19 Logistiksäkerhet – en grund för vårt välstånd

Sören Jägerhök, Pontus Svenson, Maria Andersson, Christian Carling, Anneli Ehlerding, Anders Elfving, Micael Granström och Anna Pettersson

Den exempellöst snabba välståndsökningen i det moderna samhället vilar till stor del på förmågan att snabbt, effektivt och säkert kunna transportera varor och människor. Allt fler människor pendlar och måste kunna anlända säkert och tillförlitligt. Såväl samhällets mat- och medicinförsörjning som industrier och övrigt näringsliv bygger sin existens på ”just in time”-leveranser (inget tillverkas innan kunden lagt sin beställning för att hålla nere lagerkostnader och ledtider). Störningar och avbrott i transportkedjorna kan därför snabbt skada såväl den enskilda människan som näringsliv och andra viktiga samhällsfunktioner. Kopplat till transportsektorns enorma volym och betydelse finns några speciella hot mot samhällets säkerhet.

1. Den effektiva transportapparaten utnyttjas samhällsskadligt för smuggling av alltifrån illegala ämnen såsom farliga sprängmedel, narkotika och kemikalier till piratkopierade varor, stöldgods och traffickingoffer.

2. Koncentrationen av människor och värdefulla varor i transportsystemen attraherar kriminella organisationer och terrorister.
3. Olyckor, naturkatastrofer, pandemier med mera kan påverka logistikkedjan på ett sätt som ger indirekta skador långt värre än de direkta.

Hoten kan således delas in i hot mot själva logistikkedjan, till exempel stölder, samt hot mot samhället i vidare mening, till exempel smuggling av illegala ämnen. Smuggling och stöld/bedrägeri utgör några av de allvarligaste hoten inom varutransportkedjan i Sverige. Årligen stjäls till exempel stora mängder gods från lastbilar, inte sällan då lastbilarna står parkerade på rastplatser. Stölderna är ofta organiserade av kriminella ligor. För att säkerställa transportfunktionen i det moderna samhället behövs både skydd av själva transportkedjorna (transportgodset och transportinfrastrukturen) och skydd mot smuggling och annat skadligt utnyttjande av transportkedjorna. Ett sätt att skydda samhället är tidig upptäckt och varning vid försök till illegal införsel eller utförsel av varor, till exempel stöldgods. Vad gäller terrordåd inom transportsektorn har Sverige varit förskonat. I anslutning till Behring-Breiviks attentat i Norge 2011 höjdes ändå säkerhetsnivån för delar av transportapparaten, till exempel i Göteborgs hamn. Däremot har den svenska beredskapen mot besvärliga väderförhållanden inom transportsektorn prövats vid många tillfällen. Störningar i gods- och persontrafiken på järnväg har under flera vintrar kostat många aktörer mycket pengar. Säkerhetsresurserna behöver sättas in där de gör störst nytta och där de möter de viktigaste hoten.

Artikeln beskriver inledningsvis hur man, för att avgöra vilka dessa hot är, kan använda riskanalyser. Därefter beskriver författarna olika metoder för att upptäcka hoten och vidare för att hantera/åtgärda dem. Artikeln avslutas med några reflektioner om hur svensk logistiksäkerhet kan förbättras.

Att analysera hot och risker

En förutsättning för att på ett välavvägt sätt kunna bemöta hot mot samhällets säkerhet är givetvis en relevant kännedom om vilka hot som finns och vilka risker de medför för en verksamhet. Utan en balanserad uppfattning om detta riskerar vi inte bara att överraskas av oförutsedda hot utan även att i onödan lägga resurser på skydd mot överdrivna hot.

Riskhanteringen i logistikkedjan försvåras av det stora antalet inblandade aktörer som alla har egna värderingar och preferenser när det gäller att bedöma risker och välja åtgärder. Resultatet blir ofta att risker förskjuts från en plats i kedjan till en annan, från en aktörs ansvar till en annans. Gemensamma metoder för riskanalys och riskvärdering ökar chansen att uppnå en totalt sett bättre

risksituation i logistikkedjan, men försvåras främst genom komplexiteten i systemet.

Risker för kriminalitet i logistikkedjan finns i huvudsak inom fem hotområden; stöld, bedrägeri, smuggling, kapade transporter och korruption. Olyckor och naturkatastrofer kan naturligtvis också få synnerligen allvarliga konsekvenser för varuförsörjning och transportväsen. Även om den allmänna uppfattningen är att naturkatastrofer och korruption är mindre frekventa i vårt land så måste alla hot beaktas när det gäller Sveriges sårbarhet. Logistikkedjans betydelse för världsekonomin och välståndet innebär att också terroristhotet måste beaktas, även om de faktiska förlusterna på grund av direkta terrorhandlingar inte är av samma storleksordning som de för andra hot. Indirekta konsekvenser av terroraktioner är sannolikt större än direkta, till exempel leder förändrade resemönster efter flygplanskapningar till kännbara problem för flygbolagen. Kostnaderna för säkerhetskontroller på världens flygplatser överstiger också de direkta kostnaderna orsakade av terrorhandlingar mot flygtransporter.

Riskanalys är ett moget område, med en etablerad praxis, men också många variationer. I de flesta fall bygger analysen på någon kvantitativ modell för värdering av sannolikheter och konsekvenser för olika händelser. Det uppstår dock ett metodproblem när man försöker använda dessa modeller, väsentligen utvecklade för olyckor, för brottsliga handlingar. Händelserna är ofta så ovanliga att pålitlig statistik saknas. Hoten är i dessa fall dessutom avsiktliga, planerade av en aktör som snabbt kommer att anpassa sig till de nya skyddsåtgärder som utvecklas. Detta skapar en återkoppling mellan hot-risk-åtgärd-hot som den traditionella kvantitativa riskanalysen har svårt att hantera. Därför måste den kvantitativa analysen i dessa fall kompletteras med kvalitativa metoder, exempelvis scenariometodik och spel, för att på ett kreativt sätt fånga upp oväntade risker och resonera om lämpliga åtgärder.

Att detektera hot

När ett hot mot logistikkedjan håller på att realiseras är det viktigt att det kan upptäckas, detekteras. FOI har behandlat problemet med att identifiera de avvikelser i sensorsignaler och informationsflöden som tyder på att något anmärkningsvärt eller avvikande håller på att inträffa. Det är för detta ändamål viktigt att utnyttja all tillgänglig information (från till exempel administrativa system, inpasseringssystem och sensorer). Vid val mellan olika sensorsystemlösningar är det avgörande att känna till både sensorernas prestanda och tillämpningens krav. Ofta kan olika tekniker, metoder och källor komplettera varandra så att säkerhetssystemet blir mer effektivt.

Som tidigare nämnts kan hoten delas in i hot mot samhället i vidare mening då logistikkedjan utnyttjas för skadliga ändamål och hot mot själva logistikkedjan.

Nedan exemplifieras hotdetektion vad gäller smuggling, farliga ämnen och farliga aktörer.

Att detektera smuggling och farliga ämnen

För att upptäcka smuggling behövs detektionsmetoder som kan upptäcka smuggelgods i till exempel containrar. Oftast är det av ekonomiska och praktiska skäl dock inte möjligt att scanna eller inspektera alla containrar, utan det krävs ett urval av containrar att inspektera. För att hantera detta problem utvecklas i ett projekt metoder för att beräkna riskindex för containrar och annan frakt. Riskindexberäkningarna är av nödvändighet dynamiska och använder all tillgänglig information för att försöka sortera ut containrar med störst risk för otillåtet innehåll.

Farliga ämnen gömda i bagage eller fraktgods riskerar att utgöra hot både under och efter transporter såväl på land som på fartyg och i flygplan. Ansamlingen av människor på exempelvis järnvägsstationer, tunnelbanor och flygplatser gör dem också till lockande mål för terrorister. En utplacerad bomb, spridning av giftiga gaser eller radioaktivitet kan få stora konsekvenser inte bara för det land som i första hand drabbas.

Ett allvarligt hot mot luftfarten utgörs av farliga ämnen gömda i handbagage, i kläder eller på passagerare. En stor skillnad jämfört med kontrollen av fraktgods är att flygplatser och säkerhetskontroller måste hantera ett dynamiskt varierande flöde av resenärer, varför det blir viktigt att genomföra snabba kontroller med minimal störning för de resande. Utökade och ändrade kontroller på senare år, efter att flera incidenter har inträffat, har lett till en ökad säkerhet men också till mer krångel för resenärerna. Regelverket kring medförda vätskor skärptes bland annat på grund av ett dåd 2006, där en grupp terrorister försökte detonera hemmagjorda, flytande explosivämnen på flera flygplan från Storbritannien till USA och Kanada. Nuvarande krav att passagerare endast får bära med sig små volymer vätska (100 ml per förpackning) ombord, beror på att dagens utrustning inte anses tillräckligt tillförlitlig för att skilja explosiva vätskor från ofarliga vätskor. Resultaten är särskilt svåra att utvärdera då vätskan ligger inuti bagaget, vilket förklarar att passagerarna måste ta upp de små vätskemängderna ur handbagaget. FOI arbetar i detta sammanhang med att utveckla snabbare och mer selektiva detektionsmetoder baserade på Ramanspektroskopi, en teknik för att identifiera spår av explosivämnen på handbagage som rör sig på transportband. Tekniken är både känslig och snabb samt möjliggör scanning av allt handbagage, vilket inte utförs i dag. Liknande teknik utvecklas också för kontroll av personer och fordon vid gränskontroller.

Med flygfrakt skickas årligen ca 400 000 ton gods till och från Sverige och det är svårt att identifiera sådana transporter med farliga (explosiva eller radioaktiva) ämnen. Stickprovskontroller mot explosivämnen görs med bland annat

spårhundar eller röntgenutrusning, men det saknas effektiva metoder och verktyg för att på ett bra sätt undersöka allt gods som hanteras.

Även vad gäller gömda radioaktiva källor finns idag mycket begränsad detektionskapacitet i Sverige och Europa. Endast ett fåtal system är i bruk, samtidigt som antalet incidenter med strålkällor har ökat sedan slutet av 1990-talet. Radioaktiva ämnen som har gömts luktar inte, syns inte och hörs inte. För att detektera ämnena krävs därför speciella instrument. FOI arbetar bland annat för att förbättra tekniken att hitta explosivämnen och radioaktiva ämnen i transportkedjan och få tekniken tillräckligt billig och snabb.

De detektionsmetoder som nämnts för explosivämnen och radioaktiva ämnen appliceras också på andra håll inom logistikkedjan, till exempel inom posthantering där FOI utvecklar metoder för att kunna genomsöka all post och alla paket. Systemen skulle i framtiden kunna vidareutvecklas till att även hitta spår av droger eller biologiska hotsubstanser när post och paket sorteras.

Att detektera farliga aktörer

För att upptäcka hot mot själva logistikkedjan krävs en annan sorts riskindex. Information från till exempel videoövervakningssystem för att upptäcka intrång eller avvikande beteenden blir väsentlig. Övervakningssystemen bör präglas av en helhetssyn och beakta såväl kostnader som personlig integritet och andra etiska aspekter. En viktig del vid automatisk sensoranalys i övervakningssystem är att minimera antalet falsklarm med bibehållen säker detektion av kritiska händelser. Att korrekt analysera sensordata och automatiskt tolka situationer kan ofta försvåras av variationer i väder- och ljusförhållanden. För att få en god överblick över ett område så är det fördelaktigt att utnyttja mer än en sensor och gärna sensorer av olika typ, till exempel en kombination av optiska och akustiska sensorer samt radar. Felaktiga tolkningar av sensordata uppträder sällan samtidigt i flera sensorer och genom att fusionera data från flera sensorer, samt analysera mönster i data över tiden, så kan viktiga och kritiska händelser lättare urskiljas från det som är ointressant eller har tolkats på ett felaktigt sätt i en enskild sensor. Vanligtvis vill man låta systemet lära in en ”normalbild” över området och sedan larma för avvikelser från denna. Ofta är olika avvikelser olika svåra att upptäcka och man måste därför utgå från den riskanalys som gjorts för att välja vad övervakningssystemen ska vara inställda för.

Videoövervakning är i dessa sammanhang det vanligaste systemet, men information från exempelvis rörelsedetektorer och inbrottslarm kan också ge värdefull information. För att utveckla sensorsystem till låg kostnad kan det ibland vara en fördel att använda till exempel ”billiga” videokameror och istället fokusera på metodik för att enkelt integrera dem i ett sensor- och informationsnätverk. För att med automatiska beslutsstödsfunktioner avlasta operatörerna från rutinmässigt stirrande på sensorbildskärmar behöver

sensorinformationen omvandlas och representeras mer systematiskt så att datorer kan dra slutsatser om den. Två personer nära varandra där armarna rör sig snabbt kan exempelvis vara tecken på slagsmål medan en person där armarna rör sig snabbt istället kan tyda på en åkarbrasa. Lämnar någon aktör ett föremål som kan vara en bomb efter sig? Rör sig någon aktör på ett ovanligt sätt – mot eller tvärs folkströmmen eller dröjer någon sig kvar i ett område där alla brukar hasta förbi? Genom att representera informationen på en högre nivå kan sensorinformation enklare slås samman med annan information och slutsatser dras om några aktörer i området är förknippade med högre risker än vanligt. FOI forskar bland annat kring upptäckt av avvikande beteende hos individer och grupper dels i och omkring folksamlingar, dels på parkeringsplatser för lastbilar.

All information där människors identitet kan fastställas omgärdas av regler för att hindra intrång i den personliga integriteten. Ett antal olika sätt har prövats för att skydda identiteten på personer som rör sig i sensorövervakade områden. En möjlighet är att sensorsystemet kräver en auktoriserad order (som sedan arkiveras) varje gång personidentifierande information visas/förmedlas. Ett problem med att rutinmässigt skydda identiteten på personer i bevakningsområdet är om det just är vissa individer som utgör de största hoten. Då måste larm ges om dessa individer identifieras inom området. Många gånger kan det dessutom vara önskvärt att genomföra identifiering av individer i gamla sensordata efter säkerhetsincidenter. Ny teknik provas för att möjliggöra avbildning genom tonade bilrutor och MC-hjälmvisir och tyg framför ansiktet. Automatisk igenkänning av människors rörelsemönster och att genom lager av tyg kunna se dolda vapen och sprängmedel är andra teknikområden som har utvecklats under senare år, bland annat med sikte på säkerhetskontroller av passagerare på flygplatser. Teknik utvecklas också för att det ska bli möjligt att upptäcka människor bakom väggar eller dörrar.

Att vidta åtgärder mot detekterade hot

För att aktörerna i logistikkedjan effektivt ska kunna minska hot, risker och förluster, och därmed bidra till kontinuiteten i viktiga samhällsfunktioner krävs inte bara att hoten upptäcks och identifieras. De måste också kunna stävjas på något sätt. Det räcker inte att upptäcka hoten tidigt, aktören måste också ha en planering för åtgärder som är juridiskt, ekonomiskt och etiskt försvarbara. För ändamålet kan åtgärdslistor sammanställas. Om till exempel säkerhetssystemet i en terminal upptäcker att ett par personer håller på att klättra över staketet runt området, kan det vara lämpligt att rikta fler kameror mot inkräktarna och att skicka ut en säkerhetspatrull för att avvisa dem. Ofta är det välbetänkt att dessutom kalla på polis för att ha beredskap mot en eskalerande våldsnivå och eventuellt identifiera inkräktarna för en framtida lagsökning. En god beredskap mot hot och risker förutsätter ofta att det finns en plan för vilka åtgärder som ska vidtas på vilka indikationer. Alla tänkbara åtgärder som kan vidtas på någon

indikation kan sammanställas i åtgärdslistor. När ett hot är identifierat kan åtgärdsplaneringen sedan användas för att hjälpa beslutsfattaren att välja rätt handling. För att stödja beslutsfattaren i valet utvecklar FOI stödverktyg för att resonera kring hoten. Målet är att beslutsfattarna inte bara ska få en relevant bild av hur läget är (”situationsförståelse”) utan också att händelseutvecklingen blir begriplig och att tänkbara alternativ för incidenters utveckling lätt ska kunna förutses.

Lika viktigt som att det inte finns hål i stängslet runt en terminal som behöver skydd mot intrång är det att organisationerna genomsyras av relevant säkerhets-medvetande mot till exempel korruption. Frågeställningar som rör organisationens säkerhetsmedvetande är bland annat bakgrundskontroller av anställda, tillträdeskontroll till anläggningar, inspektioner av väskor och fordon vid tillträdeskontrollerna, träning/utbildning och organisationens tålighet mot personförluster. Ett väsentligt element i korruptionsbekämpning är att attester och in/utpasseringstillstånd inte hanteras av olika befattningshavare var för sig utan att dokument kontrasigneras.

Som i andra fall är informationsutbyte mellan de olika aktörerna i logistikkedjan centralt. Både administrativ information och sensorinformation måste analyseras för att upptäcka hot av såväl indirekt karaktär, till exempel smuggling, som direkta hot, till exempel från terrorister. Informationsutbytet har både tekniska och organisatoriska aspekter. Teknikmässigt gäller det att se till att systemen kan kommunicera med varandra och att rätt nivå av säkerhet kan upprätthållas. Semantisk interoperabilitet, det vill säga att en organisation och dess informationssystem kan förstå vad ett annat menar, är ett nyckelbegrepp.

Det är slutligen viktigt att säkerhetstänkandet integreras i de tekniska systemen redan på konstruktionsstadiet. En systemlösning som är helt fokuserad på högsta effektivitet under normala förhållanden kan visa sig bli sårbar mot terrorister och brottslingar liksom mot sällsynta olyckor och naturkatastrofer. Det ger ofta bättre motståndskraft att ha fler tekniska system och en viss överkapacitet för en uppgift även om ett enda slimmat system per uppgift ter sig effektivare i normalfallet. En säkerhetsåtgärd som har visat sig mycket effektiv kan i ett slag bli överspelad av förändringar i hotens uppträdande.

Hur kan svensk logistiksäkerhet förbättras?

Det är tydligt att effektiva sensorer, informationsfusion med beslutsstödssystem och en viss redundans ger ökad tillförlitlighet för logistiksystem. Ofta ger samma åtgärder förbättringar av säkerheten i fler än ett problemperspektiv. Ett exempel på detta är att efter attentatet mot World Trade Centre 2001 höjdes säkerhetsmedvetandet inom flera områden. Det fick till följd att Internationella Sjöfartsorganisationen 2002 tog fram en ny internationell kod för skydd av sjöfart och hamnanläggningar mot terrorism. När den infördes reducerades

stölderna inom hamnområdena i ett slag. Det är därför viktigt att på något sätt i förväg värdera säkerhetsåtgärders effekter mot olika hot och risker för att möjliggöra systematisk optimering av säkerhetsåtgärderna hos olika aktörer.

Beredvilligheten att öka säkerheten i logistikkedjan varierar dock liksom inom andra sektorer med upplevd hotnivå och mellan olika organisationer. Kraven på ökad säkerhet behöver balanseras. För att få perspektiv på området behövs också insikten att alla säkerhetsåtgärder som vidtas utan att det finns relevanta hot är slöseri med pengar och urholkar konkurrenskraften för organisationer och nationer. Medan till exempel smuggling är ett omfattande problem för samhället i stort och tullen i synnerhet är det inte av så stor betydelse för fraktbolagen som mer akut oroas av svinn och avbrott i leveranskedjan.

En viktig aspekt för kommersiella aktörer är kostnaden för säkerhetssystemet. Det anses dock självklart att säkerhetsåtgärder som direkt kan avräknas mot minskat svinn, lägre försäkringspremier eller ökad marknadsandel bör genomföras. Kan ökad säkerhet och ökad effektivitet uppnås samtidigt är det heller inte svårt att övertyga beslutsfattarna att satsa på säkerhetsåtgärder. Ökad säkerhet mot mycket sällsynta händelser medför dock ofta en ökad kostnad utan någon tydlig ekonomisk fördel. Tvingande direktiv från någon myndighet om att vissa säkerhetsrutiner/åtgärder måste vidtas över hela Europa torde underlätta acceptansen för sådana åtgärder bland transportsektorns kommersiella aktörer och göra åtgärderna konkurrensneutrala över hela den inre marknaden.

Ett annat exempel på drivkrafter inom transportsäkerhetsområdet gäller frågan om flygpassagerares medförande av vätskor i handbagaget, tänkbara hotscenarior med flytande explosivämnen har ovan belysts. Säkerhetskraven i kombination med avsaknaden av en säker och billig teknik för klassificering av vätskor i plast- och glasflaskor gör att tusentals liter dryck och konserver kasseras varje år vid säkerhetskontrollerna i världens flygplatser. Det ekonomiska trycket från affärsidkarna på flygplatserna att ta bort vätskebegränsningarna är också mycket stort. När en tillräckligt säker och billig teknik finns tillgänglig kommer därför bestämmelserna att förändras. Några flygplatser i Australien har redan infört teknik som klassificerar vätskor och därmed lättat på bestämmelserna om att passagerare endast får medföra mycket små vätskemängder i handbagaget.

I de projekt inom Europeiska unionen (EU) som författarna deltar i och som denna artikel beskriver resultat ifrån, medverkar flera svenska aktörer, både som projektpartners och som medlemmar i referensgrupper och liknande. De får naturligtvis god insyn och kännedom om möjligheterna till förbättrad logistiksäkerhet. Projekten är dessutom aktiva i att sprida information. De brukar bland annat ordna demonstrationer där landvinningarna konkret visas upp. Detta gör det möjligt för aktörerna i den svenska försörjningskedjan att dra nytta av forskningen. Det är alltså en kombination av tekniska möjligheter, politiska beslut och kommersiella drivkrafter som ger samhället de säkerhetssystem det har inom logistikområdet. Det är viktigt att hela tiden låta de olika

hotperspektiven vara levande så att alla aktörer strävar efter att med sina begränsade resurser vidta de säkerhetsåtgärder som motverkar flest hot istället för att enbart fokusera på nyupptäckta akuta säkerhetsbrister.

Vidare läsning

- Franke, U., Johansson, R., Mårtenson, C. och Svenson, P. ”Fusion av information från heterogena källor”, FOI-R--3453--SE, 2012.
- Fensel, A., Rogger, M., Gustavi, T., Horndahol, A. and Mårtenson, C. ”Semantic data management: sensor-based port security use case”, EISIC 2013.
- Gustavi, T. and Svenson, P. “Taxonomy for port security systems”, SecOnT 2013.