterna. Prototypen, benämnd ”Social Media Analyzer (SMA)”, består av komponenter för inhämtning av Twitter-flöden och träning av maskininlärningsalgoritmer i syfte att klassificera Twitter-data. Vidare ingår ett webbgränssnitt där användaren kan interagera med programmet och där resultaten kan visualiseras med hjälp av deskriptiv statistik.

Linköpings universitet

Den forskargrupp på FOI inom vilken huvudelen av VIA-projektet utförts ingår i SecurityLink, regeringens strategiska satsning på säkerhetsrelaterad forskning på Linköpings universitet, FOI, KTH och Chalmers. Genom detta samarbete har gruppen bidragit till en kurs i sensor- och informationsfusion för krishantering som getts för doktorander vid SecurityLink. FOI genomför också tre mindre projekt med beröringspunkter till VIA som finansieras av SecurityLink. ”Anomalidetektion med statistical relational learning” har undersökt stabiliteten hos anomalidetektionsmetoder baserade på statistical relational learning. ”Svaga signaler för att hitta ensamagerande terrorister” vidareutvecklar den metod för fusion av svaga signaler som utvecklats av VIA. Slutligen ska ”Förbättrad hantering av IT-incidenter” undersöka hur situationsförståelse kan skapas inom cyberdomänen.

4.5 NATO

VIA-projektet har finansierat deltagande i en NATO-forskningsgrupp, NATO Research Task Group on Information Filtering and Multi Source Information Fusion, IST 106/RTG-051. Gruppen leds av Fraunhofer FKIE från Tyskland med övriga representanter från Sverige, Frankrike, Italien, Polen, Portugal, Spanien, Turkiet och USA. Målet är att ta ett konkret steg mot att förena lägre nivåers fusion (målföljning av enskilda objekt) med högre nivåers fusion (situations- och hotanalys), genom att undersöka vilken information som är av intresse att utbyta och hur denna ska struktureras. Detta kan på sikt leda till att klassificeringsinformation från sensorer kan nyttjas mer effektivt för att skapa situationsförståelse, till exempel genom att sensorutdata lagras och levereras på ett sätt som direkt kan användas som indikatorer i en hothypotes. Vice versa innebär det att kunskap om en viss situation eller hotbild kan förbättra kvaliteten på målföljningen, genom att målspårshypoteser som pekar på en utveckling som direkt strider mot till exempel en underrättelse kan undertryckas. VIA-projektets arbete kring heterogen fusion mappar väl mot NATO-gruppens målsättning.

Hittills har tre möten hunnits med. Vid uppstarten enades man om att börja med att identifiera lämpliga scenarion och datamängder att jobba kring och att undersöka huruvida Battle Management Language (BML) är lämpligt för att uttrycka informationen som ska utbytas mellan tjänster på olika fusionsnivåer.

Under möte nummer två låg fokus på att utbyta erfarenheter och definiera problemet ytterligare. Gruppen har även hunnit söka stödfinansiering från EU och anordna en panelsession, ”Multi-Level Fusion: issues in bridging the gap between high and low level fusion”, vid konferensen Fusion 2012. Vid möte nummer tre kunde FOI tyvärr inte närvara.

5 Fortsatt arbete

Flera av de verktyg, metoder och algoritmer som utvecklats inom ramen för VIA-projektet behöver utvecklas mer innan det går att avgöra vilket värde de kommer att ha för FM:s framtida informationshanterings- och analyssystem. Enligt gällande FoT-plan kommer VIA-projektet att få en uppföljare: SIA, Stödverktyg för informationsfusion och analys. SIA kommer delvis få en ny inriktning, men en del av projektmedlen är också tänkt att gå till medfinansiering av pågående och kommande samarbetsprojekt där VIA:s forskningsresultat kan förädlas.

Verktyget för multihypoteshantering har inom VIA implementerats i en första version och behöver nu testas av användare, vidareutvecklas och utvärderas. Detta kommer att göras inom ett par av de redan startade EU-projekten, CONTAIN och SAFEPOST. Planen är att sedan lyfta tillbaka resultaten av detta till Försvarmakten som underlag till framtida kravställningsarbete.

Samma förutsättningar gäller för inmatningsverktyget som har en framtid inom SUPPORT-projektet liksom i minröjningsprojektet D-BOX. Här behöver också användartester genomföras för att se om verktyget är tillräckligt intuitivt och verkligen ger den nytta som är tänkt.

En aktivitet som är gemensam för flera av de pågående EU-projekten är ”targeting” eller riskvärdering, att utifrån flera datakällor försöka avgöra vilka av en stor mängd objekt som utgör ett hot eller av annan anledning är av intresse. Den kompetens som byggts upp inom fusion av heterogen information kommer här att utnyttjas och vidareutvecklas. Även arbetet om webbanalys och svaga signaler för att identifiera hotaktörer kommer att förädlas inom denna aktivitet.

Utöver de EU-projekt som har nämnts kommer SIA från och med 2013 även att delfinansiera[6] ett EDA-projekt kallat IN-4-STARS. IN-4-STARS är ett samarbetsprojekt med Nederländerna och Estland där målet är att ta fram nya verktyg för säker informationshantering och analys av stora heterogena datamängder. Då de övergripande målen för SIA och IN-4-STARS är överlappande kommer projekten att samplaneras.

Skillnaden på VIA och den nya inriktningen för SIA kan sammanfattas som att fokus flyttar från modelldriven analys till mer datadriven. Syfte och frågeställningar från beställningen ser ut som följer:

> *Traditionella informationsanalysmetoder är ofta modellbaserade, där regler för kända förhållanden sätts upp av en domänexpert och sedan matchas mot data. Dessa riskerar dock att missa okända mönster eller oförutsedda förändringar i omvärlden. Att istället förutsättningslöst söka*

[6] SIA står för 25% av kostnaderna för den svenska insatsen, FMV för 75%.

efter mönster och trender, genom s.k. datadriven analys, ökar chanserna att tidigt upptäcka nya fenomen i data. Projektet syftar till att undersöka vilka möjligheter datadriven analys kan innebära för FMs underrättelseförmåga samt för andra förmågor med liknande behov.

Datadriven analys väcker frågor om hur interaktionen mellan analytiker och dator bör utformas. Datorn har en överlägsen förmåga till statistisk analys av stora datamängder, medan analytikern har en bredare repertoar för mönsterigenkänning och ofta bakgrundskunskap som är svår att förmedla till en dator. Projektet syftar till att undersöka hur ett bearbetningsstöd i form av en mjukvaruagent bör utformas för att åstadkomma ett effektivt samarbete mellan analytiker och dator.

Frågeställningar som projektet skall försöka besvara:

- *Hur ska en analytiker interagera med stödverktyget för att styra analysen och inkorporera mänsklig kunskap?*
- *Hur ska stödverktyget presentera och förklara ett analysresultat?*
- *Vilka krav ställer datadriven analys på signalbehandling och fusion av data från olika inhämtningsdiscipliner?*
- *Vilka algoritmer är lämpliga för vilken typ av analys på vilken typ av data?*

Under första halvåret 2013 kommer ett översikts- och inriktningsarbete göras där frågeställningar och datamängder inventeras och prioriteras i samråd med FM för att säkerställa relevansen av forskningen. En frågeställning som redan identifierats handlar om stöd för tillförlitlighetsanalyser. Här har en aktivitet redan påbörjats inom det tidigare nämnda Singaporesamarbetet, med syftet att utveckla algoritmer och verktyg för att stödja analytiker vid bedömningen av tillförlitligheten hos en sen tidigare okänd källa på internet.

6 Publikationer

Det här kapitlet listar de publikationer som producerats inom ramen för projektet. Först listas publikationer gjorda vid FOI i form av FOI-rapporter, därefter listas externa publikationer i form av konferensbidrag, tidskriftsartiklar och examensarbeten.

6.1 FOI-rapporter

1. FOI-R--3056--SE, Pontus Svenson et al., *Årsrapport Verktyg för informationshantering och analys (VIA) 2010*, 2010
2. FOI-R--3066--SE, Pontus Hörling (red.), Marianela Garcia-Lozano, Tove Gustavi, Fredrik Johansson, Ronnie Johansson, Christian Mårtenson, *Omvärldsanalys informationsfusion 2009-2010*, 2010
3. FOI-R--3214--SE, Tove Gustavi, Fredrik Johansson, Christian Mårtenson, Pontus Svenson, *Datorstöd för hypoteshantering inom underrättelseanalys*, 2011
4. FOI-R--3265--SE, Johan Dahlin, *Entity matching*, 2011
5. FOI-R--3310--SE, Tove Gustavi, Fredrik Johansson, Ronnie Johansson, Magnus Jändel, Lisa Kaati, Christian Mårtenson, Daniel Oskarsson, *Analytiska verktyg – en översikt av metoder och modeller för underrättelseanalys*, 2011
6. FOI-R--3320--SE, Christian Mårtenson et al., *Årsrapport Verktyg för informationshantering och analys (VIA) 2011*, 2011
7. FOI-R--3453--SE, Ulrik Franke, Ronnie Johansson, Christian Mårtenson, Pontus Svenson, *Fusion av information från heterogena källor*, 2012
8. FOI-R--3531--SE, Katie Cohen, *Who will be a lone wolf terrorist? Mechanisms of self-radicalisation and the possibility of detecting lone offender threats on the Internet*, 2012
9. FOI-R--3532--SE, Ulrik Franke, Fredrik Johansson, Magnus Jändel, Lisa Kaati, Marianela Garcia Lozano, *Tekniker för analys av data från webben*, 2012
10. FOI-R--3533--SE, Christian Mårtenson, Pontus Svenson, *Slutrapport Verktyg för informationshantering och analys (VIA)*, 2012

6.2 Externa publikationer

11. FOI-S--3358--SE, Joel Brynielsson, Stephen Cooper, Christine Nickell, Victor Piotrowski, Brenda Oldfield, Ali Abdallah, Matt Bishop, Bill Caelli, Melissa Dark, Elisabeth K Hawthorne, Lance Hoffman, Lance C Perez, Charles Pfleeger, Richard Raines, Corey Schou, *An exploration of the Current State of Information Assurance Education*, SIGCSE Bulletin 41(4) (2009) 109−125.

12. FOI-S--3465--SE, Johanna Högberg, Lisa Kaati, *Weighted Unranked Tree Automata as a Framework for Plan Recognition*, Proceedings of the 13th International Conference on Information Fusion (FUSION 2010), Edinburgh, UK, 26-29 July 2010, Paper Tu2.4.4, pp. 1-8.

13. FOI-S--3466--SE, Ronnie Johansson, Christian Mårtenson, *Information Acquisition Strategies for Bayesian Network-based Decision Support*, Proceedings of the 13th International Conference on Information Fusion (FUSION 2010), Edinburgh, UK, 26-29 July 2010, Paper We1.4.5, pp.1-8.

14. FOI-S--3467--SE, Pontus Svenson, Robert Forsgren, Birgitta Kylesten, Peter Berggren, Wong Rong Fah, Magdalene S. Choo, John K. Yew Hann, *Swedish-Singapore studies of Bayesian Modelling techniques for tactical Intelligence analysis*, Proceedings of the 13th International Conference on Information Fusion (FUSION 2010), Edinburgh, UK, 26-29 July 2010, Paper Th3.4.1, pp. 1-8.

15. FOI-S--3468--SE, Joel Brynielsson, Johanna Högberg, Lisa Kaati, Christian Mårtenson, Pontus Svenson, *Detecting social positions using simulation*, Proceedings of the 2010 International Conference on Advances in Social Networks Analysis and Mining, Odense, Denmark, 9-11 August 2010

16. FOI-S--3538--SE, Pontus Svenson, *Situation monitoring and threat reasoning for infrastructure protection*, Proceedings of the National Symposium on Technology and Methdology for Security and Crisis Management (TAMSEC), Linköping 27-29 oktober 2010

17. FOI-S--3539--SE, Sten F Andler, Mikael Fredin, Pontus Svenson, *Smart Tracking of Information for Maritime Domain Awareness*, Proceedings of the National Symposium on Technology and Methdology for Security and Crisis Management (TAMSEC), Linköping 27-29 oktober 2010

18. FOI-S--3540--SE, Ronnie Johansson, Christian Mårtenson, *Information Acquisition for Bayesian Network-based Threat Analysis*, Proceedings of the National Symposium on Technology and Methdology for Security and Crisis Management (TAMSEC), Linköping 27-29 oktober 2010

19. FOI-S--3576--SE, Ronnie Johansson, Christian Mårtenson, *Information Acquisition for General Bayesian Networks with Uncertain Observations*, Proceedings of the 1st International Workshop on Advanced Methodologies for Bayesian Networks (AMBN), p. 14, Tokyo, 18-19 nov, 2010

20. FOI-S--3710--SE, Johan Dahlin, *Community Detection in Imperfect Networks*, Student Thesis at Umeå University, 2011.

21. FOI-S--3711--SE, Henrik Artman, Joel Brynielsson, Björn Johansson, Jiri Trnka, *Dialogical Emergency Management and Strategic Awareness in Emergency Communication*, Proceedings of the Eighth International Conference on Information Systems for Crisis Response and Management (ISCRAM 2011), Lisbon, Portugal, 8−11 May 2011, pp. 1−9.

22. FOI-S--3760--SE, Fredrik Johansson, Christian Mårtenson, Pontus Svenson, *A Social Network Analysis of the Information Fusion Community*, Proceedings of the 14th International Conference on Information Fusion (FUSION 2011), Chicago, USA, 5−8 July 2011. IEEE, Piscataway, NJ, 2011, pp.

23. FOI-S--3798--SE, Martin Holmberg, Pontus Svenson, *Information Fusion for Collaborating Commanders at Different Levels*, Proceedings of the 16th International Command and Control Research Technology Symposium, Québec City, Canada, 21−23 June 2011. US Department of Defense CCRP, Washington, DC, 2011, Paper 089, pp. 1−11.

24. FOI-S--3799--SE, Johan Dahlin, Pontus Svenson, *A Method for Community Detection in Uncertain Networks*, Proceedings of the European Intelligence and Security Informatics Conference (EISIC 2011), Athens, Greece, 12−14 September 2011. IEEE, Piscataway, NJ, 2011, pp. 155−162.

25. FOI-S--3800--SE, Lisa Kaati, Pontus Svenson, *Analysis of Competing Hypothesis for Investigating Lone Wolf Terrorists*, Proceedings of the European Intelligence and Security Informatics Conference (EISIC 2011), Athens, Greece, 12−14 September 2011. IEEE, Piscataway, NJ, 2011, pp. 295−299.

26. FOI-S--3801--SE, Fredrik Johansson, Joel Brynielsson, Pontus Hörling, Michael Malm, Christian Mårtenson, Staffan Truvé, Magnus Rosell, *Detecting Emergent Conflicts through Web Mining and Visualization*, Proceedings of the European Intelligence and Security Informatics Conference (EISIC 2011), Athens, Greece, 12−14 September 2011. IEEE, Piscataway, NJ, 2011, pp. 346−353.

27. FOI-S--3802--SE, Robert Forsgren, Andreas Horndahl, Pontus Svenson, Edward Tjörnhammar, *Information fusion for port security decision support*, Proceedings of the European Intelligence and Security Informatics Conference (EISIC 2011), Athens, Greece, 12−14 September 2011. IEEE, Piscataway, NJ, 2011, p. 292.

28. FOI-S--3866--SE, Christian Mårtenson, Andreas Horndahl, Ziaul Kabir, *An Ontology-based Adaptive Reporting Tool*, Proceedings of the Sixth International Conference on Semantic Technologies for Intelligence, Defense, and Security (STIDS 2011), Fairfax, USA, 15−17 November 2011.

29. FOI-S--3969--SE, Lisa Kaati, Pontus Svenson, *An Analysis Method for Investigating Lone Wolf Terrorists*, Proceedings of the Second National Symposium on Technology and Methodology for Security and Crisis Management (TAMSEC 2011), Linköping, Sweden, 19−20 October 2011, p. 17.

30. FOI-S--3970--SE, Joel Brynielsson, Pontus Hörling, Fredrik Johansson, Michael Malm, Christian Mårtenson, Magnus Rosell, Staffan Truve, *Using temporal analytics for early discovery of upcoming threats*, Proceedings of the Second National Symposium on Technology and Methodology for Security and Crisis Management (TAMSEC 2011), Linköping, Sweden, 19−20 October 2011, p. 16.

31. FOI-S--3972--SE, Johan Dahlin, Pontus Svenson, *Community Detection in Uncertain Networks by Ensemble approaches*, Proceedings of the Second National Symposium on Technology and Methodology for Security and Crisis Management (TAMSEC 2011), Linköping, Sweden, 19−20 October 2011, p. 45.

32. FOI-S--3973--SE, Amin Karami, Ronnie Johansson, *Multi-attribute decision making for threat analysis*, Proceedings of the Second National Symposium on Technology and Methodology for Security and Crisis Management (TAMSEC 2011), Linköping, Sweden, 19−20 October 2011, p. 21.

33. FOI-S--3982--SE, Fredrik Johansson, Göran Falkman, *Real-time Allocation of Firing Units To Hostile Targets*, Journal of Advances in Information Fusion 6(2) (2011) 187−199.

34. FOI-S--3996--SE, Birgitta Kylesten, *Dynamic decision-making on an operative level: a model including preconditions and working method*, Cognition, Technology & Work. DOI 10.1007/s10111-012-0221-z , 2012

35. FOI-S--4039--SE, Susanna Nilsson, Joel Brynielsson, Magdalena Granåsen, Charlotte Hellgren, Sinna Lindquist, Mikael Lundin, Maribel Narganes Quijano, Jiri Trnka, *Making use of new media for pan-european crisis communication*, Proceedings of the Ninth International Conference on Information Systems for Crisis Response and Management (ISCRAM 2012), Vancouver, Canada, 22−25April 2012.

36. FOI-S--4048--SE, Joel Brynielsson, Lisa Kaati, Pontus Svenson, *Social positions and simulation relations*, Social Network Analysis and Mining 2(1) (2012) 39−52.

37. FOI-S--4090--SE, Hirad Asadi, Christian Mårtenson, Pontus Svenson, Magnus Sköld, *The HiTS/ISAC social network analysis tool*, Proceedings of the 2012 European Intelligence and Security Informatics Conference (EISIC 2012), Odense, Denmark, 22−24 August 2012. IEEE, Piscataway, NJ, 2012, pp. 291−296.

38. FOI-S--4091--SE, Fredrik Johansson, Joel Brynielsson, Maribel Narganes Quijano, *Estimating citizen alertness in crises using social media monitoring and analysis*, Proceedings of the 2012 European Intelligence and Security Informatics Conference (EISIC 2012), Odense, Denmark, 22−24 August 2012. IEEE, Piscataway, NJ, 2012, pp. 189−196.

39. FOI-S--4092--SE, Johan Dahlin, Fredrik Johansson, Lisa Kaati, Christian Mårtenson, Pontus Svenson, *Combining entity matching techniques for detecting extremist behavior on discussion boards*, Proceedings of the International Symposium on Foundation of Open Source Intelligence and Security Informatics 2012 (FOSINT-SI 2012), Istanbul, Turkey, 27−28 August 2012.

40. FOI-S--4093--SE, Joel Brynielsson, Andreas Horndahl, Fredrik Johansson, Lisa Kaati, Christian Mårtenson, Pontus Svenson, *Analysis of weak signals for detecting lone wolf terrorists*, Proceedings of the 2012 European Intelligence and Security Informatics Conference (EISIC 2012), Odense, Denmark, 22−24 August 2012. IEEE, Piscataway, NJ, 2012, pp. 197−204.

41. FOI-S--4094--SE, Mika Cohen, Andreas Horndahl, Christian Mårtenson, *First steps towards a context aware ontology-driven reporting system*, Proceedings of the 8th International Conference on Semantic Systems (I-SEMANTICS 2012), Graz, Austria, 5−7 September 2012. ACM, New Yok, NY, 2012, pp. 103−108.

42. FOI-S--4143--SE, Johanna Björklund, Eric Jönsson, Lisa Kaati, *Aspects of plan operators in a tree automata framework*, Proceedings of the 15th International Conference on Information Fusion (FUSION 2012), Singapore, 9−12 July 2012. IEEE, Piscataway, NJ, 2012, pp. 1462−1467.
43. FOI-S--4144--SE, Ala Berzinji, Ahmed Rezine, Lisa Kaati, *Detecting key players in terrorist networks*, Proceedings of the 2012 European Intelligence and Security Informatics Conference (EISIC 2012), Odense, Denmark, 22−24 August 2012. IEEE, Piscataway, NJ, 2012, pp. 297−302.
44. FOI-S--4145--SE, Tove Gustavi, Pontus Svenson, *Pattern theory in intelligence analysis*, Proceedings of the 2012 European Intelligence and Security Informatics Conference (EISIC 2012), Odense, Denmark, 22−24 August 2012. IEEE, Piscataway, NJ, 2012, p. 290.
45. FOI-S--4146--SE, Martin Holmberg, Pontus Svenson, *Lessons identified from the use of automated information fusion in collaborative environments*, Proceedings of the 2012 IEEE International Multi-Disciplinary Conference on Cognitive Methods in Situation Awareness and Decision Support (CogSIMA), 2012
46. FOI-S--4151--SE, Muhammad Adnan Tariq, Joel Brynielsson, Henrik Artman, *Framing the attacker in organized cybercrime*, Proceedings of the 2012 European Intelligence and Security Informatics Conference (EISIC 2012), Odense, Denmark, 22−24 August 2012. IEEE, Piscataway, NJ, 2012, pp. 30−37.
47. FOI-S--4152--SE, , Muhammad Adnan Tariq, Joel Brynielsson, Henrik Artman, *Storytelling for tackling organized cybercrime*, Proceedings of the 26th Annual BCS Conference on Human Computer Interaction (HCI 2012), Birmingham, United Kingdom, 12−14 September 2012. British Informatics Society Limited, London, United Kingdom, 2012.

Ej ännu publicerade

48. Katie Cohen, Fredrik Johansson, Lisa Kaati, Jonas Clausen Mork, *Detecting Linguistic Markers for Radical Violence in Social Media*, Terrorism and political violence (Special Issue, trycks januari 2013)
49. Fredrik Johansson, Pontus Svenson, *Constructing and Analyzing Uncertain Social Networks from Unstructured Textual Data*, Accepterat som bokkapitel i Studies in Mining Social Networks.
50. Henrik Artman et al., *The Secret Life of a Persona: When the Personal Becomes Private*, Inskickat till CHI 2013.