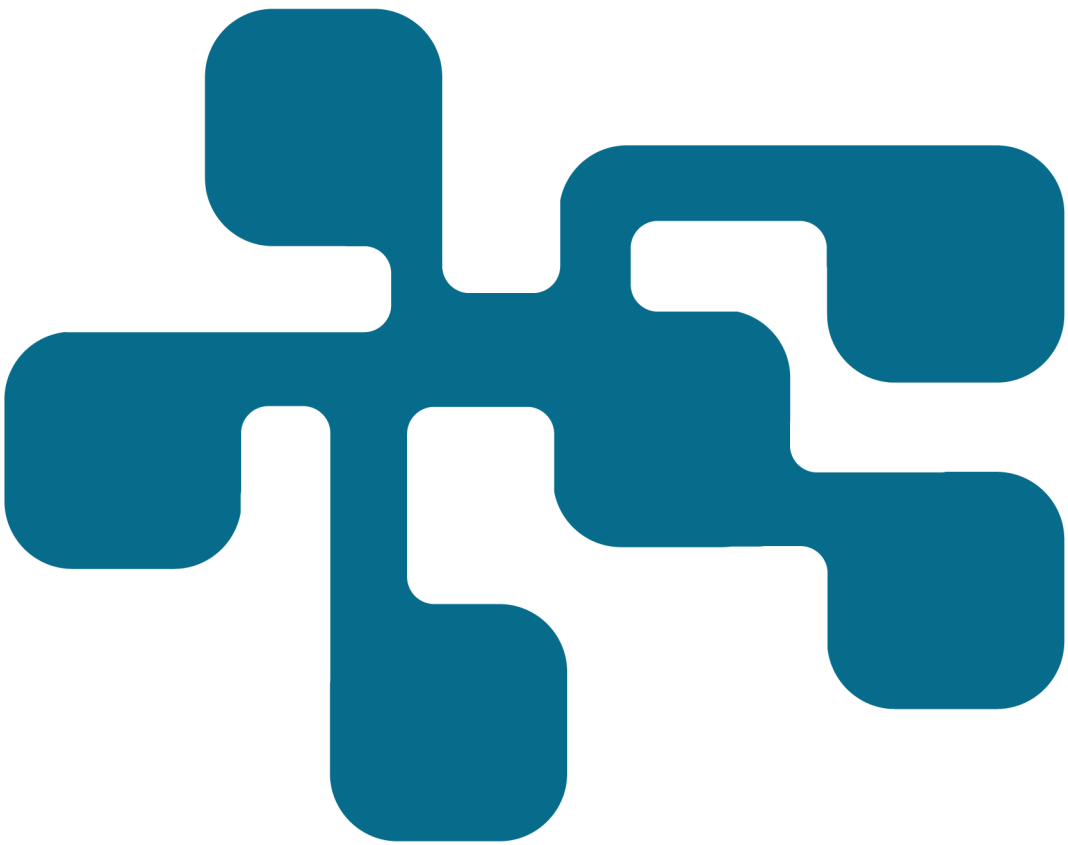
NCS3 - Hotanalys av ett informationssystem för transport av farligt gods

LARS WESTERDAHL, JOHAN BENGTSSON

FOI
MSB



FOI-R--4735--SE
MSB 2018-10654 Februari 2019
ISSN 1650-1942

Lars Westerdahl, Johan Bengtsson

Hotanalys av ett informations-system för transport av farligt gods

Titel	Hotanalys av ett informations-system för transport av farligt gods
Title	Threat analysis of an information system for the transportation of dangerous goods
Rapportnr/Report no	FOI-R--4735--SE
Månad/Month	Februari
Utgivningsår/Year	2019
Antal sidor/Pages	45
ISSN	1650-1942
Kund/Customer	MSB
Forskningsområde	4. Informationssäkerhet och kommunikation
FoT-område	Ej FoT
Projektnr/Project no	E72364
Godkänd av/Approved by	Christian Jönsson
Ansvarig avdelning	Ledningssystem
Exportkontroll	Innehållet är granskat och omfattar ingen information som är underställd exportkontrollagstiftningen.

Sammanfattning

Transport av farligt gods är reglerat i Sverige så väl som internationellt. I regelverken ADR, RID och ADN ställs bland annat krav på vilken information som ska ingå i en godsdeklaration samt var den ska finnas tillgänglig. Arbetsgruppen WG Telematics inom UNECE ser över möjligheterna att ta fram ett gemensamt informationssystem för information om transporter av farligt gods inom Europa. FOI har på uppdrag av MSB genomfört en övergripande analys av det föreslagna informationssystemet i syfte att identifiera hot och eventuella IT-säkerhetsrelaterade problem med lösningen.

Om det föreslagna systemet är adekvat eller inte för tänkta avnämare såsom tillsynsmyndigheter och räddningstjänst är svårt att avgöra utifrån analyserat material. Det står dock klart att de IT-säkerhetskrav som har identifierats i arbetsgruppens förslag inte täcker hela informationssystemet. I förslaget från WG Telematics ställs krav på de centrala delarna i informationssystemet, men de enheter som förser systemet med information utelämnas. Dessa enheter innefattar den utrustning som ska finnas på plats i exempelvis lastbilar, tåg och fartyg för att göra godsdeklarationer tillgängliga, exempelvis när myndigheter utövar tillsyn.

Nyckelord: Farligt gods, transporter, informationssäkerhet, IT-säkerhet.

Summary

Transportation of dangerous goods is regulated in Sweden as well as internationally. The regulations ADR, RID and ADN stipulate, among other things, which information is to be included in the transport documentation and where it should be available. The WG Telematics working group within UNECE is reviewing the possibilities of developing a common information system for information on transportation of dangerous goods within Europe. FOI has, on behalf of MSB, carried out an overall analysis of the proposed information system in order to identify threats and possible IT security-related problems with the solution.

If the proposed system is adequate or not for intended users such as regulatory authorities and emergency services, is difficult to determine based on the analysed material. However, it is clear that the IT security requirements that have been identified in the working group's proposal do not cover the entire information system. The requirements in the proposal from WG Telematics only concern the central parts of the information system, but the units that supply the system with information are omitted. These units include the equipment that must be in place in transportation vehicles such as lorries, trains and ships in order to make freight declarations available, for example when authorities exercise supervision.

Keywords: Dangerous goods, transportation, information security, IT-security.

Innehållsförteckning

1 Inledning

Med farligt gods avses sådant gods med egenskaper som kan vara farligt för omgivningen. Sådana egenskaper kan exempelvis vara att godset är explosivt, brandfarligt, giftigt eller radioaktiv. Transporter av farligt gods är internationellt reglerade, även när de enbart rör sig inom en nations väg- och spårnät samt vattendrag. Tillsyn av efterlevnad av dessa regelverk görs av utpekade myndigheter.

Dokumentation av farligt gods ska vara tillgänglig under transporten och kunna visas upp exempelvis vid en kontroll men även för räddningstjänsten i händelse av en olycka. För att förbättra tillgängligheten av information rörande transporter av farligt gods till berörda parter har diskussioner förts under flera år om ett informationssystem för detta behov. Ett sådant system skulle underlätta tillsyn och övervakning av transporter samt underlätta för räddningstjänst, där godsdeklaration inte alltid är tillgängligt.

1.1 Uppdrag

Myndigheten för samhällsskydd och beredskap (MSB) vill undersöka ett föreslaget informationssystem ur ett säkerhetsperspektiv och har gett detta uppdrag till *Totalförsvarets forskningsinstitut* (FOI). Uppdraget avser att beskriva det föreslagna informationssystemet, genomföra en hotanalys för det föreslagna informationssystemet, bedöma de säkerhetskrav som ställts samt att vid behov föreslå kompletteringar. Analysen genomfördes baserat på följande dokument:

- Informationssystem som definieras av det *Memorandum of Understanding* (MoU) som finns i *United Nations Economic and Social Council* (UNECE) (2018).
- *eDG Transport Document Webservices Description (04/05/2018)* (GeotransMD & Core Project 2018).
- *Lägesrapport för elektronisk information för transport av farligt gods* (Skärdin & Söderlind 2019).
- *Minnesanteckningar från WG Telematics, 20181112-14* (Skärdin & Rydberg 2019).

I början av 2019 publicerades ett utkast till Guidelines (UNECE 2019) som föreslås ersätta det MoU som analysen har utgått ifrån. Analysen som presenteras i denna rapport genomfördes innan Guidelines publicerades. I de fall det för analysen finns relevanta skillnader mellan MoU och Guidelines nämns detta i rapporten.

1.2 Läsanvisning

Inledningsvis definieras begrepp som används i rapporten i kapitel 2. Därefter ges i kapitel 3 en bakgrund till området farligt gods genom en generell hotbild mot transporter av farligt gods och mot informationssystem samt en kort beskrivning av den teknik som informationssystemet baseras på. I kapitel 4 beskrivs aktörer, information och det föreslagna informationssystemet. Detta system analyseras sedan i kapitel 5 genom en säkerhetsanalys. Studiens resultat diskuteras i kapitel 6 och slutsatser presenteras i kapitel 7.

2 Begrepp

I denna rapport används ett antal begrepp för att identifiera olika typer av aktörer som på ett eller annat sätt fyller en funktion vid transport av farligt gods. De engelska begreppen är identifierade från tabellen *Who does what* (RID/ADF/ADN 2010) och har kompletterats med svenska begrepp och definitioner från avsnitt 1.2.1 i regelverken ADR-S[1] och RID-S[2]. Om begreppen enbart är definierade i något annat dokument än de två regelverken lämnas en referens. De förändringar som föreslagits till kommande Guidelines (UNECE 2019) kommenteras också. I Tabell 1 återges dessa begrepp på engelska och, då av MSB fastslagen översättning finns tillgänglig, även på svenska. I de fall som en definition inte är hämtad från avsnitt 1.2.1 i regelverken avslutas definitionen med en sifferkombination inom parenteser som avser i vilket avsnitt i ADR-S och RID-S som begreppet används.

Tabell 1: Aktörer vid transport av farligt gods.

Svenska	Engelska	Definition
Avsändare	Shipper/ Consignor/ Sender	Med avsändare förstås ett företag som avsänder farligt gods för egen eller annans räkning. Om en transport utförs i enlighet med ett transportavtal ska med avsändare förstås den som är avsändare enligt transportavtalet.
Behörig myndighet	Competent authority	Myndighet eller annat organ som förordnas som sådan i varje stat i varje enskilt fall enligt landets lagstiftning.
Fyllare	Filler	Företag som fyller farligt gods i en tank (tankfordon, avmonterbar tank, UN-tank eller tankcontainer), i ett batterifordon eller en MEG-container, eller i ett fordon, en storcontainer eller småcontainer för transport i bulk.

[1] Svenska utgåvan av *Accord Européen Relatif au Transport International des Marchandises Dangereuses par Route*.
[2] Svenska utgåvan av *Règlement concernant le transport international ferroviaire de marchandises Dangereuses*.

Svenska	Engelska	Definition
Förpackare	Packer	Företag som fyller farligt gods i förpackningar, inklusive storförpackningar och IBC-behållare, och i förekommande fall förbereder kollin för transport.
Infrastruktur–förvaltare	Infrastructure manager	Termen finns i regelverken och MoU men definieras inte i MoU. I RID 1.2.1 definieras järnvägsinfrastruktur-förvaltning: Varje offentlig inrättning eller varje företag, till vilket särskilt överlåtits att bygga upp och underhålla järnvägsinfrastrukturen samt organisation av driftlednings- och säkerhetssystem.
Lastare	Loader	Företag som (a) lastar förpackat farligt gods, småcontainrar eller UN-tankar i eller på ett fordon eller en container, (b) lastar en container, bulkcontainer, MEG-container, tankcontainer eller UN-tank på ett fordon.
Medlem av fordons–besättningen	Driver/Crew	Förare eller annan person som medföljer föraren av skäl som avser säkerhet, transportskydd, utbildning eller drift.
Mottagare	Consignee	Mottagaren enligt transportavtalet. Betecknar mottagaren enligt de för transportavtalet gällande bestämmelserna en tredje part, så räknas denna som mottagaren i ADR/ADR-S:s mening. Sker transporten utan transportavtal så är mottagaren det företag, som övertar det farliga godset vid ankomsten.
<saknas>	Enforcement bodies	Termen finns i MoU men definieras inte i regelverken. I svenska sammanhang motsvaras detta av exempelvis Polis, Säpo och Tull.
Räddningstjänst	Emergency responders	Termen finns i MoU men definieras inte i regelverken.

Svenska	Engelska	Definition
Speditör	Freight forwarder	Termen finns i MoU och i regelverken men definieras inte.
Transportör	Carrier	Företag som genomför transport, med eller utan transportavtal.
<saknas>	Security bodies	Termen finns i MoU men definieras inte i regelverken.
<saknas>	Signatory	Den nation/myndighet som signerar MoU-avtalet. (MoU kapitel 2) Denna term finns inte med i utkastet till Guidelines.
Användare av tankcontainer eller UN-tank (ADR)	Tank-container/portable tank operator	Företag i vars namn tankcontainern eller UN-tanken registrerats.
Användare av tankcontainer, UN-tank eller cisternvagn (RID)	Operator of a tank-container, portable tank or tank-wagon	Användare av tankcontainer, UN-tank eller cisternvagn: Företag i vars namn tankcontainern, UN-tanken eller cisternvagnen registrerats eller i övrigt godkänts för trafik.

3 Bakgrund

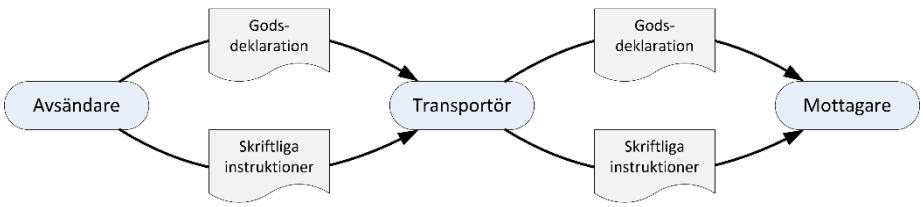
I detta kapitel ges en bakgrund till flera olika områden som är nödvändiga att ha god kännedom om för att till fullo kunna ta till sig resonemangen i denna rapport. Läsare som innehar nödvändig kunskap angående områdena som följer kan således hoppa över detta kapitel för fortsatt läsning i kapitel 4.

Kapitlet inleds med en övergripande beskrivning av området farligt gods. Därefter ges en beskrivning av den generella hotbilden mot transporter av farligt gods samt mot de tekniska system (IT-system) som utgör informationssystemet. Då det föreslagna informationssystemet för information om farligt gods använder sig av *webbtjänster* och *certifikat* ges en övergripande beskrivning av hur dessa tekniker fungerar. Kapitlet avslutas med en beskrivning av hur metoden för säkerhetsanalys fungerar. Metoden användes för att genomföra den analys av systemet som beskrivs i kapitel 5.

3.1 Farligt gods

Farligt gods utgörs huvudsakligen av ämnen, vätskor eller föremål som är explosiva, i gasform, brandfarliga, oxiderande, giftiga, radioaktiva eller frätande. Vad som utgör farligt gods definieras i *Lag (2006:263) om transport av farligt gods* (SFS 2006:263). Något förenklat kan transport av farligt gods beskrivas som aktiviteter vilka kan härledas till förflyttning av det farliga godset, utanför det område där godset tillverkas.

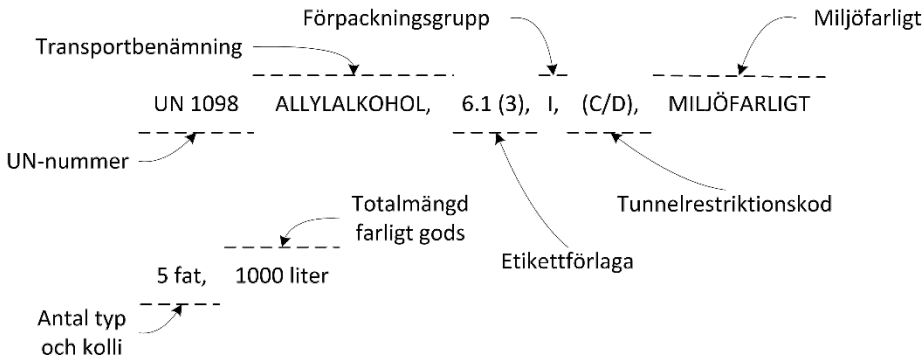
Det finns tre huvudsakliga aktörer vid transport av farligt gods (MSB 2017). Avsändaren (eng. consignor) är den part som vill få det farliga godset transporterat till en mottagare (eng. consignee). Transporten expedieras av en transportör (eng. carrier), det vill säga det företag som ansvarar för genomförandet av transporten. Begreppet transportör i det här fallet kan omfatta allt från ett åkeri med en lastbil till en kedja av speditörer, åkerier och förare. Utöver dessa tillkommer de aktörer som hanterar godset exempelvis vid förpackning, lastning, lossning och tankning (MSB 2017).



Figur 1: Övergripande bild av hantering av godsinformation.

Avsändaren ansvarar för att upprätta godsdeklarationen. Det finns inget givet formulär för detta, utan deklarationen kan exempelvis göras på fraktsedeln. Vid internationella transporter med tåg används en CIM-fraktsedel.

En godsdeklaration avser ett specifikt ämne eller föremål. Om flera ämnen eller föremål transporteras samtidigt ska alla deklareras. En godsdeklaration ska ange avsändare och mottagare samt specificera godset. Figur 2 visar ett exempel på hur en godsdeklaration kan se ut.



Figur 2: Exempel på godsdeklaration av 1 000 liter allylalkohol.

I de fall då transporten behöver tillstånd görs ansökan hos behörig myndighet. Behöriga myndigheter utgörs av Strålsäkerhetsmyndigheten, Polismyndigheten, Myndigheten för samhällsskydd och beredskap eller Transportstyrelsen beroende på vilket tillstånd som söks (SFS 2006:311).

Det finns ett antal tillsynsmyndigheter vilka har till uppgift att kontrollera att *Lag (2006:263) om transport av farligt gods* och aktuella föreskrifter följs. Tillsynsmyndigheter och deras respektive ansvarsområden regleras i *Förordning (2006:311) om transport av transport av farligt gods* och visas i Tabell 2.

Tabell 2: Tillsynsmyndigheter för farligt gods.

Myndighet	Ansvarsområde
Transportstyrelsen	Sjötransporter, lufttransporter och järnvägstransporter
Polismyndigheten	Transporter på land utom järnvägstransporter
Kustbevakningen	Gods i hamnars landområden som är avsett för vidare transport samt, på Transportstyrelsens begäran om biträde, sjötransporter
Strålsäkerhetsmyndigheten	Transporter av radioaktiva ämnen

Myndighet	Ansvarsområde
Myndigheten för samhällsskydd och beredskap	Säkerhetsrådgivare för samtliga transportslag, transportabla tryckbärande anordningar, transportskydd samt utbildning och examination av förare av transport av farligt gods på väg och i terräng

3.2 Hotbild

En hotbild kan beskrivas utifrån antagonistiska hot, det vill säga där det finns en medveten hotaktör bakom hotet, alternativt genom en mer allmängiltig beskrivning där alla möjliga faktorer som kan resultera i oönskade händelser tas upp. Antagonistiska hot skiljer sig ifrån olyckshändelser i den betydelsen att antagonisten har ett mål och att antagonistiska angrepp kan vara mer komplexa än en olycka. Med komplexitet avses här att en olycka ofta har ett singulärt ursprung (exempelvis att något går sönder eller översvämmas) och att alla följder är konsekvenser av detta ursprung. En antagonist kan å andra sidan genomföra flera oberoende angrepp (ursprung) som kan vara åtskilda i tid och rum, vilket kan ge en ökad komplexitet.

3.2.1 Studier om fysiska hot

Ett flertal studier har genomförts med inriktning mot fysiska hot mot transporter av farligt gods. Gemensamt för dessa studier är att de huvudsakligen fokuserar på fysiska hot mot godset eller fordonet. Det finns även handböcker och vägledningar som beskriver hotbilden mot transporter av farligt gods.

Målet för antagonisten i studierna är oftast stöld eller terrorism. Exempelvis presenterar Nilsson och Andersson (2007) 13 scenarier där transporter av farligt gods används i huvudsak för utpressning eller attentat, men även stöld. I dessa scenarier är ofta transporten målet för hotaktörerna alternativt kan transporten vara ett medel för att uppnå något annat mål. I flera av scenarierna kapas transporten för att användas på en annan plats än den planerade färdvägen. I samtliga fall har dock någon form av kartläggning genomförts i förväg så att hotaktören vet ungefär när en transport finns på en given plats.

Riksrevisionen (2007) trycker i sin utredning på sårbarheten för transporter och gods vid kända knutpunkter. Med detta avses platser där gods lastas om, mellanlagras eller lastas av. För flera transporttyper eller sträckor är detta ett fåtal platser, exempelvis hamnar.

MSB (2010) identifierar stöld och terrorism som de stora antagonistiska hoten mot farligt gods. I samma rapport dras slutsatsen att de ekonomiska förutsättningarna, främst beroende på konkurrenssituationen, leder till att

säkerhetsarbete främst är olycksförebyggande. Dessa icke-antagonistiska hot är mer lättgripbara och har även ett statistiskt stöd. De antagonistiska hoten mot transporter av farligt gods avser främst stöld av gods som enkelt kan omsättas till pengar.

Trafikanalys (2015) har genomfört en övergripande kartläggning av transporter av farligt gods på väg, på järnväg, till sjöss och i luften. Kartläggningen fokuserar primärt på tillgängliga statistiska uppgifter från respektive område vilket medför att mängden data varierar. Något som framgår i kartläggningen är att det inte råder en enhetlig uppfattning mellan myndigheter om vilka data, särskilt i aggregerad form, som bör omfattas av sekretess och att lagstiftningen inte alltid är tydlig. Trafikanalys publicerade den data de samlar in om transporter på vägar, medan Trafikverket var osäkra på vad de kunde lämna ut avseende transporter på järnväg. Sjöfartsverket och Säkerhetspolisen beslutade att motsvarande uppgifter om farligt gods som transporteras till sjöss inte får lämnas ut.

3.2.2 Hot mot IT-system

Hot mot IT-system, det vill säga tekniska system som är en del av ett informationssystem, kan på en övergripande nivå delas in i indirekta och direkta hot. De indirekta hoten utgörs dels av det *bakgrundsbrus* som finns på internet, dels av generiska och automatiserade angrepp som inte har ett specifikt mål. Bakgrundsbrus avser kända hot, exempelvis i form av skadlig kod, som hanteras rutinmässigt av uppdaterade antivirusprogram. De generiska angreppen är skadlig kod som letar efter specifika svagheter i program som de kan utnyttja. Dessa angrepp är opportunistiska i betydelsen att den individ eller grupp som står bakom den skadliga koden inte är ute efter att angripa en given organisation. Dessa typer av angrepp är även relativt riskfria för hotaktören. Skadlig kod utgörs i dessa sammanhang exempelvis av virus, maskar eller utpressnings-programvara, med syftet att exempelvis förstöra funktionalitet eller få ekonomisk vinning.

För riktade hot är målet en specifik organisation eller ett specifikt IT-system som hotaktören vill påverka eller utnyttja. För riktade angrepp mot organisationer är IT-system ofta ett medel och inte det övergripande målet i sig själv. Det innebär också att metoderna för angrepp varierar med hotaktörens målsättning, från kartläggning, informationsstölder, överbelastningsattacker till obehörigt nyttjande av systemfunktioner. Riktade angrepp pågår över en längre tid även om den faktiska påverkan på målsystemet generellt sett utförs under en kort tid. Ofta har mycket tid lagts innan på spaning, planering och etablering i de system som kommer att angripas.

Endast en minoritet av alla IT-system eller organisationer utsätts för riktade angrepp (Elliott 2018). Däremot bör alla som har IT-system anslutna till internet

skydda sig mot indirekta hot, då dessa är ständigt närvarande och inte gör skillnad på vem som äger ett system eller vad systemet har för syfte.

3.2.3 Hotaktörer[3]

Förutsättningarna för att ett IT-angrepp ska vara framgångsrikt beror på hotaktörens möjligheter, vilken exempelvis kan bedömas genom dennes kapacitet, intention och tillfälle. Enskilda hotaktörer är ofta mer opportunistiska medan organiserade hotaktörer enklare kan utföra storskaliga och riktade angrepp. För stora angrepp krävs utöver organisation även tid och ekonomiska resurser.

Det finns flera sätt att beskriva och kategorisera hotaktörer. En hotaktör är den individ, grupp eller stat som står bakom och som kan realisera ett hot. Individer med ett uppsåt att angripa en organisation eller ett system utgör ett antagonistiskt hot medan individer eller händelser utan uppsåt, exempelvis ett naturfenomen eller en anställd som begår ett misstag, utgör ett icke-antagonistiskt hot.

En ansats till indelning av antagonistiska hotaktörers förmåga har gjorts av *Defence Science Board* (DSB), vilka är en del av USA:s försvarsdepartement. DSB kategoriserar hotaktörers förmåga i tre större kategorier: de som kan utnyttja kända svagheter, de som kan identifiera ej tidigare kända sårbarheter, samt de som kan skapa sårbarheter i system (DSB 2013). På den lägsta nivån av DSB-kategorier är den individuella kompetensen ofta låg, det finns dock kraftfulla angreppsverktyg som är öppet tillgängliga och relativt enkla att använda eller till och med beställa (Makrushin 2017). På en högre nivå är hotaktörerna organiserade och mer affärsmässiga. De kan också vara finansierade av en organisation eller stat som vill dölja sitt deltagande eller som väljer att hyra den kompetens som de saknar. Den högsta nivån utgörs uteslutande av statsaktörer.

Ett annat sätt att se på hotaktörer är att kategorisera dem efter deras drivkrafter. De hotaktörer som identifierades i studierna i avsnitt 3.2.1, har primärt ekonomiska eller politiska motiv. Då de angrepp som beskrevs där huvudsakligen var fysiska blir dessa begränsade i tid och rum till där transportfordonet finns. Även IT-system finns fysiskt på en plats men dessa system kan även angripas på avstånd över internet. Den första hotkategorin är enskilda individer som av någon anledning angriper system. Dessa hotaktörer behöver inte ha någon särskild relation till det system de angriper även om det kan röra sig om personer som är eller har varit anställda av den organisation som de nu valt att agera mot. Anställda eller andra personer med rätt att använda de system som angrips kallas för *insiders*. Hotaktörens drivkraft är oftast personlig

[3] Delar av detta avsnitt är baserat på *Förstudie fjärrvärme* (Valassi, Hunstad & Westerdahl 2019).

men det kan också vara individer som blivit värvade eller hotade av kriminella organisationer eller främmande makt.

Politiskt motiverade hotaktörer kallas ofta för *hacktivister*. Att använda datorer i politisk aktivism, har blivit allt vanligare och hotaktörerna tenderar att vara individer eller löst sammansatta grupper av individer som utför angrepp mot ett gemensamt övergripande mål. Ofta är syftet med angreppen i första hand att få uppmärksamhet för det politiska mål gruppen agerar för, även om riktade sabotage kan förekomma.

Terrorister har historiskt fokuserat på fysiska angrepp. IT-angrepp i terrorsyfte är svårt att realisera men IT-system kan vara en källa till information för fysiska attentat.

Organiserad brottslighet inom cybervärlden är något som de senaste åren ökat. Framförallt har dessa angrepp utgjorts av utpressningsmjukvara där ett stort antal organisationer och individer drabbats. Motivet för denna typ av organiserad brottslighet är i regel ekonomisk vinning, exempelvis som vid angreppet mot Uber (Richter 2017). Dock finns även en rad andra tänkbara motiv, exempelvis ren förstörelse både digitalt och fysiskt.

Främmande makts aktiviteter inom cyberkrigföring, cyberspionage och cyberbrottslighet, har under de tio senaste åren fått allt större uppmärksamhet i media, se exempel Lagner (2013), Macaskill och Dance (2013) samt Sanchez (2015). Cyberangrepp är väldigt attraktivt för stater eftersom de medför möjligheten att rimligt förneka inblandning i angreppet. Det är svårare att knyta ett cyberangrepp till en främmande makt än ett fysiskt angrepp. Motiven för en främmande makt kretsar ofta kring kartläggning och spionage mot andra nationer i det egna närområdet. Detta inkluderar även industrispionage för att kartlägga sårbarheter och attackytor för att planera ett tillvägagångssätt om ett angrepp bedöms vara nödvändigt.

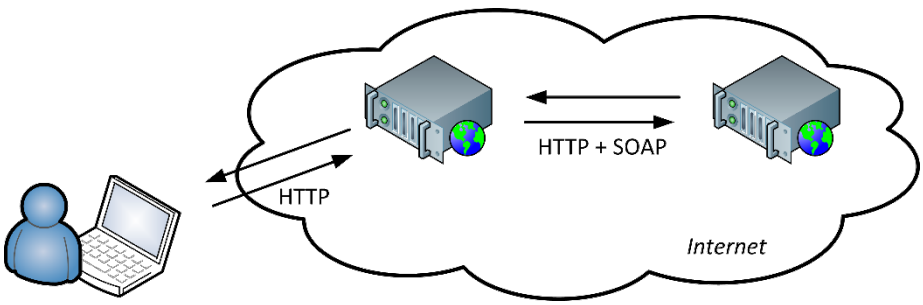
3.3 Webbtjänster

En webbtjänst används för att dela information och tjänster över internet mellan webbaserade system. Ett tjänsteanrop kan initieras av en mänsklig användare men det utbyte av information och tjänster som sedan görs sker mellan maskiner. En mer generaliserad form av tjänstebaserade system kallas för tjänsteorienterad arkitektur (eng. Service-Oriented Architecture, SOA).

Det vanligaste protokollet för webbaserade tjänster är *Hypertext Transfer Protocol* (HTTP) vilket används för att kommunicera med en webbserver. Webbtjänster använder HTTP som kommunikationsprotokoll mellan servrar och *eXtended Markup Language*-baserade (XML) standarder för att utbyta

information. SOAP[4] och *Web Services Description Language* (WSDL) är exempel på standarder som används för att skapa webbtjänster. Det finns även en konkurrerande standard, *Representational State Transfer* (REST), men den kommer inte att tas upp i denna rapport då det system som diskuteras inte är beskriven för den standarden.

SOAP anger de yttre ramarna för hur kommunikation mellan webbtjänster ska gå till genom att definiera en struktur för meddelanden och ställa krav på att XML används för att beskriva innehåll i meddelanden. WSDL beskriver en webbtjänst i XML-format. Leverantören av en webbtjänst beskriver vilken funktionalitet som erbjuds och hur en användare (ett annat system) ska kommunicera med webbtjänsten (Figur 3). Genom att användaren använder strukturen in WSDL-filen kan webbtjänsten tolka förfrågan och leverera önskad tjänst.



Figur 3 Webbtjänster.

SOAP i sin enklaste form är bara en meddelandestruktur. Likt flera andra kommunikationsprotokoll ingår inga säkerhetsfunktioner i detta, utan det är något som tjänsteleverantörer behöver tillgodose i efterhand. För SOAP finns en utökning av protokollet, *Web Service Security* (WS-Security), vilket bland annat möjliggör utbyte av autentiserings- och auktorisationsinformation samt signaturer.

3.4 Digitala certifikat

För att kunna kommunicera säkert är det nödvändigt att veta vem man kommunicerar med. Autentisering används för att verifiera motpartens identitet och är därmed en av hörnstenarna i säker kommunikation.

För inloggning till program och tjänster är kombinationen användarnamn och lösenord fortfarande en mycket vanlig metod för autentisering, även om tillämpning av flerfaktorautentisering ökar. Vid användandet av internetbaserade tjänster och maskin-till-maskinkommunikation är digitala certifikat en attraktiv

[4] Tidigare en förkortning för Simple Object Access Protocol men är nu ett eget namn.

lösning. Med ett digitalt certifikat knyts en identitet till en publik nyckel och denna koppling säkerhetsställs av en pålitlig part. Den pålitliga parten är oftast en tredje part som efter att ha säkerhetsställt att uppgifterna i certifikatet är korrekta, signerar certifikatet. En digital signatur förhindrar inte att uppgifter i ett dokument förändras, men den möjliggör att en förändring kan upptäckas. Vem som helst kan verifiera att en digital signatur är korrekt men det är mycket svårt att förfalska en sådan signatur.

Det finns ingen given standard för hur ett certifikat ska se ut eller hanteras. Dock är ITU-standarden X.509 mycket vanlig och används exempelvis i *Transport Layer Security* (TLS).

3.4.1 X.509

Vem som helst kan generera ett asymmetriskt nyckelpar och signera den publika nyckeln. Detta kallas för självsignerade certifikat och används främst internt inom system. Som autentiseringsmetod är självsignering dock inte trovärdigt. X.509 är ett certifikatbaserat system med en betrodd part som huvudaktör, en *Certificate Authority* (CA). Det är CA:n som signerar certifikaten och som ansvarar för revokering av dessa.

Ett certifikat utfördas med en bestämd giltighetsid. När giltighetstiden löper ut, upphör certifikatet att gälla. Det kan dock finnas flera anledningar att ett certifikat blir ogiltigt under dess giltighetstid. Om ägaren till ett certifikat blir av med sin privata nyckel kan inte längre en säker kommunikation genom den publika nyckeln som är kopplad till certifikatet garanteras. En annan och kanske både vanligare och mindre dramatisk anledning kan vara att certifikatägaren byter anställning eller på annat sätt gör så att personliga uppgifterna i certifikatet inte längre stämmer. I dessa fall behöver certifikatet ogiltigförklaras. Problemet med certifikat och därmed även asymmetrisk kryptering är att den publika delen av nyckelparet, den som certifikatet gäller, är avsedd att spridas. Det går således inte att återkalla certifikatet och ersätta det med ett nytt. Lösningen blir istället att CA:n publicerar en lista över tidsmässigt giltiga certifikat men som förklarats ogiltiga. Denna procedur kallas för revokering.

För en klient som tar emot ett certifikat för att hantera autentisering är det således viktigt att klienten både verifierar certifikatets signatur och kontrollerar att certifikatet inte har revokerats. Först när båda dessa kontroller är genomförda kan klienten lita på certifikatet.

3.4.2 Ömsesidig autentisering

Autentisering vid en anslutning till en webbtjänst är ofta ensidig. Det innebär att en användare ansluter till en webbserver och att webbservern bekräftar vem den är genom att skicka sitt certifikat. Användaren autentiserar sig eventuellt därefter

via en inloggning på webbtjänsten. Denna anslutningsmetod är den som är vanligast när TLS används i HTTP (HTTPS).

En lösning som ger en högre tillit till båda deltagande parter är ömsesidig autentisering. Det innebär att även användarklienten skickar ett certifikat till webbservern för att visa var anropet kommer ifrån. Certifikaten är inte personliga, men de påvisar ifrån vilken organisation som anropet kommer.

Ömsesidig autentisering är inte normalfallet för HTTPS då det dels innebär en kostnad för certifikat för användaren, vilket har betydelse om användare är en privatperson, och att det dessutom kräver mer administration. För mindre system med begränsat antal deltagare är det dock en bra lösning för att förstärka autentiseringen.

3.5 Säkerhetsanalys – en översikt

När risk- och sårbarhetsanalyser genomförs inom Försvarsmakten används metoden för Säkerhetsanalys som beskrivs i *Handbok Säkerhetstjänst Grunder* (Försvarsmakten 2013). Metoden används för analyser av allt från planerade IT-system till militära insatser. Tanken med metoden är att den ska vara användbar för alla typer av verksamheter samt att den ska vara applicerbar för både antagonistiska och icke-antagonistiska hot. I återstoden av detta avsnitt ges en övergripande beskrivning av metoden.

Under genomförandet av en säkerhetsanalys är det olika typer av information som behövs som bedömningsunderlag för att slutligen kunna bedöma de risker som anses föreligga. I en aktuell rapport från FOI (Hallberg, Bengtsson & Karlzén 2018) beskrivs de informationselement som används under en säkerhetsanalys och som tillsammans utgör den beskrivning av ett hot som slutligen används som bedömningsunderlag. De informationselement som föreslås återges i Tabell 3 med tillhörande beskrivning. De föreslagna informationselementen relaterar till varandra enligt följande.

> *Aktörer använder tillvägagångssätt för att utnyttja sårbarheter vilket, trots existerande skyddsåtgärder, kan realisera en oönskad händelse som påverkar informationssäkerhetsegenskaper hos tillgångar och resulterar i konsekvenser.*

Tabell 3: Informationselement som tillsammans utgör en beskrivning av hot vid en säkerhetsanalys. Tabell från (Hallberg, Bengtsson & Karlzén 2018).

Informations-element	Beskrivning
Tillgång	En tillgång är något som bedöms vara kritiskt eller på annat sätt ha ett särskilt värde för den verksamhet som analyseras. Tillgångar utgör utgångspunkten för genomförandet av en säkerhetsanalys.
Oönskad händelse	En oönskad händelse är något som medför en negativ påverkan på en tillgång. I kontexten säkerhetsanalys innebär en oönskad händelse en påverkan av säkerhetsegenskaper för en tillgång. Givet en tillgång och en uppsättning av säkerhetsegenskaper identifieras oönskade händelser genom att avgöra vilka kombinationer av tillgången och säkerhetsegenskaperna som är relevanta. En grundläggande uppsättning med säkerhetsegenskaper för informationstillgångar är konfidentialitet, riktighet och tillgänglighet.
Konsekvens-beskrivning	En konsekvensbeskrivning innehåller kvalitativa bedömningar av den negativa påverkan som en oönskad händelse medför, där konsekvensen beskrivs med ord, snarare än med enbart ett värde. Konsekvensbeskrivningen utgör underlag för den kvantitativa bedömningen av konsekvensen, ger spårbarhet och tydliggör bakgrunden till den kvantitativa bedömningen.
Aktör	En aktör är den part som genom ett tillvägagångssätt ligger bakom realiserandet av en oönskad händelse. Med aktör kan avses exempelvis en individ, grupp, organisation eller stat. Egenskaper som beskriver en aktör, exempelvis kapacitet, intention och tillfälle, har stor betydelse för sannolikheten för att ett hot realiseras.
Tillvägagångssätt	Tillvägagångssätt beskriver en aktörs förfarande som leder till att en oönskad händelse inträffar. Kunskap om möjliga tillvägagångssätt är nödvändigt för bedömningen av sannolikheten för att ett hot realiseras.

Informations-element	Beskrivning
Sårbarheter	Sårbarheter utgörs huvudsakligen av brister i skyddet av tillgångar. Sårbarheter kan klassificeras som organisatoriska eller tekniska. En sårbarhet är någonting som utnyttjas av en aktör i ett tillvägagångssätt för att realisera ett hot. Kunskap om sårbarheter är nödvändigt för bedömningen av sannolikheten för att ett hot realiseras.
Skyddsåtgärder	En skyddsåtgärd är något som syftar till att minska sannolikheten att ett hot realiseras genom att antingen minska sårbarheten eller påverka en aktör. Den samlade mängden skyddsåtgärder utgör skyddet av den verksamhet som analyseras. Skyddsåtgärder kan klassificeras utifrån olika egenskaper, exempelvis baserat på om de syftar till att påverka aktörers intention, kapacitet eller tillfälle alternativt baserat på när skyddsåtgärden genomförs såsom förebyggande, skadereducerande eller återställande.

Innan själva säkerhetsanalysen inleds är det nödvändigt att definiera vilken verksamhet det är som ska analyseras. Av denna anledning är det vanligt att säkerhetsanalysen föregås av en verksamhetsanalys. När verksamhetsanalysen är genomförd kan säkerhetsanalysarbetet inledas. Arbetet med att genomföra en säkerhetsanalys är indelat i följande fem steg.

1. Identifiera och prioritera skyddsvärda tillgångar
2. Bedömning av säkerhetshot
3. Bedömning av sårbarhet
4. Bedömning av risk
5. Prioritera och hantera risker

Det första steget inleds med att identifiera de skyddsvärda tillgångar som finns i verksamheten. De skyddsvärda tillgångarna är de som bedöms vara kritiska för verksamheten eller på annat sätt har ett särskilt värde för verksamheten. När de skyddsvärda tillgångarna har identifierats fortsätter arbetet med att identifiera vilka oönskade händelser som skulle ha en negativ påverkan på de skyddsvärda tillgångarna. En oönskad händelse kan exempelvis vara förlust av den skyddsvärda tillgången. Efter att ha beskrivit de oönskade händelserna görs en konsekvensbeskrivning som i ord förklarar konsekvensen av att den oönskade händelsen skulle inträffa. Konsekvensbeskrivningen kompletteras med en

konsekvensbedömning på en femgradig skala (1–5) som anger hur allvarlig konsekvensen skulle vara.

Det andra steget syftar till att identifiera konkreta hot som anses kunna leda fram till att de oönskade händelserna inträffar. Ett konkret hot fås genom att identifiera ett tillvägagångssätt som skulle kunna realisera en oönskad händelse samt en eller flera aktörer som skulle kunna använda det identifierade tillvägagångssättet. Därefter bedöms en hotnivå på en femgradig skala (1–5) som beskriver hur högt hotet är.

Det tredje steget inleds med att identifiera redan existerande skyddsåtgärder som har en påverkan på de konkreta hot som identifierades i steg 2. Därefter ska sårbarheterna identifieras. Sårbarheter är i detta sammanhang definierade som brister i skyddet. Genom att identifiera existerande skyddsåtgärder och sårbarheter fås en nulägesbild av skyddet av de skyddsvärda tillgångarna.

I det fjärde steget kommer det klassiska momentet i riskanalys där en risknivå ska bedömas för varje hot. En skillnad med säkerhetsanalys jämfört med flera andra riskmetoder är att konsekvensen redan bedömdes i det första steget efter att de oönskade händelserna identifierats. Då konsekvensen redan är bedömd återstår således att bedöma sannolikheten för att det konkreta hotet skulle inträffa och därmed realisera den oönskade händelsen. Sannolikheten bedöms på en femgradig skala (1–5). Därefter bedöms risknivån genom en sammanvägning av bedömningarna av sannolikhet och konsekvens. Den riskmatris som metoden tillhandahåller är indelad i fyra kvadranter som ger en vägledning om vilket intervall som är rimligt för risknivån sett till bedömd sannolikhet och konsekvens. Risknivån anges även den på en femgradig skala (1–5). Stor vikt läggs vid att bedömningen av risknivå motiveras väl för att visa på ett medvetet ställningstagande.

I det femte steget ska riskerna hanteras och detta arbete inleds med att riskerna prioriteras. Prioriteringen kan göras på valfritt sätt, exempelvis utifrån den bedömda risknivån. Riskerna hanteras i prioritetsordning från den högst prioriterade risken till den lägst prioriterade. För varje risk ställs frågan om den kan accepteras och om så är fallet fortgår arbetet med nästa risk. Om risken däremot inte kan accepteras behöver nya skyddsåtgärder tillföras för att få ner risknivån till en acceptabel nivå. Detta görs genom att gå tillbaka till det tredje steget och föreslå nya skyddsåtgärder för att därefter göra om steg fyra och fem med de nya skyddsåtgärderna i åtanke. Arbetet fortlöper på detta vis tills alla riskerna bedöms vara på en acceptabel nivå.

4 Informationssystem för farligt gods

I detta kapitel beskrivs informationsbehoven med avseende på de aktörer som identifierats i sammanställningen i *Who does what* (RID/ADR/ADN 2010). Därefter presenteras det system som föreslås hantera informationsflödet mellan aktörerna.

4.1 Aktörer

De huvudsakliga aktörerna för genomförandet av en transport presenterades i avsnitt 3.1, och utgörs av avsändaren, transportföretaget och mottagaren. En lite mer detaljerad vy av vad som möjliggör en transport identifierar även myndighetsaktörer och stödaktörer (Tabell 4).

Tabell 4 Exempel på aktörer som är inblandade i en transport.

Kategori	Aktör
Transportaktörer	Avsändare, Transportör, Mottagare
Stödaktörer	Medlem av fordonsbesättningen, Speditör, Lastare, Förpackare, Fyllare, Infrastrukturförvaltare
Myndighetsaktörer	Behörig myndighet, räddningstjänst och rättsvårdande myndigheter (exempelvis Polisen, Säkerhetspolisen, Tullverket)

I ADR, RID och ADN beskrivs de flesta aktörer som företag eller myndigheter. I slutändan är det dock människor eller tekniska system som agerar ut aktörens roll.

4.2 Informationsklassning

De informationselement som definieras i *Who does what*-tabellen, kategoriseras där i tre grupper: *godsdeklaration*, *övrig information* och *ny information*[5]. Ett delvis annat sätt att se på den information som beskrivs inom respektive kategori är att *godsdeklaration* utgör den information som krävs enligt avsnitt 1.2.1 i ADR/RID/ADN medan kategorin *övrig information* innefattar skriftliga instruktioner, certifikat och märkningar av gods och fordon. Gemensamt för dessa kategorier är att de är statiska från det att de upprättas till dess att godset är

[5] Transport documentation, Miscellaneous, New information.

levererat. Ny information är information om godset och transportfordonet under själva transporten. Denna information blir således dynamisk då den kan förändras under transporten.

Gemensamt för informationen i de tre kategorierna är att den i de flesta fall redan idag finns tillgänglig digitalt eller på papper, dock inte i ett gemensamt informationssystem. Skillnaden med hanteringen av information i det föreslagna informationssystemet är att informationen lagras centralt och att den blir sökbar. Informationen blir därmed även tillgänglig för betydligt fler aktörer.

4.2.1 Konfidentialitet

Huvuddelen av den information som rör farligt gods är idag offentliga uppgifter utan sekretess. Som framkom i Trafikanalys studie (Trafikanalys 2015) finns det dock vissa transporter som bedöms ha ett högre behov av sekretess än andra.

En enskild uppgift från någon av de tre kategorierna är inte skyddsvärd. Det är först när flera uppgifter sätts samman som en hotaktör kan dra några slutsatser om en enskild transport eller se ett mönster genom flera transporter. En hotaktör med tillgång till information om gods och som även har tillgång till positionsdata kan däremot följa en enskild transport med samma uppdateringsfrekvens som data samlas in, och planera ett angrepp mot en given transport.

4.2.2 Riktighet

Den information som förs in i informationssystemet kommer huvudsakligen från avsändaren av det farliga godset och från det fordon med förare som utför transporten av godset. Då dessa två aktörer inte kravställs i det MoU som beskriver det tänkta informationssystemet är det svårt att värdera riktigheten för information i systemet. Kravställning som påverkar riktigheten finns enbart för de aktörer som nyttjar informationen i informationssystemet.

4.2.3 Tillgänglighet

Tillgänglighetsbehoven av informationen är inte på millisekundnivå, utan det handlar snarare om några sekunder eller enstaka minuter. Informationen ska vara så tillgänglig att exempelvis en inspektion kan genomföras utan onödigt dröjsmål. De som enligt *Who does what*-tabellen har störst behov av snabb åtkomst till information i nuläget är den som inspekterar och räddningstjänst. Tabellen tar även upp infrastrukturförvaltare, exempelvis ägare eller myndigheter som övervakar trafik i tunnlar, som en möjlig framtida nyttjare av informationen.

Det ställs krav i MoU:t på att informationen ska lagras så att den är tillgänglig i minst tre månader. Det ställs dock inga krav på gallring av information.

4.2.4 Spårbarhet

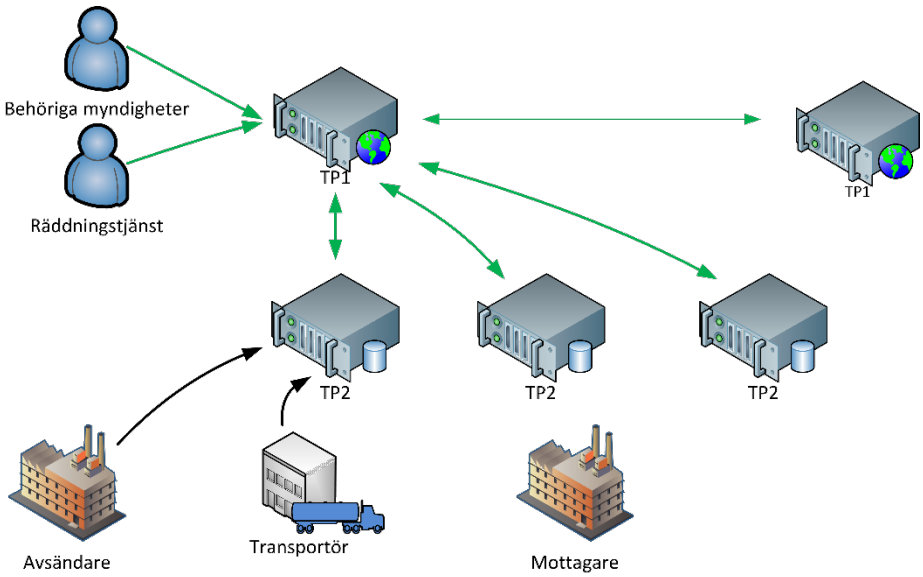
All information som hanteras i informationssystemet är inte relevant för alla intressenter. Informationen i informationssystemet är tänkt att användas för väg-, järnvägs- och sjötransporter, vilket gör att det finns speciella poster som endast är relevanta inom dessa områden. I Sverige planeras informationssystemet att enbart användas för väg- och järnvägstransporter. För sjötransporter används andra informationssystem.

Det kan vara svårt att veta i förväg exakt vilken transport som är relevant för en intressent. Det gör att det finns ett behov av spårbarhet av vem som tagit del av vilken information och varför.

4.3 Systembeskrivning

Det informationssystem som föreslås i *Memorandum of Understanding* (MoU) (UNECE 2018) syftar till att skapa en gemensam plattform för hantering av elektronisk dokumentation över transporter av farligt gods inom Europa. Informationssystemet har två huvudkomponenter: *Trusted Party 1* (TP1) och *Trusted Party 2* (TP2). En översikt av informationssystemet återges i Figur 4.

TP2 är ett system som ägs av ett transportföretag eller ett företag som erbjuder en TP2:a som tjänst till transportföretag. I en TP2:a lagras information om en transport av farligt gods. TP1 är en nationell resurs som förmedlar information om en transport till exempelvis behöriga myndigheter, räddningstjänst samt till andra TP1:or.



Figur 4 Översikt av informationssystem för farligt gods.

4.3.1 Anslutning till informationssystem

En nation kan välja att gå med i informationssystemet genom att signera det MoU-avtal som reglerar systemet. En nation får därefter möjlighet att nominera en eller flera TP1:or, alternativt kan nationen välja att ansluta till en annan nations TP1:a.

Genom att signera MoU-avtalet accepteras reglerna för hur systemet används. Det innebär att TP1:or måste stödja hela XSD-schemat som utgör *eDG Transport Information*. Det innebär också att en TP1:a accepterar andra TP1:or och svarar på förfrågningar ifrån dessa, samt att TP2:or tillåts registrera sig.

En godkänd TP1:a förs upp på en lista över godkända TP1:or. Denna lista kallas *TP1 Trusted List* och hanteras av UNECE och ERA/OTIF. På listan finns information om TP1:or som gör att den nya TP1:an kan ansluta till andra TP1:or. I informationen på TP1 Trusted List ingår en statisk IP-adress till alla TP1:or samt respektive TP1:as certifikat. När nya TP1:or tillförts listan distribuerar ansvariga myndigheter (UNECE, ERA/OTIF) listan till alla TP1:or. Detta innebär att de ansvariga myndigheterna också bör bekräfta giltigheten av respektive TP1:as certifikat innan en ny TP1 Trusted List distribueras.

4.3.2 Myndighetsaktörer

Den myndighet som godkänner MoU-avtalet (signatory) ansvarar också för att etablera en lista över godkända myndighetsaktörer som har rätt att ta del av information från informationssystemet.

4.3.3 Övergripande säkerhetslösning

Den övergripande skyddsåtgärden som framgår av MoU-avtalet är ömsesidig autentisering av de parter som kommunicerar med TP1:or. Det innebär att TP2:or och myndighetsaktörer måste skicka sina certifikat till den TP1:a som de är anslutna till. Nytillkomna TP1:or måste skicka sina certifikat till samtliga TP1:or på TP1 Trusted List. De gröna pilarna i Figur 4 indikerar vilka kanaler som är upprättade med ömsesidig autentisering.

Kommunikation mellan TP1:or och dess registrerade parter sker över HTTPS. Det innebär att en krypterad kanal mellan autentiserade parter upprättas innan innehållet kommuniceras. I det här fallet är skyddet starkare än vanligt genom den ömsesidiga autentiseringen.

MoU-avtalet ställer inga säkerhetskrav på kommunikationen till och från de transportaktörer som kommunicerar med TP2:or. Till skillnad från TP1:or där TP1:an kan vara statligt kontrollerad så förutsätts att TP2:an inte är det. Den ska också kommunicera med fler typer av system vilka inte alltid kan förutsättas ha förmåga till ömsesidig autentisering i första hand, och skyddad kommunikation med HTTPS i andra hand.

4.3.4 Trusted Party 1

De centrala enheterna inom informationssystemet är TP1:orna. Det är med TP1:orna som myndighetsaktörerna kommunicerar direkt eller indirekt via andra TP1:or. TP1:or har en viss mängd information sparade lokalt men huvuddelen av informationsmängden över farligt gods befinner sig i TP2:orna.

Ett implementationsförslag beskrivet i GeotransMD & Core Project (2018) definierar tjänsteutbud hos en TP1:a respektive en TP2:a. Implementationen är delvis en förenkling av det system som definieras i MoU-avtalet, i det avseende att alla användningsfall inte är upptagna. Implementationen visar dock på den funktionalitet som behövs och vilket typ av information som kommuniceras mellan TP1 och TP2 samt deras avnämare. I implementationen används ett enklare XML-schema än vad MoU-avtalet hänvisar till.

I dokumentationen definieras interna och externa webbtjänster för TP1. Interna tjänster erbjuder metoder för att TP1 ska kunna utbyta information med andra TP1:or och TP2:or, medan externa webbtjänster avser TP1-kommunikation med behöriga myndigheter, med mera.

En webbtjänst har ett antal metoder definierade för vad webbtjänsten kan göra. Implementationen från GeotransMD & Core Project (2018) definierar ett antal obligatoriska metoder som ska implementeras samt ett antal frivilliga metoder. Denna uppdelning framgår inte av MoU-avtalet.

TP1:ans primära funktion är att ta emot frågor och förmedla svar. För att veta vilka frågor som kan besvaras med stöd av registrerade TP2:or måste TP1:an föra ett register över aktuella transporter. MoU-avtalet specificerar att följande data lagras i TP1:

- Chassinummer (eng. Vehicle Identification Number (VIN)) för vägfordon[6]
- BIC-kod för containers
- Registreringsnummer för dragfordon och dess släp (ADR), ENI-nummer[7] (ADN), UIC-nummer[8] (RID)
- Transportens status
- Fordonstyp.

I implementationen finns även frivilliga funktioner som kan utvecklas vid ett senare tillfälle. Med dessa funktioner kan det även bli aktuellt att lagra positionsdata för transporten och larm från denna.

4.3.5 Trusted Party 2

Den huvudsakliga datalagringen sker i TP2. En TP2:a ansluter till en TP1:a (en TP1:a kan ha flera TP2:a anslutna till sig) och svarar på frågor från denna. Informationen i TP2:an kommer ifrån den deklaration av farligt gods som avsändaren av godset upprättar samt statusuppdateringar från transportören. Även om det inte framgår tydligt så är det rimligt att anta att lastbilar, tåg och fartyg kommunicerar med sina ägare och att de i sin tur meddelar TP2:an om status för aktuell transport.

Alla myndigheter har inte rätt till att ta del av all information som lagras i en TP2:a. När en myndighet ställer en fråga via en TP1:a, förmedlar TP1:an av vilken anledning informationen efterfrågas, genom att ange typ av avsändare. Räddningstjänst och liknande får exempelvis mer tillgång till information än andra myndigheter. Vid andra förfrågningar rörande exempel statistik, kan TP2:an låta blir att skicka personuppgifter kopplat transporten.

[6] Fordonets chassinummer ingår inte längre enligt Guidelines (UNECE 2019). I Guidelines har landskod tillkommit.
[7] European Number for Identification
[8] Internationella järnvägsunionen (eng. International Union of Railways)

5 Säkerhetsanalys

En säkerhetsanalys har genomförts baserat på de uppgifter som finns i MoU-avtalet (UNECE 2018) och den tekniska beskrivningen (GeotransMD & Core Project 2018) samt ett utkast av MSB:s PM *Lägesrapport för elektronisk information för transport av farligt gods* (Skärdin & Söderlind 2019). Analysen utgick från Försvarsmaktens metod för säkerhetsanalys som översiktligt beskrevs i avsnitt 3.5. För att förtydliga i säkerhetsanalysen att det är information om transporter av farligt gods som är tillgången snarare än det fysiska godset, benämns *tillgång* i detta kapitel som *informationstillgång*.

I detta tidiga skede av det föreslagna informationssystemet för transport av farligt gods har det varit nödvändigt att göra vissa avgränsningar i analysarbetet. I Tabell 5 indikeras vilka informationselement som inkluderades i analysarbetet av de som beskrevs i Tabell 3 i avsnitt 3.5. Då uppgiften var att genomföra en hotanalys avslutas säkerhetsanalysen efter att hoten har identifierats. Denna analys avser logiska hot riktade mot informationssystemet, vilket innebär att fysiska hot mot det gods som transporteras inte tas upp i analysen. Dessa avgränsningar innebär även vissa begränsningar i resultaten som blir av mer övergripande karaktär.

Tabell 5: Informationselement som inkluderades i säkerhetsanalysen.

Informationselement	Inkluderad
Informationstillgång	✓
Oönskad händelse	✓
Konsekvensbeskrivning	✓
Aktör	
Tillvägagångssätt	✓
Sårbarheter	
Skyddsåtgärder	

Analysarbetet inleddes med en inläsning av de uppgifter som fanns tillgängliga i MoU-avtalet och tekniska beskrivningar. Därefter genomfördes en workshop där fyra forskare deltog för att analysera det föreslagna systemet utifrån tillgängliga uppgifter. Alla fyra forskare arbetar inom området informationssäkerhet, men har något skilda inriktningar, vilket gav möjlighet till viss variation avseende infalls-vinklar när analysarbetet genomfördes.

Den första aktiviteten som genomfördes under workshopen var att fastställa vilken verksamhet det var som skulle analyseras för att få en tydlig inriktning för vad som skulle ingå i analysarbetet. Verksamheten definierades som alla de TP1:or som utgör det föreslagna informationssystemet, inklusive de gränssnitt som TP1:or har mot andra TP1:or, TP2:or, berörda myndigheter och räddningstjänst. Detta motsvarar TP1 och de gröna pilarna i Figur 4. Det som inte ingår i verksamheten som analyserades är TP2:or samt kommunikationen mellan TP2:or och deras underliggande aktörer, exempelvis avsändare och transportör.

Utifrån verksamhetsbeskrivningen identifierades de skyddsvärda informationstillgångarna, det vill säga de informationstillgångar som på ett eller annat sätt anses vara kritiska för den verksamhet som ska bedrivas. De skyddsvärda informationstillgångarna ger också en avgränsning av det fortsatta analysarbetet, exempelvis avseende vilka oönskade händelser som är relevanta att inkludera i analysarbetet. I Tabell 6 återges de tre grupper av information som beskrevs i avsnitt 4.2 och som hade sitt ursprung i specifikationen över hur information är tänkt att flöda i informationssystemet. De enskilda uppgifterna i varje grupp av information är inte nödvändigtvis skyddsvärda, det är först när uppgifter börjar kombineras som skyddsvärdet för dem ökar. Under analystillfället ansågs därför den samlade mängden information som återges i Tabell 6 tillsammans utgöra den skyddsvärda informationstillgången.

Tabell 6: Beskrivning av de tre grupperna av information.

Information	Beskrivning
Godsdeklaration	Utgörs av den information om godset som definieras i avsnitt 1.2.1 i ADR, RID och ADN.
Övrig information	Utgörs av skriftliga instruktioner, certifikat och märkningar av gods och fordon
Ny information	Utgörs av dynamisk information som beskriver aktuell status för gods och transportfordon, vilket är information som tidigare inte efterfrågats, men som nu tillförs i och med informationssystemet

Efter att den skyddsvärda informationstillgången hade identifierats fortsatte analysarbetet med att identifiera vilka oönskade händelser som skulle kunna ha en negativ påverkan på informationstillgången. Med negativ påverkan avses en påverkan på någon av informationstillgångens säkerhetsegenskaper. En vanlig utgångspunkt är de tre säkerhetsegenskaperna *konfidentialitet*, *riktighet* och *tillgänglighet*. Analysarbetet resulterade i fyra oönskade händelser som

bedömdes kunna ha en negativ påverkan på informationstillgångens säkerhetsegenskaper enligt Tabell 7.

Tabell 7: Oönskade händelsers påverkan på säkerhetsegenskaper.

Oönskad händelse	Konfidentialitet	Riktighet	Tillgänglighet
Informationstillgången förstörs			✓
Informationstillgången stjäls	✓		✓
Informationstillgången är otillgänglig			✓
Obehörig förändring av informationstillgången		✓	

I analysarbetet framkom att det är nödvändigt att skilja på information som stjäls och information som förloras. När information stjäls görs det av en aktör som har ett uppsåt och som förväntas använda informationen för egen vinning. Att informationen stjäls kan även innebära att informationen inte längre är tillgänglig, vilket innebär att en stöld kan ha påverkan både på konfidentialitet och på tillgänglighet. Däremot när information förstörs blir resultatet enbart en påverkan på tillgängligheten.

Det genomförda analysarbetet var endast övergripande då det föreslagna informationssystemet fortfarande är i planeringsstadiet. Beskrivningen av vilka konsekvenser de oönskade händelserna bedöms få blir därmed också övergripande.

Att *informationstillgången förstörs* bedöms få konsekvensen att information om transporter går förlorade, vilket i sin tur resulterar i att informationssystemet inte kan svara på förfrågningar som berör dessa transporter. Dessutom kan förstörelse av information innebära att spårbarhet kring transporter förloras. Konkreta tillvägagångssätt som kan leda fram till att den oönskade händelsen *informationstillgången förstörs* inträffar återges i Tabell 8.

Tabell 8: Tillvägagångssätt som kan leda till att den oönskade händelsen *informationstillgången förstörs* inträffar.

ID	Beskrivning
H1	Radering av information i informationssystemet
H2	Överskrivning av information i informationssystemet

ID	Beskrivning
H3	Fysisk förstörelse av information i informationssystemet

Att *informationstillgången stjäls* bedöms få konsekvensen att obehöriga personer får åtkomst till informationen i informationssystemet. En stöld av information kan även resultera i att informationen inte längre finns tillgänglig i informationssystemet, vilket då dessutom skulle resultera i de konsekvenser som beskrevs för den oönskade händelsen *informationstillgången förstörs*. Konkreta tillvägagångssätt som kan leda fram till att den oönskade händelsen *informationstillgången stjäls* inträffar återges i Tabell 9.

Tabell 9: Tillvägagångssätt som kan leda till att den oönskade händelsen *informationstillgången stjäls* inträffar.

ID	Beskrivning
H4	Obehörig åtkomst till information via fråga till TP1
H5	Obehörig åtkomst till information via fråga till TP2
H6	Obehörig åtkomst till information via OBU/terminal i fordon

Att *informationstillgången är otillgänglig* bedöms få konsekvensen att informationssystemet inte kan svara på förfrågningar eller ta emot information från behöriga parter. Konkreta tillvägagångssätt som kan leda fram till att den oönskade händelsen *informationstillgången är otillgänglig* inträffar återges i Tabell 10.

Tabell 10: Tillvägagångssätt som kan leda till att den oönskade händelsen *informationstillgången är otillgänglig* inträffar.

ID	Beskrivning
H7	Avbruten förbindelse till informationssystemet för myndighetsaktörer eller transportaktörer
H8	Överbelastning av informationssystemet
H9	En TP1:a stryks felaktigt från TP1 Trusted List
H10	Revokerat eller utgånget certifikat i den nationella TP1:an

Att *obehörig förändring av informationstillgången* inträffar bedöms få konsekvensen att informationssystemet ger felaktiga svar på förfrågningar.

Konkreta tillvägagångssätt som kan leda fram till att den oönskade händelsen *obehörig förändring av informationstillgången* inträffar återges i Tabell 11.

Tabell 11: Tillvägagångssätt som kan leda till att den oönskade händelsen *obehörig förändring av informationstillgången* inträffar.

ID	Beskrivning
H11	Inmatning av felaktiga uppgifter i informationssystemet
H12	Obehörig förändring av TP1 Trusted List

6 Diskussion

Säkerhetsanalysen i denna studie baserades i huvudsak på arbetsdokument som beskriver det föreslagna informationssystemet. Det innebär att även säkerhetsanalysen bör ses som en preliminär analys som behöver uppdateras allteftersom systembeskrivningen utvecklas och fastställs. Resultat och slutsatser från en säkerhetsanalys kan inte bli tydligare än vad underlaget medger.

En uppenbar brist i MoU:t är avsaknaden av säkerhetskrav på TP2:orna utöver kommunikationen med TP1:or. Det ställs inga säkerhetskrav avseende TP2:ornas kommunikation med underliggande system, exempelvis hos transportören. Detta medför en osäkerhet för hela informationssystemet avseende konfidentialitet och riktighet för informationen om transporter av farligt gods.

Resultaten av systembeskrivningen och säkerhetsanalysen av det föreslagna informationssystemet för hantering av information om transporter av farligt gods har delats upp i de tre områdena *informationssäkerhet*, *IT-säkerhet* och *fysisk säkerhet*. Områdena diskuteras var för sig i de avsnitt som följer.

6.1 Informationssäkerhet

Ur ett informationssäkerhetsperspektiv är skyddsvärdet av information om transporter av farligt gods detsamma oavsett om informationen finns i ett IT-system eller på ett papper. Det som IT-system kan medföra är en ökad tillgänglighet men samtidigt även en högre grad av exponering då IT-system ofta är anslutna till internet. Detta medför att en hotaktör inte nödvändigtvis behöver vara fysiskt närvarande vid informationen. Exponeringsgraden kan därför medföra behov av särskilda säkerhetskrav på IT-systemet.

Sett ur ett generellt informationssäkerhetperspektiv för information om transporter av farligt gods så bedöms inte enstaka uppgifter om enskilda transporter vara skyddsvärda. Däremot kan kombinationen av uppgifter om en enskild transport bli skyddsvärda, exempelvis kombinationen av uppgift om transportklassificering och fordonets aktuella position. Information om transport av farligt gods finns redan tillgänglig idag, men då utspridd i flera olika informationssystem som inte är sammankopplade. Införandet av det nya före–slagna informationssystemet skulle innebära att all information om transporter av farligt gods tillgängliggörs via ett system. Det föreslagna informationssystemet skulle då även medföra att information om transport av farligt gods blir sökbar och tillgänglig på distans. På så sätt sker en aggregering av kunskap, trots att hela informationsmängden i praktiken är utspridd över flera TP1:or och ännu fler TP2:or placerade i de deltagande länderna.

Dynamisk information såsom en transports position och kända leveransplatser kan vara intressanta för en hotaktör som vill påverka transporten. Detta är en ny

situation som uppkommer i och med införandet av det föreslagna informationssystemet, vilket gör att det bör övervägas med vilken noggrannhet och uppdateringsfrekvens som en transport ska kunna följas.

6.2 IT-säkerhet

De huvudsakliga tekniska säkerhetsfunktioner som kravställts i MoU-avtalet är ömsesidig autentisering mellan alla noder samt en säker kommunikation. Digitala certifikat har angivits som metod för autentisering och HTTPS som metod för säker kommunikation.

I normalfallet vid användning av HTTPS (HTTP över TLS) sker endast autentisering av servern (mottagaren) i kommunikationen mellan en klient (avsändare) och en server. För att uppnå ömsesidig autentisering av både avsändare och mottagare krävs att båda parter har tillgång till varandras certifikat, vilket föreslås i MoU-avtalet. Ett certifikat har normalt en begränsad giltighetstid. Hur lång denna giltighetstid är beror på användningsområdet för certifikatet. Det är dock möjligt att det kan uppstå behov av att i förtid sluta använda det nyckelpar som certifikatet stödjer, exempelvis om den privata nyckeln stulits eller på andra sätt kommit på villovägar. Då det inte är möjligt att veta exakt var alla kopior av ett certifikat finns är det nödvändigt att ha en metod för att ogiltigförklara ett certifikat. Detta kallas för att revokera certifikat och resulterar i att certifikatet sätts upp på en lista över certifikat som är ogiltiga trots att de fortfarande är inom sin normala giltighetsperiod. En klient som vill skicka ett meddelande och som redan har mottagarens (serverns) certifikat tillgängligt måste verifiera att certifikatet inte har revokerats innan det kan användas. Revokeringslistor hanteras oftast av en så kallad Certification Authority (CA), vilket är den enhet som utfärdat certifikatet.

Det finns flera utfärdare av certifikat; både privata aktörer och statliga myndigheter. En förutsättning för att certifikat ska kunna användas är att alla parter lita på varje CA som kan utfärda certifikat till aktörerna i systemet.

6.3 Fysisk säkerhet

Enligt MoU-avtalet ställs det inga särskilda krav på fysisk skydd av informationssystemet och det togs därför inte upp i säkerhetsanalysen. Det är dock nödvändigt att påpeka att den nod som är mest fysiskt exponerad och åtkomlig utgörs av de enheter som finns i transportfordonet, särskilt om det är en lastbil. Transportfordonet och dess förare måste kunna kommunicera vid minst två tillfällen (inför en transport och vid dess avslut), men sannolikt även däremellan. Det är inte klart om kommunikationen går från transportfordonet till aktuell TP2:a eller om den går via transportören. I de fall då föraren använder en portabel enhet, såsom en smart telefon eller en surfplatta, för att kommunicera

finns även en stöldrisk då denna typ av enheter är stöldbegärliga. Att enheten är portabel innebär även att det är något som föraren kan glömma att lämna över till ny förare vid förarbyte. Fast monterade enheter är mindre stöldbegärliga, men kan fortfarande utnyttjas för att påverka informationssystemet om en hotaktör får fysisk åtkomst till en enhet. Då det inte finns några IT-säkerhetsmässiga krav på TP2:or och dess underliggande system, så är det svårt ha tilltro till den information som tillförs informationssystemet.

7 Slutsatser

Ett införande av det föreslagna informationssystemet för gemensam hantering av information om transporter av farligt gods kan på sikt ersätta motsvarande hantering som i dagsläget sker i flera separata system. Att strukturera upp informationsflödet och istället samla information om transporterna i ett gemensamt informationssystem med gemensam struktur och informationsmodeller ger bättre förutsättningar för både tillsynsmyndigheter och räddningstjänst att utföra sina uppdrag. Det som ett gemensamt informationssystem tillför är funktionalitet för aggregering av transportinformation, vilket förenklar kartläggning av transporter, dock även för en antagonist. I MoU-avtalet föreslås även att varje fordon under aktiv transport har möjlighet att kontinuerligt skicka dynamisk information. Denna dynamiska information är än så länge inte obligatorisk eller helt bestämd, men föreslås exempelvis innefatta aktuell position för fordonet och larm. Det är heller inte bestämt med vilken precision den dynamiska informationen ska återges eller med vilken frekvens uppdateringarna förväntas ske.

Centralt för informationssystemet är delsystemen TP1, vilket primärt förmedlar svar på frågor från myndigheter och andra TP1:or, samt TP2 där huvuddelen av transportinformationen lagras. Informationssystemet föreslås använda ömsesidig autentisering vid all kontakt med en TP1:a, vilket stärker tilliten för båda parter avseende med vem kommunikationen sker. Utöver den ömsesidiga autentiseringen krypteras även all kommunikation med TP1:or genom att HTTPS ska användas. Krypteringen säkerställer att aktuell kommunikation inte kan avlyssnas eller förändras.

Även om MoU-avtalet innefattar flera viktiga områden så saknas information om vissa saker som kan påverka säkerheten i informationssystemet. En av dessa saker är specifikation av hur revokering av certifikat ska hanteras. Funktionalitet för att hantera revokering är något som bör finnas med i ett tidigt stadie av planeringsarbetet för ett nytt system då det ställer krav på den ömsesidiga autentiseringen som ska användas vid kommunikation med en TP1:a. För att en revokeringsfunktion ska kunna fungera krävs exempelvis att giltigheten för motpartens certifikat kontrolleras hos en CA innan kommunikationen initieras. Denna typ av funktionalitet kan vara trivial att implementera på ett tidigt stadie, men kan bli komplicerad att lägga till i efterhand.

Det ställs inga krav i MoU-avtalet om hur kommunikationen mellan TP2:an och dess underliggande system ska hanteras. Det framgår att TP2:an kommunicerar med avsändare och transportörer, men är oklart om den ska kunna kommunicera med fler parter. Det finns förslag på funktioner där aktuell position efterfrågas av andra parter, men dessa funktioner är inte obligatoriska. Då det är flera olika typer av system som eventuellt ska kunna kommunicera med en TP2:a kan det vara problematiskt att specificera detta på en allt för detaljerad nivå. Dock bör

det finnas grundläggande krav som att kommunikation exempelvis alltid ska ske krypterat, förslagsvis via HTTPS då det används i övriga delar av systemet.

Det är även otydligt vilken funktionalitet en terminal i ett fordon ska ha. Det är oklart om terminalerna enbart kommer att ha möjlighet att förse informationssystemet med information om aktuell transport, eller om terminalen även kan hämta information från informationssystem. Dessa terminaler är en del av informationssystemet och kommer att vara de enheter som har störst exponering. Det är därför av vikt att tydliggöra vilken funktionalitet terminalerna förväntas ha för att då kunna se till att en överenskommelse även inkluderar någon typ av säkerhetsmässiga grundkrav för dessa terminaler.

Informationssystemet kommer att ha flera intressenter utspridda i flera länder. Det innebär en stor möjlig exponering av information om transporter av farligt gods. Det finns vissa inbyggda begränsningar i vilka uppgifter och med vilken precision som dessa lämnas till myndigheter, men systemet bedöms inte kunna hantera sekretessbelagda uppgifter på ett adekvat sätt. Detta antagande stöds av Trafikanalys (2015) undersökning avseende tillgång till information om transporter av farligt gods. Om den informationen inte lämnas ut på begäran med hänvisning till sekretess kommer den sannolikt inte heller kunna publiceras i det föreslagna informationssystemet.

Om det föreslagna systemet är adekvat eller inte för tänkta intressenter såsom tillsynsmyndigheter och räddningstjänst är svårt att avgöra utifrån analyserat material. Det står däremot klart att de IT-säkerhetskrav som ställts i MoU-avtalet inte täcker in alla delar i det faktiska informationssystemet. Kravställningen av IT-säkerhet för informationssystemet bör även innefatta hela TP2:ans funktionalitet samt dess underliggande system för att skapa tilltro till hela systemet, från ursprunglig informationskälla till nyttjare.

Referenser

Defense Science Board (DSB) (2013). *Task Force Report: Resilient Military Systems and the Advanced Cyber Threat*. http://www.acq.osd.mil/dsb/reports/ResilientMilitarySystems.CyberThreat.pdf

Elliott, K. (2018). Targeted Attacks or Untargeted Attacks – Which is Most Common? *Tech Talk*, 13 september. https://techtalk.pcpitstop.com/2018/09/13/untargeted-targeted-attacks-untargeted/ [2019-01-30]

Försvarsmakten (2013). *Handbok för Försvarsmaktens säkerhetstjänst Grunder* (H SÄK Grunder)(M7745-734011). Försvarsmakten: Stockholm.

GeotransMD & Core Project (2018). *eDG Transport Document Webservices Description* (04/05/2018).

Hallberg, J., Bengtsson, J. & Karlzén, H. (2018). *Beskrivning av hot vid säkerhetsanalyser – Innehåll och utformning* (FOI-R--4676--SE). Stockholm: FOI.

Industry guidelines for the security of the transportation of dangerous goods by road (2016). http://www.cefic.org/Documents/IndustrySupport/RC%20tools%20for%20SMEs/Document%20Tool%20Box/Security%20Guidelines%20of%20the%20transport%20of%20dangerous%20goods.pdf

Lagner, R. (2013). *To Kill a Centrifuge – A Technical Analysis of What Stuxnet's Creators Tries to Achieve*. https://www.langner.com/wp-content/uploads/2017/03/to-kill-a-centrifuge.pdf

Macaskill, E. & Dance, G. (2013). NSA Files: Decoded. *The Guardian*, 1 november. https://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#section/1 [2018-05-18]

Makrushin, D. (2017). The cost of launching a DDoS attack. *Secure list*, 23 mars. https://securelist.com/the-cost-of-launching-a-ddos-attack/77784/ [2019-01-30]

MSBFS 2016:8. *Myndigheten för samhällsskydd och beredskaps föreskrifter om transport av farligt gods på väg och i terräng (ADR-S 2017)*. Stockholm: MSB.

MSBFS 2016:9. *Myndigheten för samhällsskydd och beredskaps föreskrifter om transport av farligt gods på järnväg (RID-S 2017)*. Stockholm: MSB.

Myndigheten för samhällsskydd och beredskap (MSB) (2010). *Antagonistiska hot mot transporter av farligt gods - Hot, skydd och förmåga* (MSB204). https://www.msb.se/RibData/Filer/pdf/25908.pdf

Myndigheten för samhällsskydd och beredskap (MSB) (2015). *Transportskydd - En vägledning vid transport av farligt gods på väg och järnväg* (MSB828). https://www.msb.se/RibData/Filer/pdf/27562.pdf

Myndigheten för samhällsskydd och beredskap (MSB) (2017). *Transport av farligt gods - Väg och järnväg 2017/2018* (MSB1085). https://www.msb.se/RibData/Filer/pdf/28256.pdf

Nilsson, U. & Andersson, D. (2007). *Transport av farligt gods som hotobjekt* (SP Rapport 2007:33). http://www.diva-portal.org/smash/get/diva2:962427/FULLTEXT01.pdf

Richter, M. (2017). To Pay or Not to Pay? Lessons from the Uber Cyber Attack [blogg]. *Assurance Software*, 30 november. http://www.assurancesoftware.com/product-blog/to-pay-or-not-to-pay-lessons-from-the-uber-cyber-attack [2018-12-08]

RID/ADF/ADN (2010). Who does what, version 8. *Report of the sixth session of the informal working group on telematics*. Hamburg, Tyskland 21–23 april 2010.

Riksrevisionen (2008). *Skyddet för farligt gods* (RiR 2008:29). https://www.riksrevisionen.se/download/18.78ae827d1605526e94b2e3b3/1518435492241/RiR_2008_29.pdf

Sanchez, G. (2015). *Case Study: Critical Controls that Sony Should Have Implemented*. North Bethessda (MD): SANS. https://www.sans.org/reading-room/whitepapers/casestudies/case-study-critical-controls-sony-implemented-36022 [2019-01-30]

SFS 2006:263. *Lagen om transport av farligt gods*. Stockholm: Justitiedepartementet.

SFS 2006:311. *Förordningen om transport av farligt gods*. Stockholm: Justitiedepartementet.

Skärdin, B. & Rydberg, G. (2019). *Minnesanteckningar från WG Telematics, 20181112-14* (MSB 2019-00347).

Skärdin, B. & Söderlind, G. (2019). *Lägesrapport för elektronisk information för transport av farligt gods* (MSB 2019-00347).

Svensk översättning av Industry Guidelines for the Security of the Transport of Dangerous Goods (2016). https://www.msb.se/Upload/Forebyggande/farligt_gods/Internationellt_regelarbete/Industry-security-guidelines_oversattning_Riktlinjer-2017.pdf

Trafikanalys (2015). *Möjligheter att kartlägga flöden av farligt gods i Sverige – en förstudie* (PM 2015:3). https://www.trafa.se/globalassets/pm/2011-2015/2015/pm2015_3_moejligheter_att_kartlaegga_floeden_av_farligt_gods_i_sverige_-_en_foerstudie.pdf

United Nations Economic and Social Council (UNECE) (2018). *Informal working group on telematics: meeting in London* (4–5 June 2018) (ECE/TRANS/WP.15/AC.1/2018/25). https://www.unece.org/fileadmin/DAM/trans/doc/2018/dgwp15ac1/ECE-TRANS-WP15-AC1-2018-25e.pdf

United Nations Economic and Social Council (UNECE) (2019). *Informal working group on telematics: meeting in Vienna* (12 -14 November 2018) (ECE/TRANS/WP.15/AC.1/2019/21). https://www.unece.org/fileadmin/DAM/trans/doc/2019/dgwp15ac1/ECE-TRANS-WP15-AC1-2019-21e.pdf

Valassi, C., Hunstad, A.G. & Westerdahl, L. (2019). *NCS3 – Förstudie fjärrvärme* (FOI-R--4738--SE). Stockholm: FOI.

Security in Industrial Control Systems

Nationellt Centrum för säkerhet i styrsystem för samhällsviktig verksamhet (NCS3) är ett kompetenscentrum med uppdraget att bygga upp och sprida medvetenhet, kunskap och erfarenhet om cybersäkerhetsasspekter inom industriella informations- och styrsystem. Centrumets är ett samarbete mellan de svenska myndigheterna FOI och MSB och dess verksamhet fokuserar på aktörer som äger och/eller driver samhällsviktig verksamhet där industriella informations- och styrsystem ingår.

The National Centre for increased security in industrial control systems is a centre of excellence focused at building and disseminating awareness, knowledge and experience about cyber security aspects in ICS. The Centre is a cooperation between the Swedish Defence Research Agency and the Swedish Civil Contingencies Agency and the activities is focused on actors that owns and/or operates critical infrastructure where ICS are a part.

FOI
Swedish Defence Research Agency
SE-164 90 Stockholm

Phone +46 8 555 030 00
Fax +46 8 555 031 00

www.foi.se

Swedish Civil Contingencies Agency
SE-651 81 Karlstad

Phone: +46 (0) 771-240 240
Fax: +46 (0) 10-240 56 00

www.msb.se