9 Lägesförståelse i informationssamhället

Ulrik Franke, Joel Brynielsson, Tommy Gustafsson, Jonas Hallberg och Pontus Svenson

Informationsteknik blir en allt viktigare del av samhället. Vi arbetar, umgås, utbildar oss och interagerar med myndigheter via nätet i en omfattning som var otänkbar för bara tio år sedan. Samtidigt förekommer brottslighet, terrorism-relaterade aktiviteter och krigföring på internet – alltifrån enklare intrångsförsök och överbelastningsattacker genomförda av enskilda amatörer till näthat eller mer sofistikerade attacker som kriminella organisationer eller främmande stater bedöms ligga bakom. Det moderna informationssamhällets vinster leder alltså också till ökad sårbarhet. En del av dessa sårbarheter tas upp i artikel 8, som diskuterar IT-angrepp på kritisk infrastruktur. Andra aspekter tas upp i artikel 21, som handlar om informationssamhällets krav på myndigheters kriskommunikation och interaktion med medborgarna. I den här artikeln diskuterar vi möjligheter och problem med att skapa lägesförståelse utifrån information på internet.

Lägesförståelse – vad och varför?

Lägesförståelse är ett mångfacetterat begrepp som kan studeras ur flera perspektiv. Den tekniska aspekten av lägesförståelse handlar om att sammanställa, bearbeta, kvalitetssäkra, jämföra och fusionera information. Detta är dock inte så mycket värt utan den kognitiva aspekten: att förstå och kunna dra slutsatser ur den tekniska lägesinformationen. Därför vill man helst mäta hur människor uppnår lägesförståelse samt lyckas behålla och vidareutveckla den över tiden. De klassiska frågeställningarna, formulerade av Mica Endsley på 1990-talet, rör beslutsfattarens förståelse för (i) vad som händer, (ii) varför det händer och (iii) vad som kommer att hända. Alla tekniska hjälpmedel för lägesförståelse syftar i grunden bara till att hjälpa beslutsfattaren besvara dessa frågor.

Intrångsförsök och överbelastningsattacker (”denial of service”) pågår hela tiden på internet. *Vad* som händer går i viss mån att överblicka. CERT-SE[7] vid Myndigheten för samhällsskydd och beredskap presenterar exempelvis en lägeskarta över infekterade datorer i Sverige på sin hemsida (se inledande figur). Men *varför* händer det? Lägesförståelse för internet handlar också om att tyda tecknen och skilja allvarliga kriser från pojkstreck och enklare cybervandalism. Ett exempel är IT-säkerhetsföretaget Symantecs avslöjande år 2012 av hur IT-brottslingar använder sig av överbelastningsattacker mot banker som avledande manövrar. När IT-driftpersonalen (ofta nattskiftet) är fullt upptagen med att hålla hemsidan uppe genomför man allvarligare intrång i andra system, som möjliggör stölder av miljoner dollar i kreditkortsbedrägerier. Detta illustrerar utmaningen i att gå från *vad* till *varför* och att sedan prioritera rätt. När är angreppen som beskrivs i artikel 8 bara en angelägenhet för det omedelbart drabbade företaget eller branschen och när är det en pusselbit i ett större sammanhang?

I det gamla totalförsvaret talade man om skymningsläget: en gråzon mellan krig och fred präglad av skenbart oförklarliga strömavbrott, sjukdomsfall och olyckor till följd av fientligt sabotage. I informationssamhället är det självklart att sådana sabotage i ökad omfattning kommer att äga rum via internet. Lika självklart är det att vi måste kunna skilja angreppen från varandra: vi kan inte förklara att riket befinner sig i krig eller krigsfara och kalla in riksdagens krigsdelegation varje gång som någon initierar en överbelastningsattack mot Regeringskansliets hemsida. Lägesförståelse på internet blir i förlängningen en förutsättning för fungerande säkerhetspolitik.

[7] CERT-SE (Computer Emergency Response Team) är Sveriges nationella CSIRT (Computer Security Incident Response Team) med uppgift att stödja samhället i arbetet med att hantera och förebygga IT-incidenter. Verksamheten bedrivs vid Myndigheten för samhällsskydd och beredskap (MSB).

I artikel 8 beskrivs hur industriella styrsystem har utvecklats från fristående till internetuppkopplade för att öka effektiviteten i styrningen av allt från enskilda pumpar till hela infrastrukturer – och vilka risker det medför. Vore det då inte klokt att satsa på att koppla bort all kritisk IT-utrustning från internet? Det är vad vi ser i Iran, där regimen håller på att skapa ett nationellt fristående internet som går att övervaka och styra. Det riskerar att bli dyrt. Att skärma av ett helt land från omvärlden får ödesdigra konsekvenser för handel, innovation och tillväxt. Teknisk isolering och lagar som begränsar utbytet och handeln med omvärlden kan omintetgöra fördelarna med informationssamhället. En bättre strategi är alltså att acceptera uppkopplingarna och korsberoendena i det moderna samhället – men att se till att ha en adekvat lägesförståelse för vad som sker.

IT-sensorer och experiment

För att skapa lägesinformation som kan bidra till ökad lägesförståelse på internet krävs flera olika tekniker. Relevanta ”IT-sensorer” behöver samla in information om överbelastningsattacker och intrångsförsök. På internet finns det massor av hot från brottslingar, reaktioner från offer, skryt från förövare, information om sårbarheter och uppmaningar till angrepp som behöver skannas av. Framförallt behöver man kunna sammanställa och analysera all den information som finns tillgänglig. Informationsfusion är det forskningsområde som handlar om hur man kan väga samman data från heterogena källor för att förstå vad som sker.

Ökad lägesförståelse kräver experiment för att avgöra både vilken lägesinformation som är möjlig att ta fram och hur den ska användas för att skapa lägesförståelse hos beslutsfattare. Delvis för detta ändamål utvecklar och underhåller FOI CRATE (Cyber Range And Training Environment), en avancerad laboratorieresurs som används för att skapa datornätverk för experiment, tävlingar och övningar i IT-säkerhet. I CRATE går det att konfigurera tusentals virtuella maskiner i en kontrollerad miljö – ett slags simulerat internet, komplett med trafik som påminner om verkligt användarbeteende.

I CRATE-miljön planeras just nu ett antal experiment med inriktning mot lägesförståelse. Tidigare forskning har ofta fokuserat på hur systemadministratörer ska titta på datorernas trafik- och paketloggar för att skapa sig en teknisk lägesförståelse. Det är en viktig del, men den behöver kompletteras med förståelse på en högre nivå. Ett planerat experiment handlar om det som brukar kallas för *information overload*. Genom att utsätta ett blått (försvarande) lag som angrips för en blandning av relevant och irrelevant information går det att utvärdera hur beslutsfattarna reagerar och skapar sin lägesförståelse. I förlängningen möjliggör det också datorverktyg för att bringa reda i kaoset. Ett annat experiment handlar om *insider*-hot. En medlem av det blåa laget får en hemlig uppgift: att agera angripare från insidan. Olika detektionssystem kan då

utprovas och testas för att se om de kan fånga sådana hot. I ett tredje experiment deltar fyra olika lag, varav ett slumpmässigt i varje omgång väljs ut att vara angripare. Uppgiften för den som angrips blir att identifiera vem det är som angriper. Just detta – attributionsproblemet – har orsakat mycket huvudbry, inte minst inom juridiken.

I alla experimenten finns det många utmaningar: hur ska information om exempelvis intrångsförsök kombineras med annan information (från bloggar eller Twitter) för att hjälpa oss att bedöma hur farlig en viss aktivitet är? Hur kan informationen sammanställas med bibehållet integritetsskydd? Vilka aktiviteter går det överhuvudtaget att hitta spår av? Att systematiskt studera dessa frågeställningar via experiment är enda sättet att få tillförlitliga svar.

Andra frågor är svårare att studera laborativt: Vilken information är viktig för aktörer som Myndigheten för Samhällsskydd och beredskap (MSB), Post- och telestyrelsen och polisen att ha för att skapa lägesförståelse för internet? Hur kan man använda internet för att skapa bättre förståelse för händelser i den fysiska världen, till exempel vid en pandemi? Hur kan man använda internet för att kommunicera med allmänheten i händelse av allvarlig kris? På FOI utvecklas teknik för att just kunna ta tillvara på och dra slutsatser från sociala medier med avseende på allmänhetens reaktioner i samband med kris. Genom att analysera den inhämtade informationen erhålls värdefull kunskap avseende hur väl ett utskickat krismeddelande har, eller inte har, uppfattats av den tänkta målgruppen. Arbetet omfattar både teknisk utveckling av maskininlärning för IT-sensorer och kognitiva aspekter som hur man bäst ska visualisera information för beslutsfattare.

Sensorer och visualisering är dock bara första steget. Lägesförståelse måste också omsättas i handlingsförmåga, vilket kan kräva nya och anpassade ledningsprocesser där den nya informationen kommer till nytta. Det kan exempelvis krävas att man har tillgång till uppdaterade listor över vad som är skyddsvärt på internet. Banker och industriella styrsystem är kanske uppenbara skyddsvärda objekt, men de IT-system som används för att styra logistiken hos stora matvarukedjor kan vara nog så viktiga att skydda. Infrastrukturen för kriskommunikation med allmänheten är kanske ytterligare ett exempel (se artikel 21), liksom nyckelbefattningshavare i samhället.

Svårigheter och begränsningar

Tieto-haveriet i november 2011, när fel hos en enda leverantör ledde till att mängder av annars orelaterade verksamheter som Apoteket, Bilprovningen och Stockholms stad fick problem, visar att det inte alltid är självklart vilka konsekvenser som störningar får eller vad som bör skyddas. Idag säljs IT ofta som en tjänst med tillgänglighetsavtal (Service Level Agreements, SLA). Olika verksamheter har olika krav: Där IT-tjänster styr fysiska industriprocesser med

stora logistikkedjor, exempelvis stålverk, vill man ha så få avbrott som möjligt även om de blir längre. Där IT-tjänster bara hanterar information, exempelvis kortbetalningar i detaljhandeln, är det bättre med många korta avbrott. Lägesförståelse måste innefatta även förståelsen för vad som egentligen står på spel i en värld av komplexa korsberoenden.

En annan komplicerande faktor är att enskilda aktörer ofta saknar incitament att sammanställa information för ökad lägesförståelse. Tvärtom kan det vara förknippat med kursras på börsen att offentliggöra intrång i IT-system eller att systemen ligger nere. Den här svårigheten är en del av ett större problemkomplex: Hur vet man att man baserar sin lägesförståelse på rättvisande uppgifter? IT-sensorerna kanske bara täcker de företag som släpper information, de drabbade som twittrar, de brottslingar som skryter, de cyberspioner som klantar sig, de angripare som använder gamla kända sårbarheter och de hot som man har tänkt på i förväg. Kan man kompensera för dessa skeva urval och ändå skapa sig en korrekt lägesuppfattning? Lägg därtill risken för avsiktlig vilseledning på internet. Vi vet att det finns gott om aktörer som avsiktligt sprider falsk information och att det finns en uppsjö av metoder för att lyckas.

Trots svårigheterna så är frågan om lägesförståelse viktig om vi vill fortsätta att njuta av informationssamhällets fördelar utan att utsätta oss för större risker än nödvändigt. Vare sig teknisk eller juridisk avskärmning från omvärlden är bra sätt att hantera informationssamhällets hot. En bättre strategi är att göra dynamiska riskbedömningar av hoten och medvetna avvägningar mellan kostnad och nytta (se även artikel 2-5). Det är i sin tur bara möjligt om vi hela tiden gör vårt bästa för att hålla reda på vad som händer, varför det händer och vad som kommer att hända i framtiden.

Vidare läsning

- Brynielsson, J., Johansson, F. and Lindquist, S. Using video prototyping as a means to involving crisis communication personnel in the design process: Innovating crisis management by creating a social media awareness tool. Proceedings of the 15th International Conference on Human-Computer Interaction, Las Vegas, Nevada, juli 2013. Yamamoto, S. (Ed.): HIMI/HCII 2013, Part III, LNCS 8018, pp. 559–568, Springer-Verlag Berlin Heidelberg 2013.
- Franke, U. Information operations on the internet, FOI-R--3658--SE, 2013.
- Sommestad, T. and Hallberg, J. “Cyber security exercises and competitions as a platform for cyber security experiments,” Proceedings of NordSec, 2012.