10 Skolskjutare och spår i den digitala sfären

Fredrik Johansson och Lisa Kaati

I denna artikel belyser författarna hur man genom digitala spår kan upptäcka och förhindra potentiella skolskjutare. Det har nämligen visat sig att det vid skolskjutningar i förhand har funnits flera spår på sociala medier och webbsidor. Tekniker för att hitta spåren är under utveckling på FOI. Författarna belyser också vilka framsteg som gjorts vid analys av sociala medier för att ge polis och andra aktörer en bättre lägesbild.

Bakgrund

Problematiken med så kallade skolskjutningar har under de senaste åren aktualiserats gång på gång genom incidenter och attacker runt om i världen. Även om Sverige lyckligtvis inte har haft så många fall med skolskjutare så har våra grannländer (och då framför allt Finland) på senare år haft ett flertal incidenter. Två tragiska exempel är de välkända skolskjutningarna i Jokelaskolan (2007) och Kauhajoki (2008). En annan mycket känd skolskjutning som fått stor massmedial uppmärksamhet runt om i världen är den så kallade Columbine-massakern som utfördes 1999 på Columbine High School i USA. Dessa är dock bara ett litet urval eftersom hundratals skolskjutningar har ägt rum i världen

under det senaste årtiondet. För svensk del inträffade den senaste skolskjutningen med dödlig utgång 1961 när en 17-åring steg in i Kungälvs läroverks gymnastiksal, drog upp en pistol och började skjuta. Följden av attacken blev att sex elever skadades och en avled. Även om Sverige varit relativt förskonat från skolskjutningar har det även här förekommit ett flertal fall där elever har hotat att utföra våldsdåd mot skolor och i ett fall 2004 stoppades en planerad massaker mot Slottsstadens skola i Malmö.

Flera olika definitioner av vad begreppet skolskjutare innefattar förekommer i litteraturen, men en ungefärlig beskrivning som stämmer in på de flesta förekommande definitioner är att det ska röra sig om en elev eller en före detta elev som utför en planerad attack gentemot skolkamrater, lärare eller andra personer som uppehåller sig på skolan eller campus. Denna beskrivning utesluter alltså attacker där någon helt plötsligt får ett vansinnesutbrott och skadar eller dödar sina kamrater, samt attacker som utförs av vuxna individer utan koppling till skolan. Själva termen skolskjutning antyder att attacken skulle utföras med hjälp av skjutvapen, men det finns också ett flertal exempel där gärningspersonen använt sig av rörbomber, Molotov-cocktails eller stickvapen som också vanligtvis faller under etiketten skolskjutning.

Svensk polis utbildas numera för att kunna hantera skolskjutningar eftersom det anses vara troligt att antalet incidenter kan öka i framtiden. Myndigheten för samhällsskydd och beredskap (MSB) uppskattar i 2012 års nationella riskbedömning respektive bedömning av krisberedskapsförmåga att sannolikheten för att en skolskjutning ska inträffa i Sverige ligger på runt 10 % på årsbasis. I rapporten målas ett skrämmande men realistiskt scenario upp där en elev i en liten svensk kommun skjuter ihjäl en lärare och sex elever för att sedan ta sitt eget liv. I samband med händelsen blir det ett stort tryck från allmänheten och media, vilket bland annat får till följd att ett omfattande utbyte av såväl korrekt information som rykten äger rum i sociala medier.

I denna artikel beskriver författarna hur just analys av sociala medier kan komma till användning dels för att i ett *proaktivt* syfte kartlägga och identifiera potentiellt intressanta grupper och individer innan en skolskjutning faktiskt äger rum (genom att samla in och fusionera digitala spår som tyder på att någon planerar en skolskjutning), dels användas *reaktivt* för att ge bättre lägesförståelse för polis och andra beslutsfattare när katastrofen väl har inträffat. För att förebygga och hantera problemet med skolskjutningar krävs tvärvetenskaplig forskning och samarbete mellan skola, polis och socialtjänst. Författarna belyser dock främst problemet från ett datavetenskapligt perspektiv. Det är viktigt att förstå att teknikutveckling i sig inte ensamt kan lösa problemet, eftersom inte minst etiska och legala aspekter måste vägas in. Ytterligare en viktig aspekt är att tekniska verktyg i bästa fall kan stödja polisen i sitt arbete, snarare än att ersätta deras analytiska förmåga.

Digitala spår i sociala medier

I merparten av alla skolskjutningar sedan 2005 har förövarna enligt existerande forskning lämnat spår på sociala medier och andra typer av webbsidor. När en skolskjutning har inträffat har det därför från olika håll, inte minst från massmedia, antytts att polisen borde ha kunnat förutse vad som var på väg att hända och agerat mer proaktivt. Polisen i Finland sägs lägga stora resurser på att övervaka diskussioner på olika forum på internet för att kontrollera eventuella hotbilder, speciellt när skolskjutningar i andra länder har inträffat eftersom man då oroar sig för så kallade *copycats*, det vill säga att någon ska ta efter och försöka imitera de gärningar som har utförts.

Att manuellt övervaka alla tänkbara sociala medier med syftet att hitta potentiella hot som tyder på en ökad risk för en skolskjutning är inte möjligt eftersom det kräver orimliga resurser. Detta faktum visar på ett behov av metoder och automatiska eller semi-automatiska verktyg för att kunna rikta in övervakningen på de forum och så kallade *communities* som är av störst intresse för att sedan kunna identifiera och värdera möjliga hot mot skolor eller andra digitala spår med så lite inverkan på den personliga integriteten som möjligt. I den här artikeln fokuserar författarna enbart på vilka digitala spår kopplat till skolskjutningar som går att hitta i sociala medier. Det är noterbart att andra typer av indikatorer så som uttalade hot mot lärare eller elever också givetvis bör vägas in, något som dock ligger utanför fokus för denna artikel.

Vad finns det då för digitala spår som skulle kunna förvarna om en möjlig attack? Om man börjar med de mest uppenbara eller explicita spåren så är det vanligare än man skulle kunna tro att gärningspersonen innan en attack har lämnat uttryckliga skriftliga hot i sociala medier. Ofta lämnas dessa i publika forum där de är åtkomliga för alla, inklusive polisen. I vissa fall är dock meddelandena inte åtkomliga publikt utan riktas till en sluten grupp mottagare. I de senare fallen finns det inte mycket mer att göra än att hoppas på att någon lämnar ett tips till polisen. De riktade hoten kan givetvis vara mer eller mindre explicita. I flera tidigare fall har gärningspersoner annonserat sina planer på YouTube i en film innan en attack, postat budskap av typen ”ready for action” och ”you will die next” eller laddat upp (politiska) manifest på olika forum. En annan form av digitalt spår som varit vanligt förekommande innan skolskjutningar är att gärningspersonen har postat bilder eller videor där denne poserar med automatvapen, liknande de bilder som efter Anders Behring Breiviks terrorattentat i Norge publicerades i många tidningar. Vanligt förekommande är också bilder där man poserar i utstyrsel och utrustning liknande den som bars av Eric Harris och Dylan Klebold vid Columbine-massakern. Att på detta sätt posera med vapen behöver givetvis inte vara olagligt, men kan fungera som en form av indikator på att något kanske inte står helt rätt till. Just referenser till tidigare skolskjutningar i allmänhet och Columbine-massakern i synnerhet är för övrigt väldigt vanligt. Exempel på detta är de

användarnamn som olika gärningspersoner har använt på sociala medier. För att nämna några så har användarnamnen ”*Todesengel*” (dödsängel), ”*verlassen4_20*” (anspelning på datumet för Columbine-massakern och Hitlers födelsedag) och ”*naturalselector89*” använts på YouTube och olika diskussionsforum av personer som senare utfört skolskjutningar. Utöver detta så finns det även ett flertal webbsidor eller forum där människor som blivit inspirerade av tidigare skolskjutningar ofta diskuterar tidigare händelser i positiva ordalag, inte helt olikt de forum som används för att sprida högerextrema eller jihadistiska budskap som manar till attacker mot samhället eller upplevda antagonister. Enligt befintlig forskning har många skolskjutare varit aktiva i denna typ av ”skolskjutar-communities” innan de har utfört sina attacker.

Det urval av digitala spår som har nämnts ovan kan användas för att på ett tidigt stadium upptäcka potentiella skolskjutare. Allt från explicita hot, bilder och videor där man poserar med vapen i hand, valda användarnamn och inlägg i kontroversiella webbforum kan användas som indikatorer på att allt inte står helt rätt till. Dessa indikatorer eller svaga signaler är ofta inte tillräckligt starka tagna var och en för sig, men kan genom att kombineras användas som tecken på att polis eller sociala myndigheter bör agera. På FOI bedrivs forskning om identifikation och fusion av svaga signaler på internet. Detta har tänkbara tillämpningsområden som exempelvis att identifiera potentiella skolskjutare eller ensamagerande terrorister men kan också användas för helt andra syften så som detektion av naturkatastrofer eller nya konflikthärdar.

Tekniker för att identifiera potentiella skolskjutare

För att kunna upptäcka potentiella skolskjutare behövs verktygsstöd för att kunna göra relevanta sökningar i sociala medier i syfte att identifiera forum, grupper eller användare som på ett eller annat sätt relaterar till ämnet skolskjutningar. Detta steg är ett exempel på så kallad *targeting*, där man försöker rikta in sina tillgängliga resurser på vad som bör övervakas. För att vara användbart bör sökningar kunna utföras på ett flertal sociala medier som exempelvis diskussionsforum, Twitter och YouTube. Det bör också finnas möjlighet att söka på en rad olika begrepp som relaterar till skolskjutningar och få resultatet presenterat på olika sätt, exempelvis som en lista på forum eller användarnamn, eller i form av sociala nätverk där kopplingar mellan olika användare beaktas. Dessa kopplingar kan utgöras av relationer som exempelvis vem som är vän med vem på Facebook, vem som följer vem på Twitter, eller vem som kommenterat någons inlägg eller uppladdade filmer på ett diskussionsforum eller YouTube. Den här formen av nyckelordsbaserad sökning är ett trubbigt verktyg men ger ändå möjlighet att på stor skala snabbt söka igenom stora mängder data och filtrera ut den information som är av intresse, något som är omöjligt med

manuella medel. Det finns idag flera olika företag som har specialiserat sig på att möjliggöra sökningar på specifika nyckelord i olika sociala medier. I forskning gjord av ryska och finska forskare har man använt sig av liknande tekniker för att skapa sociala nätverk över användare på LiveJournal som har intressen som relaterar till exempelvis skolskjutningar, massmord eller massmördare. I denna kartläggning identifierade man ett stort antal communities och användare som innehöll kända skolskjutare och deras ”vän-kopplingar”.

Sannolikt är flertalet av de användare som identifieras med en grov nyckelordssökning personer som har just ett intresse för skolskjutningar, snarare än planer på att själva genomföra en sådan handling. Med andra ord är en nyckelordssökning bara användbart för att filtrera ut information som kan vara av ett potentiellt intresse och som bör analyseras i mer detalj. När ett nätverk med potentiellt intressanta personer har extraherats kan det analyseras genom att använda sig av så kallad *SNA* (*social network analysis*). Inom detta område har FOI stor kompetens, inte minst vad gäller analys av icke-fullständiga eller osäkra sociala nätverk, vilket ofta är en fundamental egenskap hos de nätverk som tas fram på det sätt som beskrivits ovan. Analys av sociala nätverk kan användas för att identifiera inflytelserika personer, hitta delgrupperingar eller olika centrala aktörer. Den här typen av analys kan användas för att filtrera ut det mest intressanta aktörerna som bör analyseras vidare.

Nästa steg i analysen är att återgå till de indikatorer som kan tyda på att någon har intention att begå en skolskjutning. Genom att applicera sofistikerade text-, bild- och videoanalystekniker kan man automatiskt försöka identifiera denna typ av indikatorer. Inom textanalys finns det exempelvis forskning gjord på FOI där man kan träna upp algoritmer för att identifiera känslostämningar i text. På samma sätt skulle man kunna träna algoritmerna med exempel på hotfulla respektive icke-hotfulla textmeddelanden i syfte att lära systemet att automatiskt kunna känna igen hot i text. Ett alternativ till detta är att skapa lingvistiska regler för vad som karakteriserar ett hot, något som dock vanligtvis kräver djupare språklig expertkunskap. För att kunna känna igen bilder eller videor där någon poserar med vapen behövs mer forskning. Inom så kallad *CBIR* (*content-based information retrieval*) arbetar man med att ta fram algoritmer för att känna igen bilder baserade på innehåll snarare än textuell beskrivning. Denna typ av funktionalitet börjar nu återfinnas i en rad kommersiella produkter, vilket tyder på en ökad mognadsgrad som inom några år borde göra det möjligt att med relativt god precision kunna identifiera bilder eller videor där någon poserar med vapen.

Genom att använda sig av diverse olika tekniker för att kunna identifiera indikatorer som tyder på att någon har intention att begå en skolskjutning är nästa problem att indikatorerna var och en för sig inte alls behöver betyda att personen faktiskt tänker begå en skolskjutning. Det är fullt möjligt att någon har ett iögonfallande användarnamn som *natural_selector* och skriver inlägg som

handlar om skolskjutningar utan att denne har någon tanke på att utföra en skolskjutning i praktiken. Något förenklat kan man säga att indikatorerna var och en för sig kan peka på ett potentiellt hot med varierande styrka och att ju fler indikatorer som är uppfyllda, desto mer sannolikt är det att användaren planerar något, eller i varje fall att det blir desto mer relevant att göra ytterligare undersökningar kring användaren. Genom FOI:s forskning inom *informationsfusion* så finns kompetens att kunna ställa upp sannolikhetsteoretiska hotmodeller för när något ska klassas som ett tillräckligt stort hot för att en mänsklig analytiker ska studera denne individ och dess inlägg närmare.

Ett problem som knyter an till det ovanstående är att individer inte sällan använder olika alias på olika sociala medier. Eftersom det är en persons sammantagna inlägg som är av intresse vid bedömning om det föreligger någon hotbild så är det viktigt att kunna identifiera om flera olika alias tillhör en och samma individ. Detta är ett relevant forskningsproblem där en kombination av ett flertal olika tekniker såsom tidsprofilering, författarigenkänning, *SNA (social network analysis)* och namnmatchning verkar ge goda resultat enligt pågående forskning. När en användare väl har identifierats som intressant återstår problemet att knyta dennes alias till en fysisk person. Detta kan exempelvis göras genom att polismyndigheter efter en juridisk prövning begär ut information från den som tillhandahåller tjänsten för det sociala mediet i fråga, samt internetleverantörer. Det bör betonas att även om mycket av den teknik som har diskuterats ovan av nödvändighet måste automatiseras till en stor del för att minska belastningen på de mänskliga analytikerna så är det alltid den mänsklige analytikern som måste göra en slutgiltig bedömning om insamlad data är tillräckligt intressant att gå vidare med. På samma sätt föreligger vid all typ av automatiserade eller semi-automatiserade system en risk för falsklarm, där personer som egentligen inte har tänkt utföra någon skolskjutning utan ”skämtar” eller av någon annan anledning följer denna typ av diskussioner och skriver tvivelaktiga inlägg pekas ut som misstänkta eller potentiella skolskjutare. I dessa fall skulle dock ett samtal från polisen eller socialtjänsten troligtvis ändå inte skada som en väckarklocka innan något värre händer. Vidare så är det återigen alltid en mänsklig analytiker som ska ha sista ordet om vad som ska göras.

Användning av analys av sociala medier för att identifiera skolskjutningar och ge beslutsfattare en bättre lägesbild

Om ett scenario som det som har målats upp av MSB i dess nyligen utgivna rapport skulle inträffa i verkligheten i Sverige är det viktigt att polis och andra berörda myndigheter på ett så tidigt stadium som möjligt kan få en lägesbild över vad som händer på skolan. I denna typ av krissituationer används sociala medier i en allt ökande utsträckning, i takt med att användandet av sociala medier i

mobiler och surfplattor sprider sig. Sociala medier kan därför vara en viktig källa till information i sådana situationer, vilket exempelvis har visat sig vid terroristattentaten i Norge, kärnkraftsolyckan i Japan och diverse olika naturkatastrofer. Det pågår därför en hel del forskning som involverar framtagande av prototyper för att söka i och analysera data från sociala medier i real-tid, vilket möjliggör att beslutsfattare kan få en bättre lägesbild. Detta är bland annat ett viktigt forskningsproblem i EU-projektet Alert4All där FOI spelar en viktig roll. Ett problem vid analys av sociala medier är de stora mängder icke-relevant och felaktig information som cirkulerar och behöver kunna filtreras ut. Att kunna bedöma källors tillförlitlighet samt sakriktigheten i information är långtifrån ett löst forskningsproblem, men allt talar för att användningen av analys av sociala medier i kriser kommer att öka i framtiden.

Avslutning

Skolskjutningar är ett samhällsproblem som svenska myndigheter måste förbereda sig inför. Under 2013 har Rikspolisstyrelsen påbörjat en landsomfattande utbildning för svensk polis för att kunna hantera skolskjutningar taktiskt. För att kunna stoppa skolskjutningar innan de äger rum bör man även överväga att utveckla teknik för att ha möjligheten att upptäcka indikatorer för att denna typ av händelse håller på att inträffa. Det är inte bara potentiella skolskolskjutare som lämnar digitala spår på internet. Det finns många andra incidenter som exempelvis terrorbrott eller andra former av attentat riktade mot personer där man skulle kunna använda sig av liknande tekniker för att upptäcka digitala spår som tyder på att ett brott planeras.

Det finns dock en hel del problem som man bör adressera innan man kan börja analysera sociala medier för att kartlägga och identifiera individer som visar en ökad risk för att begå ett brott av något slag. Utöver existerande tekniska begränsningar finns även etiska och lagliga överväganden som måste beaktas. Exempelvis skulle det utifrån ett tekniskt eller rent operativt perspektiv kunna vara givande att sätta upp en så kallad ”honungsfälla” där man själv skapar ett alias eller ett forum där man utger sig för att ha ett osunt intresse av skolskjutningar och sprida olika typer av inlägg för att se vilka användare eller personer som väljer att följa ens inlägg. Detta beteende skulle dock vara högst moraliskt och juridiskt tvivelaktigt då det skulle kunna riskera att göra personer mer intresserade av skolskjutningar eller indirekt uppmana till brott. Framtida forskning behöver därför fokusera på att komplettera de tekniska möjligheterna med etiska och legala aspekter, för att på så sätt fungera som beslutsunderlag för huruvida denna typ av preventiv övervakning ska göras möjlig eller inte. Överlag saknas det med några få undantag publicerade forskningsresultat om tekniska aspekter på hur man skulle kunna förhindra eller i varje fall kartlägga potentiella skolskjutare. Detta kan jämföras med de hyllmeter som har skrivits om skolskjutningar från olika psykologiska och sociologiska aspekter. Den

existerande forskningen är av yttersta vikt men bör också kompletteras med forskning på hur man kan gå tillväga för att på ett tidigt stadium faktiskt upptäcka och förhindra uppkomsten av skolskjutningar genom att analysera vad som publiceras inom den digitala sfären. Genom vidare forskning skulle man kunna få en bild över hur effektiva den här typen av tekniker kan vara. Detta skulle göra det möjligt att ställa den förväntade nyttan gentemot negativa aspekter så som risk för att människor skulle känna sig övervakade eller risk för falsklarm.

Vidare läsning

- Brynielsson, J., Horndahl, A., Johansson, F., Kaati, L., Mårtenson, C. and Svenson, P. ”Analysis of Weak Signals for Detecting Lone Wolf Terrorists”, Proceedings of the 2012 European Intelligence and Security Informatics Conference, 2012.
- Dahlin, J., Johansson, F., Kaati, L., Mårtenson, C. and Svenson, P. ”Combining Entity Matching Techniques for Detecting Extremist Behavior on Discussion Boards”, Proceedings of 2012 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining, 2012.
- Johansson, F., Brynielsson, J. and Narganes Quijano, M. ”Estimating Citizen Alertness in Crises using Social Media Monitoring and Analysis”, Proceedings of the 2012 European Intelligence and Security Informatics Conference, 2012.