Processer, værktøjer og teknikker til efterforskning af kriminelle netværk

Cand. Polyt., Rasmus Rosenqvist Petersen

Efterforskninger af kriminelle netværk udført af politi, efterretnings analytikere, og undersøgende journalister involverer en række komplekse processer og opgaver relateret til håndtering af viden. Efterforskere af kriminelle netværk indhenter, bearbejder, og analysere information relateret til et specifikt efterretningskrav, for at skabe efterretnings produkter der kan rapporteres til kunden der formulerede kravet. Efterforskere skal håndtere en stigende mængde informationer fra mange forskellige kilder, især internettet, og de kan alle sammen være vigtige for efterforskernes analyse- og beslutnings-proces. Men en overflod af informationer er langt fra den eneste eller den vigtigste udfordring i forbindelse med efterforskning af kriminelle netværk, på trods af den massive opmærksomhed ``de mange informationer'' bliver givet i forskningsverdenen og af medierne, m.fl. Udfordringer såsom efterretningskredsløbet (processen), den kontekst en efterforskning foregår i, menneskelige faktorer som f.eks. problem løsning og kreativitet, og politiske beslutninger og deraf følgende lovgivning, er alle udfordringer der kan betyde succes eller fiasko for en efterforskning.

Information, proces, og menneskelige faktorer er efterforsknings relaterede udfordringer som kan adresseres ved hjælp af software systemer. Baseret på disse tre udfordringer formulerede vi vores hypotese for værktøjsunderstøttelse, og analyserede specifikke problemer relateret til hver enkelt udfordring. Vores modsvar i forhold til disse problemer er en liste med forsknings krav, der kan styre vores udvikling af nye processer, værktøjer, og teknikker der ultimativt vil reducere virkningen af udfordringerne og understøtte hypotesen. Vi foreslår hypertekst som den kerneteknologi der kan bygge bro imellem de menneske- og værktøj relaterede krav vi har til vores forskning, for at tilbyde integreret understøttelse for begge, resulterende i øgede kapaciteter der vil skabe en synergi effekt i forbindelse med efterforskning af kriminelle netværk.

Vi skaber en krav-centreret proces model der involverer indhentning og bearbejdning, syntese og forståelse (tilsammen analyse), rapportering, og samarbejde. Det er en proces model der tilskynder og støtter en iterativ og inkremental evolution af det kriminelle netværk på tværs af alle fem efterforsknings processer. Førsteprioriteten for proces modellen er at adressere de problemer som lineære proces modeller introducerer i efterforskningsarbejdet, primært adskillelser i processen, der reducerer efterforskernes ansvarsfølelse for efterforskningen samt forringer oplysninger som de passere igennem proces adskillelserne (en adskillelse kan være mellem to afdelinger i en organisation, eller f.eks. mellem to efterretningstjenester). Vi har udviklet en liste med efterforsknings opgaver der indkapsler arbejdet inden for hver enkelt proces. Opgaverne er udvalgt baseret på deres potentielle bidrag til veludført efterforskning.

Grundlæggende koncepter for efterforskning af kriminelle netværk er blevet udviklet og testet ved hjælp af såkaldte proof-of-concept prototyper, hvilket har resulteret i generiske softwarekomponenter til værktøjs understøttelse af efterforskning. Vi har anvendt disse komponenter til at bygge CrimeFighter Investigator, iteration efter iteration, og derigennem omfavnet de begreber der er indlejret i komponenterne. Vi analyserer, designer og demonstrerer understøttelse af individuelle efterforskning opgaver for hver af de fem omtalte processer, og vi beskriver også anvendelse af CrimeFighter Investigator i scenarier, der

involverer flere processer og opgaver. Vi har brugt tre metoder til at evaluere CrimeFighter Investigator: sammenligning af opgave- og model-understøttelse, slutbruger interviews, og forskellige metrikker der kan måle effektiviteten af algoritme-baserede analyse teknikker på flere områder. Ved hjælp af diagrammer har vi opsummeret relationerne mellem efterforsknings opgaver og vores opsatte forsknings krav, vi fandt at de tre evalueringsmetoder ydede god dækning af disse krav. Når vi opsummerer vores evaluering af forsknings kravene finder vi at mange er godt understøttet, imens få er nogenlunde eller svagt understøttet. Helt generelt viser vores evaluering at vi har fokuseret på de rette udfordringer, og at den gensidige afhængighed imellem forskningskravene gjorde det klart, at havde vi valgt et mere snævert fokus, f.eks. udeladt en af udfordringerne, ville det have resulteret i dårligere understøttelse af de resterende krav.

Vi kan konkludere at alle indikatorer peger imod understøttelse af den hypotese vi har stillet. I stedet for at fokusere på specifikke algoritme-baserede teknikker til netværks analyse har vi arbejdet hen imod understøttelse af slutbrugerens (efterforskerens) interaktion med og kontrol af sådanne analyse teknikker, med det formål at opnå bedre efterforskningsresultater. Vi betragter vores resultater som retningslinjer i forhold til forskning indenfor software værktøjer der understøtter efterforskning af kriminelle netværk.