Slutrapport Stödverktyg för informationsfusion och analys (SIA)

FREDRIK JOHANSSON

FOI-R--4141--SE
ISSN 1650-1942 December 2015

Fredrik Johansson

Slutrapport Stödverktyg för informationsfusion och analys (SIA)

Titel	Slutrapport Stödverktyg för informationsfusion och analys (SIA)
Title	Final report Tools for information fusion and analysis
Rapportnr/Report no	FOI-R--4141--SE
Månad/Month	Dec
Utgivningsår/Year	2015
Antal sidor/Pages	26
ISSN	1650-1942
Kund/Customer	Försvarsmakten
Forskningsområde	1. Beslutsstödssystem och informationsfusion
FoT-område	Ledning och MSI
Projektnr/Project no	E36728
Godkänd av/Approved by	Lars Höstbeck
Ansvarig avdelning	Informations- och aerosystem

Detta verk är skyddat enligt lagen (1960:729) om upphovsrätt till litterära och konstnärliga verk.
All form av kopiering, översättning eller bearbetning utan medgivande är förbjuden

This work is protected under the Act on Copyright in Literary and Artistic Works (SFS 1960:729).
Any form of reproduction, translation or modification without permission is prohibited.

Sammanfattning

Denna rapport sammanfattar verksamheten inom projektet Stödverktyg för informationsfusion och analys som löpt under åren 2013-2015. Syftet med projektet har varit att bygga upp och överföra kunskap till Försvarsmakten om möjligheter och begränsningar med datadriven underrättelseanalys.

Under projektets första år identifierades ett antal forskningsbehov hos Försvarsmakten. Detta ledde till en inriktning av projektet mot analys av trovärdighet hos information och källor på internet, med speciellt fokus på vilseledningsoperationer. Ett teoretiskt arbete genomfördes för att kartlägga olika aspekter av vilseledning på Twitter och hur sådan vilseledning kan upptäckas.

Under 2014 inleddes en teknisk utveckling med målet att bygga en plattform för att utveckla och experimentera med nya metoder och tekniker för att stödja analytiker med uppgiften att upptäcka vilseledning och påverkansoperationer i sociala medier. Det första steget mot en experimentplattform var att implementera och driftsätta en inhämtningsmodul för att skapa datamängder att experimentera med. Därefter påbörjades tre utvecklingsspår, ett med fokus på visuell datainteraktion, ett på textanalys och ett på data mining. I takt med att verktygen mognat har under projektets gång ett antal workshops anordnats med analytiker från FM i syfte att i ett tidigt skede få återkoppling på arbetet och samla in nya analys- och utvecklingsidéer.

2015 har utvecklingen av verktygen fortsatt och dessa har integrerats samman till ett gemensamt prototypsystem för detektion av påverkansoperationer på Twitter. Detta system har lyfts över på ett Hadoop-kluster i syfte att fungera för analys av väldigt stora datamängder. En slutdemo har hållits för projektet, riktad mot FM och andra relaterade intressenter.

Nyckelord: datadriven analys, underrättelseanalys, informationsfusion

Summary

This report provides a summary of the work within the project Tools for information fusion and analysis, which started in 2013 and ended in 2015. The aim of the project has been to build and transfer knowledge to the Swedish Armed Forces about possibilities and limitations with data driven intelligence analysis.

In year one, a number of research needs at the Armed Forces were identified, leading to a focus for the project on assessing the trustworthiness of information on the Internet, with a special interest in deception. A theoretical work was undertaken in order to identify various aspects of deception on Twitter and find out how such deception can be detected.

In 2014, development of a platform for experimenting with new methods and techniques to support analysts with deception detection was initiated. The first step towards such a platform was to implement and deploy a retrieval module for creating datasets to make experiments on. Furthermore, three development tracks were initiated, one focusing on visual analytics, one on natural language processing, and one on data mining. As the developed tools started to mature, analysts were engaged to give feedback and suggestions at an early stage.

During 2015, the development of the tools has continued and they have been integrated into a common prototype system for detection of influence operations on Twitter. This system has been transferred to a Hadoop cluster in order to work for analysis of big data. A final demo has been carried out with the Swedish Armed Forces and related stakeholders.

Keywords: data driven analysis, intelligence analysis, information fusion

Innehållsförteckning

1 Inledning 7

1.1 Syfte och mål ... 7

2 Enskild forskningsverksamhet 9

2.1 Vilseledning i sociala medier ... 9

2.2 Informations- och källvärdering ... 14

2.3 Samverkan NATO-grupp ... 14

2.4 Klusterteknik ... 15

3 Verksamhet inom samverkansprojekt 16

3.1 Heterogen fusion ... 16

3.2 Riskvärdering ... 19

3.3 Anonymisering ... 20

4 Övrig verksamhet 21

5 Fortsatt arbete 23

6 Publikationer 24

6.1 FOI-rapporter ... 24

6.2 Externa publikationer ... 24

1 Inledning

Vi lever i ett informationssamhälle där den tillgängliga mängden data ständigt ökar. Ökningen gäller för samhället i stort men också för underrättelseområdet. Inhämtningsdiscipliner såsom signal- och bildunderrättelser får alltmer data att arbeta med tack vare fler och mer avancerade sensorer. Även vid analys av öppna källor ökar mängden data, vilket huvudsakligen beror på tillgången till data som användare genererat genom sociala medier och så kallade öppna data-initiativ, där data från myndigheter görs tillgängligt för medborgare via webben.

Den ökade mängden data och information gör att analytiker i allt större omfattning måste sålla i de data de arbetar med. Att översköljas av data utan rätt hjälpmedel leder till överbelastning och försämrad beslutsförmåga. Givet rätt stöd att hitta vad som är relevant i datamängderna, ger däremot mer omfattande mängder data möjlighet till bättre analyser och bedömningar.

Det traditionella sättet att konstruera stödverktyg för informationsanalys baserar sig på modeller, där regler för kända förhållanden sätts upp av domänexperter och sedan matchas mot data. Dessa regler riskerar dock att missa okända mönster eller oförutsedda förändringar i omvärlden. Att istället mer förutsättningslöst söka efter mönster och trender, genom så kallad *datadriven analys*, ökar chanserna att tidigt upptäcka nya fenomen i data.

Denna rapport beskriver verksamheten som genomförts inom ramen för FoT Ledning och MSI-projektet *Stödverktyg för informationsfusion och analys* (SIA). Projektet startade 2013 och pågår till och med 2015.

1.1 Syfte och mål

Syftet med projektet SIA är att bygga upp och överföra kunskap till Försvarsmakten avseende möjligheter och begränsningar med datadriven underrättelseanalys. Resultaten är avsedda att stödja underrättelsefunktionens metodutveckling och kravställning på tekniska stödsystem.

Målet för projektet är att vid projektavslut ha utvecklat, värderat och demonstrerat nya algoritmer, verktyg och metoder för datadriven underrättelseanalys. Genom verksamheten i projektet ska kunskap också ha byggts upp som bidrar till att svara på följande frågeställningar:

1. Hur ska analytiker interagera med ett datadrivet stödverktyg för att effektivt inkorporera mänsklig kunskap?
2. Hur ska analysresultaten presenteras och förklaras?
3. Vilka algoritmer är lämpliga för vilken typ av analys på vilken typ av data?

4. Vilka krav ställer datadriven analys på signalbehandling och fusion av data från olika inhämtningsdiscipliner?

En del av projektets budget har satsat på uppbyggnad av kunskap genom relaterade EU- och EDA-projekt. Inom EDA-projektet forskar FOI på automatisk fusion av underrättelseinformation med bland annat sensordata, och inom EU-projekten om olika aspekter av underrättelseanalysverktyg inom en kontext av civil säkerhet. De medfinansierade projekten har bidragit till att svara på projektets frågeställningar och gett en hävstångseffekt på satsade forskningsmedel.

Forskningsverksamheten inom SIA kan delas upp i aktiviteter som utförts enskilt inom projektet respektive genomförts inom ramen för de medfinansierade samverkansprojekten.

2 Enskild forskningsverksamhet

Under 2013, projektets första år, genomfördes studier för att identifiera Försvarsmaktens behov av datadriven underrättelseanalys och vilka forskningsfrågor som dessa behov genererar. Resultatet ledde till en inriktning av den enskilda forskningsverksamheten mot analys av trovärdighet hos information och källor på internet, med speciellt fokus på detektion av vilseledningsoperationer.

Under 2013 utfördes även ett arbete om automatisk övningsmonitorering i samarbete med FOI-projektet RUFS (rysk utrikes-, försvars- och säkerhetspolitik). Det resulterade i en teknisk demonstration där alla artiklar från en utvald tidnings internetupplaga hämtades in och bearbetades automatiskt för att extrahera händelser som härrörde från militära övningar. De extraherade övningarna bildade en datamängd som kunde analyseras med ett verktyg för visuell datainteraktion, där en analytiker kan vrida och vända på data för att hitta intressanta mönster. Detta arbete väckte stort intresse, men har inte tagits vidare då projektets resurser istället kraftsamlats på detektion av vilseledning och påverkansoperationer i sociala medier.

2.1 Vilseledning i sociala medier

Att utveckla generella verktyg för att stödja analytiker i deras bedömningar av trovärdighet hos information och källor på Internet är svårt. Mängden informationskanaler är överväldigande, med skiftande syften, målgrupper och tekniska plattformar. Inom projektet har vi därför valt att begränsa oss till att studera vilseledning ur främst ett statsaktörsperspektiv på mikrobloggen Twitter. Projektet har också haft vissa forskningssamarbeten kopplade till att identifiera terrorgruppers användning av propaganda och spridning av våldsbejakande extremism i sociala medier.

Under hösten 2013 påbörjades ett teoretiskt arbete med att kartlägga olika aspekter av vilseledning på Twitter och hur sådan vilseledning kan upptäckas. En litteraturgenomgång genomfördes för att se vilka metoder och tekniker som föreslås i befintlig forskningslitteratur. Dessa kopplades sedan till ett antal vilseledningstaxonomier för att därigenom ge en bild av forskningsläget. Arbetet fortsatte under våren 2014 och resulterade i en översiktsartikel som presenterats vid The First International Workshop on Social Networks Analysis, Management and Security i Barcelona i augusti samma år.

Under våren 2014 inleddes den tekniska utvecklingen med målet att bygga en plattform för att utveckla och experimentera med nya metoder och tekniker för att stödja analytiker att upptäcka vilseledning. Då vilseledning till sin natur är avsedd för att luras och därför ständigt anpassas efter rådande kunskapsläge är det inte

troligt att det går att utveckla automatiska system som egenhändigt kan göra detektion. Den kontextuella förståelsen hos analytiker är därför central, men datorverktyg bidrar till att mer omfattande datamängder kan hanteras på ett mer strukturerat sätt. Det finns också aspekter av vilseledning som datorer är mer immuna mot än människor, som kan missledas av kognitiva bias.

Det första steget mot en experimentplattform var att implementera och driftsätta en inhämtningsmodul för att erhålla datamängder att experimentera med. Därefter påbörjades tre utvecklingsspår, ett med fokus på visuell datainteraktion, ett på textanalys och ett på data mining. I takt med att verktygen under hösten 2014 och våren 2015 började mogna anordnades ett antal workshops med analytiker från FM i syfte att i ett tidigt skede få återkoppling på arbetet och samla in nya analys- och utvecklingsidéer.

Under återstoden av 2015 har fokus varit att föra samman de olika utvecklingsspåren till ett gemensamt prototypsystem för detektion av påverkansoperationer i sociala medier i allmänhet och Twitter i synnerhet. Vidare så har detta system överförts till ett så kallat Hadoop-kluster, i syfte att möjliggöra analys av stora datamängder. I november 2015 har en slutdemonstration för projektet hållits där de utvecklade verktygen presenterats för intressenter från Försvarsmakten och relaterade myndigheter med intresse för påverkansoperationer på sociala medier. De olika delarna av systemet redogörs översiktligt för nedan:

Visuell datainteraktion

Ett sätt att underlätta för analytiker att skapa förståelse för de stora datamängder som varit aktuella i projektet är att använda tekniker för visuell datainteraktion: att åskådliggöra informationen från olika perspektiv och låta analytiker navigera, zooma och filtrera direkt mot underlaget för att hitta mönster och nå insikter. Exempel på frågor som analytiker kan söka svar på är: Hur identifieras användare med bedrägliga intentioner utifrån den information som kan utvinnas ur de inhämtade datamängderna? I projektet har vi tagit fram en prototyp av ett verktyg baserat på det kommersiella verktyget Spotfire där vi kan visa ett antal exempel på analyser på insamlad Twitter-data. För att förstå principen för hur analysen fungerar följer nedan inledningen till ett sådant exempel.

Figur 1 ger en översikt av ett av de flöden vi hämtar från Twitter. Ett tydligt dygns-mönster uppstår för när de flesta så kallade tweets skickas. Färgkodningen representerar hur gammalt kontot var när en tweet skickades. Skalan går från mörkt rött (sekunder–minuter) via gult (enstaka dagar) till blått (år). Avvikelser i det här perspektivet blir tydliga: Ungefär mitt i tidsperioden finns en gulfärgad kulle som indikerar aktivitet från ganska nyskapade konton.

Figur 1. En tidslinje som visar Twitter-aktivetet över en period på 10 dagar där färgkodningen representerar ålder på kontot när tweeten skickades. Varmare färg betyder yngre konto.

Genom att markera det potentiellt intressanta området direkt i tidslinjen kan analytikern zooma in och filtrera för att få en tydligare bild av händelserna (Figur 2). I nästa steg tittar vi närmare på användarna som ligger bakom denna aktivitet för att jämföra dem mot normalbilden av användare från olika perspektiv. I Figur 3 ser vi hur användare i normalfallet, för vår period på 10 dagar, ter sig i perspektivet språk och Twitter-klient: En stor majoritet av kontona har engelsk språkinställning och Twitter-klienterna är till stor del iPhone, Android och Web vilket verkar rimligt. För det avvikande utsnittet som vi hittade dyker en helt annan bild upp (Figur 4). Fördelningen av språk är helt likformig och alla 7000 användare använder samma typ av klient. Dessa mycket utmärkande karaktärsdrag leder oss in på djupare analyser av användarna och deras tweets med hjälp av prototypens olika vyer och interaktionsmöjligheter.

Figur 2: En inzoomad och filtrerad vy över Twitter-aktiviteten i en tidsperiod med mycket aktivitet av relativt nyskapade konton (många gulfärgade konton).

Figur 3. Fördelningen av användarnas språk (language) och Twitter-klient (source) i normalfallet, motsvarande det urval som gjorts i Figur 1.

Figur 4. Fördelningen av användarnas språk (language) och Twitter-klient (source) i vårt inzoomade fall, motsvarande det urval som gjorts i Figur 2.

Data mining och textanalys

Parallellt med utvecklingen av verktyget för visuell interaktion har ett antal metoder för automatisk dataanalys utvecklats. En modul för textanalys har tagits fram som möjliggör för användare att definiera ordmönster som dessa automatiskt vill detektera i Twitterflödet. Som ett exempel på hur detta kan användas för att hitta indikationer på vilseledning har vi definierat uttryck som tyder på att någon beskyller någon annan för att ljuga eller sprida desinformation. Uttrycken har testkörts på flera mindre datamängder och resultaten tyder på att metoden fungerar väl och bidrar till att ge en överblick av pågående propaganda. Med anledning av detta har vi sedan gått vidare och skapat en textanalysprocess där alla inhämtade tweets automatiskt blir föremål för olika former av vidare bearbetning, bland annat innefattande extraktion av entiteter såsom personnamn och platser, samt de ordmönster för explicita lögnuttryck som beskrivits ovan. På detta sätt kompletteras inhämtade tweets och tillhörande metadata med ännu mer

information som kan nyttjas i den interaktiva visualiseringen. Utöver detta har en prototyp av ett verktyg kallat PhraseBrowser, speciellt anpassat för textanalysen, tagits fram. PhraseBrowser kan användas för att utforska vad som skrivs om ett ämne på Twitter. Det åstadkoms genom att ladda ned tweets som innehåller någon av de söktermer som användaren specificerar. Dessa nedladdade tweets analyseras sedan med hjälp av en utvecklad textanalyskomponent, varpå resultatet visas upp i ett browserfönster. PhraseBrowser identifierar intressanta delar av varje text. Delarna kallas *fraser* eller *extraktioner*. Enkel statistik sparas för alla fraser under körningen. Användaren kan välja ut enskilda fraser och få se i vilka tweets dessa har förkommit. Gränssnittet för PhraseBrowser exemplifieras i Figur 5.

Figur 5: Gränssnittet för PhraseBrowser. Under rubriken ”Item” finns fraserna sorterade efter hur många gånger de påträffats.

En annan indikator på vilseledning är förekomsten av botar, det vill säga användarkonton som automatiskt eller semi-automatiskt postar inlägg i något specifikt syfte. Ett sådant syfte kan exempelvis vara att dränka relevanta informationsflöden, till exempel rapporter om kränkningar av mänskliga rättigheter, med annan icke-relevant information eller ”spam”. En uppsjö av olika tillvägagångssätt för att avslöja botar har identifierats i litteraturen, varav en delmängd har studerats mer ingående inom projektet.

Under 2015 har projektmedlemmar handlett två stycken examensarbetare som haft till uppgift att ta fram metoder och algoritmer för att automatiska kunna identifiera automatiserat beteende (däribland botar) samt att kunna upptäcka kapning av existerande Twitter-konton. Detta arbete har bland annat resulterat i två vetenskapliga konferensbidrag på andra upplagan av European Network and Intelligence Conference (ENIC 2015). Algoritmerna för detektion av automatiserat beteende har också implementerats och integrerats i vårt större

prototypsystem, vilket möjliggör extra filtreringsmöjligheter i den visuella datainteraktionen.

2.2 Informations- och källvärdering

Sent 2012 påbörjades en aktivitet inom FOI om värdering av öppna källor i samband med att en medarbetare påbörjade en ny fas i sina doktorandstudier. Arbetet har ingått i SIA-projektets plan och passar väl in med de konkreta behov och forskningsfrågor kring vilseledning på internet som bedrivits inom projektet.

Målet med doktorandarbetet är att ta fram stödverktyg som kan bistå analytiker i arbetet med att bedöma tillförlitlighet och sakriktighet hos öppna källor och dess information. Fokus ligger på värdering av ostrukturerad och textbaserad information från webben, till exempel bloggar, tweets och nyhetsartiklar.

Erfarenheter kring informations- och källvärdering har bland annat samlats in genom:

- intervjuer och enkäter med Försvarsmaktspersonal samt utländsk militär personal under stabsövningen CJSE 13
- enkätundersökning hos RAHS Experimentation Centre (Risk Assessment and Horizon Scanning) i Singapore
- samtal med UndSäkC
- samtal med analytiker på FM specialiserade på data från öppna källor

Slutsatserna från dessa intervjuer, enkäter och samtal har sammanställts till en vetenskaplig artikel som presenterats på 2013 European Intelligence and Security Informatics Conference.

Parallellt har också implementationen av ett verktyg påbörjats, vilket kommer att användas som experimentplattform för framtida utveckling av metodik och algoritmer.

2.3 Samverkan NATO-grupp

FOI deltar inom ramen för projektet i Nato-gruppen SAS-IST-RTG-102 Intelligence exploitation of social media. Arbetsgruppen är sammansatt utifrån två så kallade paneler inom Natos Science & Technology Organization: System Analysis and Studies (SAS) och Intelligence Systems and Technology (IST). Detta speglar både områdets komplexa natur och det stora intresset för dessa frågor. Gruppen fokuserar på hur underrättelser från öppna källor (OSINT) kan användas i militär verksamhet för att uppnå ett informationsöverläge gentemot motståndaren. I det moderna samhället där alltmer information lagras och tillgängliggörs digitalt blir Internet och sociala medier allt viktigare pusselbitar för

att uppnå ett sådant informationsöverläge. Gruppen är sammansatt av både praktiker (från försvarsmakter) och forskare (från motsvarigheter till FOI).

I oktober 2015 hade gruppen ett möte i Prag. Vid mötet deltog ungefär 15 deltagare från Nato- och PfP-länder och flera höll intressanta presentationer om sina egna erfarenheter av internetbaserad OSINT. FOI:s presentationer var i enlighet med projektets inriktning främst fokuserat på detektion av vilseledning och redogjorde för de framsteg som vi gjort under året. Generellt har FOI:s bidrag väckt stort intresse och positivt gensvar.

Nato-gruppens arbete avslutas under 2016 och arbetet med att sammanställa en rapport har påbörjats. FOI kommer att medverka främst i kapitlet om vilseledning och påverkansoperationer. Planen är dessutom att kapitlen i denna rapport ska presenteras i en speciell session på konferensen Next-Generation Analyst IV i Baltimore i april 2016.

Sammanfattningsvis kan konstateras att Nato-gruppens intresseområden ligger nära projektets och även fortsättningsvis kommer att utgöra ett värdefullt komplement till det arbete som FOI självt kan genomföra. Inte minst är gruppens blandade sammansättning av både praktiker och forskare en styrka. Det finns ett stort intresse inom gruppen att verka för en förlängning av dess verksamhet efter 2016, vilket sammanfaller väl med FOI:s önskan om att fortsätta inom detta område.

2.4 Klusterteknik

En orsak till att intresset för datadriven analys förväntas öka, är att takten med vilken information skapas och tillgängliggörs ständigt skruvas upp. Detta medför att storleken på de datamängder som ska analyseras i sig utgör ett problem, vilket kräver extraordinära lösningar, ett fenomen som populärt kallas *Big data*. En lösning för att hantera och analysera stora datamängder som vinner popularitet är Hadoop. Hadoop är ett mjukvaruramverk för att lagra och bearbeta stora datamängder på datorkluster där hårdvaran består av ”standardmaskiner”. Det medför att dessa kluster är relativt billigt i inköp och drift. När datamängden växer är det också enkelt att utöka klustren med nya (billiga) maskiner.

Flera av projektets intressenter har signalerat till FOI att de inom en snar framtid kommer att ha ett ökat behov av att hantera och analysera stora datamängder. Inom SIA-projektet har därför ett inköp av ett Hadoop-kluster genomförts. Kompetens för hantering av och utveckling mot klustret har börjat byggas upp inom ramen för SIA.

3 Verksamhet inom samverkansprojekt

En del av SIA-projektets budget har varit vikt åt medfinansiering av samverkansprojekt. Aktiviteterna inom dessa projekt är kopplade till forskningsområden som är relevanta för datadriven analys och bidrar till att svara på projektets frågeställningar. Listan nedan ger en översikt över forskningsområdena och vilka projekt som bidrar till vilket:

Område	Projekt
Heterogen fusion	SUPPORT, D-BOX, IN-4-STARS
Riskvärdering	Contain, Eurosky
Anonymisering	Fidelity

Det verktyg för multihypoteshantering som delvis utvecklats inom SIA under 2013, men framför allt inom dess föregångare VIA och EU-projektet Contain, har nu överförts till ett FMV-finansierat projekt där vidareutveckling och användarförsök genomförts under 2014 och 2015.

3.1 Heterogen fusion

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 vinsterna om man lyckas kan vara stor.

SUPPORT

Inom FP7-projektet SUPPORT har FOI varit med och tagit fram teknik och arbetsmetoder för att höja säkerheten mot terrorism och organiserad brottslighet i Europas hamnar. Den del som SIA-projektet samverkat med har utvecklat en lösning baserat på så kallade semantiska tekniker för att integrera heterogena informationskällor (olika sensorsystem, mänskliga observatörer och underrättelser) med målet att förbättra situationsförståelsen hos hamnens säkerhetsoperatörer.

Under projektet genomfördes en slutdemonstration i Stena Lines tysklandsterminal i Göteborg. Publiken var i första hand hamnsäkerhetsansvariga, hamnoperatörer samt svenska och europeiska myndigheter, däribland Försvarsmakten och FMV. Demonstrationen blev lyckad och bidrog till att ett norskt företag undersöker möjligheten att produktifiera FOI:s fusions-lösning.

D-BOX

Inom EU-projektet D-BOX, 2013-2015, tas stödverktyg för humanitär minröjning fram. Kraven på humanitär minröjning är mycket starka eftersom en incident eller olycka i ett område som meddelats som riskfritt av nationella, ansvariga myndigheter med stöd av internationella organisationer medför stora negativa konsekvenser för befolkningens förtroende. Projektet omfattar utveckling av mindetektionstekniker, IT-stöd för riskanalys, riktlinjer för kultur och etik i lokala kontakter och informationsverktyg för skyddsutrustning, träning, riskmateriel och dess oskadliggörande och bortskaffande samt stödverktyg för minröjningens planering och genomförande.

FOI ska bidra med informationshantering och -fusion i de delar som omfattar minröjningens planering. Informationssystemet ska stötta ansvariga beslutsfattare och utförare inom ett lands humanitära minröjning med beslut om och underlag för prioritering av operationer som riktas mot olika områden och klassificerande av land som riskfritt för lokal samhällsanvändning. Stödet innebär bland annat analys av vilken information som saknas, vilken information som finns tillgänglig om regionen eller inom en geografisk radie och om relevanta uppgifter från nationella och internationella Standard Operating Procedures (SOPs) har genomförts korrekt. För prioritering av vilka områden som operationer ska riktas mot kommer fusionstekniker att användas som analyserar samhällspåverkan av minröjning av ett visst område. Informationsunderlaget är omfattande och heterogent. Det inkluderar bland annat strukturerad information eller rapporter från soldater, lokala myndigheter och lokalbefolkning, satellit- och flygbilder, mätningar med mindetekterande utrustning, social och geografisk/ekonomisk information, infrastrukturinformation, krigsdokumentation, och även FN:s och nationella standardprocedurer för beslutsfattande och genomförande.

Figur 6: Screenshot av en kartvy i MineWiki

FOI har tagit fram ett informationshanteringssystem, MineWiki, med användartillgång via Internet och vanliga webbläsare, baserat på den öppna

mjukvaran Semantic Mediawiki. MineWiki utnyttjar befintliga semantiska funktioner i plattformen för att visualisera och beräkna sammanslagningar av information. En större del av arbetet har inneburit utveckling av en konceptuell modell för informationshanteringen och användarens planeringsarbete samt verktyg för inmatning av strukturerad information. MineWiki stödjer samverkan mellan användare/utförare genom en Request For Information (RFI) funktion.

Under sommaren 2015 genomfördes en demonstration med slutanvändare som målgrupp i Szczytno, Polen. Där visades verktyg som ingår i D-box projektet och FOI demonstrerade MineWiki live. I publiken ingick minröjare från bland annat Libanon och Kroatien. I utvärderingen fick MineWiki höga betyg av slutanvändarna.

År 2016 kommer en slutdemonstration hållas i Italien där slutanvändarna ska få sköta verktyget själva för att utvärdera funktionalitet och användarvänlighet.

IN-4-STARS

IN-4-STARS är ett samarbetsprojekt inom ramen för EDA med underrättelsefokus som startade i september 2013. FOI arbetar inom detta tillsammans med Thales i Nederländerna, Eindhovens tekniska universitet samt Tallinns tekniska universitet. Målet är att utveckla nya metoder och tekniker för att sätta upp säkra multilaterala samarbeten och kommunikationsflöden med underrättelseanalytikern i centrum. Projektet pågår under tre år och FOI:s medverkan är till tre fjärdedelar finansierat av FMV och en fjärdedel av Försvarsmakten genom SIA (och dess efterföljare).

I september 2015 genomfördes den andra demonstrationen inom projektet i Tartu, Estland, inför den styrgrupp bestående av representanter från Sverige, Nederländerna och Estland som finansierar och utvärderar projektets framsteg. Närvarade gjorde också kadetter från en militär utbildning i Tartu, samt ledningen för den Estländska militärens forskningsdel, vilken är helt nyinrättad. Vid demonstrationen kopplades FOI:s prototyp Impactorium samman med estniska och holländska algoritmer och sensorlösningar med hjälp av web services. Scenariot som demonstrerades bestod av en multinationell snabbinsatsstyrka som placerats ut i ett insatsområde i fredsbevarande syfte. Centralt för scenariot var en frågeställning om huruvida det finns överhängande risk för upplopp i en viss by av intresse. För att svara på denna frågeställning spelade Impactorium en viktig roll, genom att det efterfrågar och sammanställer (fusionerar) information från olika källor – i detta fall sensorer för rörelsedetektion och kamerabilder som tagits av en UAV.

I och med den lyckade demonstrationen uppfylldes den fjärde utav totalt sex milstolpar i projektet. Nästa blir en mindre demonstration i Stockholm i mars 2016, följt av en slutdemonstration i Delft i september 2016. Resten av tiden i projektet blir därför väsentligen fokuserat på genomförande av dessa.

Under 2015 har FOI förutom att medverka i demonstrationen också skrivit och fått ett vetenskapligt papper publicerat: “A Data Association Framework for General Information Fusion”. Det handlar om dataassociation, det vill säga hur data som kommer in till ett system som Impactorium kan kopplas till modellerna där (till exempel modellen för upplopp i scenariot). Resonemangen från detta följer med in i utvecklingen av scenariot och Impactorium till demonstrationen i Stockholm, där risken för konflikter/skärmytslingar mellan rivaliserande grupper kommer hanteras utöver upploppen.

I demonstrationen i Stockholm kommer även textanalysprototypen PhraseBrowser att ingå. PhraseBrowser utvecklas inom ramen för både SIA och IN-4STARS. Här används den för att avgöra den allmänna stämningen i området (sentimentanalys), vilket påverkar risken för upplopp och konflikter. Resultatet av manuell analys av OSINT med hjälp av PhraseBrowser sammanställs sedan i Impactorium med data från sensorer enligt ovan.

En viktig aspekt i projektet är att den information som skickas sänds över säkra (krypterade) informationskanaler, samt att personer, roller eller system endast får tillgång till den som de har behörighet för. FOI är inte inblandade direkt i denna utveckling men hoppas erhålla resultat som är av nytta för FM.

3.2 Riskvärdering

Inom FP7-projekten Contain och Eurosky arbetar FOI med att ta fram metoder och tekniska verktyg som kan stödja tulltjänstemän och säkerhetspersonal i arbetet med att identifiera fraktgods med potentiellt farligt eller illegalt innehåll. Inom Contain har man specifikt inriktat sig på containerfrakt och i Eurosky på flygfrakt.

Verktygen och metoderna som utvecklats av FOI inom projekten bygger på avancerade fusionsmetoder, där tillgänglig data från fraktdokument, underrättelser, information om leverantörer, transportväg samt fysiska egenskaper hos fraktförsändelserna kombineras med erfarenheter från tidigare kontroller och används för att ta fram riskprofiler för fraktförsändelserna. Tullens arbete med riskvärdering har likheter med militärt underrättelsearbete i det att det handlar om att analysera stora mängder data för att hitta svaga signaler på att något intressant (farligt, olagligt) håller på att hända.

Ett problem vid såväl riskvärdering som underrättelseanalys är att de analysmodeller som används är svåra att verifiera och behöver förändras kontinuerligt allteftersom analytikern får allt bättre kunskap om domänen och det som analyseras. Eurosky har under 2014 undersökt hur kopplingen mellan en tidigare utförd risk- och sårbarhetsanalys (till exempel med så kallade bow-tie-modeller) och de dynamiska modellerna som används för riskvärderingen kan automatiseras. Eurosky tittar också på hur insamlingen av empiriska data (i

samband med scanning av flygfrakt) kan anpassas för att ge bättre underlag till riskanalysen.

3.3 Anonymisering

SIA har också medfinansierat ett arbetspaket i EU-projektet Fidelity vilket studerat framtidens elektroniska passhantering. Arbetspaketet handlade om hur informationsteknik kan användas för att förutsäga vilka passagerare som behöver granskas extra noga i identitetskontroller. FOI:s arbete i projektet har bland annat resulterat i två vetenskapliga artiklar:

En tidskriftsartikel som beskriver en procedur för att ta beslut om en viss anonymiserad databas kan delas utan risk för att enskilda individer ska identifieras av någon obehörig har publicerats (”Decision support for releasing anonymised data”, Computers & Security 46, p48-61, 2014).

En konferensartikel (”Fusing restricted information”, Fusion 2014) har publicerats med fokus på problemet med att analysera ett system av klassificerare (byggda med hjälp av data mining-metoder baserade på databaser) där användaren inte vill riskera att läcka information om de ursprungliga databaserna, men samtidigt dela viss information (exempelvis mellan olika organisationer) via klassificerarna. Det kan exempelvis handla om att militär underrättelsedata i en internationell insats innehåller uppgifter från mänskliga källor vilka måste skyddas, men som skulle göra nytta om den kombinerades med den lokala polisens spaningsdata. Antingen delas informationen inte alls (för att skydda källorna) eller så försöker ägaren av informationen, vilket undersöks i artikeln, nyttiggöra informationen även externt genom att garantera att känslig information inte sprids.

4 Övrig verksamhet

Nedan listas några axplock av den verksamhet främst i form av informationsspridning och omvärldsbevakning som relaterar till SIA-projektet, men inte faller inom ramen för en specifik aktivitet.

- **Seminariedagar om webbanalys.** SIA har bidragit vid arrangerandet av årliga seminariedagar på Uppsala Universitet med temat webbananalys som organiserats tillsammans med Uppsala universitet och Arena Säkerhet. Exempel på presentationer som givits är:
    - analys av sociala nätverk och hur det kan användas för underrättelseanalys
    - författarigenkänning som används för att identifiera vem som skrivit hot på sociala medier
    - textanalys och hur man kan identifiera vilseledning och lögner på sociala medier
    - lingvistiska metoder för att identifiera hotfulla meddelanden eller olika personlighetstyper.
    - identifikation av våldsbejakande extremism på Twitter
    - illegala marknadsplatser och Dark Web

  Ett av syftena med seminariedagen är att fungera som en mötesplats för analytiker och forskare. Seminariedagen lockar ett stort antal deltagare från flera olika myndigheter.

- **Workshop: "Extremism and Terrorism Online: A Multidisciplinary Examination of Current Trends and Challenges", 13 – 14 October 2014, Singapore.** Projektmedarbetare Lisa Kaati var inbjuden som talare på denna workshop med fokus på terrorism. Workshopen hade forskare från bland annat Irland, Norge, Österrike, USA och Australien. Lisa presenterade forskning relaterad till tidskriftsartikeln "Detecting linguistic markers for radical violence in social media". Presentationen handlade om hur man kan använda lingvistiska markörer för att upptäcka tecken på att en person kan ha avsikt att begå ett terrorbrott. Grunden för detta finns i de psykologiska varningsbeteenden som uppvisats innan våldsamma brott har begåtts. Lisa beskrev hur vissa av dessa beteenden kan upptäckas i skriven text på exempelvis sociala medier och vilka möjligheterna är att med hjälp av tekniker för att aliasmatchning följa en person som är aktiv på flera sociala medier under olika namn.

- **Remissarbete Försvarsmaktens Handbok bearbetning och analys.** Tack vare den kunskapsuppbyggnad som SIA och tidigare VIA inneburit

kunde ett antal projektmedlemmar under 2013 bidra substantiellt till FOI:s remissyttrande över Försvarsmaktens Handbok bearbetning och analys. Under våren 2014 har yttrandet följts upp genom ett möte med representanter från UndsäkC där innehållet i remissyttrandet diskuterades.

- **EISIC**. 2013 ordnade FOI tillsammans med Uppsala Universitet och KTH konferensen European Intelligence and Security Informatics (EISIC 2013) i Uppsala. Under tre dagar presenterades inskickade forskarbidrag varvat med föredrag av inbjudna talare. Som en del av konferensen arrangerades också en så kallad Practitioners' day. Practitioners' day riktade sig till yrkesverksamma analytiker med intresse av att lära sig mer om olika kommersiella verktyg, få en inblick i ny forskning, höra om fallstudier och nätverka. Totalt lockade EISIC 2013 över 200 deltagare från hela världen, varav cirka 60 analytiker från olika svenska myndigheter deltog i Practitioners' day. EISIC planeras att 2016 återigen samarrangeras av FOI, Uppsala Universitet och KTH i Uppsala.
- **JISIC 2014.** JISIC står för Joint Intelligence Security and Informatics Conference, vilket som namnet antyder handlar om säkerhetsinformatik. Detta är ett mycket relevant forskningsområde för den forskning som bedrivs i SIA då det bland annat innefattar webbanalys och data mining för säkerhets- och underrättelsetillämpningar. Vid konferensen belönades FOI-bidraget "Time profiles for identifying users in online environments" med pris som bästa publikation på konferensen.
- **Övrig omvärldsbevakning.** Projektets medarbetare har även varit representerade vid ett antal konferenser. Ett urval av dessa är: Fusion 2014 (Salamanca), The 2nd International Conference on Future Internet of Things and Cloud inklusive The First International Workshop on Social Networks Analysis Management and Security (Barcelona), The Fifth Swedish Language Technology Conference (Uppsala), BIG DATA at SICS Software Week och SICS Big Data analytics minilab (Kista), European Chapter of the Association for Computational Linguistics (Göteborg), samt The Second European Network and Intelligence Conference (Blekinge).

5 Fortsatt arbete

Många av de verktyg, metoder och algoritmer som utvecklats inom ramen för SIA-projektet har i vår forskning och våra initiala användartester gett resultat som tyder på en stor potential för praktisk användning av verktyg för analys av data från öppna källor, inhämtad från Internet i allmänhet och sociala medier i synnerhet. För att kunna ge ett mervärde inom Försvarsmakten och dess framtida informationshanterings- och analyssystem krävs dock att dessa forskningsresultat tas tillvara och mer direkt anpassas till FM:s organisation och utmaningar.

Detta förväntas åstadkommas dels genom faktisk användning av de utvecklade verktygen och ett fördjupat kravanalysarbete, men också genom en ännu bättre dialog mellan FOI och FM inom detta område. Forskningen inom FoT-projekt som SIA ligger vanligtvis några år framåt i tiden, men på grund av den snabba teknik- och händelseutvecklingen inom detta område är det som det forskats på inom SIA-projektet av stor relevans här och nu: statsaktörer och andra aktörer använder sig av påverkans- och vilseledningsoperationer i sociala medier i skrivande stund. Detta gör det extra relevant att snabbt omsätta bedriven forskning till praktisk och direkt nytta.

SIA-projektet har en planerad uppföljare i projektet TIA: Teknik för informationsfusion och analys. I detta projekt förväntas fortsatt forskning och teknikutveckling inom webbanalysområdet. De prototyper som levererats i SIA kommer där vidareutvecklas och kompletteras med inhämtning från flera typer av källor och andra typer av data. Exempel på detta är att komplettera inhämtning från Twitter med RSS-flöden eller annan elektronisk nyhetsmedia och att kombinera textdata med bild- eller videodata. En annan förväntad utveckling är att de verktyg och metoder som tas fram i TIA i en ännu högre grad behöver hantera flödet av stora datamängder.

6 Publikationer

Detta kapitel listar de publikationer som producerats inom ramen för projektet. Först listas öppna publikationer gjorda vid FOI i form av FOI-rapporter, därefter listas ett urval av de publikationer som producerats under projektets gång:

6.1 FOI-rapporter

- Albinsson, P-A., Franke, U., Garcia Lozano, M., Johansson, F., Litsegård, P., Pelzer, B., Rosell, T., Westman, T., "Analys och detektion av vilseledning och påverkansoperationer i sociala medier", 2015
- Brynielsson, S., Nilsson, S., Rosell, M., "Återkoppling från sociala medier vid insatsledning", FOI-R-3756-SE, 2013
- Franke, U., Johansson, F., Mårtenson, C., "Datadriven underrättelseanalys", FOI-R-3680-SE, 2013
- Mårtenson, C., "Årsrapport Stödverktyg för informationsfusion och analys (SIA) 2013, FOI-R-3779-SE, 2013
- Mårtenson, C., "Årsrapport Stödverktyg för informationsfusion och analys (SIA) 2014, FOI-R-4001-SE, 2014

6.2 Externa publikationer

- Albinsson, P-A., "Visual Analytics of Deception in Social Media: Tools and Techniques", Proceedings of the NATO Workshop on Visual Analytics for Exploring, Analysing and Understanding Vast, Complex and Dynamics Data, 2015
- Biermann, J., Hörling, P., Snidaro, L., "Experiences and Challenges in Automated Support for Intelligence in Asymmetric Operations", Journal of Advances in Information Fusion, 2013
- Brynielsson, J., Johansson, F., Jonsson, C., Westling, A., "Emotion classification of social media posts for estimating people's reactions to communicated alert messages during crises", Security Informatics, 2014
- Brynielsson, J., Horndahl, A., Johansson, F. Kaati, L., Mårtenson, C., Svenson, P., "Harvesting and analysis of weak signals for detecting lone wolf terrorists", Security Informatics, 2013
- Brynielsson, J., Johansson, F., Westling, A., "Learning to Classify Emotional Content in Crisis-Related Tweets", Proceedings of the IEEE

International Conference on Intelligence and Security Informatics (ISI 2013)

- Cohen, K., Johansson, F., Kaati, L., Mork, J. C., “Detecting linguistic markers for radical violence in social media”, Terrorism and Political Violence 26(1) (2014) 246–256.
- Fensel, A., Rogger, M., Gustavi, T., Horndahl, A., Mårtenson, C., “Semantic Data Management: Sensor-based Port Security Use Case”, Proceedings of the 2013 European Intelligence and Security Informatics Conference (EISIC 2013)
- Franke, U., Rosell, M., “Prospects for Detecting Deception on Twitter”, The First International Workshop on Social Networks Analysis Management and Security, 2014
- García Lozano, M., “Trusting Open Source Information”, Proceedings of the 2013 European Intelligence and Security Informatics Conference (EISIC 2013)
- García Lozano, M., Franke, U., Rosell, M., Vlassov, V., “Towards Automatic Veracity Assessment of Open Source Information”, 4th IEEE International Congress on Big Data (BigData Congress 2015)
- Gustavi, T., Karasalo, M., Mårtenson, C., ”A tool for generating, structuring, and analyzing multiple hypotheses in intelligence work”, Proceedings of the 2013 European Intelligence and Security Informatics Conference (EISIC 2013)
- Johansson, F., Kaati, L., Shrestha, A., “Time Profiles for Identifying Users in Online Environments”, 2014 IEEE Joint Intelligence and Security Informatics Conference (JISIC 2014)
- Johansson, F., Kaati, L., Shrestha, A., “Timeprints for identifying social media users with multiple aliases”, Security Informatics, 2015.
- Johansson, R., Horndahl, A., Rosell, M. “A Data Association Framework for General Information Fusion”, IEEE 2015 International Conference on Multisensor Fusion and Integration for Intelligent Systems, 2015.
- Jändel, M., “Decision support for releasing anonymised data”, Computers & Security 46, 2014
- Jändel, M., Svenson, P., Johansson, R., “Fusing restricted information", 17th International Conference on Information Fusion (Fusion 2014)
- Karami, A., Johansson, R., “Utilization of multi attribute decision making techniques to integrate automatic and manual ranking of

options", Journal of Information Science and Engineering 30(2) (2014) 519–534.

- Teljstedt, C., Rosell, M., Johansson, F., "A semi-automatic approach for labeling large amounts of automated and non-automated social media user accounts", Second European Network Intelligence Conference (ENIC 2015)
- Trång, D., Johansson, F., Rosell, M., "Evaluating algorithms for detection of compromised social media user accounts", Second European Network Intelligence Conference (ENIC 2015)
- Westling, A., Brynielsson, J., Gustavi, T., "Mining the Web for sympathy: the Pussy riot case", 2014 IEEE Joint Intelligence and Security Informatics Conference (JISIC 2014)

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