PROTECTED –
Security inom Kombitransporter

RAPPORT



2011-03-28

Nils Andersson
Andrée Falkenberg
Samuel Forslund
Daniel Holmbom

MariTerm AB
Tel. +46 (0)42 33 31 00
Fax. +46 (0)42 33 31 02
P.O. Box 74
SE-263 21 Höganäs
SWEDEN

www.mariterm.se

Förord

Att införa ett aktivt säkerhetsarbete blir allt viktigare i en värld där hot snabbt kan förvandlas till verklighet. Detta är ett faktum som under de senaste åren blivit allt tydligare och där effekterna utgör en negativ påverkan både på företag och för samhället i stort. Samtidigt finns det inte några konkreta svar på vilka åtgärder som ska vidtas för att ett system ska kunna anses som ”säkert”. Uppfattningarna skiljer sig åt mellan olika intressenter samtidigt som hotbilden i de flesta fall är mångfacetterad. Problematiken blir inte heller mindre komplicerad av den uppsjö av standarder och initiativ som i dagsläget präglar marknaden för säkerhet, där var och en av dessa standarder syftar till att försöka klargöra hur säkerhetsarbetet ska anpassas till förhållandet mellan hot och åtgärd.

I denna rapport försöker vi belysa omfattningen av det utbud som idag ligger till grund för möjligheten att införa aktiva handlingsplaner för bättre säkerhet. Vår förhoppning är att denna sammanställning kan vara användbar för att på ett samlat och övergripande sätt ge vägledning för strukturen kring dagens säkerhetsstandarder. Vi hoppas också att vi bidrar till att öka medvetenheten kring vikten av att skapa en gemensam samsyn för säkerhetstillämpningar ur ett globalt såväl som regionalt perspektiv.

Projektet har drivits av MariTerm AB och arbetet har möjliggjorts genom finansiering av Trafikverket inom ramen för det intermodala forskningscentrat SIR-C. Som underleverantör har MariTerm AB tagit hjälp av Företagssäkerhet AB i Kungsbacka, genom Daniel Holmbom, som därmed varit ansvarig för den del som i denna rapport benämns ”Fas 1”.

Vi vill också passa på att tacka alla inblandade parter som varit behjälpliga i arbetet med att skapa denna studie.

Höganäs 28 mars 2011

Nils Andersson
MariTerm AB

Innehållsförteckning

Sammanfattning I
Frekvens I
Godsvärde I
Transportkedjans utsatta delar II
Kända säkerhetshot samt dess sannolikhet i olika delar av transportkedjan III
Ekonomisk påverkan av säkerhetshot i olika delar av transportkedjan IV
Motåtgärder i olika delar av transportkedjan V
Vilken är orsaken till den statistiska minskningen av antalet tillgrepp? VI
Sammanställning över olika säkerhetsinitiativ VII
Avgränsning av säkerhetsinitiativ XI
Jämförelse mellan utvalda säkerhetsinitiativ XIV
Generell jämförelse XIV
Jämförelse av kriterier XV
Lämpliga standarder för respektive aktör i transportkedjan XV
Avsändare/mottagare XVI
Landsvägsterminal XVII
Kombiterminal XVIII
Hamnterminal XIX
Landstransporter XX
Sjötransport XXI
Slutsatser XXII
Olika motiv till att införa ett säkerhetsinitiativ XXII
För många säkerhetsinitiativ XXII
Samverkan för bättre effektivitet XXIII
Tillgripna godsvärdet ökar XXIII
Säkerhetshotens betydelse för verksamheten XXIII
Summary XXV
Incidence XXV
Value of cargo XXV
Vulnerable parts of the transport chain XXVI
Known security threats and their likelihood in various parts of the transport chain XXVII
Economic effects of security threats in various parts of the transport chain XXVIII
Defensive measures in various parts of the transport chain XXIX
Can the absence of information or discussion about current causation factors exacerbate problem solving? XXX

What is the reason for the statistical reduction in the number of thefts? XXX
Summary of different security initiatives XXXI
The selection of security initiatives XXXV
Comparison between selected initiatives XXXVII
General comparison XXXVII
Comparison of criteria XXXVIII
Suitable standards for each individual stakeholder in the transport chain XXXIX
Sender/receiver XXXIX
Road terminal XL
Intermodal terminal XLI
Port terminal XLII
Land transportation XLIII
Sea transportation XLIV
Conclusions XLV
Various motives to security certification XLV
Too many security standards XLV
Cooperation for improved efficiency XLVI
The value of stolen goods is increasing XLVI
The security threats' impact on business XLVI
1 Inledning 1
1.1 Bakgrund 1
1.2 Syfte 2
1.3 Avgränsning 2
1.4 Metod 2
2 Intervjuer 6
3 Kända säkerhetshot och hinder samt dess sannolikhet i olika delar av transportkedjan 8
3.1 Analyserade säkerhetshot 8
3.1.1 Stöld 8
3.1.2 Skadegörelse 9
3.1.3 Smuggling 9
3.1.4 Trafficking 9
3.1.5 Terrorism 10
3.2 Transportkedjan 11
3.2.1 Avsändare 11
3.2.2 Landsvägsterminal 12
3.2.3 Kombiterminal *(Järnvägs och kombiterminal)* 12
3.2.4 Hamnterminal 13

3.2.5 Landsvägstransport ... 14
3.2.6 Kombitransport ... 15
3.2.7 Järnvägstransport ... 15
3.2.8 Sjötransport ... 16
3.2.9 Mottagare ... 16
3.2.10 Sammanfattning ... 17
4 Ekonomisk påverkan av säkerhetshot i olika delar av transportkedjan ... 18
5 Motåtgärder i olika delar av transportkedjan ... 20
5.1 Beskrivning av tre olika strategier för motåtgärder med en enkel kostnadsbedömning. ... 20
5.1.1 Fysiskt skydd ... 20
5.1.2 Elektroniskt skydd ... 20
5.1.3 Logiskt skydd ... 20
5.2 Hur skyddas olika delar i kedjan? ... 21
5.2.1 Avsändare ... 22
5.2.2 Terminal ... 22
5.2.3 Transport ... 22
5.2.4 Sjötransport ... 23
5.2.5 Mottagare ... 23
5.2.6 Sammanfattning ... 23
6 Resultat Fas 1 ... 25
6.1 Sammanfattning av resultat ... 25
6.1.1 Frekvens ... 25
6.1.2 Godsvärde ... 25
6.1.3 Kända hot ... 26
6.1.4 Ögonblicksbild ... 26
7 Teser ... 27
7.1 Tillgreppen i transportkedjan ... 27
7.2 Orsaksanalys ... 28
7.3 Minskning av antalet tillgrepp ... 28
8 Översikt av olika säkerhetsinitiativ ... 32
8.1 100 % scanning ... 32
8.2 ADR ... 34
8.3 AEO ... 35
8.4 BASC ... 37
8.5 CSI ... 39
8.6 C-TPAT ... 41
8.7 Dutch Client System ... 43

8.8 ESSTRT 45
8.9 FAST 47
8.10 Frontline 49
8.11 Föranmälan EU 50
8.12 Föranmälan USA (Advance Manifest Regulation) 52
8.13 IATA/DGR 54
8.14 IMDG-koden 55
8.15 ISO 28000:2007 56
8.16 ISPS-kod 58
8.17 PIP 60
8.18 RID 62
8.19 SAFE Port Act 63
8.20 SECCONDD 65
8.21 Secure Export Scheme 67
8.22 Secure Trade Partnership 69
8.23 SFI 71
8.24 StairSec/Servicetrappan 73
8.25 TAPA 75
8.26 WCO-SAFE 77
9 Avgränsning för djupare analys av säkerhetsinitiativ 80
9.1 Olika typer av avgränsningar 80
9.1.1 Geografiska 81
9.1.2 Påverkan på transportkedjan 83
9.1.3 Drivkraft 87
9.1.4 Säkerhetshot som förebyggs/bekämpas 90
9.2 Val av säkerhetsinitiativ 93
9.3 Tabell 3.6 – Sammanfattning av olika säkerhetsinitiativ 98
10 Beskrivning av utvalda säkerhetsinitiativ 99
10.1 AEO, Authorized Economical Operators 99
10.1.1 Inledning 99
10.1.2 Harmonisering 99
10.1.3 Transportslag 99
10.1.4 Certifiering 99
10.1.5 Förmåner 109
10.2 TAPA 110
10.2.1 Inledning 110
10.2.2 Transportslag 110

10.2.3 Initiativ 110
10.2.4 Ingående om Freight Security Requirements 111
10.2.5 Kriterier för certifiering enligt TAPA 113
10.2.6 Förmåner 116
10.3 ISO 28000 117
10.3.1 Inledning 117
10.3.2 Harmonisering 117
10.3.3 Transportslag 117
10.3.4 Certifieringsprocess 117
10.3.5 Generella certifieringskrav 118
10.3.6 Metod för uppfyllande av mål 121
10.3.7 Fördelar 121
10.4 C-TPAT 122
10.4.1 Inledning 122
10.4.2 Kopplingar 122
10.4.3 Harmonisering 122
10.4.4 Transportslag 122
10.4.5 Certifieringsprocess 123
10.4.6 Förmåner 126
10.4.7 Fördelar för importör 126
10.5 ISPS 127
10.5.1 Inledning 127
10.5.2 Kopplingar 128
10.5.3 Transportslag 128
10.5.4 Fastställande av säkerhetsnivå 128
10.5.5 Säkerhetsnivåer 129
10.5.6 Skyddsplan 130
10.5.7 Specificerade krav för fartyg 132
10.5.8 Specifierade krav för hamnar 135
10.5.9 Förmåner 139
11 Utvärdering av olika säkerhetsinitiativ 140
11.1 Jämförelse mellan utvalda säkerhetsinitiativ 140
11.1.1 Generell jämförelse 140
11.1.2 Jämförelse av kriterier 141
11.1.3 Förklaring av punkter i jämförelse 142
11.1.4 Diskussion om generell jämförelse 144
11.1.5 Diskussion om jämförelse av kriterier 147

12 Rekommendationer av olika säkerhetsinitiativ 152
12.1 Sammanställning över transportkedjans olika aktörer 152
12.1.1 Avsändare 152
12.1.2 Terminaler 153
12.1.3 Landtransporter 154
12.1.4 Sjötransport 155
12.1.5 Mottagare 155
12.2 Rekommendationer kring säkerhetsinitiativ i olika delar av transportkedjan 156
12.2.1 Avsändare/mottagare 156
12.2.2 Landsvägsterminal 159
12.2.3 Kombiterminal (Järnvägs- och kombiterminal) 162
12.2.4 Hamnterminal 164
12.2.5 Landtransporter 168
12.2.6 Sjötransport 170
13 Slutsatser 174
Olika motiv till att införa ett säkerhetsinitiativ 174
För många säkerhetsinitiativ 174
Samverkan för bättre effektivitet 175
Tillgripna godsvärdet ökar 175
Säkerhetshotens betydelse för verksamheten 176
14 Förkortningar 177
15 Referenser 178
15.1 Publicerade källor 178
15.2 Webbsidor 179
15.3 Muntliga källor 180
Bilaga 1 – Kriminologiska teorier 182
Bilaga 2 - Intervjufrågor 185

Sammanfattning

Rapporten är uppbyggd kring följande fyra faser och dispositionen för dessa är att inleda med beskrivande innehåll för att mot slutet övergå i mer diskuterande text.

- *Fas 1* Nulägesanalys av säkerhetshot mot transportkedjan
- *Fas 2* Översikt av aktuella säkerhetsinitiativ som påverkar olika delar av transportkedjan
- *Fas 3* Beskrivning och utvärdering av utvalda säkerhetsinitiativ
- *Fas 4* Avslutande rekommendationer och slutsatser

Fas 1 Nulägesanalys av säkerhetshot mot transportkedjan

I denna del beskrivs den nulägessituation som råder avseende de säkerhetshot som i dagsläget riktas mot transportkedjan. Däribland presenteras brottsstatistik och beskrivningar över de olika typer av brott som transportörer och andra logistikaktörer utsätts för.

Frekvens

Antalet tillgrepp (stöld ur eller stöld av lastbärare) minskar något år för år. En minskning återfinns i antalet polisanmälda transportrelaterade brott[1], vilka i princip enbart är mätbara år 2007 - 2008 på grund av ändringar i polisens brottskodning. Det till antalet få år där säker statistik finns på området gör att det är svårt att dra kvalitativa slutsatser, dock syns en trend. Även de i projektet deltagande organisationerna ser/uppfattar en viss minskning av nämnda brott, se vidare diskussion om orsaker i avsnitt 7.3.

Totala antalet brott under år 2008: 2140 st
Totala antalet brott under år 2007: 2377 st

- 70% av brotten sker mellan klockan 22.00 – 06.00 (Sverige)
- 81% av brotten riktades mot oskyddade lastbärare (Sverige)

Godsvärde

Det som däremot oroar i sammanhanget är att det totala tillgripna godsvärdet ökar[2], och en nästan 100% ökning syns härvid (år 2007 till år 2008). Orsaken till denna ökning kan förklaras inom tre områden:

[1] Polisens rapport om transportsäkerhet 2008, Per-Arne Nilsson, Polismyndigheten i Västra Götaland
[2] Godsvärdesanalys 2008, Projekt Transportsäkerhet, Upprättad av Riskhanterings Akademin

- Förbättrade anmälningsrutiner hos polismyndigheterna samt inom branschen.
- Kriminaliteten har blivit mer kompetent genom att organiserade ligor genomför brotten.
- Ökat antal stulna ekipage (hel godsbärare).

Beroende på vilket vis som beräkningarna samt antagandena utförs, kommer man till slutsatsen att mellan 52 och 293 miljoner SEK tillgrips under någon del transportkedjan i Sverige årligen.

Transportkedjans utsatta delar

70 – 80 % av tillgreppen går statistiskt sett att härleda till en oskyddad plats alternativt ett oskyddat ekipage. Således höjs motivationen hos en potentiell gärningsman på grund frånvaron av mekaniska/fysiska skyddsanordningar (kriminologiskt sett är det frånvaron av en kapabel väktare).

Följande graf påvisar att där ett gott skydd finns, minskar riskerna för säkerhetshot. Grafen åskådliggör den statistik som finns inom området, samt de intervjuade organisationernas uppfattningar. Linjen motsvarar aktuell säkerhetsnivå i respektive del av transportkedjan. Angreppen inträffar vanligast där grafens färg är som mörkast.

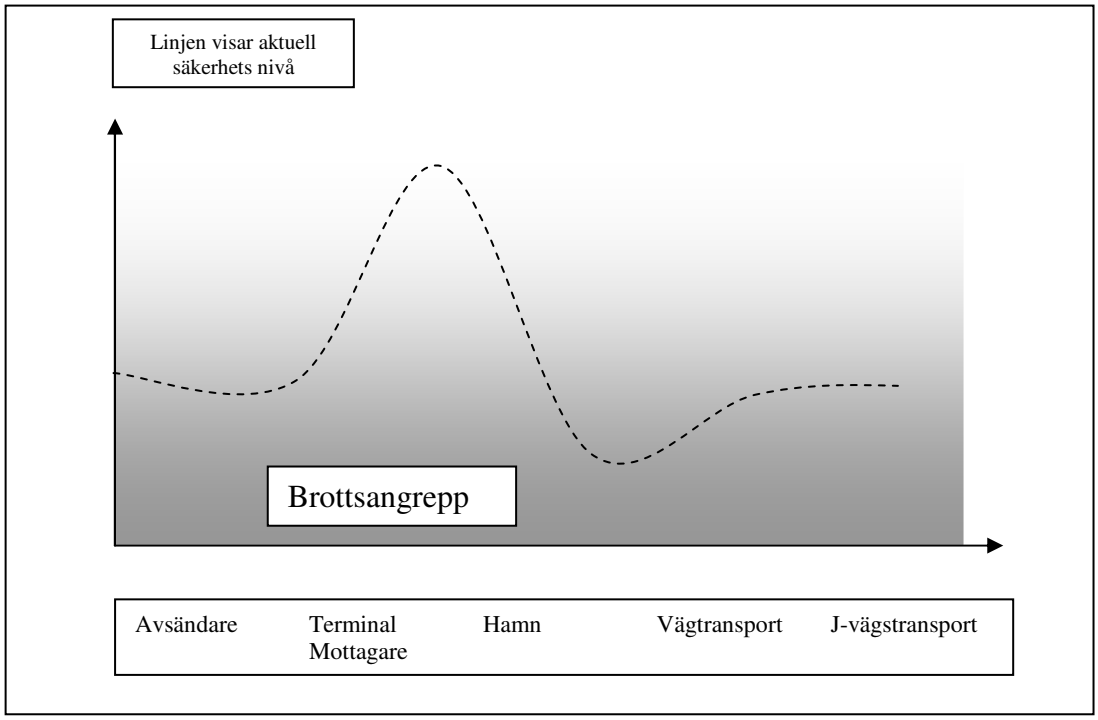


Diagram 4 - Förhållandet mellan säkerhetsnivå och risk för säkerhetshot i olika delar av den intermodala transportkedjan

Kända säkerhetshot samt dess sannolikhet i olika delar av transportkedjan

Matrisen nedan åskådliggör en kvalitativ sannolikhetsbedömning över risker/hot mot transportkedjan, som är aktuell i detta projekt. I bedömningen har det tagits hänsyn till statistikunderlag samt till resultaten från de intervjuer som genomförts. De kända hoten som beskrivits i projektet är: stöld, skadegörelse, smuggling, trafficking samt terrorism.

Bedömningskriterierna har utgått från skala 1-5 där fem är det mest sannolika och där således ett är minst sannolikt.

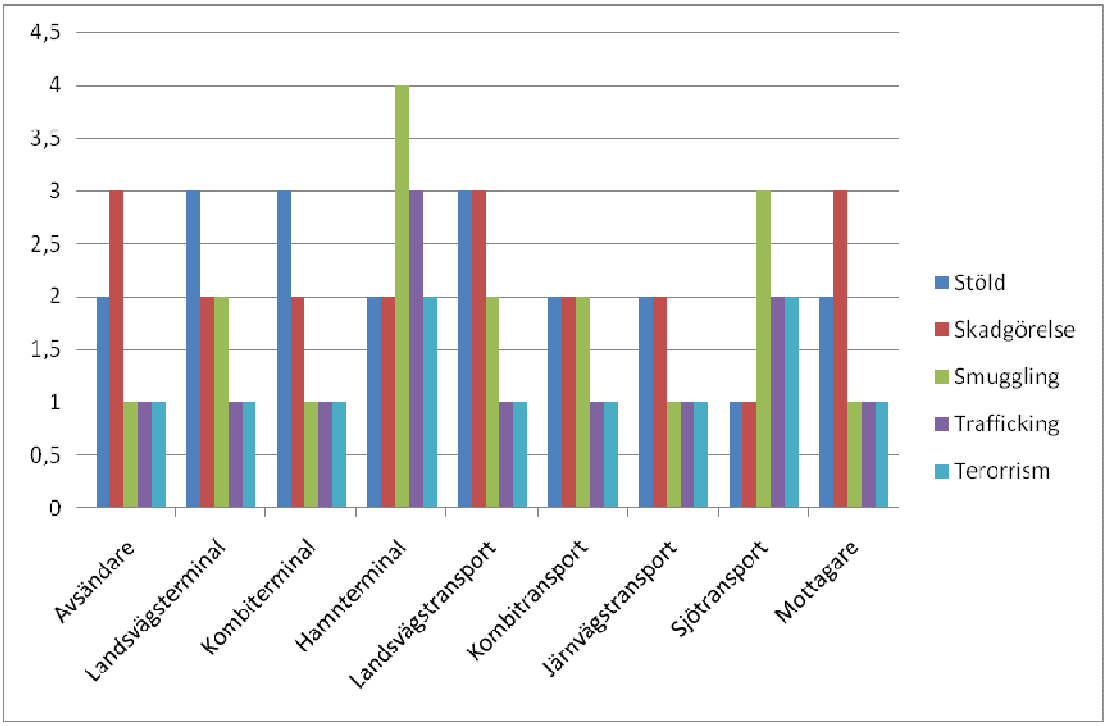


Diagram 1 - Sannolikheten för olika säkerhetshot i en intermodal transportkedja

Ekonomisk påverkan av säkerhetshot i olika delar av transportkedjan

Diagrammets staplar visar den ekonomiska effekt tillgreppen utgör, variablerna är satta mellan ett och fem där 1 är lägst (knappt märkbar påverkan) och där 5 är högst (extrem påverkan).

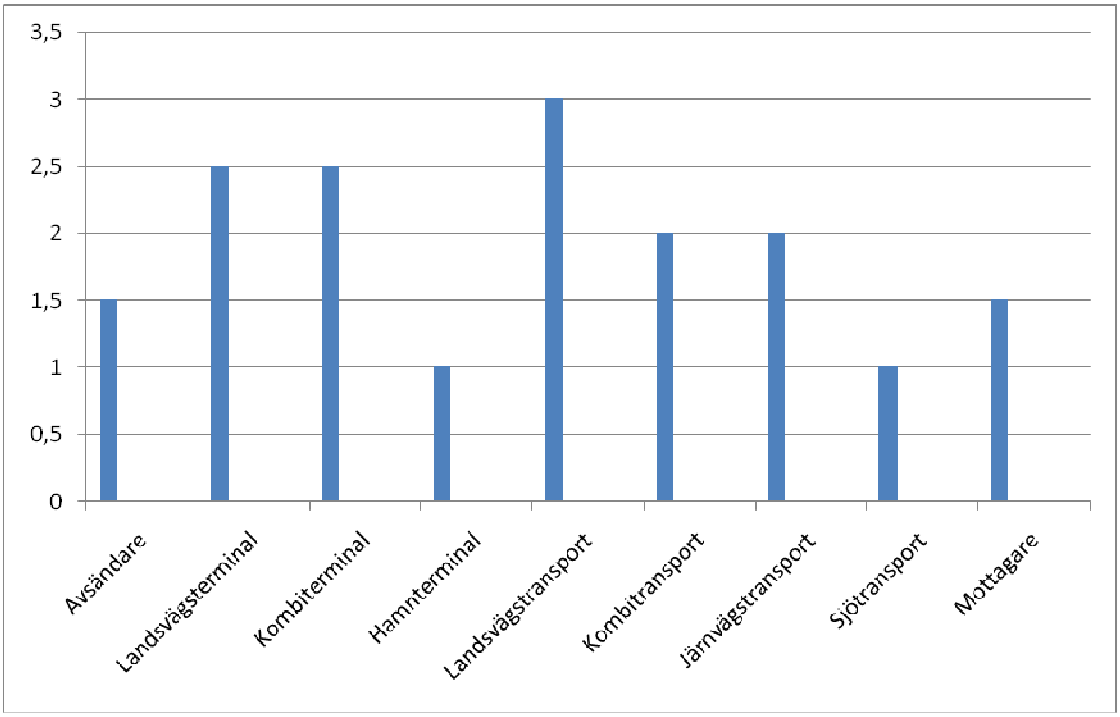


Diagram 2 - Ekonomisk påverkan av säkerhetshot i olika delar av en intermodal transportkedja

Motåtgärder i olika delar av transportkedjan

Nedanstående diagram är en kvalificerad bedömning över vilka ekonomiska medel som satsas inom vilken del av transportkedjan. Staplarna är ej säkerställda utifrån området 0 till 3, utan bör ses som jämförbara sinsemellan med intervallen låg 1, medel 2 eller hög 3. Höjden på staplarna samt förhållandet dem emellan, påvisar vilka skillnader som föreligger.

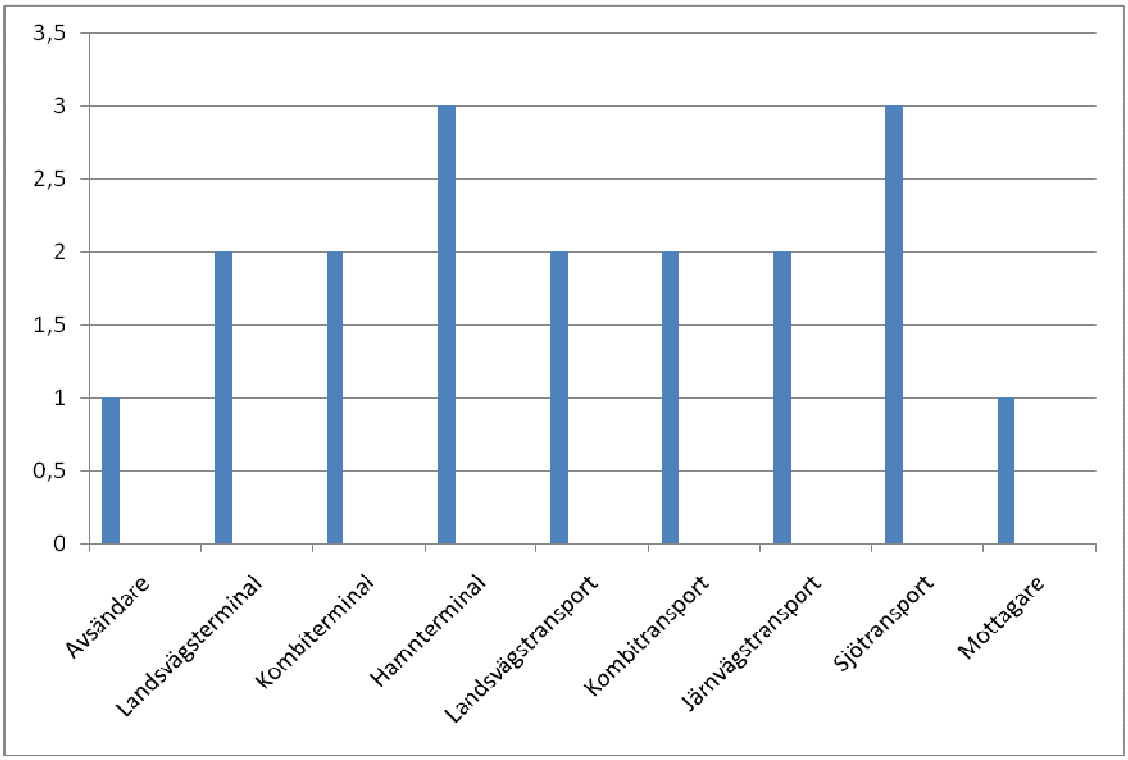


Diagram 3 - Ekonomiska medel som satsas på att motverka säkerhetshot i olika delar av en intermodal transportkedja

Vilken är orsaken till den statistiska minskningen av antalet tillgrepp?

Svar: Den statistik som polisen levererar till samhället bygger enkom på brott som kommit till polisens kännedom. Detta medför att den inte till 100 % återspeglar verkligheten och ett mörkertal finns som skapas både inom polisens såväl som inom branschens led. För att kommentera orsakerna kort kan nämnas, att det ofta är svårt för transportören att veta exakt vilket gods som tillgripits eller att gränsen mellan stöld, skadegörelse eller godsskada kan vara svår att överblicka. Tidspress är ett annat skäl till varför tillgrepp ibland inte anmälts eller att det stulna beloppet inte motsvarar kostnaden för en egen självrisk. Således återfinns ett mörkertal[3] i detta sammanhang.

En bedömning är att de två största orsakerna till minskningen av tillgrepp är:

- att polismyndigheten i Skåne, Halland, Jönköping och Kronobergs samt Västra Götalands län har fokuserat på området och bildat en samverkansgrupp. Detta arbete har lett till en ökad tvärsektoriell samverkan mellan polis och hela transportbranschen, där man genom seminarier och workshops ökar intresset för frågorna och där det uppnåtts en ökad kunskap om problembild samt relevanta skyddsåtgärder. Även tillverkare (Volvo Lastvagnar och Scania) har tagit till sig kunskap och förändrat exempelvis lås och säkerhet.
- att en ökad professionalism bland förövarna skapar färre antal tillgrepp, om än med betydligt högre ”träffsäkerhet” och därigenom ett ökat godsvärre per tillgrepp.

[3] Kvoten mellan den faktiska och den registrerade brottsligheten.

Fas 2 Översikt av aktuella säkerhetsinitiativ som påverkar olika delar av transportkedjan

I denna del presenteras en beskrivning över de säkerhetsinitiativ som i dagsläget kan tillämpas för att försvåra brottshandlingar mot transportkedjan.

Sammanställning över olika säkerhetsinitiativ

Följande är en översikt av utvalda säkerhetsinitiativ. Valda utifrån dels vilken påverkan de har för godstransporter från Sverige och dels hur de påverkar flödena av gods i världen. Vissa beskrivs också med syftet att erhålla en mer komplett översikt. En del av initiativen har tagits i kraft, andra är under utveckling och bedrivs som pilotprojekt medan några initiativ är rena forskningsprojekt.

Ett gemensamt mål är att genom tekniska lösningar, regler/krav och samarbete, utveckla säkerheten i godstransporter samtidigt som den fria kommersiella världshandeln kan fortgå och utvecklas både i effektivitet och kvantitet.

Den övervägande delen av de beskrivna säkerhetsinitiativen initierades som en reaktion på terrorattentatet mot USA 9/11 2001. Även om logistikkedjan i sig inte var inblandad den gången väcktes en oro för vad legitima godstransporter skulle kunna utnyttjas för i terroristsammanhang. Massförstörelsevapen skulle kunna smugglas i containers på fartyg eller i landtransporter (järnväg och väg).

Den globala och interkontinentala transportkedjan i sig kan vara mål för terrorism vilket skulle få enorma ekonomiska konsekvenser och påverka den globala världshandeln.

Många säkerhetsinitiativ initierade i USA har gemensamt att det primära målet är förhindrande av terrorattentat. Det medför däremot att andra illegala aktiviteter också förhindras såsom smuggling, trafficking osv.

The *SAFE Port Act* är en lag som trädde i kraft 2006 och var dåvarande administrationens svar på det ökade terroristhotet. Innebörden är att varje hamn har ansvarsskyldighet för den egna och landets säkerhet. Den behandlar åtgärder som bör införas för att stärka det maritima säkerhetsskyddet. Lagen har kopplingar till *C-TPAT, CSI, SFI* och *100% scanning*.

CSI, Container Security Initiative, är inriktat på ökad säkerhet i den maritima transportkedjan. Initiativet påverkar skeppning av gods till USA och därtill hörande hantering i hamnterminaler. Den grundläggande tanken är att flytta en del av kontrollarbetet till den hamn där lastning av fartyget sker. Målet är att förhindra att massförstörelsevapen etc. når amerikanskt territorium, där det kan orsaka massiv skada redan i hamnområdet och på fartyg nära land.

SFI, Secure Freight Initiative, har många likheter med *CSI*. Målet med *SFI* är till skillnad från *CSI* att fler än bara de containers som bedöms som högriskgods ska skannas. Skanningen utlokaliseras till utländsk hamn och full implementering har skett i några ”pilothamnar”.

100% scanning, är ett initiativ som likt CSI och *SFI* behandlar skanning av godscontainers för att upptäckta farligt material såsom radioaktivt material. Från juli 2012 ska allt gods som anländer till USA ha skannats innan lastning på fartyg, alternativt vid ankomst. I den nya Commission Act från 2007 är målet skärpt och kravet är att skanning av gods ska ske innan lastning på fartyg.

Strategin i *C-TPAT, Customs-Trade Partnership Against Terrorism*, är att jobba alltmer förebyggande med säkerhetsarbetet innan godset anländer fysiskt till gränskontrollen. Det sker bland annat genom att tidigt i logistikkedjan analysera tillgänglig transportinformation och rikta in arbetet på gods som bedöms utgöra hög risk. Fokus ligger på ett involverande av aktörerna i transportkedjan i säkerhetsarbetet och en certifiering av dessa.

Advance Manifest Regulation, påverkar gods som exporteras till USA och utgör krav på att en elektronisk föranmälan av gods ska skickas in till CBP (U.S. Customs and Border Protection) senast 24 timmar innan lastning på fartyg med USA som destination (med vissa undantag).

Hittills nämnda amerikanska säkerhetsinitiativ påverkar alla globala transporter med USA som mottagare eller transitland.

FAST:s, Free and Secure Trade:s, inriktning är att förenkla transport av gods mellan USA, Kanada och Mexicos gränser samtidigt som säkerheten stärks för försvårande av smuggling och terrorism. Landsvägstransporter påverkas. Omfördelning sker av tullmyndigheternas resurser från att omfatta den större delen av allt gods till koncentration av kontroller till högrisksändningar. Det är möjligt genom samarbete med och certifiering av aktörerna i logistikkedjan inklusive de enskilda chaufförerna.

Många länder har likt USA ett eller flertalet säkerhetsinitiativ som påverkar transport av gods över gränserna med fokus på import. Australiens *Frontline*, Kanadas *PIP*, Nya Zeelands *Secure Export Scheme*, Singapores *Secure Trade Partnership*, Nederländernas *Dutch Client System* och Sveriges *StairSec/Servicetrappan* är de exempel som presenteras översiktligt i denna rapport.

Frontline, är den australiensiska tullmyndighetens program som initierades 1991 vars huvudsakliga mål är försvårande av kriminell aktivitet över Australiens gränser gällande både import och export. Till skillnad från de flesta andra initiativ världen över syftar *Frontline* till att stärka säkerheten inom områden från smuggling av droger, djur etc. till trafficking och pengatvätt. Detta sker genom samarbete med företag på frivillig basis.

Kanadas *PIP, Partners In Protection*, togs i likhet med *Frontline* i kraft 1995 redan innan terrorattentaten 2001. Det huvudsakliga syftet förövrigt var att främja företagens medvetenhet och efterlevnad av de dåvarande tullreglerna som var mycket

tuffa. Kriminellt utnyttjande av legitima godstransporter kunde drabba åkerierna hårt eftersom transportmedel som användes för smuggling fick beslagtas. Det första *PIP* initiativet var därför en önskan från företagens sida att utöka samarbetet med tullen för att på så sätt ha ett upparbetat förtroende att falla tillbaka på om dess transporter skulle utsättas för kriminella handlingar. Efter 9/11 förändrades kraven på Kanadas tullmyndighets arbete och ett nytt program initierades 2008 med samma namn. Det nya säkerhetsinitiativet utformades för att vara kompatibelt med *C-TPAT* vilket underlättar samarbete länderna emellan och underlättar transporter.

Secure Export Scheme är den Nya Zeeländska tullens program med inriktning på att förbättra säkerheten i logistikkedjan genom att öka effektiviteten i tullarbetet och underlätta för landets exportföretag att verka på den globala arenan. *Secure Export Scheme:s* är kompatibelt med internationella krav såsom WCO:s standarder.

Singapore är ett nav i världshandeln och dess säkerhetsinitiativ *Secure Trade Partnership* har som mål att värna den positionen. Det arbete som bedrivs av Singapores tull är av högsta vikt för säkerheten i den globala logistikkedjan. Medlemskap innebär, förutom lättnader, färre antal kontroller av tullen, överensstämmelse med internationella standarder.

Dutch Client System är de nederländska tullmyndigheternas interna program som syftar till att bedöma transportkedjans aktörers tillförlitlighet och vilket säkerhetshot transporterna utgör. Med hjälp av riskanalys avgörs vilken typ av transportkontroll som bör ske. Kopplingen till *AEO* är stark och från 2007 kan holländska företag genom *Dutch Client System* söka AEO-status (tullen står för certifieringsförfarandet).

Servicetrappan är ett program som togs i kraft 2002 i Sverige med drivkraften att förenkla och kvalitetssäkra tullhanteringen. Tullens arbete skulle inriktas på företag som löper en hög risk för att utnyttjas i olaglig verksamhet. Efter certifiering i olika steg (därav servicetrappan) erhålls lättnader i företagens tullhantering. *Stairsec* utvecklades under 2003 som Servicetrappans säkerhetsprogram men avvecklades i slutet av 2010 som ett led i ett utökat samarbete mellan tullmyndigheterna inom EU och säkerhetsinitiativet *AEO*.

AEO, Authorized Economical Operators, är ett av tullmyndigheterna i EU gemensamt initiativ skapat för att införa enhetliga riktlinjer gällande hantering och kontroll av godsflöden. Kompabilitet finns med de närliggande standarderna *WCO-SAFE* och *ISO 28000. AEO* ger certifierade företag tillgång till förenklingar i tullhanteringen. AEO-status söks i företagets hemland men gäller i hela EU. Kraven för att erhålla AEO-status är detaljerade och tuffa krav ställs på aktörens säkerhetsåtgärder både praktiska och gällande tullhanteringen.

Föranmälan EU, är även det ett i EU gemensamt initiativ med målet att försvåra kriminell aktivitet över EU gemenskapens yttre gräns. I korthet måste import av gods till EU föranmälas med en viss bestämd tidsfrist beroende på transportslag.

Arbetet med säkerheten inom logistikområdet går mot en allt större internationalisering med säkerhetsstandarder på en global nivå med *ISPS-koden*, *WCO-SAFE* och *ISO 28000*. De nationella initiativen (även i samarbeten som EU) anpassas efter de globala programmen men även efter andra säkerhetsinitiativ med genomslagskraft, ofta med USA som initiativtagare.

ISPS-koden, *International Ship and Port Facility Security Code*, är IMO:s (International Maritime Organization) program med syftet att minska risken för att sjötransporter används direkt eller indirekt vid genomförande av terrorattacker. Den är utformad som grundläggande krav och rekommendationer som alla länder bör uppfylla och implementera.

WCO, World Customs Organization, har som verksamhetsmål att underlätta den globala handeln genom att etablera gemensamma mål och regler. Säkerhetsfrågan har blivit allt viktigare och WCO:s ramverk för detta är *SAFE* med mål att bland annat; flytta fokus på säkerhetsarbetet från importerande till exporterande land, införa internationella standarder för att främja säkerheten i transportkedjan på en global nivå, anpassa existerande regler för den nya tidens utmaningar m.m.

ISO 28000 är en standard som togs i kraft 2007 och är utarbetad för att öka säkerheten i leveranskedjan. Standarden är inriktad på att ge övergripande riktlinjer för ledning av frågor gällande säkerhet för internationella transporter. Ett uppfyllande av *ISO 28000* ger en bra grund för certifiering enligt andra säkerhetsinitiativ som exempelvis *ISPS-koden, AEO, C-TPAT* med flera.

Initiativtagare till de hittills nämnda initiativen är staten, statliga tullmyndigheter och internationella sammanslutningar av länder och dess resp. myndigheter. I tillägg till dessa presenteras en överblick av två säkerhetsinitiativ, *BASC* och *TAPA*, som sammanslutningar av företag står bakom.

BASC, the Business Alliance for Secure Commerce, är ett säkerhetsinitiativ skapat av en sammanslutning av aktörer i Sydamerika. Det har som mål att genom samarbete mellan företag och myndigheter effektivt motverka smuggling av illegitima varor i lagliga godstransporter. Med tiden har det utvecklats till ett komplett system för hantering av säkerhetsfrågor med konkreta krav på säkerhetsåtgärder.

TAPA, the Technology Asset Protection Association, är ett initiativ fokuserat på att öka säkerheten för lastbilstransporter och då som främsta drivkraft att minska antalet stölder. Initiativtagare är en sammanslutning av företag inom produktion och transport av främst högt värderat gods och varor.

Presenteras görs också två säkerhetsinitiativ som närmast kan beskrivas som rena forskningsprojekt *ESSTRT* och *SECCONDD*.

ESSTRT, European Security: High Level Study on Threats, Responses and Relevant Technologies, är en studie som utförts åt EU kommissionen av försvarskoncernen Thales, med syftet att analysera hoten mot den Europeiska säkerheten och föreslå åtgärder för att förbättra densamma med fokus på metoder att förhindra terrorism.

SECCONDD, Secure Container Data Device standardisation, är ett forskningsprojekt med inriktning på att göra containerhantering säkrare. Det syftar främst till möjligheterna att kontrollera om containerns innehåll har förändrats under transporterns väg.

I rapporten presenteras också några av föreskrifterna/säkerhetsinitiativen för transport av farligt gods. Sedan ca 5 år tillbaka har det dock tillkommit regler i föreskrifterna för transportskydd, med syftet att minimera stöld eller obehörigt förfarande med farligt gods, som kan skada personer, egendom eller miljö.

ADR, RID, IMDG-koden och *IATA/DGR* är samtliga byggda på rekommendationer som en expertkommitté inom FN:s ekonomiska och social råd (ECOSOC) arbetar fram.

Fas 3 Beskrivning och utvärdering av utvalda säkerhetsinitiativ

I fas 3 görs ett urval av de standarder som blev beskrivna under fas 2 i syfte att på ett mer detaljerat och ingående sätt förklara innebörden av dessa standarder.

Avgränsning av säkerhetsinitiativ

I projektets fas 2 finns en översikt där 26 olika säkerhetsinitiativ är kortfattat beskrivna. Målet med projektets fas 3 är att göra ett urval av dessa initiativ och detaljstudera dem.

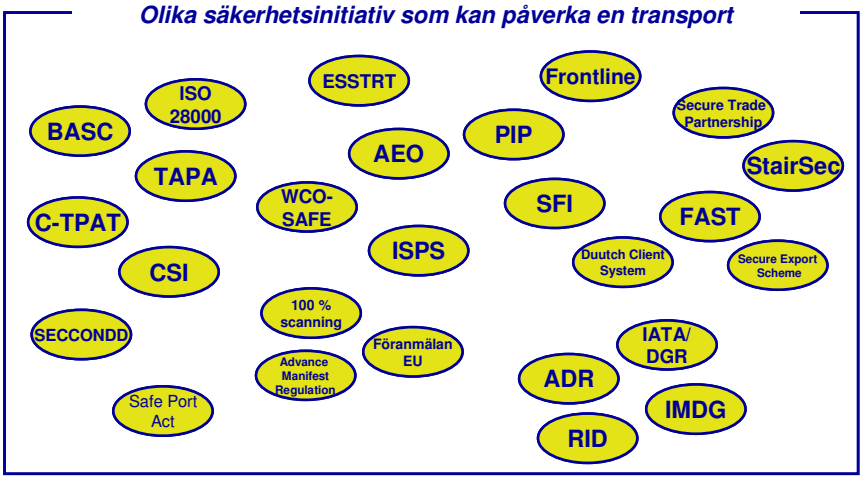


Bild 2.1 – Olika säkerhetsinitiativ som kan påverka en transport

Målet för urvalet har varit att säkerhetsinitiativen i första hand ska beröra kombitransporter inom EU, då det är ett övergripande mål för V-FUD SirC. För att göra detta urval har fyra typer av avgränsningar analyserats:

- *Geografiska:* Säkerhetsinitiativet ska vara verksamt i Europa
- *Påverkan på transportkedjan:* Säkerhetsinitiativet ska påverka så många delar av transportkedjan som möjligt
- *Drivkraft:* Önskvärt är om säkerhetsinitiativet leder till någon form av förenkling eller effektivisering
- *Vilka säkerhetshot som förebyggs/bekämpas*: Säkerhetsinitiativet ska helst täcka de olika säkerhetshoten.

Varje avgränsning har analyserats och resultatet presenteras i olika tabeller och bilder som visar vilka samband mellan olika säkerhetsinitiativ det kan finnas inom de olika avgränsningarna.

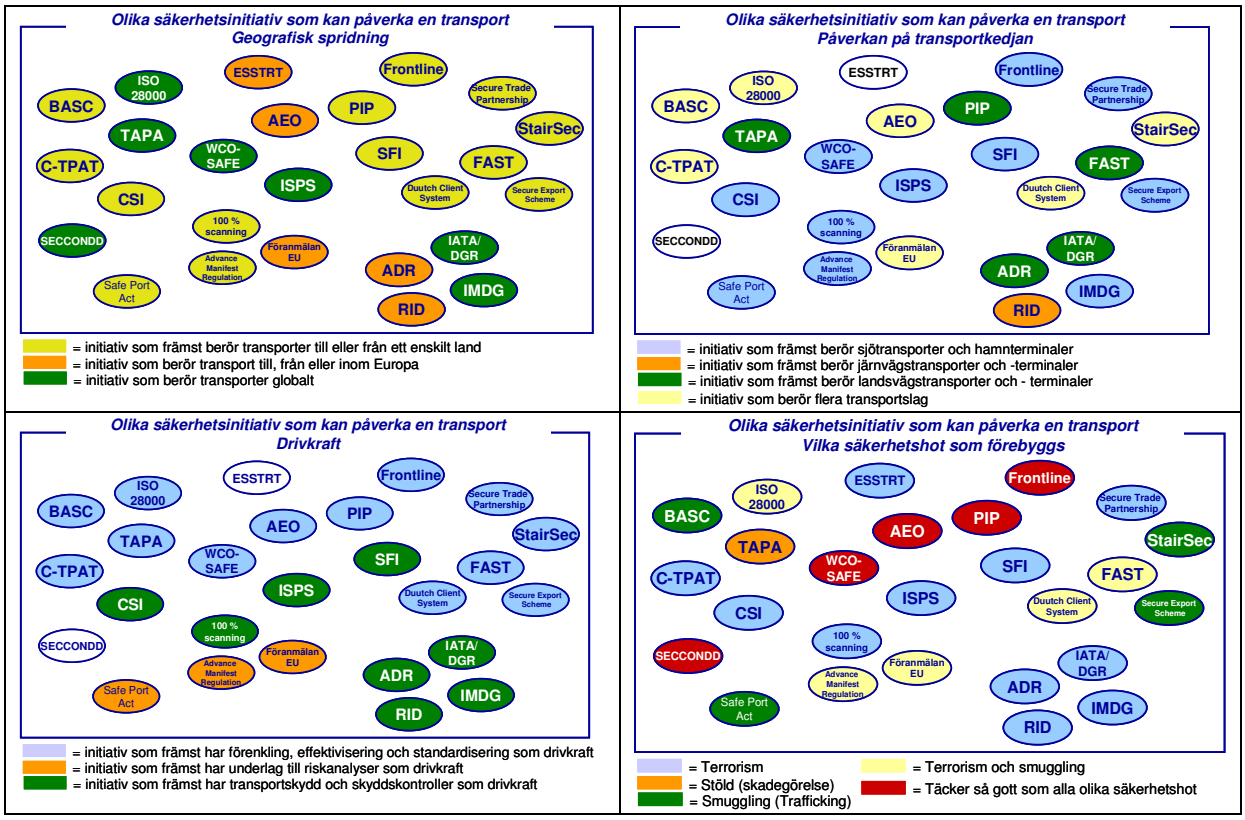


Bild 2.2 – Olika typer av avgränsningar

En analys avslutade urvalsproceduren och denna sammanfattas i tabellen till höger. Analysen gav att tre av säkerhets-initiativen, AEO, ISO 28000 och WCO-SAFE täcker samtliga fyra avgränsningar. Av dessa tre initiativ valdes WCO-SAFE bort på grund av de starka kopplingarna till och likheterna med AEO. AEO valdes på grund av sin adekvata geografiska spridning.

Som referens till dessa två initiativ, *AEO* och *ISO 28000*, valdes ytterligare tre initiativ ut; *C-TPAT, ISPS* och *TAPA*.

Säkerhetsinitiativ	**Avgränsning**				
	Geografisk	**Påverkan på trpkedjan**	**Drivkraft**	**Inblandade säker-hetshot**	**Antal som täcker målen**
100 % scanning					
ADR	X				1
AEO	X	X	X	X	4
BASC		X	X		2
CSI					
C-TPAT					
Dutch Client System		X	X		2
ESSTRT	X	(X)	X		2
FAST					
Frontline			X	X	2
Föranmälan EU	X	X	X		3
Föranmälan USA					
IATA/DGR	X				1
IMDG-kod	X				1
ISO 28000:2007	X	X	X	X	4
ISPS-kod	X				1
PIP			X		1
RID	X				1
SAFE Port Act					
SECCONDD	X	(X)		X	2
Secure Exporte Scheme			X		1
Secure Trade Partnership			X		1
SFI					
StairSec		X	X		2
TAPA	X				1
WCO-SAFE	X	X	X	X	4

Jämförelse mellan utvalda säkerhetsinitiativ

I nedanstående tabell har ett antal kriterier sammanställts för att kunna möjliggöra jämförelse mellan de olika säkerhetsinitiativen. Tabellen har delats in i två avsnitt där den första delen beskriver de övergripande kriteriegrunderna medan den andra delen är inriktad mot beskrivningen av de specifika åtgärder som respektive standard täcker.

Generell jämförelse	**AEO**	**C-TPAT**	**TAPA**	**ISPS***	**ISO**
Allmänt om certifiering					
Erhållande av direkta förmåner i tullhantering	x				
Tillgänglig för aktörer globalt	x	x	x	x	x
Statlig eller överstatlig initiativtagare	x	x			
Inriktning på gods					
Globalt gods			x	x	x
Import till USA		x			
Import och export EU	x				
Säkerhetshot som primärt ska förebyggas					
Terrorism	x	x		x	x
Stöld	x		x		
Smuggling	x			x	x
Trafficking	x				
Transportslag					
Lastbilstransporter	x	x	x		x
Tåg	x	x			x
Flyg	x	x			x
Fartyg	x	x		x	x
Kopplingar till utvalda initiativ					
AEO			x		x
C-TPAT					
TAPA	x				
ISPS					
ISO	x				

Jämförelse av kriterier	AEO	C-TPAT	TAPA	ISPS*	ISO
Lokaler och områden					
Skydd av lokaler (perimetersäkerhet såsom stängsel, lås osv.)	x	x	x	x	x
Övervakning av lokaler (exempelvis kameraövervakning)		x	x	x	x
Bemanning eller bevakning av olåsta portar och accesspunkter till område	x	x	x	x	
Tillträdeskontroll	x	x	x	x	x
Godshantering					
Användande av tekniska lösningar för att hindra olovligt handhavande av gods (användning av högsäkerhetssigill, utrustning för stillastående fordon m.m)		x	x	x	
Rutiner för kontroll av inkommande gods med avseende på att gods är registrerat i logistiksystemet	x	x	x	x	x
Kontroll av sigill på inkommande gods	x	x		x	x
Separat förvaring av olika typer av gods (exempelvis utländskt-, högvärdes-, farligt gods m.m.)	x	x	x		x
Användande av tekniska lösningar för att spåra/följa gods					
Kvalitétsinspektion av packning (om denna sker hos extern part)	x				x
Lastning av gods					
Övervakning under lastning av gods i lastbärare av aktörens personal	x		x		
Rutiner för hur utgående gods förseglas och hur detta kontrolleras	x				x
Kontroller över att gods som lastas matchar godsdokumentation		x	x	x	
Personal					
Rekrytering och avveckling av personal (bakgrundskontroller, intervjuer med personal som lämnar företaget osv.)	x	x	x		x
Utbildning av personal (fortlöpande utbildning i säkerhetsfrågor, riskmedvetande osv.)	x	x	x		x
Informationsspridning (intern och extern information om företagets/aktörens säkerhetsrutiner)		x		x	x
Informationssäkerhet					
Kvalitetssäkring för data och informationssystem		x			x
Skydd av affärsinformation	x	x	x		x
Informationsutbyte med tullmyndigheterna	x	x			x
Nätverk och affärssystem					
Säkerhetshanteringssystem (definierade och dokumenterade säkerhetsförfaranden, interna och externa säkerhetsrevisioner osv.)	x	x			x
Utvärderingssystem för affärspartners (leverantörer, samarbetspartners, kunder)		x	x		x
Etablering av samarbete med tullmyndigheter eller andra myndigheter som utövar gränskontroller. Förfarande för att anmäla avvikelser eller olaglig aktivitet.	x	x	x	x	x

Fas 4 Avslutande rekommendationer och slutsatser

I denna fas presenteras rekommendationer kring vilka standarder som genom projektet har ansetts vara mest lämpliga att tillämpa för varje enskild aktör i transportkedjan.

Lämpliga standarder för respektive aktör i transportkedjan

För att bedöma i vilken utsträckning respektive aktör inom transportkedjan kan tillämpa de utvalda säkerhetsinitiativen, har en översiktlig kartläggning genomförts. Sammanställningen har utgått från ett urval kriterier som för varje enskild intressent har bedömts som särskilt betydelsefulla, vilka därtill har ställts i relation till de standarder som projektet valt att fokusera på. I huvudsak har den standard som uppfyllt flest kriterier också varit den standard som visat sig bäst lämpad för certifiering av den aktuella verksamheten. Det har dock förekommit situationer då även andra aspekter varit nödvändiga att väga in i resonemanget, vilket då oftast har gett upphov till ett annat resultat. En kostandsjämförelse har också sammanställts

genom utformningen av nedanstående beräkningsmodell. Maximal kostnad motsvarar 6 poäng och minimal kostnad motsvarar 0 poäng.

	Låg	Medel	Hög	
Logiskt skydd	0	1	2	
Elektroniskt skydd	0	1	2	
Fysiskt skydd	0	1	2	
Summa	**0**	**3**	**6**	**Poäng**

Avsändare/mottagare

Kriteriegrunder

	AEO	TAPA	ISO
Kriteriegrund			
Säkerhetshot som primärt ska förebyggas - Stöld	X	X	
Skydd av lokaler	X	X	X
Övervakning av lokaler		X	X
Bemanning och/eller bevakning accesspunkter	X	X	
Tillträdeskontroll	X	X	X
Användande av tekniska lösningar för att hindra olovligt handhavande av gods		X	
Kontroll av sigill på inkommande gods	X		X
Övervakning under lastning av gods i lastbärare av aktörens personal	X	X	
Rutiner för hur utgående gods förseglas och hur detta kontrolleras	X		X
Kontroller över att gods som lastas matchar godsdokumentationen		X	
Rekrytering och avveckling av personal	X	X	X
Utbildning av personal (fortlöpande utbildning i säkerhetsfrågor, riskmedvetande)	X	X	X
Skydd av affärsinformation	X	X	X
Sammanställning – täckning av kriterier			
Summa	**10**	**11**	**8**

Kostnadsbild

	Låg	Medel	Hög	
Logiskt skydd	0	0	0	
Elektroniskt skydd	0	1	0	
Fysiskt skydd	0	1	0	
Summa poäng	**0**	**2**	**0**	**2**

Enligt tabellen framgår det att TAPA täcker flest kriterier av de utvalda säkerhetsinitiativen. Det ska samtidigt påpekas att detta resultat troligen följer av att TAPA är anpassad till de förutsättningar som gäller för aktörer som har stark koppling till varuintresset. TAPA är på så sätt ett initiativ som ska förstärka dessa aktörers möjligheter till att försvara rätten till godset och därmed minska förekomsten av bland annat stölder. Trots att TAPA uppfyller flest kriterier ska det noteras att det även finns begränsningar såsom exempelvis bristen på kompabilitet för tillämpning på intermodala transporter. TAPA är endast utvecklad för att hantera gods som transporteras med lastbilstransporter och detta försvårar kraftigt möjligheten till global distribution. I detta perspektiv kan det därför spekuleras i huruvida det kan bli mer ekonomiskt lönsamt att istället tillämpa AEO, då denna certifiering skulle innebära att samtliga intermodala transportslag blir tillämpbara. Nackdelen med AEO kan dock å

andra sidan bestå i bristen på förstärkta åtgärder mot intrång i aktuell lastbärare, exempelvis genom utebliven tillämpning av högsäkerhetssigill.

Avsändaren bör genom detta resonemang överväga att antingen införa AEO eller TAPA, beroende på vilka kriterier som väger tyngst i respektive fall. Karaktären kring avsändarens verksamhet är därför avgörande i bedömningen av vilket av dessa alternativ som har bäst förutsättningar för effektiv tillämpning. Steget mot att istället införa ISO 28000 anses vara alltför stort då denna standard inte föreskriver några direkta åtgärder för att minska risken för stöld eller handling som utgör motsvarande intrång på avsändarens godsintresse.

Landsvägsterminal

Kostnadsbild

	Låg	Medel	Hög	
Logiskt skydd	0	1	0	
Elektroniskt skydd	0	0	2	
Fysiskt skydd	0	1	0	
Summa poäng	**0**	**2**	**2**	**4**

Kriteriegrunder

	AEO	TAPA	ISO
Kriteriegrund			
Säkerhetshot som primärt ska förebyggas - Stöld	X	X	
Skydd av lokaler	X	X	X
Övervakning av lokaler		X	X
Bemanning och/eller bevakning accesspunkter	X	X	
Tillträdeskontroll	X	X	X
Användande av tekniska lösningar för att hindra olovligt handhavande av gods		X	
Rutiner för kontroll av inkommande gods med avseende på att gods är registrerat i logistiksystemet	X	X	X
Kontroll av sigill på inkommande gods	X		X
Separat förvaring av olika typer av gods	X	X	X
Övervakning under lastning av gods i lastbärare av aktörens personal	X	X	
Rutiner för hur utgående gods förseglas och hur detta kontrolleras	X		X
Kontroller över att gods som lastas matchar godsdokumentationen		X	
Rekrytering och avveckling av personal	X	X	X
Utbildning av personal (fortlöpande utbildning i säkerhetsfrågor, riskmedvetande)	X	X	X
Skydd av affärsinformation	X	X	X
Sammanställning – täckning av kriterier			
Summa	**12**	**13**	**10**

Tjänsteutbudet inom logistiksektor omfattar idag mer än att erbjuda transporter och för terminalen kan detta bl.a. beröra tullhanteringen. Det kan därför vara väsentligt att poängtera de uppenbara tullhanteringsfördelar som erbjuds inom ramen för AEO, samt att TAPA med högst poängsättning i tabellen ovan, inte erbjuder denna service. För terminaler med omfattande tullhantering kan denna faktor utgöra ett viktigt avgörande för vilket standardalternativ som i förlängningen anses vara mest lämpligt.

Om terminalens åtaganden omfattar både omlastning och efterföljande transport så innebär detta att terminalaktörens intresseområde utvidgas till att även omfatta säkerhetsarbetet utanför terminalområdet. Konsekvensen av detta blir samtidigt att fler åtgärder måste utvecklas och eftersom risken för stöld är stor under landsvägstransporter bör företag som förbinder sig till sådana åtaganden, överväga att använda utökade säkerhetsåtgärder för att försvåra stöldangrepp. Användning av

högsäkerhetssigill är en sådan åtgärd och det bör därför påpekas att det endast är TAPA som föreskriver krav kring detta.

TAPA brister i kompabiliteten med intermodala flöden, vilket försvårar möjligheten att tillämpa denna standard då terminaler ofta vidaretransporterar gods via andra transportslag längs transportkedjan. ISO 28000 föreskriver samtidigt inga åtgärder för att förhindra stölder och är därför av mindre intresse för landsvägsterminaler som även utför transportarbetet. I annat fall kan ISO 28000 vara ett alternativ, då stölder endast ska förhindras inom den interna organisationen.

Kombiterminal

Kriteriegrunder

	AEO	TAPA	ISO
Kriteriegrund			
Säkerhetshot som primärt ska förebyggas - Stöld	X	X	
Skydd av lokaler	X	X	X
Övervakning av lokaler		X	X
Bemanning och/eller bevakning accesspunkter	X	X	
Tillträdeskontroll	X	X	X
Användande av tekniska lösningar för att hindra olovligt handhavande av gods		X	
Rutiner för kontroll av inkommande gods med avseende på att gods är registrerat i logistiksystemet	X	X	X
Kontroll av sigill på inkommande gods	X		X
Separat förvaring av olika typer av gods	X	X	X
Övervakning under lastning av gods i lastbärare av aktörens personal	X	X	
Rutiner för hur utgående gods förseglas och hur detta kontrolleras	X		X
Kontroller över att gods som lastas matchar godsdokumentationen		X	
Rekrytering och avveckling av personal	X	X	X
Utbildning av personal (fortlöpande utbildning i säkerhetsfrågor, riskmedvetande)	X	X	X
Skydd av affärsinformation	X	X	X
Sammanställning – täckning av kriterier			
Summa	**12**	**13**	**10**

Kostnadsbild

	Låg	Medel	Hög	
Logiskt skydd	0	1	0	
Elektroniskt skydd	0	0	2	
Fysiskt skydd	0	1	0	
Summa poäng	**0**	**2**	**2**	**4**

Angående stöldrisken så påverkas terminalernas beslut om motåtgärder av samma resonemang som för landsvägsterminalerna, dvs. huruvida järnvägs- och kombiterminalen även ansvarar för tidigare/efterföljande transporter. Detta avgör till stor del vilka resurser som terminalbolaget ålägger säkerhetscertifieringen och det finns i sammanhanget avgörande skillnader mellan de standarder som kan vara lämpliga i denna situation. Den största skillnaden utgörs av den brist i tillämplighet som TAPA har vad gäller möjligheten att använda standarden för andra transportslag än lastbilstransporter. Konsekvensen av detta är att standardens inskränkning gör det praktiskt omöjligt att få effektivitet i ett system där syftet med verksamheten är att sammanföra olika transportslag. Om TAPA skulle användas trots nackdelarna med ett sådant upplägg, skulle detta innebära ytterligare standardcertifiering för att täcka de säkerhetsluckor som uppstår då TAPA inte gäller. I detta perspektiv borde det därför vara mer effektivt att redan från början anpassa systemet efter en standard som täcker de områden som verksamheten kommer i kontakt med. AEO är i sammanhanget det standardalternativ som bäst uppfyller de krav som en operatör av järnvägs- och

kombiterminaler bör ställa. ISO 28000 föreskriver inga åtgärder mot stöldangrepp och är därför inte lika lämplig att införa.

Hamnterminal

Kostnadsbild

	Låg	Medel	Hög	
Logiskt skydd	0	1	0	
Elektroniskt skydd	0	0	2	
Fysiskt skydd	0	1	0	
Summa poäng	**0**	**2**	**2**	**4**

Kriteriegrunder

	AEO	TAPA	ISO
Kriteriegrund			
Skydd av lokaler	X	X	X
Övervakning av lokaler		X	X
Bemanning och/eller bevakning accesspunkter	X	X	
Tillträdeskontroll	X	X	X
Rutiner för kontroll av inkommande gods med avseende på att gods är registrerat i logistiksystemet	X	X	X
Kontroll av sigill på inkommande gods	X		X
Separat förvaring av olika typer av gods	X	X	X
Rekrytering och avveckling av personal	X	X	X
Utbildning av personal (fortlöpande utbildning i säkerhetsfrågor, riskmedvetande)	X	X	X
Skydd av affärsinformation	X	X	X
Sammanställning – täckning av kriterier			
Summa	**9**	**9**	**9**

Enligt tabellen ovan så uppfyller de tre jämförbara standarderna lika många kriterier, kriterier med särskild betydelse bör därför selekteras för att öka möjligheten att bedöma vilken standard som är mest lämplig. Eftersom det är få skillnader i de faktiska åtgärdspaketen så är det av större vikt att bedöma helheten och den viktigaste aspekten i detta sammanhang består av den globala tillämpbarheten. Hamnen är en internationell aktör och genom att tillämpa en standard som både inskränker möjligheten till global distribution såväl som möjligheten till intermodala transporter, kan det blir svårt att erhålla effektivitet i säkerhetsarbetet. För global distribution är det endast TAPA samt ISO 28000 som direkt möjliggör dessa flöden. AEO kan via kopplingar till WCO antas kunna anpassas för global distribution men tillvägagångssättet är ej behandlat i detta projekt. För intermodalitet svarar både AEO samt ISO 28000 medan TAPA endast tillämpas på lastbilstransporter, vilket i praktiken utesluter möjligheten för standarden att bli gångbar för säkerhetscertifiering av hamnar. I ett annat perspektiv täcker samtidigt ISO 28000 samma säkerhetsrisker som ISPS och det är därför väsentligt att ifrågasätta värdet av att certifiera enligt ISO 28000 eftersom verksamheten ändå måste uppfylla kraven enligt ISPS. AEO, som även täcker stöld och trafficking, underlättar samtidigt tullhanteringen vilket kan vara av stor betydelse i valet av en standard som även syftar till att skapa effektivitet. AEO täcker därmed tillräckligt många kriterier för att utgöra intresse för hamncertifiering.

Landstransporter

Kriteriegrunder

Kriteriegrund	AEO	TAPA	ISO
Användande av tekniska lösningar för att hindra olovligt handhavande av gods (användning av högsäkerhetssigill, utrustning för stillastående fordon m.m.)		X	
Övervakning under lastning av gods i lastbärare av aktörens personal	X	X	
Rutiner för hur utgående gods förseglas och hur detta kontrolleras	X		X
Kontroller över att gods som lastas matchar godsdokumentationen		X	
Rekrytering och avveckling av personal	X	X	X
Utbildning av personal (fortlöpande utbildning i säkerhetsfrågor, riskmedvetande)	X	X	X
Skydd av affärsinformation	X	X	X
Sammanställning – täckning av kriterier			
Summa	**5**	**6**	**4**

Kostnadsbild

	Låg	Medel	Hög	
Logiskt skydd	0	0	0	
Elektroniskt skydd	0	1	0	
Fysiskt skydd	0	0	0	
Summa poäng	**0**	**1**	**0**	**1**

Det är uppenbart att det framförallt är stölder och skadegörelse som prioriteras ur transportörernas synvinkel och med bakgrund av detta så framträder TAPA som den starkaste standarden enligt tabellen ovan. TAPA täcker till stora delar samtliga av de kriterier som valts ut som särskilt betydelsefulla och det är samtidigt endast TAPA som täcker den förmodligen viktigaste åtgärden, användningen av högsäkerhetssigill. När denna används i kombination med en solid lastbärare såsom containers är det betydligt svårare för obehöriga att få tillgång till godset, vilket därtill är en av få verkningsfulla åtgärder som direkt försvårar intrång i enheter som annars förblir obevakade. För vägtransporter bör TAPA därför utgöra ett lämpligt alternativ i fall då den aktuella lastbäraren endast ska distribueras med lastbilstransporter.

För järnvägstransporter är TAPA inte en lämplig standard att använda till följd av att den enbart kan tillämpas för vägtransporter. Detta utesluter dock inte möjligheten att ändå använda högsäkerhetssigill för att kunna upprätthålla den godssäkerhet som standarden föreskriver, vilket i så fall bör ske i kombination med certifiering av någon av de återstående standarderna. AEO är i detta avseende ett intressantare alternativ mot bakgrund att tillämpningen även täcker hot som avser stöld, vilket inte täcks under ISO 28000. Detta utgör en så viktig grundförutsättning att det praktiskt sett inte finns någon egentlig anledning till att välja certifiering enligt ISO 28000. Bägge alternativen är dock kompatibla med intermodala flöden och i detta avseende brister däremot TAPA. Konsensus är därför att både väg- och järnvägstransporter som avser ingå i den intermodala logistikkedjan, bör överväga certifiering enligt AEO, såväl som järnvägstransporter bör överväga AEO framför ISO 28000 i alla förekomna fall.

Sjötransport

Kostnadsbild

	Låg	Medel	Hög	
Logiskt skydd	0	0	0	
Elektroniskt skydd	0	0	0	
Fysiskt skydd	0	0	0	
Summa poäng	**0**	**0**	**0**	**0**

Kriteriegrunder

	ISPS	AEO	TAPA	ISO
Kriteriegrund				
Skydd av lokaler	X	X	X	X
Övervakning av lokaler	X		X	X
Bemanning och/eller bevakning accesspunkter	X	X	X	
Tillträdeskontroll	X	X	X	X
Användande av tekniska lösningar för att hindra olovligt handhavande av gods (användning av högsäkerhetssigill, utrustning för stillastående fordon m.m)	X		X	
Rutiner för kontroll av inkommande gods med avseende på att gods är registrerat i logistiksystemet	X	X	X	X
Kontroll av sigill på inkommande gods	X	X		X
Kontroll över att gods som lastas matchar godsdokumentationen	X		X	
Rekrytering och avveckling av personal		X	X	X
Utbildning av personal (fortlöpande utbildning i säkerhetsfrågor, riskmedvetande)		X	X	X
Informationsspridning (intern och extern information om företagets/aktörens säkerhetsrutiner)	X			X
Skydd av affärsinformation		X	X	X
Sammanställning – täckning av kriterier				
Summa	**9**	**8**	**10**	**9**

TAPA är enligt tabellen ovan den standard som uppfyller flest av de utvalda kriterierna men med hänsyn till avsaknaden av kompabilitet med fartygstransporter, kan standarden inte utgöra något troligt underlag för certifiering av sjötransportörer. AEO brister samtidigt i den globala tillämpligheten vilket försvårar certifiering enligt denna standard, med hänsyn till sjöfartens internationella karaktär. AEO är dock sammankopplad med WCO och mot bakgrund av detta så bör den globala täckningen i praktiken inte utgöra något större problem. Det kan dock konstateras att AEO kompletterar ISPS-koden väl på de områden som ISPS brister och AEO bör därför kunna utgöra ett potentiellt alternativ om ytterligare steg ska tas mot förbättrad säkerhet. Framförallt utökas säkerheten mot stöldangrepp och trafficking, vilket varken täcks av ISPS-koden eller ISO 28000. I övrigt skapar ISO 28000 inga mervärden utöver AEO och de kriterier som redan är täckta av ISPS-koden. Certifiering enligt ISO 28000 medför därför en lägre säkerhetsnivå än i fallet då ISPS-koden kompletteras med certifiering enligt AEO. Det ska dock konstateras att det troligen kan räcka med att sjötransportören uppfyller de åtaganden som krävs ur den tvingande lagregleringen, då några direkta fördelar med utökad certifiering är svår att finna.

Slutsatser

Projektets syfte har under arbetets fortskridande modifierats, vilket ansetts nödvändigt för att skapa en rapport som kan bidra med användbart innehåll till studiens intressenter. Rapporten har därför i nuvarande upplaga försökt belysa de säkerhetsstandarder som är mest relevanta för respektive aktör inom transportkedjan, samt beskriva vilka kriterier som dessa aktörer bör fokusera på. Slutsatserna av detta arbete presenteras i denna del.

Olika motiv till att införa ett säkerhetsinitiativ

Olika aktörer prioriterar olika åtgärder för att minska riskerna inom ett för aktören viktigt område, vilket försvårar arbetet med en universellt fungerande standard med den helhetstäckande säkerheten i fokus.

Det har under projektet tydligt framgått att det finns intressekonflikter i de säkerhetsinitiativ som respektive standard förespråkar. Detta innebär i praktiken att olika intressenter prioriterar olika åtgärder i syfte att minska risken för intrång på de områden som respektive aktör framhåller som särskilt betydelsefulla. Ett system där säkerheten till viss del baseras på denna valfrihet skapar också försvårande omständigheter avseende det faktum att säkerhetsriskerna många gånger tillhör de länkar där säkerhetsåtgärderna är som lägst. Ett tydligt exempel som illustrerar denna problematik är i fall då intresset av att skydda gods mot stöld är viktigare än risken för att en transportbärare används för smugglingsändamål. Ett sådant system skapar säkerhetsluckor på grund av att en övergripande global standard saknas eller i vart fall inte är fullständigt utbyggd.

För många säkerhetsinitiativ

Det stora antalet säkerhetsstandarder försvårar arbetet med att finna en gemensam överenskommelse inom vilket den övergripande säkerheten ska kunna harmoniseras.

Med bakgrund av det stora utbudet av säkerhetsstandarder så kan det konstateras att ytterligare initiativ till nyetableringar inte löser problematiken med ineffektiva certifieringsprocesser. I förlängningen innebär avancerade certifieringsprocedurer både minskad säkerhet och förlorad effektivitet, där resultaten av dessa troligen skulle bli bättre genom konsolidering och minskning av antalet standarder. AEO är dock ett exempel på standard som uppvisar tecken på att öka transparensen gentemot andra standarder, däribland WCO, TAPA, och ISO 28000. Detta kan vara ett första steg mot ett effektivare och mer globalt täckande säkerhetssystem.

Samverkan för bättre effektivitet

Myndigheter bör samarbeta på internationell nivå för att genomföra en översyn av effektiviteten i det nuvarande säkerhetssystemet. Det finns risk för att dagens konstruktion skapar ineffektiva säkerhetslösningar som i förlängningen verkar negativt på den globala säkerhetsnivån. Stater bör därför samverka för att på så sätt lämna förslag på hur effektivisering ska kunna uppnås.

Det råder stor brist på internationella samarbeten för att möjliggöra en effektivare utveckling av ett fungerande säkerhetsarbete på global nivå. Ett tydligt exempel som beskriver konsekvensen av sådan utebliven samverkan är de hårda regler som USA på kort tid försökt att implementera för fartygstransporter med USA som destination. Till dessa hör exempelvis 100%-scannning som ålägger en mycket stor arbetsbörda på de hamnar som trafikerar amerikanska farvatten och där det faktiska värdet av en sådan åtgärd inte är helt klargjord. Kontrasten mellan åtgärder av denna karaktär och åtgärder i den övriga internationella sjöfarten är mycket stor och samtidigt uppstår säkerhetshoten framförallt i de delar av kedjan där säkerheten är som lägst. Det är därför motiverat med internationell reglering som utjämnar denna snedfördelning och därmed möjliggör bättre resursfördelning, vilket troligen också minskar risken för över- kontra underdimensionerade säkerhetssystem.

Tillgripna godsvärdet ökar

Det är konstaterat att värdet på det gods som tillgrips inom transportkedjan ökar kraftigt, vilket påverkar kostnadsstrukturen och skadelidandet för varje enskilt tillfälle. Angreppen blir alltmer kännbara och troligen ökar detta ambitionen att förstärka skyddet gentemot verksamheten från utomstående..

Värdeökningen för den totala mängden tillgripet gods kan bero på ett antal faktorer. Under projektarbetet har det framkommit uppgifter om att Polisen infört nya rutiner kring brottsrubriceringen av angrepp mot transportkedjan. Tidigare kamouflerades den verkliga kostnaden för dessa brott genom att det inte förekom någon separering mellan olika former av stölder. Genom förbättrad brottskodning är det därför numera möjligt att följa upp kostnadsbilden för varje enskilt angrepp riktat mot transportkedjan. Det har också framkommit uppgifter om att kunskapsbasen kring planering och tillvägagångssätt för angrepp har ökat bland kriminella, vilket med stor sannolikhet ökar precisionen och inriktningen av angreppet. En sådan inriktning är stölder av hela ekipage, något som i likhet med ökad kunskap troligen har bidragit till den senaste tidens stegring av det tillgripna godsets värde.

Säkerhetshotens betydelse för verksamheten

Transportbranschen upplever att det framförallt är stölder och skadegörelse som orsakar mest skada utifrån de säkerhetshot som blivit beskrivna i detta projekt.

Eftersom transportbranschen många gånger består av eller representerar de aktörer som besitter godsintresse, är det inte förvånande att säkerhetshot som avser stöld och

skadegörelse är högt prioriterade av dessa aktörer. Branschen är samtidigt enig om att smuggling utgör ett problem men anser samtidigt inte att enskilda transportföretag ska lösa detta problem. Terrorism och trafficking är säkerhetshot som inte medför några kännbara konsekvenser för den enskilde aktören och åtgärder mot sådana angrepp prioriteras därför inte.

Summary

The report is structured around four phases and the disposition of these is to start with descriptive content to the end turning into more discursive text.

- Phase 1 Situational analysis of security threats against the transport chain
- Phase 2 Overview of recent security initiatives affecting different parts of the transport chain
- Phase 3 Description and evaluation of selected security initiatives
- Phase 4 Final recommendations and conclusions

Phase 1 Situational analysis of security threats against the transport chain

This part describes the present situation of security threats targeting the transport chain. Among this, crime statistics are presented as well as descriptions of various types of crimes that carriers and other logistics players are subjected to.

Incidence

The number of thefts (thefts of or from cargo carriers) decreases each year and this decrease is reflected in the number of transport-related crimes[4] reported to the police. These statistics can only be compared for year 2007 and 2008, due to changes in the police crime coding system. Because there are so few years with statistics in this area, it is difficult to draw qualitative conclusions. However, a trend is nevertheless apparent here. The organizations participating in this project have also noticed a certain decrease in this kind of crime. For a discussion on a possible reason for this, see section 7.3.

Total number of crimes reported in year 2008: 2140
Total number of crimes reported in year 2007: 2377

- 70% of the crimes occurs between 10 p.m. and 6 a.m. (Sweden)
- 81% of the crimes were committed against unprotected cargo carriers (Sweden)

Value of cargo

What is troubling in this context, however, is that the total value of the cargo stolen is increasing[5] (an increase of almost 100% between year 2007 and 2008 is noted here).

[4] Police Report on Transport Security 2008, Per-Arne Nilsson, Västra Götaland County Police
[5] Analysis of Cargo Value 2008, Transport Security Project. Established by the Risk Management Academy

The reason for this increase can be explained by the following three factors:

- Improved reporting routines used by the police and the industry.
- More competent criminality, due to organized gangs committing the crimes.
- Increase in the number of stolen rigs (entire cargo carriers).

Depending on the method of calculation and the assumptions used, the conclusion is that cargo worth SEK 52 - 293 million was stolen in the process of transport in Sweden each year.

Vulnerable parts of the transport chain

Of the thefts, 70 – 80 % can be statistically associated with an unprotected location, or alternatively, an unprotected cargo transport unit. Thus, the willingness of a potential perpetrator increases when mechanical or physical means of protection take the place of a capable guard.

The following graph shows that security risks decrease where there is adequate protection. The graph reflects the statistics in this field, as well as the views of the organizations interviewed. The line corresponds to the level of security pertaining to each part of the transport chain. Thefts occur most commonly where the color of the graph is darkest.

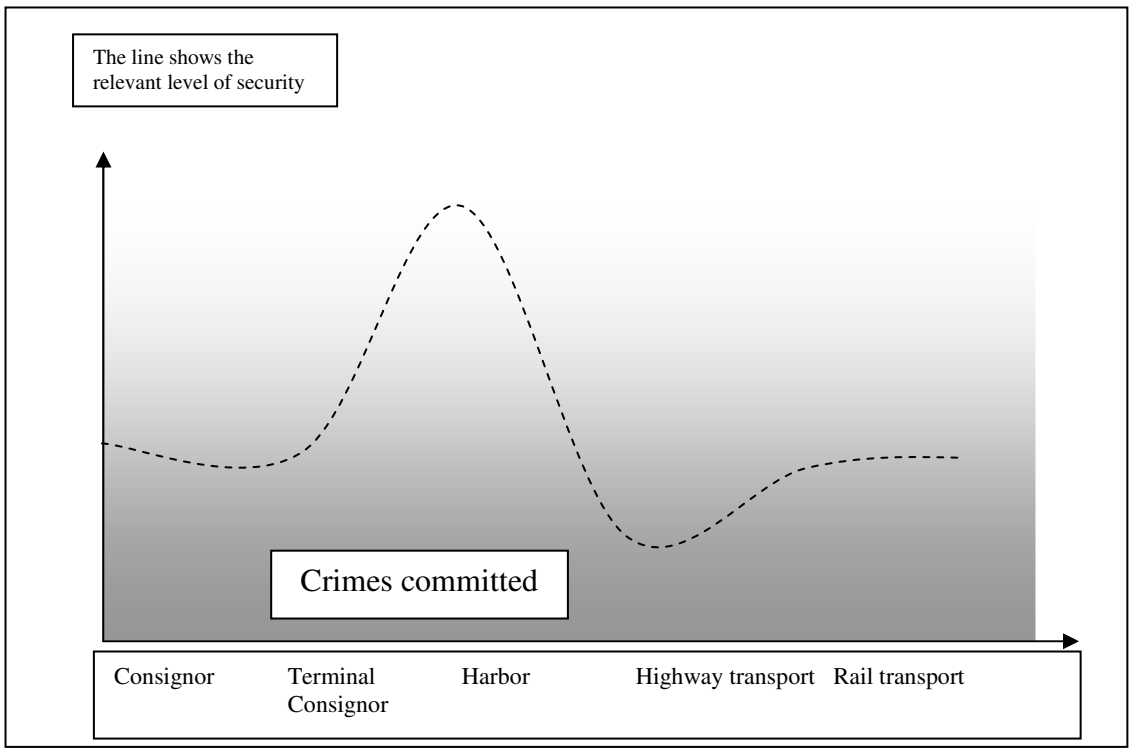


Chart 4 - Relation between the level of security and the risk of threats in different parts of the intermodal chain of transport

Known security threats and their likelihood in various parts of the transport chain

The matrix below shows a qualitative probability assessment of the risks and threats included in this project. The result is based on the statistic data and result from the interviews conducted. The known threats described in this project are theft, vandalism, smuggling, trafficking and terrorism.

The assessment criteria are rated from one (least likely) to five (most likely).

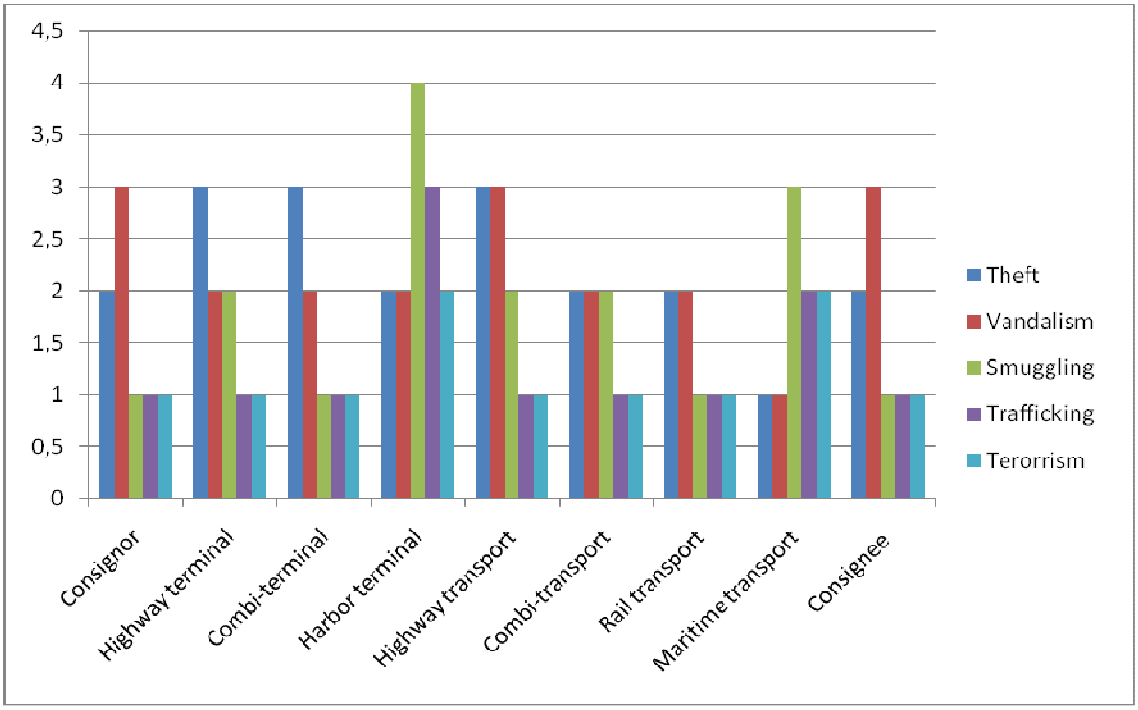


Chart 1 –Probability for different security threats in the intermodal chain of transport

Economic effects of security threats in various parts of the transport chain

The bars of the diagram show the economic effect of the crimes. The variables are set between one (hardly any effect) to five (extreme effect).

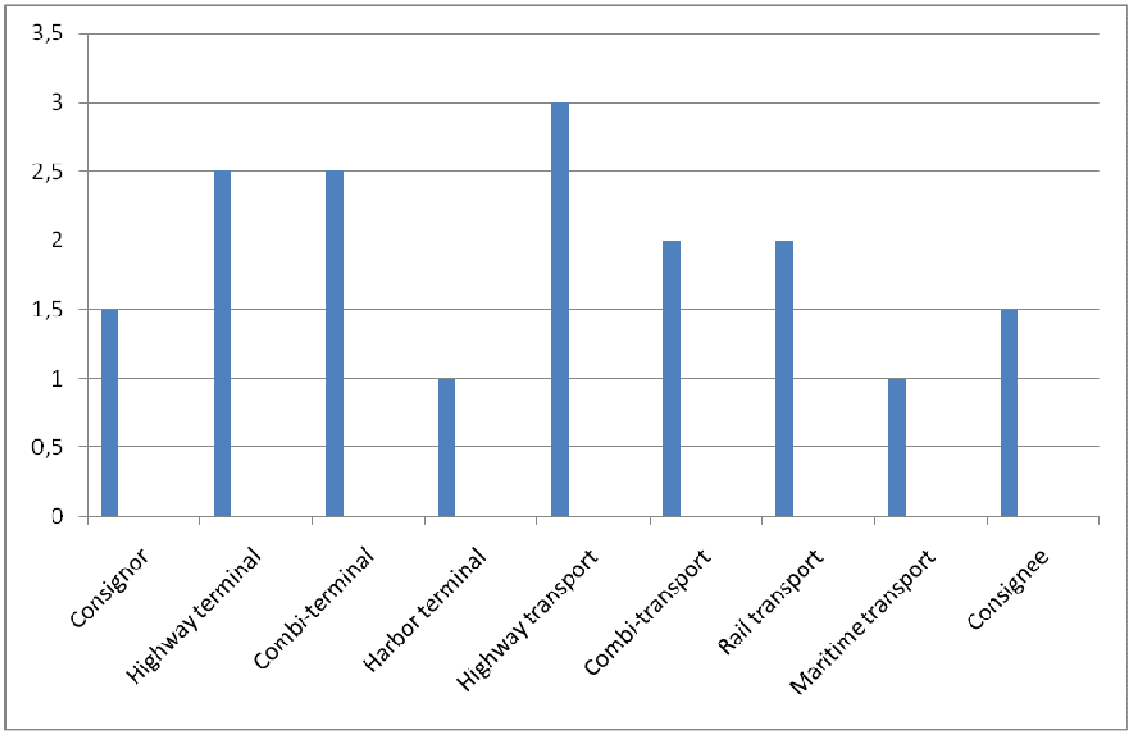


Chart 2 – Economic effect of crimes in different parts of the chain of transport

Defensive measures in various parts of the transport chain

The diagram below represents a qualified assessment of which economic measures are taken in the various parts of the transport chain. Although the bars do not claim any quantitative precisions, they can be used for purposes of comparison, with 1 representing low, 2 representing medium and 3 representing high. However, the relative height of the bars shows the differences that exist.

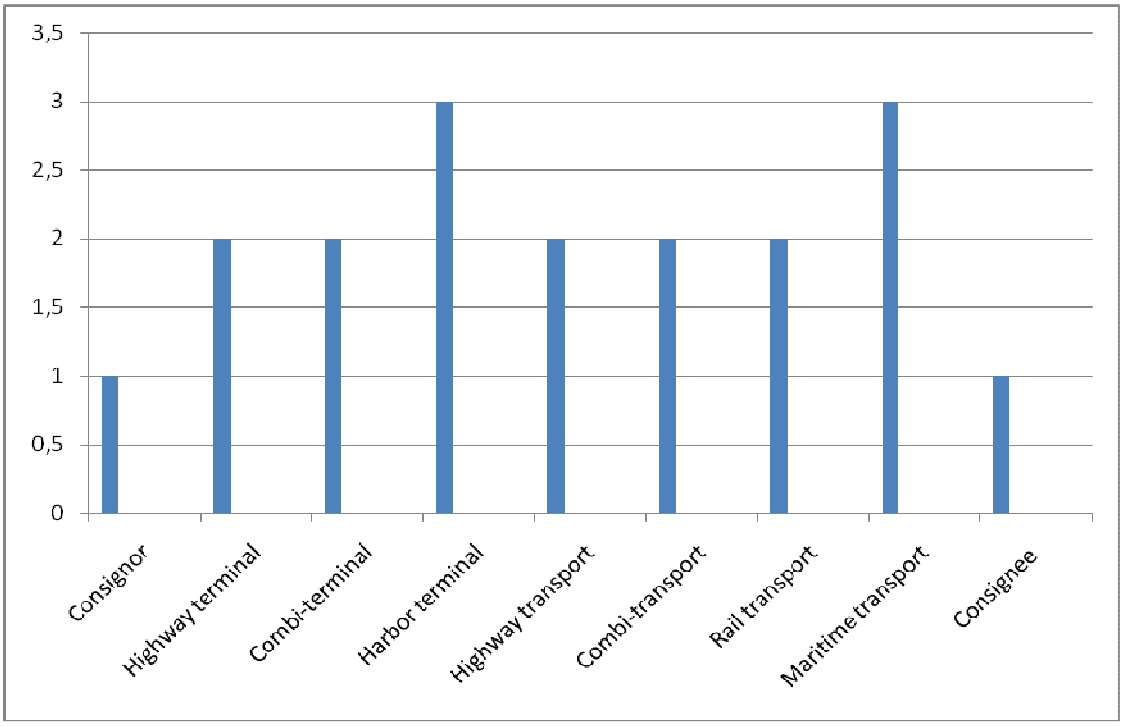


Chart 3 – Level of economic measures to counteract security threats in different parts of the chain of transport

Can the absence of information or discussion about current causation factors exacerbate problem solving?

The answer must undeniably be YES. However, this is a very difficult issue, and it isn't claimed to be able to provide a comprehensive answer to this question. Appendix 1 (Bilaga 1), contains a number of criminological theories and conclusions[6], which are accepted by society and criminological institutions, and are suitable for providing a broad factual background to this issue.

In addition, a few simple conclusions may be summarized:

- There are some potential perpetrators who exist regardless of cause.
- The crimes are committed due to segregation and/or alienation.
- The crimes are committed partly because of existing criminality, which spreads and recruits new "weak" individuals.
- The crimes are committed in a society that provides opportunities to do so.
- The crimes are committed when and where the lack of capable guards[7] is most pronounced.

What is the reason for the statistical reduction in the number of thefts?

Answer: As the statistics that the police provide the government are based solely on those crimes of which the police are aware, they do not fully reflect reality. The reasons for unreported crime relate both to the police and the industry. Briefly, these reasons include the difficulty of the transporter to ascertain exactly which items have been stolen, and the fuzzy line between theft, vandalism and damage to goods. Time pressures are another reason why thefts are sometimes not reported, as are cases where the amount of the theft is below the insurance deductible. All these lead to unreported thefts[8].

The two most important reasons for the decrease in thefts appear to be:

- The fact that the police in the counties of Skåne, Halland, Jönköping and Kronoberg, as well as Västra Götaland, have focused on this area and established a coordination group. This work has led to increased inter-sector coordination between the police and the entire transport industry, including seminars and workshops to increase interest in these issues, and an increased understanding of the problem and relevant protective measures. In addition, manufacturers (Volvo Lastvagnar and Scania) have internalized this information and changed locks and security, for example, as a result.
- An increased level of professionalism among the perpetrators has resulted in fewer, but more lucrative, thefts, thereby increasing the amount stolen per theft.

[6] Jerzy Sarnecki, Introduktion till kriminologi (Textbook,Introduction to Criminology)
[7] Lack of various protective measures, logical, physical and electronic protection
[8] Ratio of non-reported crimes to total crimes

Phase 2 Overview of recent security initiatives affecting different parts of the transport chain

This part is presenting a description of the security initiatives currently available for preventing crimes against the transport chain.

Summary of different security initiatives

The following content is an overview of selected security initiatives. Selected from what impact they have on freight from Sweden and also how they affect the flow of cargoes in the world. Some initiatives are also described with the purpose of obtaining a more complete overview. Some of the initiatives have been in force whilst others are under development, a few initiatives are pure research projects.

A common goal is to use technical solutions, regulations / standards and cooperation, development of security in freight transport while the free world commercial trade can continue to develop both in efficiency and quantity.

The vast majority of the described security initiatives were launched in response to the terrorist attack on U.S. 9 / 11 2001. Although the logistics chain was not involved itself, a concern about what the legitimate freight could be used for in the terrorist context was raised. Weapons of mass destruction could be smuggled in containers on ships or in land transport (rail and road).

The global and intercontinental transport chain itself may be targets of terrorism, something which would have enormous economic consequences, affecting the global world trade.

Many security initiatives launched in the U.S. have in common that the primary goal is the prevention of terrorist attacks. This action does also prevent the presence of other illegal activity, such as smuggling, trafficking, etc.

The *SAFE Port Act*, a law that took effect in 2006, was the former administration's response to the increased terrorist threat. The implication is that each port has accountability for the health and national security. It deals with measures to be introduced to strengthen maritime security protection. The law is linked to *C-TPAT, CSI, SFI and 100% scanning*.

CSI, Container Security Initiative, focuses on improving the security of the maritime transport chain. The initiative affects shipping of goods to the United States and associated management of port terminals. The basic idea is to move a part of the inspection to the port of vessel loading. The goal is to prevent weapons of mass destruction, etc. to reach U.S. territory, where it can cause massive damage both to the port and nearby ships.

SFI, the Secure Freight Initiative, has many similarities to *CSI*. The purpose of *SFI* is, in contrast to *CSI*, to scan more containers and not just those who have been classified as high-risk cargo. The scanning has to be done in a foreign port and full implementation has occurred in some ports as an examination test".

100% scanning is an initiative that, like *CSI* and *SFI*, deals with scanning of containers with the intention of detecting hazardous materials such as radioactive materials. From July 2012, all goods arriving to the United States have to be scanned before loading onto a ship, or upon arrival. In the Commission Act of 2007, the objective and stringent requirement is that the scanning of goods must be done before loading onto the ship.

The strategy of *C-TPAT*, *Customs-Trade Partnership Against Terrorism*, is to work increasingly with preventive security before the cargo arrives physically to the border control. This is accomplished by analyzing available transport data in an early stage, in order to focus on goods that are high-risk rated. The focus is kept by the involvement of stakeholders to the transport security work and the certification thereof.

Advance Manifest Regulation affects goods exported to the United States and it is a requirement to submit an electronic pre-notification of the goods to the CBP (U.S. Customs and Border Protection) 24 hours before loading onto a ship which has the U.S. as destination (with some exceptions).

The *FAST's, Free and Secure Trade Union*, focus is to facilitate the transport of goods between the border of United States, Canada and Mexico while the security is strengthened for the presence of smuggling and terrorism. Road transports are affected. Redistribution is done by the customs authorities' resources from covering a majority of goods to the concentration of controls for high-risk shipments. It is possible through cooperation with and certification of operators in the logistics chain, including the individual lorry drivers.

Many countries have, like the U.S. one or several security initiatives affecting the transport of goods across the borders, focusing on imports. Australia's *Frontline*, Canada's *PIP*, New Zealand's *Secure Exports Scheme*, Singapore *Secure Trade Partnership*, Netherlands *Dutch Client Systems* and the *Swedish StairSec / Stairway* are the initiatives presented briefly in this report.

Frontline is an Australian Customs Service program initiated in 1991, where the main objective is to aggravate the criminal activity of Australia's existing borders, both regarding imports and exports. Unlike most other initiatives worldwide *Frontline* aims to strengthen security against smuggling of drugs, animals, trafficking and money laundering. This is done by working with companies on a voluntary basis.

Canada's *PIP, Partners In Protection*, was like *Frontline* taken into action before the terrorist attacks 2001. The main purpose was to promote corporate awareness of and compliance with the custom’s regulation which were very tough. Criminal abuse of legitimate goods could affect hauliers in a negative way because the transport unit used for smuggling could be confiscated. The first *PIP* initiative was therefore a desire made by businesses with the intention to expand the cooperation with the custom,

which could be useful in case where a shipment would be subjected to a criminal act. After 9 / 11 the requirements for Canada customs authority's work changed and a new program was initiated in 2008 with the same name. The new security initiative was designed to be compatible with *C-TPAT*, which facilitates cooperation between countries but also the transport work.

Secure Exports Scheme is the New Zealand Customs' program focused on improving security in the logistics chain by improving the efficiency of customs operations, which facilitates the country's export companies to operate on the global arena. The *Secure Exports Scheme* is compatible with international standards such as the WCO standards.

Singapore is an important hub in the world trade and its security initiative, the *Secure Trade Partnership*, aims to safeguard that position. The work undertaken by the Singapore Customs is of great importance for the security in the global logistics chain. Membership involves, apart from facilities, fewer controls by customs and compliance with international standards.

Dutch Client System is the Dutch customs' internal program, designed to assess the reliability of the transport chain actors and what security threats the transports are dealing with. Using risk analysis the type of control can be determined. The link to the *AEO* is strong and by year 2007 Dutch companies can apply for an *AEO* status through certification by the *Dutch Client System*.

Stairway is a program which was taken into action in Sweden by 2002 with the urge to simplify and assure the quality of customs procedures. Customs' work should be focused on companies that carried a high risk for being used in illegal activities. After certification in various steps the company obtained relief in customs handling. *StairSec* was developed in 2003 as the *Stairway's* security program but was closed in the end of 2010 as part of increased cooperation between customs authorities in the EU and the competition to the security initiative *AEO*.

AEO, Economical Authorized Operators, is an initiative developed by the European customs authorities, created with the intention to establish uniformed guidelines in the handling and control of cargo flows. *AEO* is compatible with the *WCO SAFE* and *ISO 28000* standards and *AEO* provides certified companies access to the simplification of customs procedures. Application for certification regarding *AEO* status should be applied to the customs authority in the same country as where the company is registered, the certification is valid throughout the EU. The requirements for obtaining *AEO* status is detailed and measures for security taken by the operator are tough in order to be certified.

Pre-register EU is also a joint initiative within EU, with the aim to make it more difficult for criminal activity across the EU external frontier. Briefly, cargo imported to the EU has to be pre-notified by a certain period of time before crossing the border, where the actual time depends on the mode of transport.

The work for security in the logistics field goes towards an increasing internationalization of security standards on a global level, where the *ISPS Code, the*

WCO SAFE and the *ISO 28000* are well represented. The national initiatives (including partnerships as for the EU) are being adapted by the global programs but also by other security initiatives with impact, often with U.S. guidance.

The *ISPS Code*, the *International Ship and Port Facility Security Code*, is the International Maritime Organization's program to mitigate the risk of using ships in the execution of terrorist attacks, both directly and indirectly. The code consists of basic requirements and recommendations that all countries should comply with and implement.

WCO, World Customs Organization, intends to facilitate global trade by establishing common goals and rules. The security issue has become increasingly important and the WCO Framework for execution is called *SAFE*, with the objective to relocate the focus on security from the importing to the exporting countries, to introduce international standards to promote security in the transport chain on a global level, to adapt existing rules for the new challenges of the future, etc.

ISO 28000 is a standard that took effect in 2007 and it is designed to increase the security of the supply chain. The standard is focused on providing comprehensive guidelines for the management of matters in security of international transport. Compliance with *ISO 28000* provides a good basis for certification according to other security initiatives such as the *ISPS Code, AEO, C-TPAT*, and others.

The promoters of the initiatives mentioned so far are the state, the national customs administrations and international associations of countries and their respective authorities. In addition to these an overview of two other security initiatives are presented, *BASC* and *TAPA*, which many companies prefer.

BASC, the Business Alliance for Secure Commerce, is a security initiative created by a group of stakeholders in South America. It aims, through cooperation between companies and authorities, to effectively work against smuggling of illegitimate goods in legitimate transports. Over time it evolved into a complete system for management of security issues with specific security requirements.

TAPA, the Technology Asset Protection Association, is an initiative focused on increasing the security of road transports and reducing the number of thefts as the main driving force. The initiative is an association of companies within production and transport of high valued goods and commodities.

ESSTRT, European Security: High Level Study on Threats, Responses and Relevant Technologies, is a study by the European Commission of the defense group Thales, with the aim to analyze the threats to the European security and to propose measures to improve the level of security, with focus on methods to prevent terrorism.

SECCONDD, Secure Container Data Device Standardisation, is a research project focusing on making container handling safer. It primarily aims to control if the container's content have changed during transports by road.

The report also presents some of the rules /security initiatives for the transportation of dangerous goods. Since about 5 years ago there have been additional rules in the Regulations for the transport security, in order to minimize theft or misuse of dangerous goods that may be dangerous to persons, property or environment.

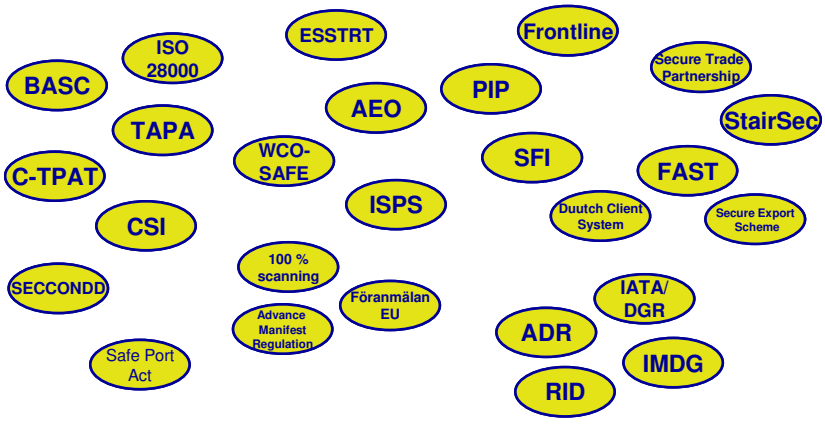
ADR, RID, IMDG, IATA / DGR are all built on the recommendations of an expert committee of the UN Economic and Social Council (ECOSOC).

Phase 3 Description and evaluation of selected security initiatives

In Phase 3, a selection of the standards described in Phase 2 is made, in order to make more detailed descriptions of these standards.

The selection of security initiatives

The project's phase 2 consists of an overview where 26 different security initiatives have been briefly described. The aim of the project's phase 3 is to make a selection of these initiatives and study them in detail.

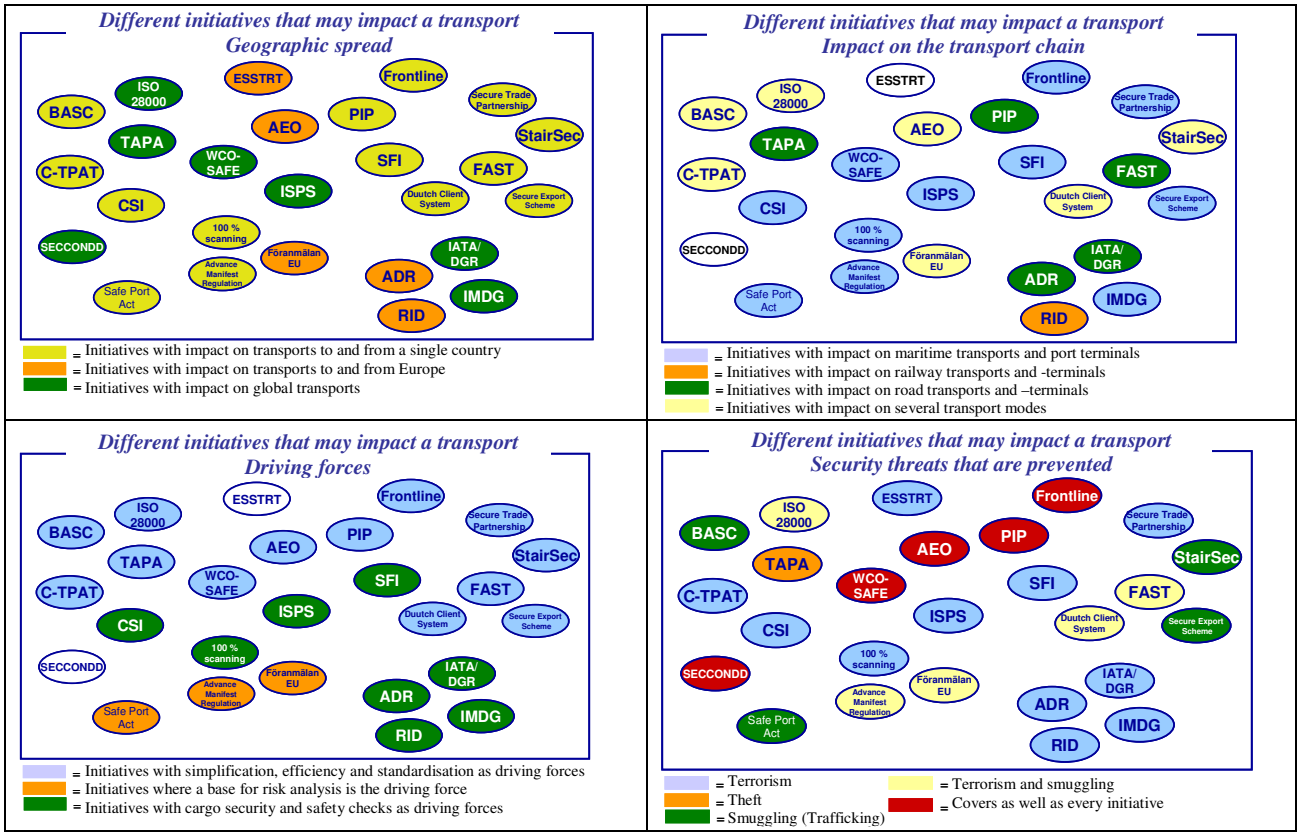


Picture 2.1 – Various security initiatives that may affect a transport

The aim of the selection has in the first place been to study the impacts for combined transports in Europe, where such a study manages the objective of the V-FUD SirC. The disposition of the selection, four types of criteria have been considered and analyzed:

- *Geography*:	Security initiative will be active in Europe
- *Impact on transport*:	Security initiative will affect as many parts of the Transport chain as possible
- *Driving force:*	The security initiative results in some sort of simplification or efficiency
- *Which threats to be prevented:*	The security initiative should prevent as many threats as possible.

Every selected initiative has been analysed and the results are presented in various tables and pictures that shows the link between the different initiatives.



Picture 2.2 – Various types of criteria

The selection procedure was finalized with an analysis, presented in the table at right. The result was that three initiatives, AEO, ISO 28000 and WCO-SAFE cover all four criteria. Out of these three initiatives WCO-SAFE was removed since it has strong similarities to AEO, which was selected. Caused by its adequate geograpchical spread.

As references to AEO and ISO 28000, C-TPAT, ISPS and TAPA were selected.

Security initiatives	Criteria matrix				
	Geographic	Impact on the transport chain	Driving force	Involved security threats	Number of covered criteria
100 % scanning					
ADR	X				1
AEO	X	X	X	X	4
BASC		X	X		2
CSI					
C-TPAT					
Dutch Client System		X	X		2
ESSTRT	X	(X)	X		2
FAST					
Frontline			X	X	2
Föranmälan EU	X	X	X		3
Föranmälan USA					
IATA/DGR	X				1
IMDG-kod	X				1
ISO 28000:2007	X	X	X	X	4
ISPS-kod	X				1
PIP			X		1
RID	X				1
SAFE Port Act					
SECCONDD	X	(X)		X	2
Secure Exporte Scheme			X		1
Secure Trade Partnership			X		1
SFI					
StairSec		X	X		2
TAPA	X				1
WCO-SAFE	X	X	X	X	4

Comparison between selected initiatives

The following table consists of a selection of criteria compiled to allow comparison between the various security initiatives. The table has been divided into two sections with the first part describing the overall criteria and the second part focusing on the description of the specific measures covered by each standard.

General comparison	**AEO**	**C-TPAT**	**TAPA**	**ISPS***	**ISO**
Certification in general					
Obtaining benefits in customs procedures	x				
Available globally	x	x	x	x	x
Statlig eller överstatlig initiativtagare	x	x			
Type of cargo					
Global cargo			x	x	x
Import to USA		x			
Import and export EU	x				
Security threats to be prevented					
Terrorism	x	x		x	x
Theft	x		x		
Smuggling	x			x	x
Trafficking	x				
Transport modes					
Road transports	x	x	x		x
Railway	x	x			x
Aviation	x	x			x
Maritime shipping	x	x		x	x
Link to selected initiatives					
AEO			x		x
C-TPAT					
TAPA	x				
ISPS					
ISO	x				

Comparison of criteria	AEO	C-TPAT	TAPA	ISPS*	ISO
Buildings and areas					
Security of buildings	x	x	x	x	x
Monitoring of buildings		x	x	x	x
Staffing and coverage of unlocked doors and access points to a restricted area	x	x	x	x	
Passing check	x	x	x	x	x
Cargo handling					
Usage of technical solutions preventing unauthorized access to the goods		x	x	x	
Procedures for the control of incoming goods, compliance with registered cargo	x	x	x	x	x
Checking the seal of incoming goods	x	x		x	x
Separate storage of different types of goods	x	x	x		x
Usage of technical solutions for track and trace					
Quality check of packages	x				x
Cargo loading					
Monitoring loading procedures by authorized personnel	x		x		
Procedures for sealing and check of damage	x				x
Check of cargo compliance to cargo documentation		x	x	x	
Personnel					
Recruitment and settlement of personnel	x	x	x		x
Education of personnel	x	x	x		x
Dissemination of information		x		x	x
Information security					
Quality check of data and information systems		x			x
Business information security	x	x	x		x
Information exchange with customs	x	x			x
Networks and business systems					
Security systems	x	x			x
Evaluation systems for business partners		x	x		x
Established cooperation with customs and other authorities.	x	x	x	x	x

Phase 4 Final recommendations and conclusions

This part is presenting recommendations regarding the standards which by the report have been considered most appropriate for application, regarding each individual stakeholder in the transport chain.

Suitable standards for each individual stakeholder in the transport chain

To assess the extent to which each stakeholder in the transport chain can implement the selected security initiatives, a general survey has been made. The compilation was based on criterion of great importance for each stakeholder, which in addition have been related to the standards selected. In essence, the standards which satisfied most criteria also proved to be the most suitable for certification of the particular business. However, there have been situations where other aspects have been necessary to take into account, which then usually has given rise to a different result. A cost comparison has also been made through the formulation in the following calculation. Maximum cost is equivalent to 6 points and minimal cost corresponds to 0 points.

	Low	Average	High	
Logical protection	0	0	0	
Electronic protection	0	0	0	
Physical protection	0	0	0	
Sum	**0**	**0**	**0**	**Points**

Sender/receiver

Set of criteria

	AEO	TAPA	ISO
Criteria			
Security threats to be prevented - theft	X	X	
Security of buildings	X	X	X
Monitoring of buildings		X	X
Staffing and coverage of unlocked doors and access point to a restricted area	X	X	
Passing check	X	X	X
Usage of technical solutions preventing unauthorized access to the goods		X	
Checking the seal of incoming goods	X		X
Monitoring loading procedures by authorized personnel	X	X	
Procedures for sealing and check of damage	X		X
Check of cargo compliance to cargo documentation		X	
Recruitment and settlement of personnel	X	X	X
Education of personnel	X	X	X
Business information security	X	X	X
Compilation			
Sum	**10**	**11**	**8**

Costs

	Low	Average	High	
Logical protection	0	0	0	
Electronic protection	0	1	0	
Physical protection	0	1	0	
Sum points	**0**	**2**	**0**	**2**

According to the table TAPA appears to cover most of the criteria of the selected security initiatives. However it should be noted that this probably results by the fact that TAPA is adapted to the conditions that apply to stakeholders who have strong links to the goods. TAPA is thus an initiative that will strengthen these actors' ability to defend the right to their goods and thereby reduce the incidence of particular thefts. Although TAPA meets most criteria it should be noted that there are limitations such as lack of compatibility for the application of intermodal transports. TAPA is only designed to handle goods that are transported by road transports and this hugely complicates the ability for global distribution. In this perspective, it can be speculated whether it might be more economical to apply to the AEO, which with this certification would make intermodal transports applicable. The disadvantage of the AEO may, however, consist in the lack of stronger measures against carrier infringement.

The sender should by this reasoning, consider that either introduce AEO or TAPA, depending on the criteria of most importance in each case. The character of the sender's activity is crucial in assessing which of these options offer the best opportunities for effective enforcements. The step of introducing the ISO 28000 instead of AEO or TAPA is considered too great since this standard does not impose any immediate measures to reduce the risk of theft or similar activity with impact on the sender's goods interest.

Road terminal

Costs

	Low	Average	High	
Logical protection	0	1	0	
Electronic protection	0	0	2	
Physical protection	0	1	0	
Sum points	**0**	**2**	**2**	**4**

Set of criteria

	AEO	TAPA	ISO
Criteria			
Security threats to be prevented - theft	X	X	
Security of buildings	X	X	X
Monitoring of buildings		X	X
Staffing and coverage of unlocked doors and access point to a restricted area	X	X	
Passing check	X	X	X
Usage of technical solutions preventing unauthorized access to the goods		X	
Procedures for the control of incoming goods, compliance with registered cargo	X	X	X
Checking the seal of incoming goods	X		X
Separate storage of different types of goods	X	X	X
Monitoring loading procedures by authorized personnel	X	X	
Procedures for sealing and check of damage	X		X
Check of cargo compliance to cargo documentation		X	
Recruitment and settlement of personnel	X	X	X
Education of personnel	X	X	X
Business information security	X	X	X
Compilation			
Sum	**12**	**13**	**10**

The range of services offered by the logistics sector comprises of more than providing transportation and it is not unusual that custom clearance is managed by the terminal. It may therefore be important to point out the duty management

benefits offered by the AEO, whilst TAPA with the highest score in the table above doesn't offer this service. For terminals with extensive customs handling this factor may be of major importance.

If the terminal's commitments include both the transhipment and subsequent transport, this means that the terminal interests are expanded to also include the security work outside the terminal area. The consequence is that more measures must be developed and because the risk of theft is high in road transports, terminal companies with transport activities should consider usage of improved security measures to prevent theft attacks.

TAPA lacks in compatibility with intermodal flows, which makes it difficult to apply the standard for terminals transporting goods by different modes of transport. ISO 28000 requires at the same time, no measures to prevent theft and is therefore of less importance for terminals with an own transport department.

Intermodal terminal

Set of criteria

	AEO	TAPA	ISO
Criteria			
Security threats to be prevented - theft	X	X	
Security of buildings	X	X	X
Monitoring of buildings		X	X
Staffing and coverage of unlocked doors and access point to a restricted area	X	X	
Passing check	X	X	X
Usage of technical solutions preventing unauthorized access to the goods		X	
Procedures for the control of incoming goods, compliance with registered cargo	X	X	X
Checking the seal of incoming goods	X		X
Separate storage of different types of goods	X	X	X
Monitoring loading procedures by authorized personnel	X	X	
Procedures for sealing and check of damage	X		X
Check of cargo compliance to cargo documentation		X	
Recruitment and settlement of personnel	X	X	X
Education of personnel	X	X	X
Business information security	X	X	X
Compilation			
Sum	**12**	**13**	**10**

Costs

	Low	Average	High	
Logical protection	0	1	0	
Electronic protection	0	0	2	
Physical protection	0	1	0	
Sum points	**0**	**2**	**2**	**4**

Regarding the risk of theft the terminals' decisions for developing preventing actions, is concluded by the same reasoning as for road terminals, ie. whether the rail or combined transport terminal is responsible also for previous / subsequent shipments. This determines to a large extent the resources which the terminal company will spend on a security certification and in this context there are crucial differences between the standards appropriate for this situation. The biggest difference is the lack of applicability of TAPA, regarding the possibility of using the standard for other than road transport modes. The consequence is that this restriction makes it impossible to achieve efficiency when the business purpose is to integrate different transport modes. If TAPA would be used despite the drawbacks of such an

arrangement, this would require an additional standard certification for covering the actions not applied by TAPA. In this perspective, it should probably be more efficient to adapt a standard that covers the areas which the company will be connected to. AEO is in this context, the option which meets the requirements for an operator of rail and combined terminals, the best. ISO 28000 has no actions for preventing thefts and is therefore not suitable to adopt.

Port terminal

Costs

	Low	Average	High	
Logical protection	0	1	0	
Electronic protection	0	0	2	
Physical protection	0	1	0	
Sum points	**0**	**2**	**2**	**4**

Set of criteria

	AEO	TAPA	ISO
Criteria			
Security of buildings	X	X	X
Monitoring of buildings		X	X
Staffing and coverage of unlocked doors and access point to a restricted area	X	X	
Passing check	X	X	X
Procedures for the control of incoming goods, compliance with registered cargo	X	X	X
Checking the seal of incoming goods	X		X
Separate storage of different types of goods	X	X	X
Recruitment and settlement of personnel	X	X	X
Education of personnel	X	X	X
Business information security	X	X	X
Compilation			
Sum	**9**	**9**	**9**

According to the table above, the three comparable standards meet the same amount of criteria, criteria of particular relevance should therefore be selected to increase the ability to assess which standard is the most appropriate. Since there are few differences in the actual measures it is of major importance to assess the overall performance and the most important aspect in this context is the global applicability. The port is an international operator and by applying a standard which both reduces the possibility of global distribution as well as access to intermodal transports, it may become difficult to ensure the effectiveness of the security system. For global distribution, only TAPA and ISO 28000 are enabling these flows. AEO may however be adapted for global transports via the link to the WCO, but this possibility is not discussed further in this report. For intermodality both AEO and ISO 28000 are applicable, while TAPA is not, which probably excludes the possibility for TAPA to be an established standard for security certification in ports. In a different perspective ISO 28000 covers the same security risks as ISPS and it is therefore important to questioning the value of certification according to ISO 28000, since the port still has to comply with ISPS. AEO covers theft and trafficking as well as facilitating customs clearance, which may be of importance since it also generates efficiency.

Land transportation

Set of criteria

	AEO	TAPA	ISO
Criteria			
Usage of technical solutions preventing unauthorized access to the goods		X	
Monitoring loading procedures by authorized personnel	X	X	
Procedures for sealing and check of damage	X		X
Check of cargo compliance to cargo documentation		X	
Recruitment and settlement of personnel	X	X	X
Education of personnel	X	X	X
Business information security	X	X	X
Compilation			
Sum	**5**	**6**	**4**

Costs

	Low	Average	High	
Logical protection	0	0	0	
Electronic protection	0	1	0	
Physical protection	0	0	0	
Sum points	**0**	**1**	**0**	**1**

It is obvious that it is mainly thefts and vandalism that are priority from the carriers' point of view and from the table above TAPA appears to be the strongest of the selected standards. TAPA covers largely all of the critera as well as the single most important measure, high security seal. When a high security seal is used in combination with a solid cargo carrier, such as a container, it is much more difficult for unauthorized persons to gain access to the cargo. For road transports TAPA should therefore constitute a suitable alternative in cases where the actual carrier is to be transported by truck only.

For rail transports TAPA is not appropriate to use since it can only be applied to road transports. This does not exclude the possibility to use high security seals in order to obtain a high level of cargo security. AEO is an interesting option for land transportation operators since the application covers threats related to theft, which is not covered in ISO 28000. Actions for the prevention of thefts are of such importance as there is no reason to choose ISO 28000 for certification.

Sea transportation

Costs

	Low	Average	High	
Logical protection	0	0	0	
Electronic protection	0	0	0	
Physical protection	0	0	0	
Sum points	**0**	**0**	**0**	**0**

Set of criteria

	ISPS	AEO	TAPA	ISO
Criteria				
Security of buildings	X	X	X	X
Monitoring of buildings	X		X	X
Staffing and coverage of unlocked doors and access point to a restricted area	X	X	X	
Passing check	X	X	X	X
Usage of technical solutions preventing unauthorized access to the goods	X		X	
Procedures for the control of incoming goods, compliance with registered cargo	X	X	X	X
Checking the seal of incoming goods	X	X		X
Check of cargo compliance to cargo documentation	X		X	
Recruitment and settlement of personnel		X	X	X
Education of personnel		X	X	X
Dissemination of information	X			X
Business information security		X	X	X
Compilation				
Sum	**9**	**8**	**10**	**9**

TAPA meets most of the selected criteria, but given the lack of compatibility with sea transportation the standard is not a proper basis for certification of maritime transport. AEO, on the other hand, lacks in the global applicability but since AEO is linked to the WCO, the global coverage should probably not be a major problem. It must, however, be noted that AEO complements ISPS Code well in areas where ISPS is lacking and the AEO should therefore be considered as a potential alternative if additional steps shall be taken to improve the security level. Certification according to AEO will, in particular, increase the security against thefts and trafficking, which are neither covered by the ISPS Code or ISO 28000. In addition ISO 28000 adds no further value beyond the AEO and criteria already covered by the ISPS Code. At the same time it should be noted that it probably would be enough for maritime carriers to meet the commitments required in the mandatory rules. However, direct benefits of expanded certification are difficult to find.

Conclusions

The aim of the project has been modified during the process, which has been necessary in the creation of a report with useful content. The report is therefore in the current edition sought to highlight the security standards that are of most relevance to each operator in the transport chain, as well as describing the security criteria these operator should focus on. The conclusions of this work are presented in this part.

Various motives to security certification

Different operators prioritize various measures to reduce risks in areas of importance for the operator, which complicates the work of a universal standard functioning with a wide security focus in mind..

It is in the report demonstrated that there are conflicts of interest in the security initiatives. In practice this means that different stakeholders prioritize different measures to reduce the risk of disadvantages in fields which have been set out as important to the individual stakeholder. A system in which the security to some extent is based on this choice also creates aggravating circumstances related to the fact that security risks often occurs in links where the security measures are low. An example of this problem is in cases where the interest of protecting the cargo against theft is more important than the risk of usage of a transport carrier for smuggling purposes. Such a system creates lacking security since an overall global standard is missing, or at least is not fully developed.

Too many security standards

The large number of security standards makes it difficult to find a common agreement in which the overall security will be harmonized.

According to the wide range of security standards it can be concluded that further initiatives do not solve the problem of inefficient certification processes. Today it is too difficult to find global solutions that are internationally as well as nationally efficient. By extension, this means both reduced security and loss of efficiency, where the results of these would probably be better by consolidating and reducing the number of standards. This is above all an important aspect seen from the stakeholders' perspective because simplified certification processes are likely to give rise to greater ambition for certification. AEO is simultaneously an example of standard which appears to increase transparency in relation to other standards, including the WCO, TAPA, and ISO 28000. This may be a first step towards a more efficient and globally wide security system.

Cooperation for improved efficiency

Governments should cooperate internationally to carry out a survey of the effectiveness in the current security system. There is a risk that today's structure creates inefficient security solutions that ultimately seem to affect the global security. States should cooperate in order to make suggestions on how efficiency can be achieved.

There is a considerable lack of international cooperation in order to enable a more efficient development of effective global security. An example over the consequences of such non-cooperation is the harsh rules which in short should be implemented for shipping to the U.S. as a destination. These implements include 100% scan which imposes a huge burden on ports with operating traffic to U.S. waters, the value of such a measure is at the same time not entirely clear. The contrast between the actions of this character and actions taken in the rest of the international shipping industry is very large, the security threats occurs at the same time particularly in those parts of the chain where the security is at its lowest. It is justified by international regulation to make a correction of this imbalance, thus allowing better allocation of resources, which probably also reduces the risk of over- versus under sized security measures.

The value of stolen goods is increasing

It has been stated that the value of goods stolen within the transport chain is considerably increasing, which affects the structure of cost as well as the damage for every single occasion. The attacks are getting more severe and probably this increases the ambition for strengthen the security against non-authorized persons.

The increased value of stolen goods may depend on several factors. During the work of this project information about new routines for coding criminal activities against the transport chain, developed by the Swedish police, has been taken into account. Before these routines were introduced the true cost for cargo crimes was camouflaged since no separation was made between different types of thefts. Through better coding it is nowadays easier to follow up the costs associated to attacks targeting the transport chain. The project has also experienced that the knowledge of planning criminal activity, as well as methods for completion, is increasing among criminals, which likely increases the precision and approach of the attacks. Such an approach might be thefts of entire trailers, which equaly to increased knowledge probably causes the current increase in stolen goods value.

The security threats' impact on business

The transportation industry is experiencing that thefts and vandalism are the crimes that cause most damange of the security threats that have been described in this project.

Since the transportation industry often consists of or represents stakeholders with their interest focused on the goods, it is not incomprehensible that crimes regarding thefts and vandalism are high priority among these actors. The industry is also agreed that smuggling is a problem but they don't believe this should be solved by the individual carrier. Terrorism and trafficking are threats that do not involve any appreciable impact on the individual actor and action against such attacks is therefore not a priority.

1 Inledning

I en värld som blir allt osäkrare ökar också kraven på aktiva åtgärder för att förhindra att kriminella handlingar kan fullbordas. Beroende på vad som avses så innebär detta att resurser i varierad omfattning måste avsättas från samhället samtidigt som regler måste utformas för att skapa incitament i preventivt och reparativt syfte. För att lösa en del av denna problematik har standarder på senare tid haft stor betydelse då certifieringsprocesser genom kvalitetsgranskning fastställer om en förbestämd säkerhetsnivå kan upprätthållas eller inte.

Olika verksamhetsområden utsätts för olika typer av säkerhetshot och särskilt påtaglig är hoten som riktas mot transportbranschen. Att risken för säkerhetsintrång är extra hög i denna verksamhet sammanfaller med det behov av förflyttning som vissa typer av brott mot säkerheten kräver. Till sådana brottshandlingar hör framförallt smuggling och trafficking, där den bakomliggande avsikten till brotten är att realisera det mervärde som följer av att egendom eller person förflyttas mellan två platser. På samma sätt så kan följdeffekterna av sådana handlingar bli mycket allvarliga, framförallt om smuggling är ett delmoment i fullbordandet av en terroristhandling. I ett sådant perspektiv är det också lätt att förstå hur viktigt det är med kontrollfunktioner som övervakar transportkedjan, för att på så sätt täppa till säkerhetsluckor och förhindra uppkomsten av negativa sidoeffekter.

1.1 Bakgrund

De ökade kraven på reglering i syfte att förhindra realisering av de säkerhetshot som riktas mot transportbranschen, har på senare tid givit upphov till en snabb utveckling av nya säkerhetsstandarder. Den utlösande faktorn för denna expansion får anses tillhöra terroristattackerna mot USA som inträffade den 11:e september 2001. Denna händelse blev startskottet för en kraftig efterfrågan på säkerhetsrutiner och till de första standarderna hör ISPS-koden, som har till uppgift att försvåra terroristbrott i anknytning till hamn- och fartygsverksamhet. Detta är enbart en av många standarder och det är inte ovanligt med specifika ändamål där åtgärdspaketen endast täcker en viss del av transportkedjan, likt ISPS-koden.

Den snabba utvecklingen av säkerhetsstandarder har emellertid inneburit att någon samverkan varit svår att genomföra, vilket har skapat ett relativt svårgenomsiktligt kluster med brister i den övergripande helhetsbilden. Detta innebär förutom försvårande certifieringsprocesser och merarbete, också att säkerheten kan komma att påverkas negativt då nivån av säkerhet till största delen beror på vilken standard som tillämpas på den aktuella transporten. Införandet av säkerhetsstandarder är således inte att betrakta som en enhetlig och fulländad åtgärd som garanterar en förbestämd säkerhetsnivå för alla transporter och alla transportslag. Särskilt påtagligt är detta resonemang i fall då en aktör endast har ambition att uppfylla de obligatoriska säkerhetskraven, som exempelvis ligger till grund för ISPS-koden, och där andra standarder med hårdare krav och tuffare åtgärder i praktiken kan lämnas utan avseende.

1.2 Syfte

Syftet med detta projekt har varit att kartlägga och undersöka vilka åtgärder som kan vidtas för att öka säkerheten inom transportkedjan. Detta har skett genom att analysera utbudet av säkerhetsstandarder, både de som måste uppfyllas genom tvingande reglering samt de som är fria att tillämpa beroende på den egna ambitionsnivån. Denna analys har resulterat i en mer utförlig och djupgående kartläggning där det primära syftet varit att skapa ett urval av standarder för att därtill kunna undersöka vilka kriterier som ligger till grund för respektive standard. Till detta har projektet haft till syfte att skapa en nulägesbild över de säkerhetsrelaterade hot som transportkedjan utsätts för, samt att beskriva i vilken omfattning som verkställande hot kan anses förekomma.

1.3 Avgränsning

Projektet har inte behandlat effekterna av tillämpade standarder för enskilda transportarbeten. Detta innebär att innehållet i denna rapport istället bygger på att skapa förståelse för det arbete som i dagsläget krävs för att kunna upprätthålla en bestämd nivå av säkerhet, och att i sammanhanget presentera ett urval av tillgängliga standarder. Rapporten kan i detta perspektiv därför med fördel användas som grund för fortsatt forskning och fördjupning inom området, där fokus mycket väl kan vara att utvärdera effekterna för specifika transporter.

1.4 Metod

Metodiken som använts i arbetet med att framställa denna rapport har i huvudsak anpassats efter de olika faser som studien bygger på. Dessa moment beskrivs i följande avsnitt.

Fas 1.
Arbetet påbörjades med ett antal interna projektmöten där projektets mål, tidsplan och syften bearbetades. I ett tidigt skede sammanställdes även ett antal frågor vilka sedan användes under de intervjuer som genomfördes. Deltagande företag/organisationer var förutbestämda i projektets förstudie. De frågor som låg till grund för intervjuerna kvalitetssäkrades genom Högskolan i Borås, med hjälp av professor Håkan Torstensson. Även Polismyndigheten fick tillfälle att yttra sig över de frågor som skulle användas i intervjuerna.

I nästa skede intervjuades ett antal företrädare för transportnäringen, vilka bestod av följande företrädare:

1. Högskolan i Borås, Prof Håkan Torstensson
2. Polismyndigheten i Västra Götaland, Kriminalinspektör Per-Arne Nilsson
3. Göteborgs hamn, Säkerhetschef Thomas Fransson
4. Green Cargo, Head of Security Tommy Ahlestedt
5. Cargo Net Magnus, Berg Labor
6. Schenker, Corporate Risk Manager – Security Daniel Ekwall

Utöver personliga intervjuer så har det huvudsakliga arbetet bestått av faktainsamling, bearbetning och förståelse, vilket har skapat en god kunskapsbas för det material som har sammanställts i denna rapport.

Fas 2.
Arbetet under fas 2 inriktades på att försöka beskriva de säkerhetsstandarder och förordningar som under projekttiden fanns tillgängliga på marknaden, i syfte att skapa en god översikt över utbudet.

Metodiken under projektfasen bestod till största delen av omfattande litteratursökning, både i tryckt och digital skrift. Arbetet koncentrerades därefter på att försöka sammanställa de data som framkom genom litteratursökningarna då några jämförande uppgifter inte fanns tillgängliga. Detta resulterade i en sammanställning där innehållet för respektive standard anpassades för att kunna användas för analog jämförelse dem emellan.

Fas 3.
Under detta avsnitt användes uppgifterna från föregående fas för att genomföra ett urval bland de standarder som blev beskrivna. Detta innebar en detaljerad genomgång över innehållet i respektive standard och ett antal urvalskriterier fastställdes därefter som metod för urvalet. De standarder som genom denna process valdes för en mer detaljerad beskrivning sammanställdes sedan i en matris för att underlätta jämförelse. Kriterierna i denna matris består av både generella och detaljerade parametrar vilket skapat en bättre förståelse för vilka åtgärder som ligger till grund för samt styr valet av standard. Resultatet av dessa jämförelser har sedan analyserats och diskuterats i arbetets senare del för att på detta sätt skapa ökad möjlighet till tolkning och förståelse. Underlaget till detta avsnitt har huvudsakligen utgått från uppgifter hämtade från både tryckt och digital skrift.

Fas 4.
Fas 4 består av rekommendationer kring vilka faktorer som respektive aktör i logistikkedjan bör ta hänsyn till vid beslut om införande av ett säkerhetsinitiativ. Dessa rekommendationer baseras uteslutande på de uppgifter som rapportens tidigare faser har behandlat och arbetet i denna del har huvudsakligen baserats på förståelse av innebörden kring dessa uppgifter. Kopplingar har gjorts både till fas 1 och 3 genom att slutsatserna från dessa delar kopplats samman under den fjärde fasen. Avsnittet utgår till största delen från egna reflektioner och texten är därför anpassad till diskussionsformatet snarare än att utgöra en ren faktapresentation. Delfasen avslutas med projektets slutsatser.

FAS 1 – Nulägesanalys av säkerhetshot mot transportkedjan

2 Intervjuer

Det kunde under intervjuerna konstateras att samtliga deltagare i princip har samma inställning till problemen, med endast ett fåtal skillnader. Nedan följer ett antal punkter som sammanfattar resultaten från samtalen. Frågeställningarna återfinns som bilaga 2.

- Samtliga anser att hela den aktuella problematiken är ett bekymmer, vilket kostar onödigt mycket pengar. I en rapport från TAPA[9] beskrivs att ett logistikföretag har ett securityrelaterat svinn på ca 0,025 % till 0,14 % av omsättningen. En intressant parallell är att huvuddelen av projektdeltagarna (transportföretag & organisationer) påstår att de har betydligt större kostnader för godsskador än för kriminella handlingar. I branschen finns det företag som har godsskador på upp mot 3 % av transporterat godsvärde om året. Detta är ett extremt fall och siffran återfinns bland dem som transporterar särskilt ömtåliga produkter.

- Aktuellt problem uppstår i huvudsak under uppställning terminalnära, eller under uppställningstider på annan plats (gäller både väg & järnväg).

- De nationella aktörerna påstår att det är ett problem att polismyndigheterna runt om i landet saknar nationell samordning av dessa tillgreppsbrott. Stora problem uppstår således då ett brott begås i ett län och upptäcks i ett annat. Vidare försvåras den enligt många så vikiga informationsspridningen över landet av detta faktum.

- Samtliga har investerat stora pengar på fysiskt skydd av terminaler/ lokaler/områden. Det har dock inte kommit till detta projekts kännedom om vilka summor det handlar om. Inte heller vilka kostnader problemen står för, då aktörerna hänvisar till polisens statistik och säger att kostnaderna ligger i linje med denna statistik, Göteborg hamn är undantaget då det inte tillgripits något under år 2008 samt år 2009. Detta på grund av de omfattande säkerhetsinstallationerna vilka har genomförts.

- Samtliga aktörer är överens om att framtiden är svår att förutse, dock påstås det (vilket går att säkerställa på kriminologisk väg) att brottslighetens modus operandi (tillvägagångssätt) flyttas geografiskt. Påståendet att den kriminalitet som i dagsläget finns i Östeuropa, samt till viss del i området kring London, kommer att drabba Sverige i framtiden, är sannolikt. Vilket i sin tur ger för handen att kapningar, utpressning och väpnade rån inte bör överraska någon inom en 10 års period.

[9] The Transported Asset Protection Association (TAPA) is a unique forum that unites global manufacturers, logistics providers, freight carriers, law enforcement agencies, and other stakeholders with the common aim of reducing losses from international supply chains.

- Daniel Ekwall Schenker säger att ”en orsaksdiskussion bör föras till aktuellt resonemang; alla pratar om security men få talar om problemen/orsakerna”. Detta diskuteras vidare under tes 2, se vidare avsnitt 7.2.

- Mörkertalet inom antalet anmälda brott och genomförda brott kan antas vara stort, trots att de olika aktörerna påstår att alla brott anmäls. En anledning kan vara att kunskap om brottets existens saknas, det vill säga att brottet kanske inte alltid uppfattas som ett brott. Det kan lika gärna uppfattas vara saknat gods, eller att kunden i sin tur ställer krav på avsändaren i tron om att det är felhanterat, i stället för att polisanmäla brottet. Med de stora volymerna som transporteras dagligen är denna konsekvens fullt naturlig, se vidare avsnitt 7.3.

- Branschen känner en viss avsaknad av engagemang eller delaktighet från försäkringsbolagens sida i aktuell diskussion. Transportrelaterade säkerhetshot är ett problem som samtliga aktörer inom hela transportkedjan måste engagera sig i, varvid försäkringsbolagen har en given plats. Främst vad gäller krav på de aktörer som fysiskt hanterar godset, men även som en samhällsaktör med god insikt i skadekostnader såväl som statistik.

3 Kända säkerhetshot och hinder samt dess sannolikhet i olika delar av transportkedjan

Detta kapitel avslutas med en sammanfattande matris som åskådliggör en kvalitativ sannolikhetsbedömning över risker/hot mot transportkedjan som är aktuella i detta projekt. I bedömningen har det tagits hänsyn till statistikunderlag samt till resultaten från de intervjuer som genomförts. De kända hoten som beskrivs i projektet är: stöld, skadegörelse, smuggling, trafficking samt terrorism.

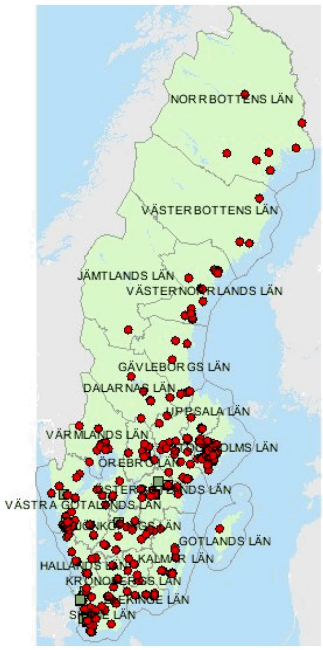
Bedömningskriterierna har utgått från en skala 1-5 där fem är det mest sannolika och således ett är minst sannolikt.

3.1 Analyserade säkerhetshot

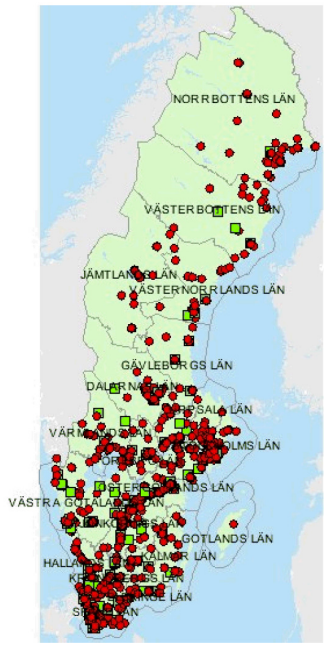
3.1.1 Stöld

När det gäller stöld är statistikunderlaget[10] tämligen gott i rapporten från Polismyndigheten Västra Götaland & Skåne. Av vikt är att känna till skillnaden mellan de två olika aktuella brottskoderna, *9803* (tillgrepp av lastbil, släpfordon eller lastbärare avsedd för yrkesmässig godsbefordran) och *9804* (stöld ur eller från lastbil, släpfordon eller lastbärare avsedd för yrkesmässig trafik). Under år 2008 anmäldes det i hela Sverige totalt 528 tillgrepp med brottskod 9803 varav 333 st av fordon överstigande 10 ton samt 1625 tillgrepp med brottskod 9804.

Totala antalet brott under år 2008: 2140 st.



Figur 1a - Anmälda brott med brottskod 9803 under 2008[12]



Figur 1b - Anmälda brott med brottskod 9804 under 2008[12]

Röd prick motsvarar ett brott, grön ruta 2-5

[10] Polisens rapport om transportsäkerhet 2008, Per-Arne Nilsson, Polismyndigheten i Västra Götaland

3.1.2 Skadegörelse

Enligt statistik från brottsförebyggande rådet har det under år 2008, i hela Sverige anmälts 45 486 brott som rubriceras som skadegörelse mot motorfordon. För att kunna analysera omfattningen görs ett antagande att den totala andelen fordon för yrkesmässig transport är 5 gånger mindre[11] än för privata fordon. Detta ger ett knapphändigt underlag att nästan 10 000 av dessa brott per år i Sverige, är riktade mot fordon avsedda för yrkesmässig godsbefordran. Ett mer exakt antagande om värdet av detta görs inte, men en försiktig tanke kan vara att om varje brott kostar i storleksordningen 5000:- (exklusive avbrottskostnader och nedlagda resurser) så ger det en summa av 50 miljoner.

3.1.3 Smuggling

Enligt statistik från brottsförebyggande rådet anmäldes 3413 smugglings- och tullbrott i Sverige under år 2008. Nedan följer en tabell över utvecklingen av dessa brott (samtliga siffror kommer från brottsförebyggande rådet):

År	Smugglings- och tullbrott
2008	3413
2007	2934
2006	2156
2005	1704

När det gäller dessa tullbrott slår i princip samtliga i projektet inblandade parter ifrån sig och påstår att det är en Tullproblematik, dock inte polismyndigheten som påstår att detta är ett mycket stort hot mot samhället. Behov föreligger således att fördjupa sig i denna fråga, av vikt torde vara att knyta samverkansband mellan Tullmyndigheten och transportkedjans aktörer, det syns inte minst i den analys som följer om lagstiftningar (frivilliga/påtvingade standarder).

3.1.4 Trafficking

Trafficking har inte någon av projektets deltagare kommit i kontakt med och det kan således enbart konstateras att det under år 2008 upprättades 15 stycken polisanmälningar i detta avseende.

[11] Statistik från Transportbilsguiden.se/ antalet nyregistrerade bilar under början av 2009.

3.1.5 Terrorism

Enligt statistik från Högskolan i Borås[12] kan nämnas att under år 2006 genomfördes totalt 6653 terroristattentat, varav 152 skedde i Västeuropa med 6 döda (av totalt 12 065 döda) samt 35 skadade (av totalt 20 969 skadade) som följd. Sifforna tyder på att detta utgör ett hot om än i mindre omfattning.

Ingen av de intervjuade aktörerna kunde se hur de rimligen kan drabbas av ett terroristbrott. Detta gör att risken för terrorism inte bedöms hög men det fråntar inte tyngden/värdet av att diskutera denna fråga vidare. Här följer en kort sammanfattning av vad som nämndes kring dessa frågor:

- Bra att det kommer lagstiftning inom området, vilket ger argument som syftar till att höja säkerhetsnivån.
- Hur skall man skydda sig mot terrorister?
- Sverige är ju ett lågriskland, det kommer inte att hända här.

[12] D.Ekwall Transportindustriförbundets securitykommitté, möte om securityfrågor 23 mars

3.2 Transportkedjan

Nedan följer en uppställning utifrån de länkar som kan ingå i en intermodal transportkedja. För varje länk har en bedömning av nuläget gjorts som bygger på tillgänglig statistik samt resultat från gjorda intervjuer. Sannolikheten för att säkerhetshoten ska uppträda är bedömda i en femgradig skala, där 5 är det mest sannolika och således 1 minst sannolikt.

3.2.1 Avsändare

Med avsändare avses normalt den punkt där transportkedjan startar, t.ex. utlastningen på en industri eller en lagerpunkt. En avsändare är då den som lastar godset i den last-bäraren som sedan används i hela den intermodala transportkedjan.

Säkerhetshot	Sannolikhet	Kommentar
Stöld	2	Relativt låg omfattning, då de flesta stölderna sker terminalnära på en obevakad uppställningsplats. Det brott som sker hos avsändare är främst bedrägeri. Tittar man internationellt är det hos avsändaren en något högre risk för rån mot transportören.
Skadegörelse	3	Sker med viss omfattning, helt beroende på geografiskt läge. Terminaler är inte särdeles utsatta även om det förekommer. Företag vilka har godsutlastning är i högre grad utsatta för både olaga intrång samt skadegörelse.
Smuggling	1	Ingen uppgift, varför den bedöms som mycket låg. Dock är det ett växande problem med smuggling som får stora konsekvenser för samhället.
Trafficking	1	Ingen uppgift, varför den bedöms som mycket låg.
Terrorism	1	Ingen uppgift, varför den bedöms som mycket låg.

3.2.2 Landsvägsterminal

Med en landsvägsterminal avses en terminal där godset troligtvis lastas om från en lastbärare till en annan. I vissa fall förekommer det mellanlagring av godset. Alla enheter som kommer till och från terminalen går med landsvägstransport. Ett exempel på en landsvägsterminal kan vara en DHL- eller Schenker terminal.

Säkerhetshot	Sannolikhet	Kommentar
Stöld	3	Stölder förekommer med viss omfattning. Under senare tid har stölderna blivit grövre/större då hela ekipage stjäls.
Skadegörelse	2	Förekommer, dock utgör det inget större problem för branschen. Som kommentar kan sägas att det i vissa fall anmäls ett skadegörelsebrott som egentligen skulle kunna vara förberedelse till stöld (kapellskärning).
Smuggling	2	Utgör inget problem, dock förekommer det inom landsvägsterminaler där utrikesgods hanteras. Erfarenheten säger att ett antal aktörer inom transportkedjan hanterar smuggelgods i sina ekipage utan att veta om det, så kallad extralastning.
Trafficking	1	Ingen uppgift, varför den bedöms som mycket låg.
Terrorism	1	Ingen uppgift, varför den bedöms som mycket låg.

3.2.3 Kombiterminal *(Järnvägs och kombiterminal)*

På en järnvägsterminal sker omlastning från väg till järnväg eller omvänt. Till skillnad från en kombiterminal sker även omlastning av godset mellan olika lastbärare t.ex. från järnvägsvagn till trailer, växelflak eller container. På en kombiterminal sker enbart en omlastning med en och samma lastbärare från väg till järnväg eller vice versa.

Säkerhetshot	Sannolikhet	Kommentar
Stöld	3	Stölder förekommer med viss omfattning. Under senare tid har stölderna blivit grövre/större då hela ekipage stjäls
Skadegörelse	2	Förekommer, dock utgör det inget större problem för branschen. Som kommentar kan sägas att det i vissa fall anmäls ett skadegörelsebrott som egentligen skulle kunna vara förberedelse till stöld (kapellskärning).
Smuggling	1	Ingen uppgift, varför den bedöms som mycket låg.
Trafficking	1	Ingen uppgift, varför den bedöms som mycket låg.
Terrorism	1	Ingen uppgift, varför den bedöms som mycket låg.

3.2.4 Hamnterminal

På en hamnterminal sker omlastning från landsväg eller järnväg till en sjötransport eller omvänt. Eftersom det framförallt är intermodala transportkedjor som analyserats är utgångspunkten att det inte sker någon omlastning av godset till någon annan lastbärare.

Säkerhetshot	Sannolikhet	Kommentar
Stöld	2	Det har förekommit i hög utsträckning. I Göteborgs Hamn, som är aktuellt i detta projekt, har det under de senaste två åren gjorts ett par större säkerhets-höjande investeringar. Detta har i nuläget bidragit till en total avsaknad av inbrott/stölder.
Skadegörelse	2	Det har förekommit i hög utsträckning. I Göteborgs Hamn, som är aktuellt i detta projekt, har det under de senaste två åren gjorts ett par större säkerhets-höjande investeringar. Detta har i nuläget bidragit till en total avsaknad av skadegörelse.
Smuggling	4	Förekommer och anledningen till den höga siffran i matrisen är att i hamnterminalen kanaliseras smugglingen. Införandet av ISPS samt de nationella förordningarna, vilka hanterar främst terrorist-brotten, utgör en försvårande hantering för denna kriminalitet. Därför kommer det med stor sannolikhet bli helt nya smugglingsvägar, exempelvis andra intermodala transportvägar.
Trafficking	3	Det förekommer människosmuggling inom hamnområdet, vilket inte nödvändigtvis utgörs av traffickingbrott[13] utan mer troligt personer vilka vill in eller ut ur Sverige.
Terrorism	2	Enligt rikspolisstyrelsen är risken låg för en terrorhandling i Sverige, skulle det ske är en hamnanläggning eller fartyg inget otänkbart scenario.

[13] Med trafficking brott menas förflyttning av fattiga människor under slavliknande förhållanden till vad som mer eller mindre är tvångsarbete.

3.2.5 Landsvägstransport

Med landsvägstransport avses transport som sker med motordrivet fordon på väg utanför terminalområden. Eftersom det framförallt är intermodala transportkedjor som analyserats är lastbäraren sannolikt en trailer (påhängsvagn), växelflak eller container.

Säkerhetshot	Sannolikhet	Kommentar
Stöld	3	Under körningen är det i princip ingen risk för stöld. Internationellt syns en ökad trend av falska poliser alternativt falska trafikolyckor vilka kan leda till ett oplanerat stopp med tillhörande brottslig aktivitet. I Sverige är detta mycket ovanligt. Här är det på uppställningsplaster risken är betydande och då framför allt på ”osäkra” platser, vilka är belägna ”terminalnära”. Statistiken säger att brotten begås där de största transportlederna går, (Helsingborg, Göteborg, Åstorp, Jönköping samt Stockholm)
Skadegörelse	3	Här är det uppställningsplaster risken är betydande, framför allt på ”osäkra” platser, vilka är belägna ”terminalnära”. Statistiken säger att brotten begås där de största transportlederna går, (Helsingborg, Göteborg, Åstorp, Jönköping samt Stockholm)
Smuggling	2	Utgör inget problem, dock förekommer det inom landsvägstransporter där utrikesgods hanteras. Erfarenheten säger att ett antal aktörer inom transportkedjan hanterar smuggelgods i sina ekipage utan att veta om det, så kallad extralastning
Trafficking	1	Ingen uppgift, varför den bedöms som mycket låg.
Terrorism	1	Ingen uppgift, varför den bedöms som mycket låg.

3.2.6 Kombitransport

Med kombitransport avses transport som sker på järnväg utanför terminalområden. Lastbäraren, vanligtvis en trailer (påhängsvagn), växelflak eller container, är lastad på en järnvägsvagn.

Säkerhetshot	Sannolikhet	Kommentar
Stöld	2	Under förflyttning är det i princip ingen risk för stöld. Här är det på uppställningsplaster som risken är betydande, framför allt på ”osäkra” uppställningsplaster. När det gäller spårbundna transporter syns ett visst problem på stickspår i samband med personalbyte.
Skadegörelse	2	Här är det på uppställningsplaster/bangårdar som risken är betydande, framför allt på ”osäkra” uppställningsplatser.
Smuggling	2	Utgör inget problem, dock förekommer det inom kombitransporter där utrikesgods hanteras. Erfarenheten säger att ett antal aktörer inom transportkedjan hanterar smuggelgods i sina ekipage utan att veta om det, så kallad extralastning.
Trafficking	1	Ingen uppgift, varför den bedöms som mycket låg.
Terrorism	1	Ingen uppgift, varför den bedöms som mycket låg.

3.2.7 Järnvägstransport

Med järnvägstransport avses transport som sker på järnväg utanför terminalområden med gods som är lastat på järnvägsvagnar.

Säkerhetshot	Sannolikhet	Kommentar
Stöld	2	Relativt låg omfattning vilken inte utgör något stort problem. De problem som infinner sig är på bangårdar, samt till viss del på stickspår i samband med personalbyten
Skadegörelse	2	Förekommer i låg omfattning. Problemen återfinns på uppställningsplatser vilkas geografiska läge gör det möjligt för ungdomar att begå skadegörelse i form av klotter.
Smuggling	2	Utgör inget problem, dock förekommer det inom järnvägstransporter där utrikesgods hanteras. Erfarenheten säger att ett antal aktörer inom transportkedjan hanterar smuggelgods i sina ekipage utan att veta om det, så kallad extralastning.
Trafficking	1	Ingen uppgift, varför den bedöms som mycket låg.
Terrorism	1	Ingen uppgift, varför den bedöms som mycket låg.

3.2.8 Sjötransport

Med sjötransport avses transport som sker med fartyg på öppet hav utanför hamnområden. Inre vattenvägar har inte varit föremål för några diskussioner i denna rapport.

Säkerhetshot	Sannolikhet	Kommentar
Stöld	1	Ingen uppgift, varför den bedöms som mycket låg.
Skadegörelse	1	Ingen uppgift, varför den bedöms som mycket låg.
Smuggling	3	Förekommer med viss omfattning främst inom container- samt trailertransporter från tredjeland. Erfarenheten säger att ett antal aktörer inom transportkedjan hanterar smuggelgods i sina ekipage utan att veta om det, så kallad extralastning.
Trafficking	2	Det förekommer människosmuggling inom sjötransporter, vilket inte nödvändigtvis utgörs av traffickingbrott[14] utan mer troligt av ”fripassagerare” vilka vill in eller ut ur Sverige.
Terrorism	2	Enligt rikspolisstyrelsen är risken låg för en terrorhandling i Sverige, skulle det ske är ett fartyg dock inget otänkbart scenario.

3.2.9 Mottagare

Med mottagare avses den part som är slutdestinationen i transportkedjan.

Säkerhetshot	Sannolikhet	Kommentar
Stöld	2	Relativt låg omfattning, då de flesta stölderna sker terminalnära på obevakad uppställningsplats. Det brott som sker hos mottagare är främst bedrägeri. Tittar man internationellt är det hos avsändaren en något högre risk för rån mot transportör.
Skadegörelse	3	Sker med viss omfattning, helt beroende på geografiskt läge. Terminaler är inte särdeles utsatta även om det förekommer. Företag vilka har godsutlastning är i högre grad utsatta för både olaga intrång samt skadegörelse.
Smuggling	1	Ingen uppgift, varför den bedöms som mycket låg. Dock är det ett växande problem med smuggling som får stora konsekvenser för samhället.
Trafficking	1	Ingen uppgift, varför den bedöms som mycket låg.
Terrorism	1	Ingen uppgift, varför den bedöms som mycket låg.

[14] Är förflyttning av fattiga människor under slavliknande förhållanden till vad som mer eller mindre är tvångsarbete.

3.2.10 Sammanfattning

Bedömningen av sannolikheten för de olika säkerhetshoten i respektive länk i den intermodala transportkedjan sammanfattas i tabellen nedan.

Länk/ Säkerhetshot	Stöld	Skade-görelse	Smugg-ling	Traf-ficking	Terrorism
Avsändare	2	3	1	1	1
Landsvägsterminal	3	2	2	1	1
Kombiterminal	3	2	1	1	1
Hamnterminal	2	2	4	3	2
Landsvägstransport	3	3	2	1	1
Kombitransport	2	2	2	1	1
Järnvägstransport	2	2	1	1	1
Sjötransport	1	1	3	2	2
Mottagare	2	3	1	1	1

Grafen nedan åskådliggör sannolikheten för tidigare nämnda och analyserade säkerhetshot. Med en koppling till var inom den intermodala transportkedjan hoten eventuellt inträffar.

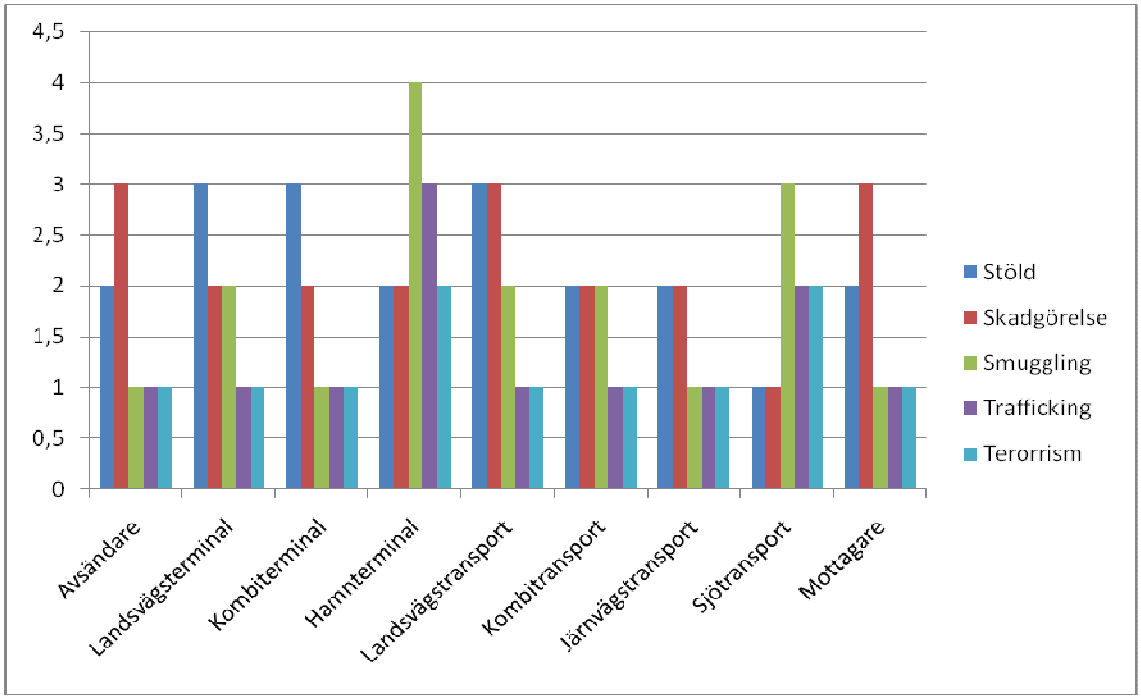


Diagram 1 - Sannolikheten för olika säkerhetshot i en intermodal transportkedja

Källa: D.Ekwall Transportindustriförbundets securitykommitté, möte om securityfrågor 23 mars./ EWC Freight Crime Bulletins 2002-2009

4 Ekonomisk påverkan av säkerhetshot i olika delar av transportkedjan

Under projektet har det varit mycket svårt att få ta del av exakta uppgifter om den ekonomiska påverkan, då det i branschen uppfattas som företagshemlig information. Även andra liknande projekt eller forskare har inte kunnat mer exakt beskriva denna påverkan, vilket påvisar att detta område skulle behöva analyseras ytterligare.

Bedömningen i detta dokument är grundad på polisens uppfattning om antalet tillgrepp (brottskod 9803 och 9804) samt ett beräknat medianvärde vad avser det anmälda godsvärdet. Beräkningar påvisar att respektive tillgrepp har en kostnad på cirka 5000 SEK. Då är hela den inrapporterade summan fördelat på samtliga brott inom Sverige under år 2008. Motsvarande siffra för år 2007 är 2400 SEK.

Om man sedan delar upp det totala antalet brott under transportkedja erhåller man resultatet i diagrammet nedan. Diagrammets staplar visar den ekonomiska effekt tillgreppen utgör, variablerna är satta mellan ett och fem där 1 är lägst (knappt märkbar påverkan) och 5 är högst (extrem påverkan).

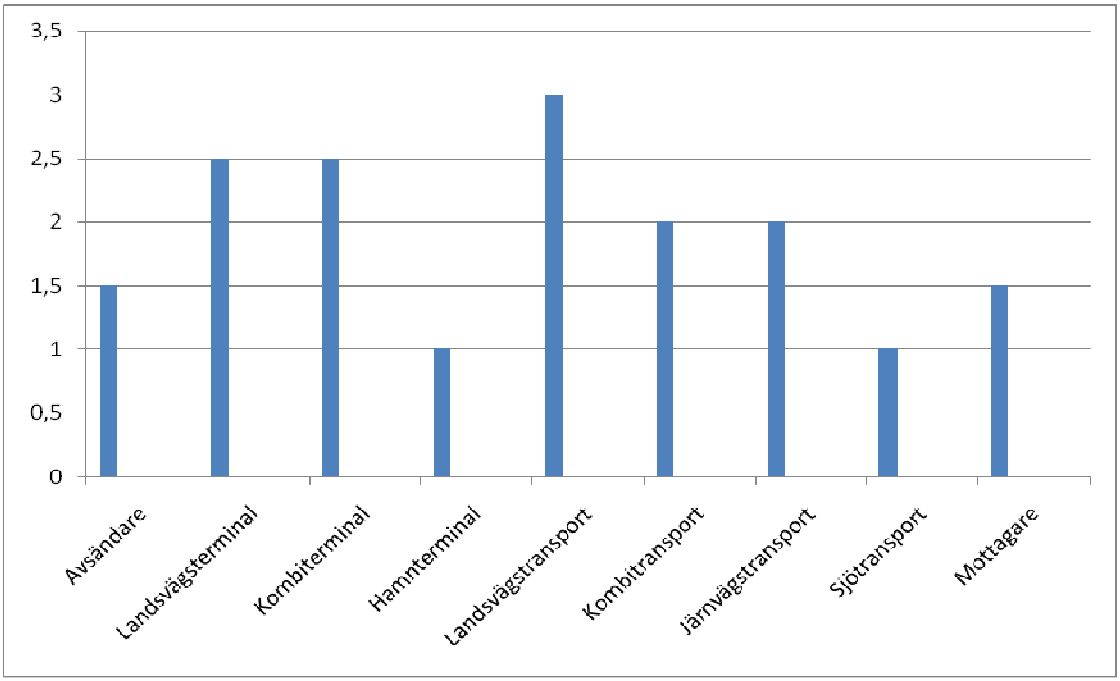


Diagram 2 - Ekonomisk påverkan av säkerhetshot i olika delar av en intermodal transportkedja

Då denna transportkedja är en utgångspunkt i projektet är diagrammet presenterat utifrån denna. Med enkla medel kan man utifrån EWC Freight Crime Bulletins 2002-2009, dra parallellen att exempelvis en säker parkering orsakar 30% mindre ekonomiska skador än en osäker parkering.

I Europa uppgår svinnet till 75 miljarder kronor[15] inom hela transportkedjan, Sveriges andel anses ligga på ca 2 miljarder kronor. Detta är siffror från Europaparlamentet och avser troligen hela varuflödet från fabrik, utlastning, terminalhantering, transport samt leverans till butikens hyllor motsvarande. Således återfinns det i dessa siffror ett antal förluster som inte är definierade i detta projekt.

Polisen rapporterar att det anmälda godsvärdet för tillgripit gods under år 2008 är 10,8 miljoner SEK.

Siffror gör gällande (SIKA 2006) att det transporteras gods till ett totalt värde av 2061,6 miljoner SEK årligen i Sverige. TAPA påstår att totalsvinnet uppgår till 0,025 – 0,14 % av värdet på transporterat gods. Således skulle spannet bli 51,4-288,6 miljoner SEK årligen. Av detta påstås att 10 % utgörs av stölder, således blir en annan uträkning av kostnaden för stöldskador 5,1 till 28,8 miljoner SEK årligen.

[15] Transportsäkerhetsdagarna 2009, Per-Arne Nilsson, Polismyndigheten i Västar Götaland

5 Motåtgärder i olika delar av transportkedjan

5.1 Beskrivning av tre olika strategier för motåtgärder med en enkel kostnadsbedömning.

5.1.1 Fysiskt skydd

Fysiskt skydd utgörs av hinder vilka syftar till att sänka motivationen hos en gärningsman. Detta görs genom att förlänga tiden för forcering av en byggnads omslutningsyta (dörrar, fönster, portar, väggar eller tak hit hör även låssystemet). Även ett visst mått av buller/oljud i samband med forceringen sänker motivationen hos förövaren. Kostnaden för dessa skydd kan över tiden ses som relativt låga, även om summan vid investeringen kan ses som hög men den långa livslängden hos dessa skydd gör de goda ur riskekonomisk synvinkel.

5.1.2 Elektroniskt skydd

Elektroniskt skydd utgörs av elektronik (inbrottslarm, passage system, kameraövervakning) vilka syftar till att få en tidig detektion av brottet. Detektionen måste sedan leda till en åtgärd, antingen av teknisk eller logisk karaktär. Den tekniska delen av åtgärden kan vara att genom fysisk påverkan på gärningsmannens närmiljö med exempelvis högt ljud eller ljus tvinga fram ett upphörande av angreppet. Alternativt att åtgärden är kopplad till det logiska skyddet med en personell insats av polis eller bevakningspersonal. Kostnaden för detta kan nog ses som relativt hög, både vad avser inköp samt drift av systemen. Här kan även nämnas den allt mer förfinade spårningstekniken vilket möjliggör att i realtid följa godsets position med hjälp av satelliter (gps) eller annan radiopejl-utrustning.

5.1.3 Logiskt skydd

Logiskt skydd utgörs främst av administrativa skyddsåtgärder som genom riktlinjer, instruktioner och rutiner, syftar till att människor skall vidta korrekta åtgärder vid vissa i förväg definierade tillfällen. Som exempel kan nämnas besöksrutiner, godsleveransrutiner, rutiner då anställning upphör samt riktlinjer för bedömning av ny leverantör. Även personell bevakning får sortera under logiska skyddsåtgärder, vilket kan utföras av egen eller inhyrd bevakningspersonal. Kostnaden för dessa åtgärder får anses vara låga eller mycket låga, med ett möjligt undantag för inhyrd bevakningspersonal.

Det har varit mycket svårt för projektet att få reda på faktiska summor över vilka ekonomiska resurser som investeras inom säkerhetsområdet. Således är nedanstående diagram en kvalificerad bedömning över vilka ekonomiska medel som satsas inom vilken del av transportkedjan. Staplarna är inte säkerställda utifrån området 1 till 3, utan bör ses som jämförbara sinsemellan med intervallen låg 1, medel 2 eller hög 3. Dock kan höjden av dem samt förhållandet dem emellan påvisa vilka skillnader som föreligger.

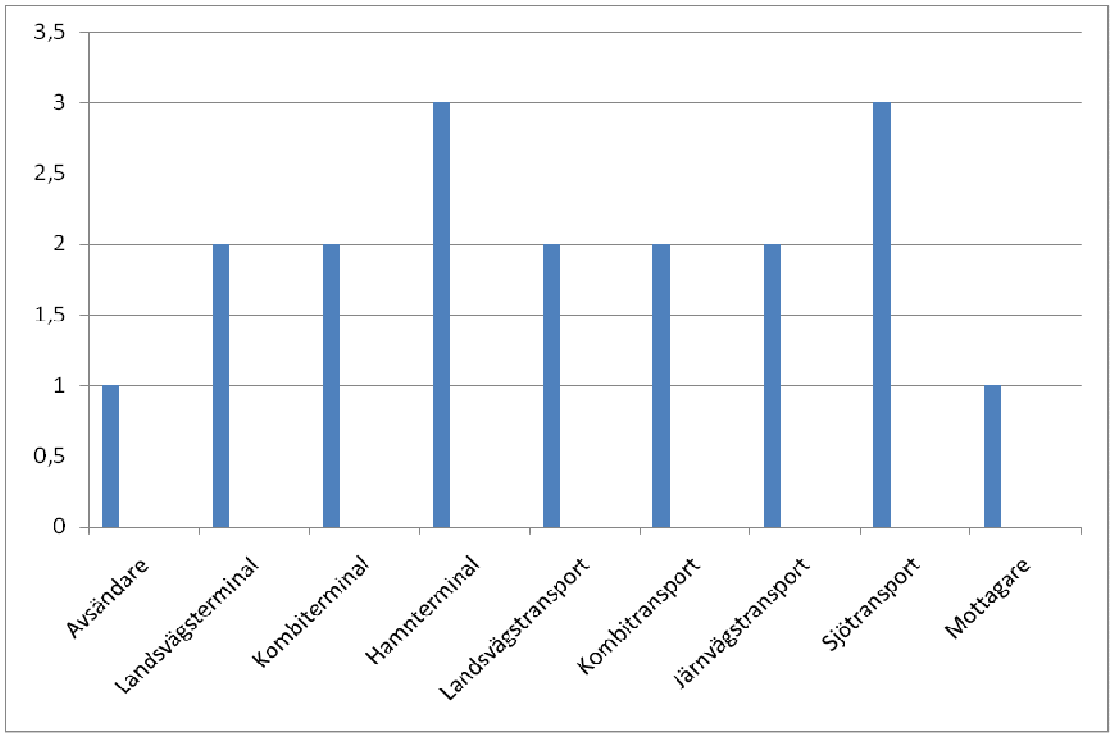


Diagram 3 - Ekonomiska medel som satsas på att motverka säkerhetshot i olika delar av en intermodal transportkedja

5.2 Hur skyddas olika delar i kedjan?

För att erhålla ett bredare svar på denna punkt läggs fokus på vilka delar i transportkedjan som kan skyddas och på vilket sätt. Resultaten är en samlad bedömning över intervjuresultaten och en erfarenhetsbedömning över de strategier, vilka sett ur ett ekonomiskt perspektiv, skulle kunna användas för att erhålla det eftersträvade resultatet.

Som ett genomgående förslag för samtliga delar av kedjan skulle god effekt uppnås genom en bättre samverkan mellan samtliga aktörer. Ett gott exempel på detta är Polismyndigheten i Västra Götaland som tillsammans med Skåne och Jönköpings län har startat ett samarbetsprojekt. Det är genom samverkan som möjliga åtgärder åskådliggörs bäst, och utifrån dem kan dessa hot bäst mötas.

Vidare påstår samtliga deltagare i projektet, att en attitydförändring skulle vara positiv, dels för att stärka statusen hos medarbetare, dels för att stärka lojaliteten till sitt yrke.

5.2.1 Avsändare

Statistik visar att under detta skede är den största risken bedrägeri, samt till viss del stöld av gods. Således skulle ett gott skydd kunna uppnås genom att det logiska skyddet förstärks, det vill säga att goda rutiner finns för gods/personal hanteringen.

5.2.2 Terminal

I detta avsnitt redovisas de fyra ”terminallänkarna” i den intermodala transportkedjan tillsammans eftersom de har liknande problematik och sätt de ska lösas på. De fyra länkarna är:

- Landsvägterminal (typ Schenker)
- Kombiterminal (typ CargoNet)
- Järnvägsterminal (typ Green Cargo)
- Hamnterminal (typ Göteborg Hamn)

Terminaler kan i mångt och mycket jämföras med avsändaren, med det undantaget att i denna del av transportkedjan skulle troligen ökad informationssäkerhet bidra till en bättre säkerhetsmiljö. Enligt polisen är minst 30% av brotten insiderrelaterade.

Stärka personalens status skulle enligt många även få en klart förbättrad effekt, inte minst kriminologiskt stärks denna tanke. Trivs jag på arbetet och är stolt över min arbetsgivare är jag i allra högsta grad med och skyddar detsamma.

Samtliga i detta projekt intervjuade personer påstår att en brist i deras organisationer är frånvaron av ett gott säkerhetsmedvetande genom stora delar av organisationen. Eller rättare sagt detta område går att förbättra.

Här återfinns givetvis även de rent fysiska säkerhetsinvesteringarna såsom staket, lås, larm, bevakning och kameraövervakning. Investeringarna ger god brottspreventiv effekt, då som motivationssänkare av en potentiell gärningsman.

Statistiken påvisar dock att det är i de terminalnära skedena som de flesta säkerhetshot uppstår.

5.2.3 Transport

I detta avsnitt redovisas de tre ”transportlänkarna” i den intermodala transportkedjan tillsammans eftersom de har liknande problematik och sätt de ska lösas på. De tre länkarna är:

- Landsvägtransport (Distribution/Fjärr)
- Kombitransport
- Järnvägstransport

När det gäller transporterat gods och hoten mot dessa finns det mycket åtgärder att vidta. Framförallt påvisas det i polisen statistik att 81 % av brotten är riktade mot oskyddade transporter (kapellskärning alternativt stöld ur olåst trailer/lastbil). Problemen inträffar oavsett om det rör sig om väg eller järnvägstransport då godset står still, antingen på stickspår eller på vägrastplatser. Således skulle ett fysiskt skydd av lastbärare bli effektivt i denna del av transportkedjan.

Beräkningar påvisar att låsta/skyddade lastutrymmen i sammanhanget inte är särdeles kostsamma.

Utbildning och information till medarbetare i hela kedjan är givetvis en god metod i syfte att utföra allt från riskbedömningar till att enskilda chaufförer skall äga kännedom om problematiken och därigenom med enkla medel undvika riskområden/tillfällen.

5.2.4 Sjötransport

Sett ur ett nationellt perspektiv är detta det område där det satsas mest kapital för säkerhetsskydd (uppskattat värde per enhet). Orsaken till detta är ISPS kodens införande med tillhörande nationella lagar, vilka förskriver vilken skyddsnivå respektive hamnanläggning skall ha. Skadekostnaderna efter dessa investeringar är som tidigare nämnt mycket låga. För vidare studier i detta ämne hänvisas till en rapport utgiven av Högskolan i Borås[16]

5.2.5 Mottagare

Statistik visar att under detta skede är den största risken bedrägeri, samt till viss del stöld av gods. Således skulle ett gott skydd kunna uppnås genom ett så kallat logiskt skydd. Det vill säga att goda rutiner finns för gods- och personalhanteringen.

5.2.6 Sammanfattning

Nedan följer en sammanfattande matris med exempel på åtgärder, som kan användas inom olika delar av transportkedjan. Denna matris har skapats helt utan applikatoriskt exempel och är således helt enkelt generella teoretiska förslag. Detta gäller även för den enkla kostnadsuppskattning som genomförts, med intervallen låg, medel och hög. Givetvis styrs kostnaden helt beroende på aktuellt objekts storlek och hotbild.

[16] Impacts of the ISPS code on port activities, (Arsham Mazaheri)

Länk i transportkedjan	Logiskt skydd		Elektronisk skydd		Fysiskt skydd	
Avsändare	- Tillträdesrutiner - Godshanteringsrutiner - Besökshanteringsrutiner - Nyckelhanteringsrutiner		- Inbrottslarm (ute/inne) - Passagesystem		- Perimeterskydd (staket, grindar) - Skalskydd - Låssystem	
	Kostnad	Låg	Kostnad	Medel	Kostnad	Medel
Terminal	- Tillträdesrutiner - Besökshanteringsrutiner - Bevakning - Informationssäkerhet		- Inbrottslarm (ute/inne) - Passagesystem - Kameraövervakning		- Perminterskydd (staket, grindar) - Skalskydd - Låssystem - Lås på ”ej kopplade trailers”	
	Kostnad	Medel	Kostnad	Hög	Kostnad	Medel
Transport	- Riskbedömning - Utbildning - Samverkan - Rutiner för uppställning		- Inbrottslarm (lastbärare) - Spårningsutrustning		- Uppskärningsskydd av kapell - Låsta skåp	
	Kostnad	Låg	Kostnad	Medel	Kostnad	Låg
Sjötransport	- Riskbedömning		- Inbrottslarm (lastbärare) - Spårningsutrustning		- Uppskärningsskydd av kapell - Låsta skåp	
	Kostnad	Låg	Kostnad	Låg	Kostnad	Låg
Mottagare	- Tillträdesrutiner - Godshanteringsrutiner - Besökshanteringsrutiner - Nyckelhanteringsrutiner		- Inbrottslarm (ute/inne) - Passagesystem		- Perimeterskydd (staket, grindar) - Skalskydd - Låssystem	
	Kostnad	Låg	Kostnad	Medel	Kostnad	Medel

6 Resultat Fas 1

6.1 Sammanfattning av resultat

6.1.1 Frekvens

Antalet tillgrepp (stöld ur eller stöld av lastbärare) minskar något från år till år. En minskning återfinns i antalet polisanmälda transportrelaterade brott[17], vilka i princip enbart är mätbara år 2007 samt år 2008 på grund av ändringar i polisens brottskodning. Det antalet få år där statistik finns på området, gör att det är svårt att dra fulländade slutsatser, dock syns en trend. Även de i projektet deltagande organisationerna ser en viss minskning av nämnda brott.

6.1.2 Godsvärde

Det som däremot oroar i sammanhanget är att det totala tillgripna godsvärdet ökar[18], och en nästan 100% ökning syns härvid (enbart år 2007 till år 2008). Beroende på vilket sätt som beräkningarna samt antagandena utförs blir slutsatsen att mellan 52 och 293 miljoner SEK tillgrips under transportkedjan i Sverige årligen.

Orsaken till denna ökning kan förklaras inom tre områden:

- Polisen har under senare år blivit bättre på att skapa kvalitativa anmälningar över dessa tillgrepp. Därför förs det numera oftare in i polisanmälan vilket värde tillgreppet är uppskattat till.

- Vid analys av utredningar där det finns gärningsmän, kan man konstatera att dessa kan delas in i fyra grupper; personer med anknytning till kriminella MC-gäng, designade kriminella nätverk, kriminella från Balkan boende i Skåne samt andra etniska nätverk. Man kan anta att dessa med tiden ökar sin kunskapsmassa vad avser planering och tillvägagångssätt, vilket leder till ett ökat godsvärde per tillgrepp.

- En parallell från punkten ovan är att det under senare tid (år 2008), blir allt mer vanligt att man tillgriper ett helt ekipage (lastbilar/släp/trailers). Om detta är en produkt av ett allt mer avancerat brottsmodus eller allmän förändring går inte att svara på i nuläget.

[17] Polisens rapport om transportsäkerhet 2008, Per-Arne Nilsson, Polismyndigheten i Västra Götaland
[18] Godsvärdesanalys 2008, Projekt Transportsäkerhet, Upprättad av Riskhanterings Akademin

6.1.3 Kända hot

Samtliga intervjuade företag har i princip gett samma svar på frågan om vilket säkerhetshot som utgör den största risken - det som är allvarligast sett ur detta projekts perspektiv är kriminella handlingar med tyngdpunkten på stölder (brottskod 9803 och 9804). Det påpekas även att skadegörelse är ett bekymmer, om än inte av den storleken som stölder. Alla är eniga om att det stämmer som polisen säger att smuggling är ett stort samhällsproblem. Dock är detta inte en fråga för ett enskilt transportföretag. Trafficking och terrorism är inget som företagen tänker på, de bara använder moderna lagar för att höja säkerheten och därigenom skapas den ytterst viktiga säkerhetskulturen.

För att åskådliggöra dessa hot har en tabell och en kurva/matris (se avsnitt 3.2.10) arbetats fram. Dessa bygger i mångt och mycket på den kunskap som erhölls från intervjuerna och befintlig statistik. Det ska poängteras att den inte är 100 % förankrad i verkligheten, utan det är en samlad bedömning som ligger till grund för kurvan.

6.1.4 Ögonblicksbild

- 1% av alla kommersiella fordon är utsatta för brott varje år[19]
- Kostnaderna i EU uppskattas till 75 miljarder SEK år 2007[20]
- 70% av brotten sker mellan klockan 22.00 – 06.00 (Sverige)[21]
- 81% av brotten riktades mot oskyddade lastbärare (Sverige)[22]

[19] ECMT Annual Report 2002
[20] Europaparlamentet/Polismyndigheten i Västra Götaland
[21] Polisens rapport om transportsäkerhet 2008, Per-Arne Nilsson, Polismyndigheten i Västra Götaland
[22] Polisens rapport om transportsäkerhet 2008, Per-Arne Nilsson, Polismyndigheten i Västra Götaland

7 Teser

Under projektets gång har tre teser växt fram för att belysa vad som är viktigt att förstå eller utveckla i projektets kommande faser. Nedan följer en beskrivning av dessa teser samt resonemanget bakom dem.

7.1 Tillgreppen i transportkedjan

Tes 1:

Tillgreppen i en intermodal transportkedja sker främst på oskyddade terminalnära platser.

Diskussion om tes 1:

70 – 80 % av tillgreppen går statistiskt sett att härleda till en oskyddad plats alternativt ett oskyddat ekipage, således höjs motivationen hos en potentiell gärningsman på grund av utevaron av mekaniska/fysiska skyddsanordningar alternativt bevakning (kriminologiskt sett är det utevaron av en kapabel väktare).
Vidare är det klarlagt att en stor säkerhetsinvestering lönar sig om syftet är att minska antalet brottsliga angrepp, klart påvisat i exempelvis Göteborgs hamn där man vidtagit dessa åtgärder. Kriminaliteten tycks fungera som parallella kommunicerande kärl då man under senare tid fått ett ökat antal angrepp mot de i området närliggande bangårdarna.

Följande graf påvisar att där ett gott skydd finns, minskar riskerna för säkerhetshot. Grafen åskådliggör den statistik som finns inom området, samt de intervjuade organisationernas uppfattningar. Linjen motsvarar aktuell säkerhetsnivå i respektive del av transportkedjan. Angreppen inträffar vanligast där grafens färg är som mörkast.

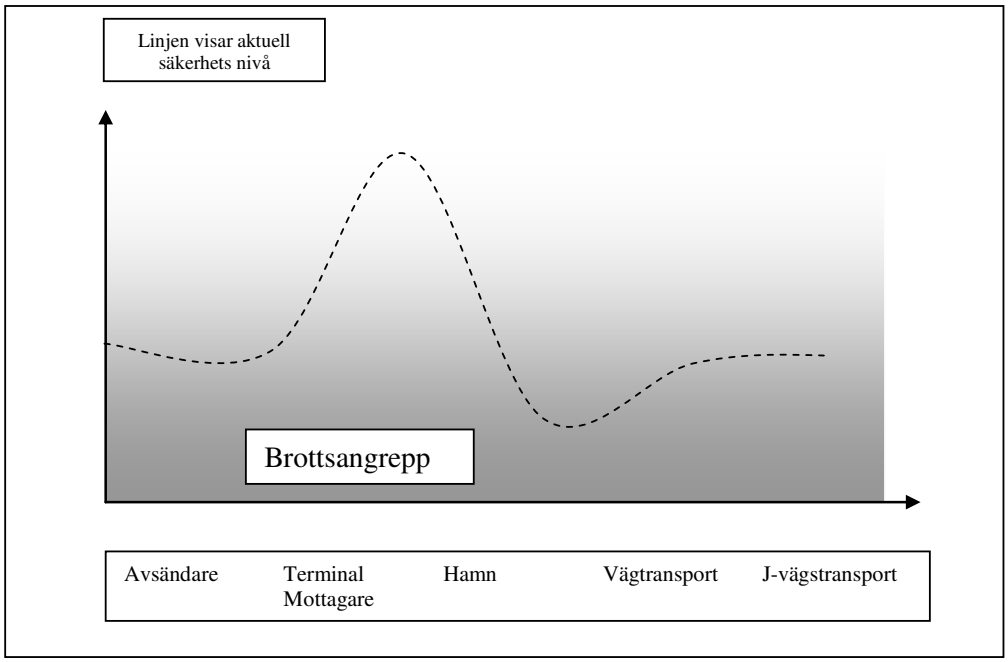


Diagram 4 - Förhållandet mellan säkerhetsnivå och risk för säkerhetshot i olika delar av den intermodala transportkedjan

7.2 Orsaksanalys

Tes 2:

Frånvaron av kunskap/resonemang om aktuella orsaksproblem kan ligga till grund för en försvårad problemlösning

Diskussion om tes 2:
Denna tes bottnar i en svår frågeställning och svar på frågan kan inte ges fullt ut i denna rapport. Dock följer ett antal kriminologiska ansatser/slutsatser[23] i bilaga 1. Dessa bedöms som accepterade inom samhället och dess kriminologiska institutioner och för detta ändamål väl lämpade som en bred informationsbakgrund till tesen. Emellertid är redan det presenterade urvalet tillräckligt för att inse att flera teorier utgår från samma empiriska verklighet.

Vid läsning av bilaga 1 fås en mycket ytlig inblick i den kriminologiska världen där det storskaliga svaret återfinns och förhoppningsvis skapas en förståelse för tesens existens, samt vilka kunskaper som ligger bakom den. Vidare kan ett per enkla slutsatser dras i korthet:

- Det finns potentiella gärningsmän, oaktat orsaken
- Brotten begås dels på grund av segregation/utanförskap
- Brotten begås dels på grund av en befintlig kriminalitet vilken sprider sig och tar upp nya ”svaga” individer
- Brotten begås i ett samhälle där tillfällen ges
- Brotten begås där/då avsaknad av kapabla väktare[24] är som störst

7.3 Minskning av antalet tillgrepp

Tes 3:

Trenden är att antalet tillgrepp minskar i transportkedjan

Diskussion om tes 3:
Den statistik som polisen levererar till samhället bygger enkom på brott som kommit till polisens kännedom. Detta medför att den inte till 100 % återspeglar verkligheten och ett mörkertal finns som skapas både inom polisens såväl som inom branschens led. För att kommentera orsakerna kort kan nämnas att det ofta är svårt för transportören att veta exakt vilket gods som tillgripits. Gränsen mellan stöld, skadegörelse eller godsskada kan vara svår att överblicka. Tidspress är ett annat skäl till varför det ibland inte anmäls eller att det stulna godsets värde inte motsvarar kostnaden för en egen

[23] Jerzy Sarnecki, Introduktion till kriminologi
[24] Utevaron av olika skyddsåtgärder, logiska, fysiska eller elektroniska skydd

självrisk. Således återfinns ett mörkertal[25] i detta sammanhang. Detta mörkertal sänker noggrannheten i polisens statistik och kan utgöra en liten del av den statistiska minskningen.

Bedömningen är dock att de två största orsakerna till minskningen är:

- att polismyndigheten i Skåne, Halland, Jönköping och Kronobergs samt Västra Götalands län har fokuserat på området och bildat en samverkansgrupp. Detta arbete har lett till en ökad tvärsektoriell samverkan mellan polis och hela transportbranschen, där man genom seminarier och workshops ökar intresset för frågorna och där det uppnåtts en ökad kunskap om problembild samt relevanta skyddsåtgärder. Även tillverkare (Volvo Lastvagnar och Scania) har tagit till sig kunskap och förändrat exempelvis lås och säkerhet.

- att en ökad professionalism bland förövarna skapar färre antal tillgrepp om än med betydligt högre ”träffsäkerhet” och därigenom ett ökat godsvärde per tillgrepp.

[25] Kvoten mellan den faktiska och den registrerade brottsligheten.

FAS 2 – Översikt av aktuella säkerhetsinitiativ som påverkar olika delar av transportkedjan

8 Översikt av olika säkerhetsinitiativ

8.1 100 % scanning

Benämning:	100 % scanning
Initiativtagare:	USA:s kongress
Inriktning:	Lagkrav på säkerhetskontroller
Drivkraft:	Använda ”nonintrusive imaging equipment” för att upptäcka WMD i containers
Geografiskt område:	Globalt gods till USA
Kopplingar:	Ingår som en del i SAFE Port Act
Togs i kraft:	Ska vara i kraft senast juli 2012[26]
Säkerhetshot som främsta ska förebyggas:	Terrorism
Påverkar främst vilka delar i transportkedjan:	Hamnterminaler

100% scanning är ett säkerhetsinitiativ uppkommet som en reaktion på terrorattentatet 9/11. Målet är att 100% av alla containers som anländer till USA från juli 2012 ska skannas vid ankomst, alternativt ska ha skannats innan lastning på fartyg, med målet att upptäcka radioaktiv strålning *”shielded and unshielded nuclear and radiological material”*. Det indikerar försök till införsel av massförstörelsevapen eller därtill hörande material som kan användas vid en terrorattack .

Initiativet är godkänt av både kongressen och president Bush i början av 2009 men har fått kritik för att vara mycket svår att genomföra. Först var kravet att all skanning skulle ske vid ankomst till amerikansk hamn men den nya Commission Act från 2007 fokuserar på;

”A container that was loaded on a vessel in a foreign port shall not enter the United States (either directly or via a foreign port) unless the container was scanned by nonintrusive imaging equipment and radiation detection equipment at a foreign port before it was loaded on a vessel also mandate scanning”

Kritikerna hävdar att hela initiativet är grundläggande fel och att kraven är helt orimliga i proportion till uppnådd säkerhet och några av problemen belyses i artikeln ”A different theory for 100 percent container scanning” [27] ;

- Begränsande av de globala transportflödena. Krav på skanning av gods innan lastning på fartyg kommer orsaka stockning av gods i bland annat Europas hamnar.

[26] The 9/11 Commision Act of 2007
[27] Security Info Watch, DR. Jim Giermanski, *A different theory for 100 percent container scanning (2009)*

- Innebär drastiskt höjda logistikkostnader med risk för att begränsa den globala handeln med varor.
- Skanning av containers i hamn som i sig kan vara ett mål för terrorister (själva hamnen/hamnområdet) och därför bör skanning ske innan ankomst till hamn.
- Någon användbar teknik för att genom containerskanning upptäcka *"shielded radiation",* är inte kommersiellt utvecklad.

Den teknik (PVT portal machines) som finns kommersiellt tillgänglig och som används i nuläget av CBP (U.S Customs and Border Protection) kan inte upptäcka *"highly enriched or shielded"* uran vilket är material som kan användas i WMD:s. DNDO (Domestic Nuclear Detection Office) är ansvariga för utvecklandet av den nya tekniken ASP (Advanced Spectroscopic Portals) för att upptäcka all typ av "farlig" strålning, vilket inte tros vara i närheten av en användbar teknik år 2012.[28]

Många inflytelserika aktörer (regeringar, rederier, handelspartners m.m) är emot säkerhetsinitiativet. Det återstår att se i vilken omfattning det genomförs med färdigutvecklad teknik eller inte.

Exempelvis uttrycker den tyska regeringens talesman för sjöfartsfrågor mångas åsikter i följande citat[29];

"Security is important, but please no one-sided approach to the disadvantage of our port and transport industries"

[28] Security Info Watch, DR. Jim Giermanski, *A different theory for 100 percent container scanning (2009)*
[29] Security Info Watch, U.S Shippers Oppose 100 Percent Cargo Inspections *(2009)*

8.2 ADR

Benämning:	ADR/ADR-S
Initiativtagare:	En expertkommitté inom FN:s ekonomiska och social råd (ECOSOC) samt två underkommittéer till expertkommittén arbetar kontinuerligt med FN:s rekommendationer vad gäller transport av farligt gods
Inriktning:	Föreskrifter för transport av farligt gods på väg
Drivkraft:	Minska risken för olyckor och tillbud under hantering och transport av farligt gods
Geografiskt område:	Europa + några nordafrikanska länder
Kopplingar:	Främst till de andra föreskrifterna för farligt gods för andra transportslag – RID (järnväg), IMDG (sjö) och IATA/DGR (flyg)
Togs i kraft:	Utkommer med ny version vart annat år. Senaste version började gälla i Sverige 16 februari 2009.
Säkerhetshot som främsta ska förebyggas:	Stöld och terrorism
Påverkar främst vilka delar i transportkedjan:	Avsändare, landsvägstransportörer, landsvägsterminaler

ADR är en förkortning av det franska "Accord Européen Relatif au Transport International des Marchandises Dangereuses par Route" eller motsvarande på engelska "European Agreement Concerning the International Carriage of Dangerous Goods by Road".

ADR utvecklas fortlöpande och fastställs av FN:s ekonomiska kommission för Europa (United Nations Economic Commission for Europa, UNECE). Arbetsgruppen som ansvarar för ADR benämns Working Party 15 (WP.15). 45 länder är anslutna till ADR. Via EU-direktiv blir det svensk lagstiftning och hanteras av MSB Myndigheten för Samhällsskydd och Beredskap.

WP.15 utvecklar och fastställer innehållet i ADR med FN-rekommendationerna och de rådgivande besluten från Joint-mötet som grund. Dessutom tillkommer bestämmelser som är unika för vägtransporter, ex. krav på förarutbildning och krav på fordon.

Sedan 2006 finns det i ADR 2006 ett kapitel 1.10 med bestämmelser om transportskydd. Med transportskydd och skydd avses försiktighetsåtgärder som ska vidtas för att minimera stöld eller obehörigt förfarande med farligt gods, som kan skada personer, egendom eller miljö.

I ADR kapitel 1.10 finns regler för vilka försiktighetsåtgärder som ska vidtas vid överlämnandet och transport av farligt gods, krav på utbildning för de som är inblandade i transporten och extra krav på farligt gods med hög riskpotential t.ex. skyddsplaner, speciella anordningar, anmälningsplikt, förutbestämda transportvägar etc.

8.3 AEO

Benämning:	AEO – Authorized Economical Operators (Godkänd ekonomisk aktör)
Initiativtagare:	Europaparlamentet - tullmyndigheter
Inriktning:	Certifiering av aktörer i godsflödet
Drivkraft:	– Effektiviseringar – Snabb återhämtning vid incident
Geografiskt område:	EU
Kopplingar:	CSP – Customs Security Program, Föranmälan EU import och export (24-timmars-regeln), WCO SAFE och ISO 28000
Togs i kraft:	1 januari 2008 / juli 2009
Säkerhetshot som främsta ska förebyggas:	Generell förbättring av säkerheten i logistikkedjan
Påverkar främst vilka delar i transportkedjan:	Alla transportslag – både import och export

AEO är ett initiativ av tullmyndigheterna i EU för att skapa enhetliga riktlinjer gällande hantering och kontroll av godsflöden. Till skillnad från flertalet andra säkerhetsinitiativ som främst är inriktade mot sjötransporter är AEO utformad för att gälla samtliga transportslag.

Under utvecklingen av AEO har det varit ett grundläggande önskemål att harmonisera det nya ramverket med de redan existerande närliggande standarderna WCO SAFE och ISO 28000, vilka båda behandlar hur säkerheten i transportkedjan ska hanteras för att möta den nya tidens hot.

Likt andra säkerhetsinitiativ, såsom WCO SAFE, bygger införandet av AEO på att skapa incitament för företag att certifieras såsom;

- Lättare tillgång till förenklingar i tullhantering gällande både import och export
- Färre visuella- och dokumenteringskontroller
- Prioritering när kontroll ändå görs
- Möjligt att anhålla om plats för kontroll[30]

Alla de företag vilka ingår i transportkedjan kan bli AEO certifierade om en tillräckligt hög säkerhetsnivå kan påvisas. Det gäller övergripande delar exempelvis företagens kontrollsystem men också att befintliga tullregler efterlevs och att så har varit fallet under viss tid.

Certifiering innebär att aktören erhåller någon av de tre AEO-status typerna; tullrutin, säkerhet och skydd samt de föregående kombinerat. Erhålls en certifiering i en av EU:s medlemsstater erhålls samma status i övriga EU länder. De absoluta kraven för att erhålla vissa förenklingar i tullförfarandet kan däremot skilja länder emellan.

[30] European Commission, *Authorised Economic Operators Guidelines (2007)*

AEO riktlinjerna ger detaljerade krav på säkerhetsåtgärder till respektive AEO-status däribland;

- Regler gällande tillträde till gods
- Användande av godkänd plomberingsutrustning
- Kontroll av behörig personal
- Rutiner för inrapportering av utgående gods m.m.

De tydliga och detaljerade kraven gör att företagets samtliga tullrutiner och flöden av varor måste kvalitetssäkras men dessutom de av verksamheten använda säkerhetsrutinerna. Detta kan vara en kostsam och omfattande process men ger förutom ett certifierande i de flesta fall positiva effekter i det dagliga arbetet, exempelvis färre stölder.

Viss kritik har framkommit gällande de krav som ställs för en AEO certifiering där det bland annat framförs att lättnaderna i form av exempelvis färre tullkontroller inte tillräckligt kompenserar det merarbete som läggs ner av företagen[31]. Fler uppgifter än tidigare ska exempelvis lämnas om godset innan transporten lämnar det avsändande landet.

[31] Tollkonsuly, *www.tollkonsult.no/uploads/DagensHandel.pdf*

8.4 BASC

Benämning:	The Business Alliance for Secure Commerce
Initiativtagare:	Sammanslutning av aktörer i Sydamerika
Inriktning:	Främja säkra globala transporter
Drivkraft:	Att genom samarbete mellan företag och myndigheter effektivt motverka smuggling
Geografiskt område:	Latin Amerika och Karibien
Kopplingar:	C-TPAT, AEO-WCO
Togs i kraft:	Grundades 1996
Säkerhetshot som främsta ska förebyggas:	Smuggling
Påverkar främst vilka delar i transportkedjan:	Hela transportkedjan

BASC, The Business Alliance for Secure Commerce, är en sammanslutning av företag som bildades 1996 för att främja säkra globala transporter. Det var initialt ett projekt för att motverka smuggling av illegitima varor i lagliga godstransporter. Med tiden omformades initiativet till ett komplett system för hantering av säkerhetsfrågor och konkreta krav på säkerhetsåtgärder.

BASC agerar i tätt samarbetet med de statliga kontrollorganen såsom U.S Customs and Border Protection och andra internationellt verksamma organisationer.

Syftet med BASC är att arbeta mot smuggling i kommersiella logistikkedjor exempelvis utnyttjandet av legitima containertransporter för smuggling av oredovisat innehåll (i extremfall material för terroristattacker).

Kraven för certifiering i BASC standarden avser rent praktiska aspekter såväl som managementfrågor exempelvis;

- Kontroll av personal, tillträdeskontroll och behörighetsfrågor
- Fysiskt skalskydd (Staket, dörrar, larm, belysning)
- Rutiner för lastdokument, uppföljning m.m.

Stor vikt läggs på personalsäkerheten där bland annat regelbundna kontroller ska genomföras avseende personers beteende och dess kontakter även utanför arbetstid.

Rutiner för lastdokument innefattar att dessa inte utfärdas i sista minuten utan att det sker enligt utarbetade rutiner då det är visat att kriminella använder metoden för att minimera riskanalys av aktuellt gods.

Då BASC är en ”privat” organisation finns inget lag krav för aktörer att ansluta sig. Det är istället baserat på en vilja att dra nytta av fördelarna ett BASC anslutande innebär, bland annat;

- Påvisar ett engagemang i säkerhetsfrågor
- Innebär att aktören uppfyller minst den lägsta nivån i C-TPAT och AEO-WCO
- Regelbunden kontakt med tullmyndigheter

I dagsläget har mer än 2500 företag[32] verksamma inom export, import, sjötransport m.m. certifierats i något av de till BASC 13 anslutna länderna i Latin Amerika och Karibien.

BASC stöds, förutom av tullorganisationerna i Sydamerika, dessutom av tull och organisationer internationellt, däribland den spanska och franska tullen i Europa.

Då BASC blivit ett väletablerat säkerhetsinitiativ efterfrågas det bland annat av kunder/ leverantörer och underlättar export avsevärt till andra kontinenter.

[32] BASC, *www.wbasco.org (2010-04-27)*

8.5 CSI

Benämning:	Container Security Initiative
Initiativtagare:	U.S. Customs and Border Protection (CBP)
Inriktning:	Import till USA
Drivkraft:	Förhindra WMD (Weapons of Mass Destruction) att smugglas till USA via containertransport
Geografiskt område:	Globalt gods till USA
Kopplingar:	SFI, Megaports, SAFE Port Act (formaliserade CSI initiativet till lag), 100% skanning
Togs i kraft:	Initierades 2002
Säkerhetshot som främsta ska förebyggas:	Terrorism
Påverkar vilka delar i transportkedjan:	Skeppning av gods till USA och därtill hörande hantering i hamnterminaler

CSI, Container Security Initiative, är ett säkerhetsinitiativ inriktat på ökad säkerhet i den maritima transportkedjan. Som många andra initiativ, framförallt i USA men även globalt, har det sitt ursprung i det ökade terroristhotet efter 9/11. CSI är inriktat på att upptäcka och avskräcka terrorister från att smuggla in massförstörelsevapen.

I storleksordningen 11 miljoner (år 2005) containers anländer till USA:s hamnar varje år vilket utgör 95 procent av den totala importen. Det gör containerfartygen till en potentiell möjlighet för terrorister att smuggla material som kan användas vid en terroristattack. Risken finns förutom att container används för transport av terrormaterial, att själva logistikkedjan utsätts för en attack till sjöss eller i hamn. Konsekvensen om en av de större hamnarna utsätts för en terroristhandling antas vara enorma påfrestningar för ekonomin på grund av kraftigt begränsad handel.

Det som gör CSI unikt är den grundläggande tanken att flytta en del av det faktiska kontrollarbetet till den exporterande hamnen;

”The Container Security Initiative is a revolutionary program to extend our zone of security by pre-screening containers posing a potential security risk before they leave foreign ports for U.S. seaports.” [33]

För att göra det möjligt har CBP överenskommelser med länder om att dess personal får arbeta med säkerhetsfrågor på plats. Fokus ligger på att, med hjälp av underrättelse-information och riskbedömningar, analysera containerflödet för att identifiera högriskobjekt och då främst avseende risken för innehåll av WMD.

Bedöms containern som högrisk är det upp till värdlandets tull-/myndighetspersonal att utföra den fysiska kontrollen efter förfrågan av CBP:s utsända personal, vilket görs med skanning eller praktisk genomsökning.

[33] U.S. Customs and Border Protection, *Container Security Initiative (2006)*

Fyra grundkomponenter har definierats[34];

- Identifiera högriskcontainers med hjälp av förhandsinformation och tidigare erfarenheter (underrättelseinformation)
- Skanna containers (för analys av innehåll och upptäckande av strålning) redan innan skeppning (i exporterande hamn)
- Effektivitet i säkerhetsarbetet (skanningprocessen) för att inte negativt påverka godsflödet
- Öka containerns egensäkerhet för att förhindra och lättare upptäcka intrång

Förutom ökad säkerhet i den maritima containertransportkedjan har målet samtidigt varit att bibehålla eller förbättra genomflödet av gods sett till tullens hamnhantering. Det ska uppnås genom att effektivt utnyttja containers stilleståndstider i dagens transportsystem som oftast är innan lastning på fartyg. Vanligtvis utförs tullarbetet vid ankomst av gods vilket kan innebära förseningar i logistikkedjan i de fall en tullkontroll görs.

Att utnyttja containers stilleståndstid blir ännu viktigare om lagförslaget 100% skanning (se avsnitt 2.1) införs. Annars kan det, om processen görs vid ankomst, skapa allvarliga problem i arbetet med att upprätthålla effektiviteten i exporten till USA vilket påverkar hela den globala logistikinfrastrukturen negativt. Skannas containers istället innan lastning på fartyg kan stilleståndstiden bättre utnyttjas.

Göteborgs hamn utgör som enda svenska hamn en av 58 CSI anslutna hamnar (2007). Samarbetspartners finns i Sydamerika och Karibien, Europa, Asien, Mellanöstern och Afrika.

[34] U.S. Customs and Border Protection, *Container Security Initiative (2006)*

8.6 C-TPAT

Benämning:	Customs-Trade Partnership Against Terrorism
Initiativtagare:	U.S. Customs and Border Protection (CBP)
Inriktning:	Import till USA (flyg även export)
Drivkraft:	Minska säkerhetsrisken med import av gods
Geografiskt område:	USA
Kopplingar:	CSI, FAST
Togs i kraft:	Initiativ startades november 2001
Säkerhetshot som främsta ska förebyggas:	Terrorism
Påverkar främst vilka delar i transportkedjan:	Från avsändare (leverantör) till mottagare över gränskontroll gällande import av varor

C-TPAT infördes som ett initiativ av CBP för att öka landets säkerhetsnivå efter terroristattacken 9/11 2001 genom att förbättra säkerheten i den globala leveranskedjan. Målet är att förhindra terrorister och vapen att komma in i USA. Till skillnad från traditionellt tullarbete bygger C-TPAT på ett utökat samarbete mellan CBP och de företag som utgör navet i den omfattande importen av varor till USA.

Med tanke på volymen av importerat gods är CBP tvunget att hitta metoder att kombinera en omfattande och noggrann kontroll men samtidigt uppehålla en effektivitet i varuflödet genom gränskontrollerna.

Strategin är att jobba alltmer förebyggande innan godset anländer fysiskt till gränskontrollen bland annat genom att tidigt analysera tillgänglig information och rikta in aktiviteten på gods som bedöms ha hög risk. Fokus från CBP sida är att involvera företag i samarbetet vilka hanterar stora volymer gods men med låg risk.

Fokus i C-TPAT initiativet är att låta företagen bli än mer involverade i att säkra upp hela transportkedjan genom omfattande arbete med den passiva säkerheten och därmed underlätta tullens arbete. Som ett led i detta bör samarbetet mellan importör (i USA) och exportör fördjupas med mål att öka kontrollen av det egna godset med avseende bland annat på att försvåra att lasten ändras eller manipuleras innan sändning och under transportens gång.

Företagens drivkraft bakom en C-TPAT certifiering är tullförenklingar, ökad ”intern” säkerhet samt underlättande av handel med andra C-TPAT medlemmar. Tre certifieringssteg finns med varierande grad av tullförenklingar:

- Steg 1 för certifierade medlemmar; färre antal kontroller (uppskattningsvis 5-8 gånger färre än icke medlemmar) och tillgång till FAST-lane servicen till Kanada och Mexico.
- Steg 2 för certifierade och validerade medlemmar (uppfyller de lägsta säkerhetskraven); ytterligare färre kontroller och när transport väl granskas görs det prioriterat före övriga godskontroller.

- Steg 3 för de medlemmar som överträffar de grundläggande säkerhetskraven och allmänt bedöms ha antagit bra säkerhetsförfaranden; ännu färre kontroller och är ett första steg mot fria tullpassager (endast enstaka slumpvisa kontroller).

Vad kan företagen tjäna på samarbetet förutom rent tullrelaterade fördelar?

Enligt CBP ger en C-TPAT certifiering positiva följdeffekter i form av interna verksamhetsvinster (i övriga logistikkedjan) såsom; minskade stölder, säkrare arbetsmiljö och införande av bra säkerhetsrutiner och –processer.

I början av 2007 var 6375 företag partners[35]. Motsvarande mer än 96% av all containerlast via fartyg är certifierat enligt C-TPAT[36]. Det kan nämnas att 11.3 miljoner containers passerade USA:s gränser år 2008 varav 1 av 33 kontrollerades[37].

[35] U.S. Customs and Border Protection, *Written testimony of W.Ralph Basham, Comissioner (2007)*
[36] U.S. Customs and Border Protection, *Securing the Global Supply Chain (2004)*
[37] U.S. Customs and Border Protection, *A Guide To Program Benefits (2008)*

8.7 Dutch Client System

Benämning:	Dutch Client System
Initiativtagare:	Holländska tullen
Inriktning:	Fokusera tullens arbete på kontroll av gods med högre risk
Drivkraft:	Underlätta handel och transport av varor
Geografiskt område:	Export och import till Nederländerna
Kopplingar:	AEO
Togs i kraft:	Möjlighet till AEO certifiering från september 2007
Säkerhetshot som främsta ska förebyggas:	Smuggling, terrorism m.m.
Påverkar främst vilka delar i transportkedjan:	Interkontinentala transporter både import, export och transit genom Nederländerna

Dutch Client System är de nederländska tullmyndigheternas interna program som syftar till att bedöma aktörerna i transportkedjans tillförlitlighet. Fokus ligger på att genom bedömning av företagen bakom godset/-transporten avgöra vilket säkerhetshot godset utgör och med riskanalysen som utgångspunkt avgöra vilken kontroll av gods som bör ske.

Ett utökat samarbete mellan företag och tull blir allt viktigare i takt med att den hanterade mängden gods ökar. Från dagens nivå på 10 miljoner containers årligen uppskattas antalet containers i godsflödet över de nederländska gränserna öka till 30-35 miljoner per år. Att underlätta handel och transport av varor över gränserna ses som en nödvändighet om ett effektivt godsflöde ska kunna upprätthållas. Förutom den ökade volymen gods blir kraven på bättre säkerhet för att förebygga smuggling, terrorism m.m. i godstransporter allt högre. [38]

För att klara de nya utmaningarna har den nederländska tullmyndigheten en vision om att gå ifrån det traditionellt hierarkiska tullkontrollsystemet till ett ”platt” system där säkerheten i logistikkedjan främjas genom samarbete med näringslivet. Antagande av säkerhetsinitiativet AEO är det viktigaste steget för att uppnå målsättningarna. Från och med september 2007 kan holländska företag söka AEO-status. Tullen står för certifieringsförfarandet och några av de grundläggande principerna för tullens certifieringsarbete är;

- Ett i grunden bra samarbete mellan tull och företag som möjliggör ett ”platt” säkerhetsarbete för att skapa effektivitet och säkerhet i logistikkedjan.
- Företag delas upp i kategorier efter verksamhetsområde och större företag med högt godsflöde kan erhålla ett individualiserat hanteringssätt.
- Första steget i processen är att identifiera de lämpligaste lösningarna för den aktuella aktören och göra en första bedömning om certifiering är möjlig innan fortsatt arbete.

[38] http://www.douane.nl/zakelijk/aeo/en/ [2010-07-20]

- Analysera hur ett kontrollsystem av företaget skulle kunna utformas med utgångspunkt från tidigare erfarenheter, redan existerande säkerhetssystem, riskanalys av företaget och aktuell bransch.

8.8 ESSTRT

Benämning:	European Security: High Level Study on Threats, Responses and Relevant Technologies
Initiativtagare:	Europeiska kommissionen
Inriktning:	Analysera hoten mot Europas säkerhet och rekommendera lösningar för bekämpandet av terroristhandlingar inom EU.
Drivkraft:	Att förhindra terroristdåd i EU
Geografiskt område:	Europa
Kopplingar:	Inga direkta kopplingar
Togs i kraft:	Ett forskningsprojekt som slutfördes 2006
Säkerhetshot som främsta ska förebyggas:	Terrorism
Påverkar främst vilka delar i transportkedjan:	När det gäller godstransporter ges i studien allmänna rekommendationer på åtgärder som bör införas

ESSTRT (European Security: High Level Study on Threats, Responses and Relevant Technologies) är en studie som utförts åt EU kommissionen av försvarskoncernen Thales, the International Institute for Strategic Studies and Chrises Management Initiative med syftet att analysera hoten mot den Europeiska säkerheten och föreslå åtgärder för att förbättra densamma. Studien är främst inriktad på metoder att förhindra terrorism.

Det konstateras bland annat att de flesta EU länder ännu inte har analyserat och åtgärdat de nationella säkerhetsproblemen, ej heller utarbetat en strategi för att lösa dessa. Vidare konstateras vikten av internationella standarder och att kontinuerligt utvärdera riskerna.

EU rekommenderas att tillsammans med viktiga partners i den globala handeln utarbeta standarder för att motverka terrorism och i större utsträckning samarbeta inom ramen för redan existerande initiativ såsom Container Security Initiative.

ESSTRT studien gjordes för att visa på lämpliga områden som forskning bör ske inom. Den konstaterar att följande säkerhetstekniker är användbara om de är utvecklade:

- Skanners för container- och ”fordons”skanning för att upptäcka vapen och farliga substanser framförallt bör forskning ske med mål att förfina teknikens förmåga att skilja mellan farligt och ofarligt gods
- ”Smart container” teknologi där inbyggda sensorer upptäcker intrång, rapporterar och lagrar position, upptäcker olagligt innehåll m.m.
- Smart kameraövervakning för områdes-, skal- och gränsskydd med teknik för att automatiskt identifiera misstänkt beteende

Studien betonar att de tekniska säkerhetslösningarna ska användas med viss försiktighet då ingen teknik kan litas fullt ut på och att riskbedömning alltid bör ske utifrån aktuell situation och givna förutsättningar. Exempelvis kan användande av röntgenteknik ge mycket svårtolkade bilder vid skanning av enheter med mer komplext innehåll såsom containers.

8.9 FAST

Benämning:	Free and Secure Trade
Initiativtagare:	USA, Kanada, Mexicos tullmyndigheter
Inriktning:	Förenkla transport av gods mellan USA, Kanada och Mexicos gränser
Drivkraft:	Omfördela resurser till kontroll av högriskgods
Geografiskt område:	USA, Kanada och Mexico
Kopplingar:	C-TPAT, PIP
Togs i kraft:	Initierades i slutet av 2002. Första gränsövergång mellan Mexico och USA introducerades 2003 och därefter kontinuerlig utveckling
Säkerhetshot som främsta ska förebyggas:	Smuggling och terrorism
Påverkar främst vilka delar i transportkedjan:	Landsvägstransporter

FAST, Free and Secure Trade är ett initiativ mellan Canada Border Service Agency (CBSA) och U.S. Customs and Border Protection (CBP) samt mellan USA och Mexico med syfte att främja säkerheten i den landburna logistikkedjan med fokus på lastbilstransporter parallellt med ökad effektivitet i gränskontrollerna.

Säkerhetshot som ska förebyggas är smuggling, smuggling i legitima transporter, organiserad brottslighet och terrorism. Det ska primärt ske genom att underlätta, utifrån erfarenhet från lagliga transporter, gränspassage med följden att resurser frigörs. Mer arbete kan istället läggas på att undersöka misstänkta högriskgodstransporter genom bland annat fysisk undersökning av innehåll, skanning osv.

För att få tillgång till tullförenklingarna i FAST måste alla aktörer i logistikkedjan vara C-TPAT certifierade, vilket innebär att kraven i C-TPAT initiativet är uppfyllda och aktörerna är identifierade som låg risk.

För transporter mellan Mexico och USA gäller att; hela kedjan från tillverkare, transportbolag, importörer, men dessutom de enskilda lastbilschaufförerna (87 000 är inregistrerade i FAST)[39], är C-TPAT certifierade samt att containers förses med högsäkerhetssigill enligt CBP kravspecificering.

Vid gränspassage mellan Kanada och USA är kraven lägre då inga krav finns på tillverkaren i logistikkedjan.

Förutom certifiering enligt C-TPAT programmet gäller fördelarna med FAST endast för godstransporter mellan USA, Kanada och Mexico. De särskilda ”FAST lanes” finns vid 55 av totalt 105 gränspassager.

[39] Free and Secure Trade FAST Fact Sheet, U.S. Customs and Border Protection

Fördelarna med FAST är ett förenklat tullförfarande vilket innebär;

- Snabbare och effektivare gränspassage genom ”FAST lanes”
- Färre antal kontroller av godstransporter
- Vid kontroll prioriteras ”FAST” transporter
- Mindre byråkrati – dokumentation krävs
- Ekonomiska besparingar tack vare snabbare leveranser och minskad risk för förseningar på grund av kontroll

Tullförfarandet vid gränspassage kan ske antingen helt papperslöst ”FAST” med elektronisk överföring av uppgifter eller enligt ”PAPS” Pre Arrival Processing System som är ett pappersbaserat teknisk lösning med användande av streckkoder. Kontroll av uppgifterna sker i systemen BCS Border Cargo Selectivity och ATS (ett system för risknivåbedömning).

8.10 Frontline

Benämning:	Frontline
Initiativtagare:	Australian Customs Service
Inriktning:	I samarbete med industrin arbeta mot illegitim import och export
Drivkraft:	Försvåra kriminell aktivitet över Australiens gränser
Geografiskt område:	Australien
Kopplingar:	Inga
Togs i kraft:	Initierades 1991
Säkerhetshot som främsta ska förebyggas:	Smuggling (droger, djur m.m.), trafficking, pengatvätt
Påverkar främst vilka delar i transportkedjan:	Interkontinentala godstransporter gällande både import och export till/från Australien

Frontline initierades i början av 90-talet och är ett säkerhetsinitiativ för att i samarbete med industrin arbeta mot kriminell verksamhet. Programmet är brett och innefattar säkerhetshot från smuggling av droger, vapen, djur osv. till trafficking och pengatvätt. Inriktningen ligger på både import och export.

Medlemmar får utbildning i att identifiera misstänkta kriminella aktiviteter/transporter och rapporterar in dessa till tullmyndigheten. Medlemmarna ska också fortlöpande förbättra sina säkerhetsprocedurer och -arrangemang

I gengäld etableras ett gott samarbete mellan medlemmar och tullen vilket främjar båda parter i samarbete och kontakt. Det underlättar tullens arbete att förenkla och göra tullprocedurer effektivare för företag.

Det som främst skiljer Frontline från andra säkerhetsinitiativ såsom C-TPAT, CSI osv. är bristen på konkreta åtgärder och krav som medlemmar måste införa och uppfylla för att förbättra den fysiska säkerheten. I Frontline ska Australian Customs Services mål uppfyllas med hjälp av ett bättre informationsflöde av misstänkta aktiviteter.

Programmet är helt frivilligt och bygger på att intresserade företag blir medlemmar genom att teckna ett icke bindande avtal med Australian Customs Service för att formalisera samarbetet.

Hösten 2007 fanns runt 700 medlemsföretag verksamma inom någon typ av handel/transport på en global nivå.

8.11 Föranmälan EU

Benämning:	Föranmälan EU
Initiativtagare:	Europas gemenskap
Inriktning:	Hindra farliga varor från att transporteras in och ut från EU
Drivkraft:	Försvåra kriminell aktivitet över EU gemenskapens yttre gränser
Geografiskt område:	EU
Kopplingar:	AEO
Togs i kraft:	1 juli 2009
Säkerhetshot som främsta ska förebyggas:	Smuggling, terrorism m.m.
Påverkar främst vilka delar i transportkedjan:	Interkontinentala godstransporter gällande både import och export till/från EU:s yttre gränser

Föranmälan EU är ett initiativ för att främja säkerheten i den globala leveranskedjan. Det infördes dels för att förebygga att illegitima transporter sker över EU ländernas gemensamma yttre gräns samt för att uppfylla krav i internationella säkerhetsinitiativ. Säkerhetsinitiativet togs i kraft den 1 juli 2009.

För aktörerna i transportkedjan innebär föranmälan att en elektronisk deklaration måste skickas in till tullmyndigheten en bestämd tid innan export/import sker till/från EU:

- Vid sjötransport gäller för containers att anmälan ska ha inkommit till tull senast 24 timmar innan gods lastas på fartyg med en destination i icke EU land. För bulk- eller partigods gäller 4 timmar.
- Vid transport med flyg gäller att anmälan skall ha inkommit senast 30 minuter före flygets avgång om flyget är destinerat till land utanför EU.
- Gods som transporteras på väg ska anmälas 1 timme innan avgång från utfartstullkontoret, vilket betyder när transport lämnar EU. För vägtransporter med avgång i Sverige med destination i land utanför EU innebär i realiteten tidsfristen ingenting.
- Motsvarande för järnvägstransporter är 2 timmar.

Reglerna för export är dock redan idag att exportdeklarationen ska göras innan varorna lämnar det exporterande företagets lagerplats, vilket innebär att tidsfristen för föranmälan i de flesta fall i realiteten endast gäller transport med fartyg från Sverige med destination till land utanför EU alternativt via annat EU land.

Om logistikkedjan innefattar flera transportslag gäller tidsfristen för den transport som lämnar EU:s gemensamma gräns, vilket ofta sker med containerfartyg och då gäller alltså att föranmälan måste ha inkommit till tullmyndighet senast 24 timmar innan fartyg lastas.

Reglerna om föranmälan gäller inte för transporter inom EU gemenskapen med undantag om: ”godset transporteras mellan EU (med undantag av de franska

utomeuropeiska departementen, Azorerna, Madeira eller Kanarieöarna) och Grönland, Färöarna, Ceuta, Melilla, Norge, Island, hamnar i Östersjön, Nordsjön, Svarta Havet, Medelhavet eller samtliga hamnar i Marocko – 2 timmar innan fartyget lämnar sista hamn i EU."

Föranmälan behöver ej göras vid transport mellan EU och länder inom den så kallade säkerhetszonen (EU, Norge och Schweiz).

Om föranmälan inte lämnats eller inte inkommit i tid enligt bestämda tidsfrister stoppas transporter vid EU:s gräns till dess att den kommit in och att riskanalys på transporten genomförts. Syftet med säkerhetsinitiativet är att tid ska finnas för analys av gods, avsändare, vilken mottagaren är, med mera.

För export från EU finns följande föranmälan:

- Exportdeklaration innehållande kompletta uppgifter om godstransport, varor m.m. vilken gäller när varor ska lämna gemenskapens tullområde.
- Summarisk utförseldeklaration ska lämnas endast i de fall gods transiteras från ett EU land, via land utanför EU, till EU land.
- Transiteringsdeklaration

Ansvaret för att anmälan görs ligger vid export av varor från EU hos exportören. Vid import är det transportören som är ansvarig för att föranmälan sker enligt en bestämd tid innan ankomst av varor till EU.

8.12 Föranmälan USA (Advance Manifest Regulation)

Benämning:	Advance Manifest Regulation (Föranmälan USA)
Initiativtagare:	En del i ”Trade Act of 2002”
Inriktning:	Hindra farliga varor från att transporteras in och ut från USA
Drivkraft:	Försvåra kriminell aktivitet och förhindra terrorism
Geografiskt område:	USA
Kopplingar:	CSI, C-TPAT, ACE med flera
Togs i kraft:	Januari 2004
Säkerhetshot som främsta ska förebyggas:	Smuggling, terrorism m.m.
Påverkar främst vilka delar i transportkedjan:	Import av gods till USA

Som en del i handlingsplanen ”Trade Act of 2002” efter terrorattentaten i USA den 9/11 2001 infördes Advance Manifest Regulation vilket är en reglering över föranmälan av gods som ska exporteras till USA. De reviderade bestämmelserna togs i kraft i januari 2004.

Advance Manifest Regulation, föranmälan USA, är ett säkerhetsinitiativ för att förebygga att import av gods till USA utgör ett hot mot landets säkerhet samt är mål för illegitimt gods. Den påverkar gods som exporteras till USA.

För aktörerna i transportkedjan innebär Advance Manifest Regulation att en elektronisk föranmälan måste skickas in till CBP (U.S. Customs and Border Protection) innan godsankomst enligt nedanstående;

- Vid sjötransport för containers gäller att den elektroniska deklarationen ska ha inkommit senast 24 timmar innan lastning på fartyg.
- För bulk- eller partigods gäller för sjötransporter kortare än 24 timmar att föranmälan ska ske senast vid avgång från främmande hamn.
- För sjötransporter av bulk- eller partigods längre än 24 timmar gäller att deklarationen ska ha erhållits av CBP senast 24 timmar innan ankomst till amerikansk hamn.[40]

Den elektroniska föranmälan ska innehålla bland annat;

- Sista utländska hamn innan fartyget sätter kurs mot amerikansk hamn
- Preliminärt ankomstdatum
- Precis beskrivning av gods eller HTS-kod (en kod som anger godsets typ)
- Transportörens och mottagarens uppgifter

[40] http://www.cbp.gov/xp/cgov/trade/trade_outreach/advance_info/ [2010-07-20]

Informationen analyseras i CBP:s system ATS (Automated Targeting System) för att välja ut containers/gods som bör kontrolleras vid ankomst. Det sker efter förbestämda kriterier med fokus på terrorrisken.

Advance Manifest Regulation påverkar både den utländska exportören (eller det amerikanska företag som exporterar till USA), importören och transportbäraren/rederiet då informationen i föranmälan har sitt ursprung från alla dessa aktörer. Det är också av aktörernas gemensamma intresse att uppgifterna är korrekta.

Om den elektroniska deklarationen inte är komplett, felaktig eller inkommen för sent kan;

- CBP förhindra lastning av fartyg med ekonomiska konsekvenser som följd; hamnavgifter för rederiet och försenade leveranser för exportör och importör.
- Skeppningen utsättas för detaljgranskning av CBP.
- Försenas tillstånd alternativt förnekas att lossa gods i amerikansk hamn vid ankomst.[41]

Ett gott samarbete och bra kommunikation mellan de i godsets transportkedja ingående aktörerna är alltså av yttersta vikt.

I likhet med föranmälan EU finns regler också för övriga transportslag även om dessa sällan påverkar de interkontinentala transporterna;

- För transport med tåg ska anmälan ha inkommit senast två timmar innan ankomst till den amerikanska gränsen.
- När godstransport sker på väg ska gods föranmälas senast en timme innan ankomst till gräns och en halvtimme innan för medlemmar i FAST.
- För flyg gäller fyra timmar innan avgång från flygplats i Mexico och Canada samt syd- och Centralamerika (ovanför ekvatorn).

De väl tilltagna tiderna för föranmälan (24 timmar för containertransport på sjö) omöjliggör för rederierna att acceptera sändningar efter deklarationens insändningsdeadline vilket underlättar rederiernas lastplanering men försämrar samtidigt flexibiliteten i logistikkedjan för avsändarföretagen.

[41] Dictionary of International Trade, Handbook of the global trade community 8th edition, Edward G. Hinkelman

8.13 IATA/DGR

Benämning:	IATA/DGR (Dangerous Goods Regulations)
Initiativtagare:	En expertkommitté inom FN:s ekonomiska och social råd (ECOSOC) samt två underkommittéer till expertkommittén arbetar kontinuerligt med FN:s rekommendationer vad gäller transport av farligt gods. När det gäller flygtransporter är det flygoperatörernas egen organisation IATA som fastställer regler (DGR) men dessa bygger på FN rekommendationerna.
Inriktning:	Föreskrifter för flygtransport av farligt gods
Drivkraft:	Minska risken för olyckor och tillbud under hantering och transport av farligt gods
Geografiskt område:	Internationellt
Kopplingar:	ICAO/IT och till de andra föreskrifterna för farligt gods för andra transportslag – ADR (väg), RID (järnväg) och IMDG (sjö)
Togs i kraft:	Utkommer med ny version varje år och gäller från 1 januari. År 2010 är det den 51:a versionen av IATA/DGR som gäller.
Säkerhetshot som främsta ska förebyggas:	Terrorism
Påverkar främst vilka delar i transportkedjan:	Avsändare, landsvägstransportörer, landsvägsterminaler

För luftfartens del återfinns den rättsliga regleringen av farligt gods i ICAO Technical Instructions (ICAO-TI) som den Internationella Civila Luftfartsorganisationen (ICAO) publicerar. Instruktionerna är bindande för de länder som har biträtt konventionen om internationell civil luftfart (Chicago-konventionen).

Därutöver har flygbolagen inom den internationella luftfartsorganisationen (IATA) utarbetat regler som är baserade på ICAO-TI och kompletterade med bolagens tilläggsregler. Dessa regler har benämningen Dangerous Goods Regulations (DGR).

Transportstyrelsen är behörig myndighet för lufttransporter av farligt gods och företräder Sverige i arbetet med att utveckla ICAO-TI.

Transportsäkerheten har alltid varit högre inom flygbranschen redan innan händelserna i New York 2001. Men efter den 9/11 2001 har ett kapitel 1.6 om transportsäkerhet tillkommit i IATA/DGR.

I likhet med övriga transportslag återfinns regler för vilka försiktighetsåtgärder som ska vidtas vid överlämnandet och transporten av farligt gods, krav på utbildning för de som är inblandade i transporten och krav på skyddsplan för farligt gods med hög riskpotential.

8.14 IMDG-koden

Benämning:	IMDG-koden (International Maritime Dangerous Goods Code)
Initiativtagare:	En expertkommitté inom FN:s ekonomiska och social råd (ECOSOC) samt två underkommittéer till expertkommittén arbetar kontinuerligt med FN:s rekommendationer vad gäller transport av farligt gods. För sjötransporter är det den internationella sjöfartsorganisationen IMO
Inriktning:	Föreskrifter för sjötransport av farligt gods
Drivkraft:	Minska risken för olyckor och tillbud under hantering och transport av farligt gods
Geografiskt område:	Internationellt
Kopplingar:	ISPS och till de andra föreskrifterna för farligt gods för andra transportslag – ADR (väg), RID (järnväg) och IATA/DGR (flyg)
Togs i kraft:	Utkommer med ny version vart annat år. Senaste version IMDG 34-08 var frivillig år 2009 och är obligatorisk från och med 1 januari 2010.
Säkerhetshot som främsta ska förebyggas:	Terrorism
Påverkar främst vilka delar i transportkedjan:	Avsändare, landsvägstransportörer, landsvägsterminaler

Vid internationella transporter av förpackat farligt gods till sjöss ska IMDG-koden (International Maritime Dangerous Goods Code) tillämpas. IMDG-koden utarbetas av den internationella sjöfartsorganisationen IMO (International Maritime Organization).

IMO har även utarbetat rekommendationer för hantering av farligt gods i hamnar (Recommendations on the Safe Transport of Dangerous Cargoes and Related Activities in Port Areas).

På vissa rutter mellan Danmark, Tyskland, Polen, Finland, Estland, Lettland, Litauen och Sverige kan även det s.k. Östersjöavtalet tillämpas (Memorandum of Understanding for the Transport of Dangerous Goods on Ro-Ro Ships in the Baltic). Östersjöavtalet syftar till att underlätta transport av farligt gods som sker med ro-ro-fartyg i Östersjön, genom att göra avsteg från de regler som normalt gäller vid internationell sjötransport dvs. IMDG-koden.

Transportstyrelsen är behörig myndighet för sjötransporter av farligt gods och företräder Sverige i arbetet med att utveckla IMDG-koden, hamnrekommendationerna och Östersjöavtalet.

Sedan 2006 finns det i IMDG-koden ett kapitel 1.4 med bestämmelser om transportskydd med tydliga hänvisningar till ISPS-koden för personalen ombord (besättning) och i hamnen (stuveri). I övrigt reglerar IMDG-koden framförallt landpersonalens försiktighetsåtgärder som ska vidtas vid överlämnandet och transporten av farligt gods, krav på landpersonalens utbildning och extra krav på farligt gods med hög riskpotential med krav på skyddsplan.

8.15 ISO 28000:2007

Benämning:	International Organization for Standardization
Initiativtagare:	De till ISO anslutna nationella standardiseringsorganisationerna
Inriktning:	”Specification for securing management systems for the supply chain”
Drivkraft:	Skapa en internationell standard för arbete med säkerhetsfrågor
Geografiskt område:	Globalt
Kopplingar:	AEO
Togs i kraft:	2007
Säkerhetshot som främsta ska förebyggas:	Smuggling, pirat- och terroristhot
Påverkar främst vilka delar i transportkedjan:	Hela transportkedjan

ISO 28000 är utarbetad för att öka säkerheten i leveranskedjan. Standarden är inriktad på att övergripande ge riktlinjer för ledning av frågor rörande säkerhet för internationella transporter i både mindre och större företag. Den är tillämpbar för verksamheter inom produktion, lager, hantering och transport av gods i alla skeden.

Standarden kräver att säkerhetsmiljön, ledning- och kontrollsystem, i vilken företaget är verksamma inom, bedöms enligt givna riktlinjer.

Genomgången av verksamhetens säkerhet ska ske regelbundet och om brister identifieras bör dessa åtgärdas genom införande av lämpliga processer och uppföljningssystem.

Metoden för att uppfylla målen är i ISO: standarden baserad på PDCA (Plan-Do-Check-Act) och den kan kort förklaras som;

- Plan: identifiera och definiera vilka åtgärder som måste införas för att uppfylla önskade mål gällande säkerheten.
- Do: genomför åtgärder enligt punkt 1.
- Check: följ upp genomförda åtgärder och säkerställ att de definierade målen uppfyllts enligt säkerhetspolicyn.
- Act: gör kontinuerliga förbättringsåtgärder av säkerhetsledningssystemet.

ISO 28000 riktar sig således till alla företag inom mycket diversifierade branscher men med en sak gemensam – en vilja att utarbeta/införa/förbättra hur säkerhetsfrågorna hanteras.

Ytterligare en viktig faktor är, förutom det egna företagets säkerhetsrutiner, att kunna visa andra vilken säkerhetspolicy som används och hur denna säkerställs i den löpande verksamheten.

Mycket övergripande är det generella kravet att säkerhetsledningssystemet ska: identifiera säkerhetsrisker, behandla riskbedömningar, hur risker kan kontrolleras och konsekvenser mildras. Riskerna innefattar allt från olyckor och naturkatastrofer till uppsåtliga attentat på verksamheten.

Ett uppfyllande av ISO standarden ger, på grund av det principiella och systematiska sättet säkerhetsfrågorna hanteras, en bra grund för certifiering enligt flertalet säkerhetsinitiativ såsom ISPS-koden, AEO och C-TPAT.

8.16 ISPS-kod

Benämning:	International Ship and Port Facility Security Code
Initiativtagare:	International Maritime Organization (IMO)
Inriktning:	Sjötransporter på en internationell nivå
Drivkraft:	Att minska risken för att sjötransporter används direkt eller indirekt vid genomförande av terrorattack
Geografiskt område:	Globalt (167 medlemsländer)
Kopplingar:	Finns som tillägg i SOLAS (Safety of Life at Sea) vilken behandlar säkerhetsfrågor till sjöss.
Togs i kraft:	Antogs 2002 sattes i kraft juli 2004
Säkerhetshot som främsta ska förebyggas:	Terrorism
Påverkar främst vilka delar i transportkedjan:	Hamnar, rederier, sjötransporter

ISPS-koden är IMO:s svar på den ökade hotbilden efter händelserna den 9/11 i USA. Risken för terroristattacker blev plötsligt ett verkligt hot mot transportnäringen världen över. Kort efter händelserna beslutade IMO att försöka definiera vilka åtgärder som bör införas för att förebygga att en liknande händelse inträffar inom sjöfarten och vilket tillvägagångssättet skulle vara. Uppgiften försvåras av de snabba förändringar som sker kontinuerligt men kanske framförallt skillnader länder emellan.

ISPS-koden är utformad för att vara ett grundläggande krav med rekommendationer sett på ett globalt plan, vilket således utgör en minimal säkerhetsnivå som alla länder bör uppfylla. Det är ländernas individuella ansvar att med ISPS som utgångspunkt göra bedömningar om vilka säkerhetsåtgärder som krävs för tillfället och kommunicera dessa till berörda parter såsom fartyg och hamnar.

ISPS-koden består både av krav och frivilliga rekommendationer. Riskbedömningar måste göras i varje enskilt fall där det fastslås vilka åtgärder som är nödvändiga.

ISPS är ett ramverk för att bedöma risker och tillhandahåller sätt på hur sårbarheten kan minskas. Fartyg och hamnar måste, efter ISPS-kodens införande, visa på att ett korrekt tillvägagångssätt används i bedömningen av risker.

Koden omfattar kortfattat följande kravområden;

- Att information avseende hot mot säkerheten samlas in och utvärderas
- Utbyte av sådan information stater emellan
- Att resurs för larmning finns vid hot mot säkerheten
- Obehöriga ska förhindras tillträde till fartyg, hamnar och skyddsområden
- Likaså vapen, explosiva medel m.m.
- Fartyg och hamnar ska ha skyddsplaner och utbildad personal som övar i dessa

I ISPS-koden finns tre säkerhetsnivåer med följande kortfattade innebörd;

- Nivå 1, för fartyg gäller att: kontroll ska ske av personer som går ombord och deras tillhörigheter, bevakning göras av skyddsområden så att endast behöriga personer får access, övervakning av däck, lasthantering samt förråd. För hamnar gäller att tillträdet till hamnen kontrolleras, lasthantering, förråd samt områden med begränsat tillträde övervakas för att endast behörig personal får tillträde.
- Skyddsnivå 2 och 3, nivån på skyddsåtgärder utökas från nivå 1.

ISPS-koden är en del i IMO:s SOLAS konvention och är därmed obligatorisk för de till SOLAS 148 tillhörande staterna.

8.17 PIP

Benämning:	Partners In Protection
Initiativtagare:	CBSA – Canada Border Services Agency
Inriktning:	Import till Kanada
Drivkraft:	Initialt att förbättra företagens efterlevnad av tullreglerna. I det nya programmet är drivkraften att skapa kompatibilitet med bland annat C-TPAT
Geografiskt område:	Kanada
Kopplingar:	C-TPAT, FAST
Togs i kraft:	1995, nytt program 2008
Säkerhetshot som främsta ska förebyggas:	Organiserad brottslighet, terrorism, smuggling
Påverkar främst vilka delar i transportkedjan:	Gods som passerar gränser

PIP, Partners In Protection är ett säkerhetsinitiativ grundat 1995 av den kanadensiska tullmyndigheten. Det huvudsakliga syftet var att främja företagens medvetenhet och efterlevnad av de dåvarande tullreglerna. De kanadensiska reglerna var mycket tuffa gällande smuggling, bland annat fick transportmedel som användes beslagtas och ofta används kommersiella logistiktransporter för kriminella handlingar. Åkerierna kunde därför drabbas hårt. Det första säkerhetsinitiativet var därför en önskan från företagens sida att få tillstånd ett närmare samarbete med tullmyndigheten för att på så sätt ha ett upparbetat förtroende om logistikkedjan skulle utsättas för smugglingsförsök.

Efter terrorattacken i USA 2001 ändrades kraven på CBSA:s arbete och PIP introducerades i sin nuvarande form i mitten av 2008. Nu ligger mer fokus på säkerhet i logistikkedjan, vilket innefattar både fysisk säkerhet (skalskydd m.m.) och rutiner i det kontinuerliga säkerhetsarbetet samt hur detta bör utvecklas hos aktuell aktör. Fortfarande ligger emellertid huvudfokus på att motverka stöld och smuggling än terrorism, vilket är i linje med den mindre risk för terroristattacker som åligger jämfört med USA. Den nya utvecklingen av PIP beror primärt på en önskan om att skapa en överensstämmelse med CBP:s (U.S. Customs and Border Protection) säkerhetsinitiativ och därmed underlätta handeln länderna emellan.

Det nuvarande PIP (2008) är därför utvecklat för att vara kompatibelt med CBP:s (U.S. Customs and Border Protection) säkerhetsinitiativ C-TPAT (Customs-Trade Partnership Against Terrorism). Överensstämmelsen initiativen emellan har gjort det möjligt för CBSA och CBP att ingå avtal om ett gemensamt säkerhetsarbete med mål att underlätta transport av gods länderna emellan. Gods som passerar den gemensamma gränsen kontrolleras enligt samma rutiner/regler oavsett från vilket land det anländ ifrån.

För Canada Border Services Agency innebär PIP att mer fokus kan läggas på identifiering, analys och kontroll av högriskgods samtidigt som lågriskgods effektivare

transporteras mellan främst USA och Kanada (handeln över gränsen uppskattas till 2 miljarder dollar per dag)[42].

Till skillnad från exempelvis C-TPAT ger PIP inte några krav på vilka exakta åtgärder som måste införas för att uppfylla certifieringskraven.

PIP certifiering är från 2002 obligatorisk för kanadensiska företag för medlemskap i FAST (Free And Secure Trade) vilket är ett initiativ för underlättande av godstransporter (exempelvis godstransporter in i Kanada). Certifiering är frivillig, men i likhet med andra initiativ, är ett deltagande förutom direkta fördelar (färre kontroller m.m.), en bra väg att stärka den övergripande hanteringen av säkerhetsfrågor i verksamheten och att inge förtroende hos kunder och leverantörer.

Enligt den utvärdering som gjordes av PIP 2006 var antalet medlemmar cirka 1600 varav merparten, 70 procent, är åkerier och 82 procent företag med sin bas i Kanada. Deltagandet är relativt lågt ställt i relation till exempelvis det totala antalet åkerier som är runt 6000. I importörsledet, som PIP också riktar sig till, är deltagandet mycket lågt, uppskattningsvis något över en procent.[43] Det låga intresset för PIP certifiering tyder på att de fördelar ett medlemskap innebär inte kompenserar det merarbete som det innebär att uppfylla kraven.

[42]Canada Border Services Agency, *http://www.cbsa-asfc.gc.ca/media/release-communique/2008/2008-07-02-eng.html (2010-04-28)*
[43] Canada Border Services Agency, *http://cbsa-asfc.gc.ca/agency-agence/reports-rapports/ae-ve/2006/pip-pep-eng.html (2010-05-11)*

8.18 RID

Benämning:	RID/RID-S
Initiativtagare:	En expertkommitté inom FN:s ekonomiska och social råd (ECOSOC) samt två underkommittéer till expertkommittén arbetar kontinuerligt med FN:s rekommendationer vad gäller transport av farligt gods
Inriktning:	Föreskrifter för transport av farligt gods på järnväg
Drivkraft:	Minska risken för olyckor och tillbud under hantering och transport av farligt gods
Geografiskt område:	Europa + några nordafrikanska länder
Kopplingar:	Främst till de andra föreskrifterna för farligt gods för andra transportslag – ADR (väg), IMDG (sjö) och IATA/DGR (flyg)
Togs i kraft:	Utkommer med ny version vart annat år. Senaste version började gälla i Sverige 16 februari 2009.
Säkerhetshot som främsta ska förebyggas:	Terrorism
Påverkar främst vilka delar i transportkedjan:	Avsändare, landsvägstransportörer, landsvägsterminaler

RID är en förkortning av *Règlement concernant le transport international ferroviaire de marchandises Dangereuses.* RID utvecklas fortlöpande och fastställs av den mellanstatliga organisationen Intergovernmental Organisation for International Carriage by Rail (OTIF). Arbetsgruppen som ansvarar för RID benämns RID-Fachausschuss (RID-FA). RID utgör bihang C till fördraget om internationell järnvägstrafik (Convention concerning International Carriage by Rail, COTIF). 44 länder är anslutna till RID.

RID-FA utvecklar och fastställer innehållet i RID med FN-rekommendationerna och de rådgivande besluten från Joint-mötet som grund. Dessutom tillkommer bestämmelser som är unika för järnvägstransporter, exempelvis krav på cisternvagnar och märkning av vagnar.

MSB och Transportstyrelsen företräder Sverige i RID-FA. MSB utarbetar RID-S som är benämningen på föreskrifterna som i Sverige gäller för transport av farligt gods på järnväg. Föreskrifterna innehåller både internationella och nationella bestämmelser.

Sedan 2006 finns det i RID 2006 ett kapitel 1.10 med bestämmelser om transportskydd. Med transportskydd och skydd avses försiktighetsåtgärder som ska vidtas för att minimera stöld eller obehörigt förfarande med farligt gods, som kan skada personer, egendom eller miljö.

I RID kapitel 1.10 finns regler för vilka försiktighetsåtgärder som ska vidtas vid överlämnandet och transporten av farligt gods, krav på utbildning för de som är inblandade i transporten och extra krav på farligt gods med hög riskpotential t.ex. skyddsplaner, speciella anordningar, anmälningsplikt, förutbestämda transportvägar etc.

8.19 SAFE Port Act

Benämning:	Security and Accountability for Every Port Act (SAFE Port Act)
Initiativtagare:	USA:s då republikanska kongress med George W. Bush
Inriktning:	Öka säkerheten i sjötransporter till USA:s hamnar
Drivkraft:	Försvåra kriminell aktivitet och förhindra terrorism
Geografiskt område:	USA
Kopplingar:	C-TPAT, 100% scanning, CSI, SFI mfl.
Togs i kraft:	I lagstiftning i oktober 2006
Säkerhetshot som främsta ska förebyggas:	Smuggling av illegitimt gods däribland material som kan användas för terrorism
Påverkar främst vilka delar i transportkedjan:	Globala godstransporter med fartyg till USA

The Security and Accountability for Every Port Act, SAFE Port Act, är en lag som trädde i kraft i oktober 2006 och var Bush administrationens respons på det ökade terroristhotet. Innebörden i SAFE Port Act är att varje hamn har ansvarskyldighet för det egna området och landets säkerhet. Lagen är grunden till många av övriga amerikanska säkerhetsinitiativ och det utvecklande arbetet inom den marina säkerheten bedrivs av the Department of Homeland Security (DHS).

The SAFE Port Act omfattar flertalet områden, bland annat att;

- Säkerhetsplaner ska finnas utarbetade för hur sjötransportvägarna ska säkras efter en säkerhetsincident till havs, exempelvis en miljökatastrof, en kraftig störning i transportsystemet m.m.
- Tillträde till containerfartyg, verksamma i interkontinentala godstransporter, noga kontrolleras med mål att förhindra obehöriga personers åtkomst till last
- För personer som arbetar med utvecklande och implementering av anläggningssäkerhetssystem krävs amerikanskt medborgarskap alternativt en komplett bakgrundskontroll inklusive check så att personen inte är efterlyst terrorist.
- The Secretary of Homeland Security (the head of Department of Homeland Security) minst två gånger per år, verifierar effektiviteten i fartyg och anläggningars säkerhetssystem, inklusive minst en oannonserad inspektion.
- Myndighetsgemensamma centra för hamnsäkerhet etableras i prioriterade högriskhamnar och finansieringshjälp för hamnar att införa åtgärder för att förebygga terroristhandlingar.
- Att 100% av containers skannas i avsändande utländsk eller mottagande hamn.
- DHS utvärderar säkerheten i utländska hamnar involverade i amerikansk handel.

För att klara av att skapa en komplett säkerhet är DHS uppfattning att det totala maritima säkerhetsskyddet måste byggas upp av flertalet system både på amerikansk mark men därtill omfatta alla aktörer i den globala logistikkedjan. Ansvaret för och arbetet med att analysera transportens säkerhet, sträcker sig från tillverkaren

(avsändaren) vidare till den exporterande hamnen, övriga transportaktörer och rederiet, innan transporter anländer till USA:s gräns. Ju fler inblandade aktörer i transportkedjan som aktivt jobbar med säkerheten desto större är sannolikheten att ett potentiellt säkerhetshot upptäcks.

Hög säkerhet är prioriterat men samtidigt betonas, av DHS, att säkerhetsinitiativen måste göra mer nytta än vad de försvårar den kommersiella handeln och vikten av att resurserna prioriteras rätt.

Samtidigt finns inte ens, när detta skrivs 2010, utvecklad teknik för att genomföra the SAFE Port Act fullt ut, exempelvis saknas tekniska lösningar för ett komplett införande av 100% scanning då all typ av strålning inte kan upptäckas. DHS uttryckte det i april 2007 som:

”The department does not believe that, at the present time, the necessary technology exists for such solution. The department is actively working with industry to test different technologies and methodologies that would provide economically and operationally viable enhancements to container security” [44]

DHS vill till skillnad från the SAFE Port Act i högre grad prioritera användande av riskbedömningar och fokusera på de delar i logistikkedjan som utgör en hög risk, medan den största delen av det kommersiella godset bör tillåtas att transporteras obehindrat.

[44] Lloyd’s handbook of maritime security, Rupert Herbert-Burns, Peter Lehr

8.20 SECCONDD

Benämning:	Secure Container Data Device standardisation
Initiativtagare:	Thales Research and Technology (UK) Ltd, Selex Communications S.p.A, Cotecna Inspection Ltd, HM revenue and Customs och European Committee for Standardization (CEN)
Inriktning:	Att ”säkra” containers
Drivkraft:	Att genom smart teknik göra frakt med containers säkrare
Geografiskt område:	Globalt
Kopplingar:	Inga direkta kopplingar
Togs i kraft:	Under utveckling
Säkerhetshot som främsta ska förebyggas:	Stöld, smuggling, terrorhot
Påverkar främst vilka delar i transportkedjan:	Hela transportkedjan för containers

Hela projektet (forskningsprojektet) med SECCONDD grundar sig i en önskan att göra containerhantering säkrare. Det syftar framförallt till möjligheterna att kontrollera om containerns innehåll förändras under transporten. Bakom SECCONDD står två koncerner inom försvars- och säkerhetsfrågor; Thales och Selex Communications, verksamma inom utveckling av försvarssystem och avancerad kommunikationsutrustning.

Målet med SECCONDD är att utveckla ett standardgränssnitt för ”smarta containers” vilka med hjälp av tekniska innovationer kommer möjliggöra; kontroll av aktuell position, registrering av vart containern varit och vart den är på väg. Grundsystemet kan kompletteras med utrustning för upptäckande av; intrång i container samt om innehållet är korrekt. Initialt är målet att initiera en internationell standard för gränssnittet mellan sändare (den tekniska ”kommunikations” utrustningen i containers) och mottagare (i hamn eller gränsövergång).

Tanken är att genom att introducera ny och smart teknik i containers ge berörda parter möjlighet att göra icke visuella kontroller under containers transportväg. Det skulle ge fördelar för alla inblandade;

- Transportbeställaren (säljaren) minimerar risken för kontroll av container, vilket kan försena leverans.
- Logistikaktören minskar risken att ovetandes bidra i exempelvis smuggling av vapen.
- Tullmyndigheter kan fokusera mer på kontroll av högriskgods om en större andel containers kan passera gränserna utan visuell kontroll.
- Mottagare av gods garanteras att innehållet i containern är samma som det avsändaren skickade.

En ”smart container” kan alltså vara en del i arbetet med att förhindra smuggling men hittills saknas dock överkomlig (till pris och installationsmöjlighet) tekniska sensorer

för att upptäcka exempelvis sprängämnen och droger. Däremot är det fullt möjligt att analysera temperaturförändringar, upptäcka intrång, bestämma position osv.

Marknaden har redan börjat växa och framåt 2012 väntas ”smarta containers” omsätta uppåt 4 miljarder dollar.[45] Definitionen innefattar emellertid hela skalan av ”smarta containers” allt från ett enkelt inbrottsskydd till interface som kan ge information om exempelvis vem som lastat, containerns ursprungsplats/-land och destination, vart den befinner sig osv.

Som ett sekundärt mål är det tänkt att den tekniska utrustning och gränssnittet också ska kunna användas som en del i automatiserade lasthanteringssystem.

Första steget har redan tagits då ISO i april 2007 antog en standard (ISO 18185) för elektroniska plomberingar som upptäcker intrång i containers. Enligt forskningsprojektet SECCONDD behövs vidare arbete för att etablera en standard gällande ett komplett system.

[45] http://www.logasiamag.com/article-1190-smartcontainers-LogisticAsia.html, James Giermanski, 1/3 2009

8.21 Secure Export Scheme

Benämning:	SES, Secure Export Scheme
Initiativtagare:	New Zealand Customs Service
Inriktning:	Förbättra säkerheten i logistikkedjan samt visa överensstämmelse med internationella standarder/regler samt USA:s säkerhetsinitiativ
Drivkraft:	Underlätta för exportföretag att verka på den globala arenan samt förbättra tullarbetets effektivitet (fokusera på högriskgods)
Geografiskt område:	Nya Zeeland men export globalt
Kopplingar:	WCO:s standarder
Togs i kraft:	Inleddes 2004
Säkerhetshot som främsta ska förebyggas:	Smuggling, sabotage m.m.
Påverkar främst vilka delar i transportkedjan:	Godstransport från Nya Zeeland med alla transportslag

Nya Zeelands Secure Export Scheme SES är ett frivilligt program mellan New Zealand Customs Service och de företag som är verksamma inom export. Målet är att skydda godstransporter från att utsättas för smuggelgods, sabotage m.m. och på ett globalt plan, förhindra terrorism.

Initiativet är också utformat för att medlemsföretagens godstransporter ska uppfylla de internationella krav som finns, däribland WCO:s standarder och the U.S. Container Security Initiative CSI. Det minskar risken att exportgods fastnar i säkerhetskontroller och därmed blir försenat till kund.

För att uppnå målen analyserar medlemsföretagen i konsultation med tullen vilka åtgärder som behöver införas för att skydda gods genom hela logistikkedjan mot aktuella säkerhetshot. Exempelvis förseglas containers innan skeppning med av tullen godkänd plombering. I gengäld garanterar SES partnern att allt containerinnehåll är redovisat och att ingenting annat återfinns i containern.

Fördelarna för medlemmarna är:

- Lägre avgifter för lagring av avgående gods i hamn
- Säkerheten i logistikkedjan ökar
- Att visa samstämmighet med internationella säkerhetsinitiativ/-standarder ökar trovärdigheten hos importerande kund/företag
- Effektivare tullklarering i MRA[46] länder
- Hjälp från New Zealand Customs om problem med MRA tullmyndighet uppstår
- Minskat antal kontroller av gods

[46] MRA, Mutual Recognition Agreement, finns hittils med Japan och USA där varandras arbete med säkerheten i leveranskedjan erkänns

SES hade i början av 2010 mer än 120 medlemmar[47] som är mycket nöjda med de lättnader i kontroller som varit följden av medlemskap.

”Prior to the partnership, container inspection was a frequent as fortnightly. After becoming an approved partner, this gradualy extended to monthly, then to quarterly, to what seems to be now as little as two containers per year”.[48]

Detta enligt ansvarig på det Nya Zeeländska företaget Click Clack tillverkare av konsumentprodukter med export till mer än 50 länder.

[47] www.scoop.co.nz/stories/BU1002/S00283.html, CMP Canterbury join Customs’ Secure Exports Scheme, [2010-06-17]
[48] www.customs.govt.nz/exporters/Secure+Exports+Scheme.html, [2010-06-17]

8.22 Secure Trade Partnership

Benämning:	STP, Secure Trade Partnership
Initiativtagare:	Singapore Customs
Inriktning:	Förbättra säkerheten i logistikkedjan samt visa överensstämmelse med internationella säkerhetsstandarder/-regler samt USA:s säkerhetsinitiativ
Drivkraft:	Värna Singapores position som ett nav i världshandeln
Geografiskt område:	Globalt
Kopplingar:	Överensstämmelser med internationella standarder bland andra WCO SAFE Framework
Togs i kraft:	Maj 2007
Säkerhetshot som främsta ska förebyggas:	Terrorism
Påverkar främst vilka delar i transportkedjan:	Import och export

Secure Trade Partnership är ett frivilligt säkerhetsinitiativ för att förbättra säkerheten i den globala logistikkedjan. Bra säkerhet i transporter till och från Singapore är av högsta vikt då Singapore är ett nav i den världsomspännande handeln.

Singapore är den hamn som tar emot flest containers i världen med nästan 30 miljoner enheter per år (2008)[49]. Det övervägande antalet når inte längre än till hamnen där de omlastas för fortsatt skeppning (transshipment), vilket ökar risken för att containers innehåller olagliga varor.

På grund av detta är det säkerhetsarbete som bedrivs av Singapore Customs av högsta vikt för säkerheten i hela den globala leveranskedjan. Samarbetet med USA är väl utvecklat och Singapore är partner i USA:s program CSI (Container Security Initiative).

STP, Secure Trade Partnership, är utformat för överensstämmelse med internationella standarder såsom World Customs Organisation (WCO) SAFE Framework of Standards.

Med mål att:

- Skapa medvetenhet om vikten av ett helhetsgrepp om säkerheten i logistikkedjan
- Visa på Singapore som ett säkert nav för de globala transportflödena
- Främja ett effektivt flöde av varor
- Skapa incitament för företag att säkra de egna logistikprocesserna

Medlemskap kräver att den ansökande aktören antagit lämpliga och tillräckliga säkerhetsåtgärder för den egna transportkedjan, antingen enligt eget utvecklat system och processer (om dessa motsvarar eller överträffar kraven i STP), alternativt genom

[49] http://www.mardep.gov.hk/en/publication/pdf/portstat_2_y_b5.pdf

att följa STP utvecklade riktlinjer. Singapore Customs har erkänt internationella säkerhetsinitiativ såsom ISPS (International Code for the Security of Ships and of Port Facilities), TAPA (Transported Asset Protection Associations) med flera och syftar inte till att ersätta dessa. Målet är istället att komplettera och ytterligare utveckla samarbetet mellan tullmyndighet och företag i syfte att stärka säkerheten i den globala logistikkedjan.

Genom att anta lämpliga säkerhetsåtgärder och följa kraven i STP, alternativt andra internationella initiativ, visar företag/aktör på en vilja att skapa en säker logistikkedja. Följande fördelar ges:

- Godstransporter säkrade enligt STP löper mindre risk att utsättas för kontroll
- Fördelar i importerande lands gränskontroll
- Att visa samstämmighet med STP ökar trovärdigheten hos importerande kund/företag

8.23 SFI

Benämning:	SFI, Secure Freight Initiative
Initiativtagare:	U.S. Customs and Border Protection (CBP)
Inriktning:	Import i containers till USA
Drivkraft:	Förhindra WMD (Weapons of Mass Destruction) att smugglas in i USA och därmed förebygga terroristattacker
Geografiskt område:	Globalt gods till USA
Kopplingar:	CSI, Megaports, SAFE Port Act, 100% scanning
Togs i kraft:	December 2006
Säkerhetshot som främsta ska förebyggas:	Terrorism
Påverkar främst vilka delar i transportkedjan:	Främst gods som transporteras med containerfartyg till USA

SFI, Secure Freight Initiative, utgör en del i the SAFE Port Act som var kongressens svar på det ökade terroristhotet och togs i kraft 2006. Säkerhetsinitiativet SFI har som mål att förhindra att massförstörelse vapen smugglas in i USA via det legitima godsflödet av containers. DHS:s (Department of Homeland Security) Secretary Michael Chertoff:

”Our highest priority and greatest sense of urgency has to be aimed at preventing a nuclear weapon or dirty bomb attack against homeland”[50]

Målet med SFI är:

”Radiation scanning is a key link in the effort to enhance global supply chain security through more secure freight while facilitating legitimate trade to help preserve the world economy”[51]

Till skillnad från CSI är målet med SFI att fler än bara de containers som bedöms som högriskgods ska skannas. Skanningen ska upptäcka kärnvapen och radioaktivt material genom användning av röntgen-, gamma- och analytisk optisk teknik.

Unikt med SFI initiativet är att tekniken utlokaliseras till den utländska hamnen från vilket godset lastas. Det förhindrar terroristattacker även mot själva logistikkedjan som i sig kan vara ett mål. Ett attentat mot ett containerfartyg alternativt en amerikansk hamn kan få enorma konsekvenser.

Full implementering av SFI, 100% scanning av containers, har skett i bland annat Port Qasim, Karachi, Pakistan (mars 2007) och Puerto Cortés, Honduras (april 2007).[52]

[50] www.cbp.gov/xp/cgov/border_security/secure_freight_initiative/
[51] http://www.cbp.gov/linkhandler/cgov/newsroom/fact_sheets/trade_security/sfi/sfi_scanning.ctt/sfi_scanning.pdf, [2010-07-22]
[52] Maritime Security, Michael McNicholas

Informationen tolkas av CBP (U.S. Customs and Border Protection) utsänd personal och misstänkta containers undersöks fysiskt och kan stoppas från ombordlastning.
Puerto Cortés, Honduras, valdes som en av ”pilothamnarna” då den är en av de hamnar i Latinamerika med störst andel trafik till USA, utgörande totalt 0,73 procent motsvarande 74 500 containers per år. Antalet skapar en förståelse för vilket projekt 100% scanning av all containertrafik med USA som destination är.

Tekniken som används i Puerto Cortés, Honduras är:

”Radiation Portal Monitor (RPM) systems to detect radiation, Non-Intrusive Inspection (NII) equipment for imaging, and hand-held Radiation Isotope Identification Devices (RIIDs), as well as other technologies to ensure the integrity of the scanning process.”[53]

[53] http://www.cbp.gov/linkhandler/cgov/newsroom/fact_sheets/trade_security/sfi/sfi_honduras.ctt/sfi_honduras.pdf, [2010-07-22]

8.24 StairSec/Servicetrappan

Benämning:	StairSec/Servicetrappan
Initiativtagare:	Tullverket
Inriktning:	Rikta in verksamheten på företag som utgör en hög risk
Drivkraft:	Förenkling och kvalitetssäkring av tullhantering
Geografiskt område:	Sverige
Kopplingar:	AEO
Togs i kraft:	StairSec togs i kraft 2002 och avvecklas i slutet av 2010
Säkerhetshot som främsta ska förebyggas:	Smuggling
Påverkar främst vilka delar i transportkedjan:	Alla tranportslag

Servicetrappan är ett program som togs i kraft 2002 och syftade till att förbättra tullsystemet främst med avseende på samarbetet mellan tullverket och aktörerna i logistikkedjan. Projektet byggde därutöver på en kvalitetssäkring av tullhanteringen både när det gällde faktiska kontroller och det administrativa.

Fokus på tullarbetet skulle inriktas mer mot företag som bedömdes utgöra hög risk för att utnyttjas i olaglig verksamhet. Företag som i riskanalysen bedöms som lågriskverksamheter erhålls förenklingar i tullhanteringen, något som gynnar både tullverket och det enskilda företaget. Förutom låg risk krävs ett bra track record gällande regelverksefterlevnad och bra samarbete.

Lättnader i tullhanteringen kan erhållas i fem steg, därav ”servicetrappan”, efter certifiering av Tullverket. Ju mer information om företagens varu- och informationsflöden Tullverket får ta del av desto fler förmåner och förenklingar i tullhanteringen. För företagens del innebär det färre störningar i godleveranser/-transporter och minskade kostnader.

Stegen innebär:

- *Steg 1*, Icke certifierade företag med oförändrad tullhantering
- *Steg 2*, Fortfarande gällande icke certifierade företag och därmed oförändrad tullhantering. Har däremot tillstånd till handlingsförfaranden som krävs vid exempelvis ”förenklat deklarationsförfarande vid import”
- *Steg 3*, Första steget för en förenklad tullhantering. Har genomgått Tullverkets certifieringsprocess och minst en tullrutin är certifierad vilket bland annat innebär att godflödet tillhörande den certifierade rutinen inte kommer att undersökas av tullverket vid gränspassage
- *Steg 4*, Alla tullrutiner är certifierade medförande att företagets godsflöde kan passera landets gränser utan kontroll av Tullverket
- *Steg 5*, Det högsta steget i servicetrappan vilket innebär att alla aktuella förenklingar och fördelar erbjuds. Kravet är ett komplett godsspårningssystem för alla tullrutiner.

För tullverkets del innebär servicetrappan att mer av verksamhetens resurser kan användas för riskanalys, underrättelseprocesser och gränsskydd. Det utökade samarbetet med aktörerna i logistikkedjan innebär att företag i utbyte mot förenklade tullrutiner åtar sig att anmäla misstänkt tullbrottslighet såsom smuggling.

Under 2003 utvecklades StairSec som servicetrappans säkerhetsprogram med mål att, genom samarbete med svenska aktörer inom transportkedjan och utländska tullmyndigheter, erbjuda förenklingar till legala företag inom import och export. Detta samtidigt som säkerheten i hela logistikkedjan från producent till mottagare skulle säkerställas.

Som ett led i utökat internationellt samarbete inom logistiksäkerhet avvecklades StairSec i slutet av 2010 till förmån för säkerhetsinitiativet AEO som infördes inom hela EU den 1 januari 2008.

Det innebar att certifiering enligt StairSec och placering i servicetrappans högre steg från 2011 inte längre gäller. Kraven för en AEO certifiering överensstämmer däremot enligt Tullverket helt med kriterierna enligt servicetrappan och dess säkerhetsprogram StairSec vilket underlättar företagens nya certifieringsprocess för att erhålla AEO status.

I tillägg innebär en AEO certifiering förutom nationella förenklingar även lättnader i hanteringen av tullrutiner i hela EU-gemenskapen.

8.25 TAPA

Benämning:	TAPA – The Technology Asset Protection Association
Initiativtagare:	TAPA är en sammanslutning av företag inom produktion och transport av främst högt värderade varor/gods
Inriktning:	Lastbilstransporter
Drivkraft:	Minska förluster på grund av stölder
Geografiskt område:	Globalt
Kopplingar:	AEO
Togs i kraft:	2005 uppdaterades 2007
Säkerhetshot som främsta ska förebyggas:	Stöld
Påverkar främst vilka delar i transportkedjan:	Vägtransporter med aktörer som åkerier, industri, terminaler

TAPA är en sammanslutning av företag verksamma inom produktion och transport av högvärdigt gods. När den internationella föreningen grundades 1997 var den främst riktad mot tillverkare i högteknologiska branscher vilka kände ett behov att motverka de ökande säkerhetsriskerna. Med tiden har fler företag, även inom andra branscher, anslutit och det geografiska verksamhetsområdet har utökats från att gälla bara USA till Europa, Mellanöstern, Afrika och Asien.

TAPA har i dagsläget (2010) över 600 medlemmar varav många världskända företag som exempelvis Apple, Microsoft och Volvo. I logistikkedjan återfinns DHL, Posten med flera.

Incident Information Service (IIS), Freight Security Requirements (FSR) och Trucking Security Requirements (TSR) är säkerhetsinitiativ införda av TAPA.

FSR reglerar vilka krav som ställs på de olika aktörerna i transportkedjan för säkra transporter och lagring både sett till inre och yttre säkerhet. Kraven i FSR är uppdelade efter klassningsklass och är konkreta regler för hur säkerhetssystemen bör vara utformade i de olika delarna i transportkedjan. Exempel på några specifikationer för ”fysisk” säkerhet är; kameraövervakning av lastbryggor och passerkontroll för anställda och besökare.

Utöver den ”fysiska” säkerheten finns krav för hur processerna ska hanteras gällande dokumenthantering avseende bland annat; rapportering av förlorat gods och att bara nödvändig information om hanterat gods ges till inblandade parter. FSR reglerar också personalens tillgång till ”känsligt” gods. Exempelvis bör allt tillträde till lokal där gods hanteras enligt FSR vara begränsat till enbart berörd personal.

TSR är en detaljerad kravspecifikation, baserad på FSR och som är ämnad för lastbilstransporter. Exempelvis finns instruktioner för hur lastbilar och last ska skyddas från stöld och inbrott med larm- och spårningsutrustning etc. Specificerat finns därutöver krav på: personalkontroll, rapportering om tillbud väl inträffar, hur parkering bör ske för minskad risk, att en handlingsplan finns m.m.

Initiativet IIS är ett samarbete som bygger på informationsutbyte medlemmarna emellan samt myndigheter gällande kriminalitet inom området. Information om en incident samlas i en central kunskapsbas vilket underlättar undersökning och uppklarande av aktuellt brott, men används också i förebyggande syfte med mål att minska riskerna.

Vetskapen om brott blir tillgänglig för medlemsföretag och en riskbedömning utgående från den egna verksamheten kan göras. Ytterligare en fördel med IIS är att informationen om en stöld snabbt blir känt i branschen vilket kan förbättra chanserna att hitta det stulna godset. Informationen i IIS hjälper medlemsföretag och myndigheter att göra statistiska riskbedömningar.

8.26 WCO-SAFE

Benämning:	SAFE
Initiativtagare:	World Customs Organization
Inriktning:	Att öka säkerheten och förenkla för den internationella handeln
Drivkraft:	Ökad säkerhet och effektivare transporter
Geografiskt område:	Globalt
Kopplingar:	AEO
Togs i kraft:	2005 uppdaterades 2007
Säkerhetshot som främsta ska förebyggas:	Förbättra den totala säkerheten
Påverkar främst vilka delar i transportkedjan:	Är ett initiativ för att säkerheten i och underlätta handel på det globala planet varför främst interkontinentala transporter påverkas

World Customs Organization – WCO har som huvudmål att underlätta handel på det internationella planet genom att etablera gemensamma mål och regler. Det senaste decenniet har säkerhetsfrågan blivit än mer aktuell när det gäller att förebygga framförallt smuggling av material som kan användas vid exempelvis terrorattentat men även försvåra attentat mot transportsystemet i sig.

WCO:s medlemsländer står för 99 procent av den globala handeln[54] och därigenom blir de regler och rekommendationer, vilka beslutas inom ramen för WCO, bestämmande för internationella transporter. Det övergripande syftet är att, genom samarbetet i WCO, fastslå krav som tar hänsyn till andra mellanstatliga överenskommelser men även är anpassade för dagens högeffektiva transportsystem där möjligheten till manuell kontroll av gods är marginaliserad.

WCO:s ramverk för dessa frågor, SAFE, har bland annat som mål att;

- Flytta fokus på säkerhetsarbetet från importerande land till exporterande lands tullmyndighet
- Införa standarder för att främja säkerhet i transportkedjan på en global nivå
- Integrera logistiksystemen för alla transportslag
- Anpassa regler för att bättre passa den nya tidens utmaningar och möjligheter
- Främja effektiv men samtidigt säker transport på det internationella planet

För att uppnå målen har fyra huvudprinciper fastslagits, vilka är att;

- Samordna godsets elektroniska information.
- Fastslå gemensamma regler för hantering av risker och hot.
- Att importerande land kan, i samförstånd med exporterande land, kräva att en rimlig kontroll av gods görs i linje med det importerande landets krav och

[54] WCO SAFE Framework of Standards (June 2007)

- önskemål. Importerande land kan framföra krav på att högriskgods skannas (med ”non-intrusive” metoder) innan lastning i exporterande land.
- Tullmyndigheter ska erbjuda företag, vilka följer de grundläggande kraven gällande säkerhet och ”best practices”, fördelar som ökar drivkraften att uppfylla dessa.

Den elektroniska informationen ska lätt kunna utbytas tullmyndigheter emellan för att möjliggöra identifiering av högriskgods redan innan ankomst till gränskontroll. Aktörerna i logistikkedjan ska kunna krävas på information som är nödvändig för tullens riskbedömning. Om godset anses ha hög risk ska det exporterande landets tull kontrollera godset innan transporten påbörjas (exempelvis lastning på fartyg).

Tullmyndigheterna ansvarar för att information relaterad till godset och transporten skyddas. Likaså anses alla aktörer i logistikkedjan gemensamt ansvara för den totala säkerheten som framförallt innefattar ett förhindrande av manipulering, stöld och skadegörelse.

149 av 171 WCO medlemmar har (fram till juni 2007) godkänt en avsiktsförklaring i att införa SAFE ramverket varav både USA och EU antagit dess principer[55]

[55] WCO SAFE Framework of Standards, Fifth special meeting of the counter-terrorism committee 2007-10-29, Michael Schmitz

FAS 3 – Beskrivning och utvärdering av utvalda säkerhetsinitiativ

9 Avgränsning för djupare analys av säkerhetsinitiativ

Efter terrorattentaten i USA 9/11 2001 exploderade antalet säkerhetsinitiativ med mål att förbättra säkerheten i den globala logistikkedjan. I Fas 2 i forskningsprojektet Protected återfinns en översikt av 26 st olika säkerhetsinitiativ. I detta kapitel görs ett urval av dessa säkerhetsinitiativ genom att använda olika typer av avgränsningar.

Målet för urvalet har varit att säkerhetsinitiativen i första hand ska beröra kombitransporter inom EU, då det är ett övergripande mål för V-FUD SirC.



Bild 3.1 – Olika säkerhetsinitiativ som kan påverka en transport

9.1 Olika typer av avgränsningar

För att göra ett urval bland de olika säkerhetsinitiativen som vidare ska detaljstuderas behövs det någon form av avgränsning. Tanken är att finna ett par säkerhetsinitiativ som tydligt påverkar en kombinerad transportkedja inom EU. Avgränsningar kan göras på en mängd olika kriterier; geografisk spridning, initiativtagare, inriktning, giltighet, vilka säkerhetshot som förebyggs, vilka delar av transportkedjan som påverkas. Efter en del diskuterande har fyra avgränsningar valts ut som bedömdes vara väsentliga:

- *Geografiska:* Säkerhetsinitiativet ska vara verksamt i Europa
- *Påverkan på transportkedjan:* Säkerhetsinitiativet ska påverka så många delar av transportkedjan som möjligt
- *Drivkraft:* Önskvärt är om säkerhetsinitiativet leder till någon form av förenkling eller effektivisering
- *Vilka säkerhetshot som förebyggs/bekämpas*: Säkerhetsinitiativet ska helst täcka de olika säkerhetshoten.

9.1.1 Geografiska

De internationella transporterna är visserligen av mer eller mindre global omfattning vilket gör att de flesta av säkerhetsinitiativen direkt eller indirekt påverkar kombitransporter inom EU. Men genom att ta reda på den geografiska omfattningen av olika säkerhetsinitiativ kan detta ge en fingervisningen vilka säkerhetsinitiativ som inte i första hand berör transporter inom EU.

Analys
Nedan finns en sammanställning av de olika initiativen och var de har sin geografiska omfattning.

Säkerhetsinitiativ	**Geografisk omfattning**
100 % scanning	USA: Globalt gods till USA
ADR	Europa: 45 länder främst i Europa men några nordafrikanska
AEO	EU
BASC	Latinamerika/Karibien
CSI	USA: Globalt gods till USA
C-TPAT	USA: Globalt gods till USA
Dutch Client System	Nederländerna
ESSTRT	Europa
FAST	USA, Kanada och Mexico
Frontline	Australien: Gods till och från Australien
Föranmälan EU	EU: Globalt gods till EU
Föranmälan USA	USA: Globalt gods till USA
IATA/DGR	Globalt
IMDG-kod	Globalt
ISO 28000:2007	Globalt
ISPS-kod	Globalt
PIP	Kanada: Import gods
RID	Europa: 44 länder främst i Europa men några nordafrikanska
SAFE Port Act	USA: Globalt gods till USA
SECCONDD	Globalt
Secure Exporte Scheme	Nya Zeeland: Globalt gods från Nya Zeeland
Secure Trade Partnership	Singapore: Globalt gods via Singapore
SFI	USA: Globalt gods till USA
StairSec	Sverige: Gods till och från Sverige
TAPA	Globalt
WCO-SAFE	Globalt

Tabell 3.1 – Geografisk omfattning av olika säkerhetsinitiativ

Av sammanställning framgår det att 7 stycken av initiativen verkar globalt, 5 st inom Europa och 14 st mellan två eller flera länder. Av de senare är det 7 av dessa som påverkar transportkedjor med gods till/från USA.

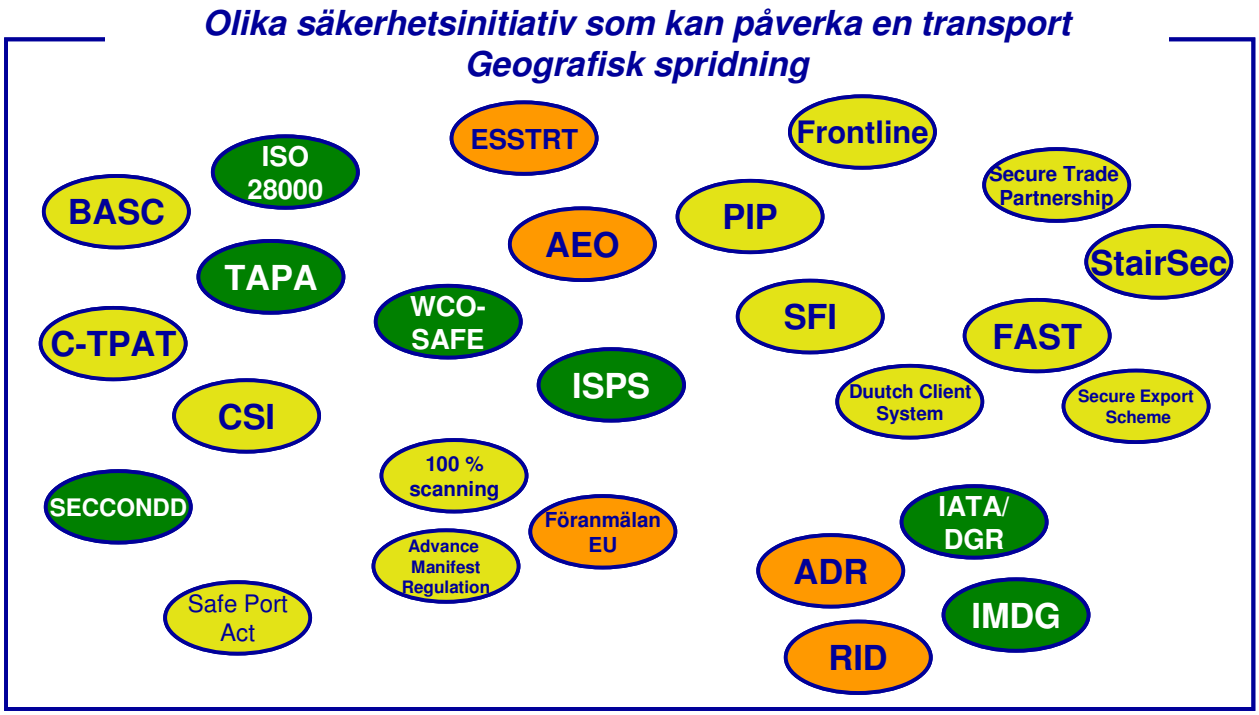


Bild 3.2 – Geografisk spridning av olika säkerhetsinitiativ

9.1.2 Påverkan på transportkedjan

En transportkedja kan innehålla ett antal olika länkar och nedan följer en kort beskrivning av de länkar som även har använts i projekts första fas.

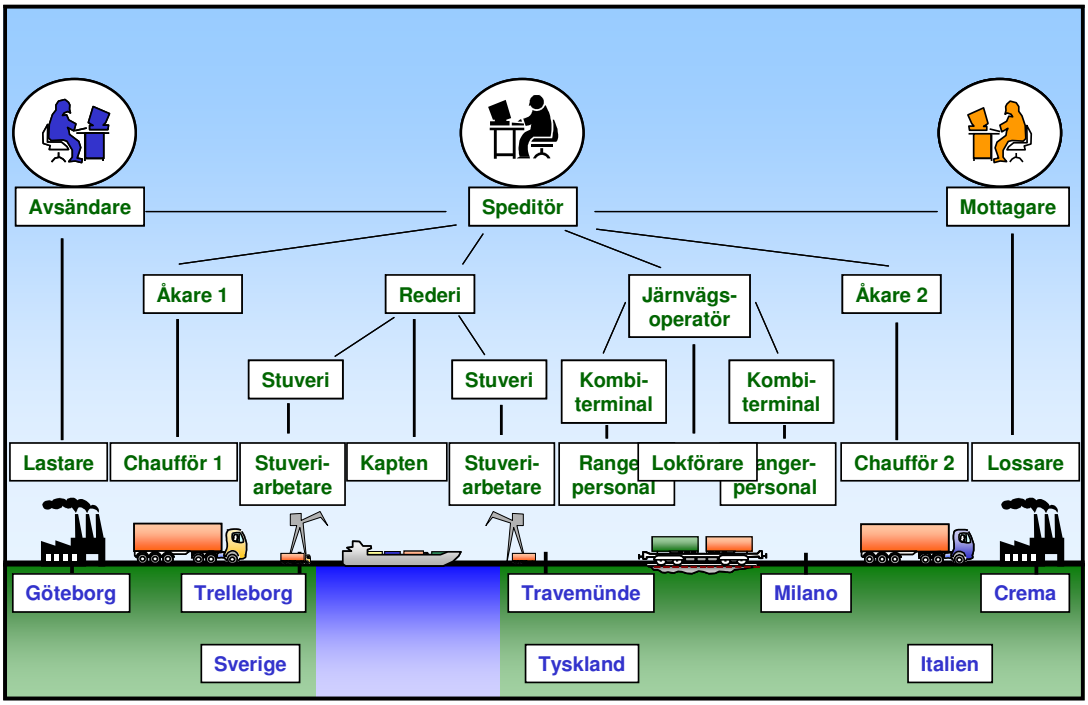


Bild 3.3 – Exempel på olika aktörer i en transportkedja

Avsändare: Med avsändare avses normalt den punkt där transportkedjan startar, t.ex. utlastningen på en industri eller en lagerpunkt. En avsändare är då den som lastar godset i den lastbäraren som sedan används i hela den intermodala transportkedjan.

Landsvägsterminal: Med en landsvägsterminal avses en terminal där godset troligtvis lastas om från en lastbärare till en annan. I vissa fall förekommer det mellanlagring av godset. Alla enheter som kommer till och från terminalen går med landsvägstransport. Ett exempel på en landsvägsterminal kan vara en DHL- eller Schenker terminal.

Kombiterminal: På en järnvägsterminal sker omlastning från väg till järnväg eller omvänt. Till skillnad från en kombiterminal sker även omlastning av godset mellan olika lastbärare t.ex. från järnvägsvagn till trailer, växelflak eller container. På en kombiterminal sker enbart en omlastning med en och samma lastbärare från väg till järnväg eller vice versa.

Hamnterminal: På en hamnterminal sker omlastning från landsväg eller järnväg till en sjötransport eller omvänt. Eftersom det framförallt är intermodala transportkedjor som analyserats är utgångspunkten att det inte sker någon omlastning av godset till någon annan lastbärare.

Landsvägstransport: Med landsvägstransport avses transport som sker med motordrivet fordon på väg utanför terminalområden. Eftersom det framförallt är intermodala transportkedjor som analyserats är lastbäraren sannolikt en trailer (påhängsvagn), växelflak eller container.

Kombitransport: Med kombitransport avses transport som sker på järnväg utanför terminalområden. Lastbäraren, vanligtvis en trailer (påhängsvagn), växelflak eller container, är lastad på en järnvägsvagn.

Järnvägtransport: Med järnvägstransport avses transport som sker på järnväg utanför terminalområden med gods som är lastat på järnvägsvagnar.

Sjötransport: Med sjötransport avses transport som sker med fartyg på öppet hav utanför hamnområden. Inre vattenvägar har inte varit föremål för några diskussioner i detta projekt.

Mottagare: Med mottagare avses den part som är slutdestinationen i transportkedjan.

Analys
En genomgång har gjorts av de 26 säkerhetsinitiativen som har bedömts efter hur mycket de påverkar olika delar av transportkedjan. Resultatet har sammanställts i tabellen på nästa sida. Graderingen i tabellen är

1 – stor påverkan på länken i transportkedjan
2 – viss påverkan på länken i transportkedjan
3 – liten påverkan på länken i transportkedjan
- – ingen på verkan alls på länken i transportkedjan

Av sammanställningen över vilken del av transportkedjan som ett initiativ påverkar framgår det att 11 stycken av initiativen framför allt påverkar sjötransporter och terminal, 4 stycken påverkat främst järnvägstransporter och endast ett säkerhetsinitiativ (RID) påverkar främst järnvägstransporter. Av de 26 initiativen är det 6 stycken som berör flera transportslag.

Säkerhetsinitiativ	**Avsändare**	**LV-term**	**LV-trp**	**Kombi-term**	**Kombi-trp**	**Jvg-trp**	**Hamn-term**	**Sjötransport**	**Mottagare**
		Landsvägs-transporter		Järnväg/Kombi-transporter			Sjö-transporter		
100 % scanning	3	-	-	-	-	-	1	2	-
ADR	1	1	1	2	2	-	2	2	2
AEO	1	1	1	1	1	1	1	1	2
BASC	1	1	2	1	2	2	1	2	2
CSI	2	-	-	-	-	-	1	2	-
C-TPAT	1	1	1	1	1	1	1	1	2
Dutch Client System	1	1	1	1	1	1	1	1	2
ESSTRT		-	-	-	-	-	-	-	-
FAST	-	1	1	-	-	-	-	-	2
Frontline	1	-	-	-	-	-	1	2	1
Föranmälan EU	1	1	1	1	1	1	1	1	-
Föranmälan USA	1	-	-	-	-	-	1	1	-
IATA/DGR	1	3	3	-	-	-	-	-	3
IMDG-kod	1	2	2	-	-	-	1	1	2
ISO 28000:2007	1	1	1	1	1	1	1	1	1
ISPS-kod	-	-	3	-	3	3	1	1	-
PIP	-	1	1	-	-	-	-	-	-
RID	1	-	2	1	1	1	-	-	1
SAFE Port Act	1	-	-	-	-	-	1	1	-
SECCONDD	-	-	-	-	-	-	-	-	-
Secure Exporte Scheme	1	2	2	2	2	2	1	1	3
Secure Trade Partnership	1	-	-	-	-	-	1	1	-
SFI	-	-	-	-	-	-	1	2	-
StairSec	1	2	1	2	1	1	1	2	2
TAPA	1	1	1	-	-	-	-	-	2
WCO-SAFE	1	1	1	1	1	1	1	1	2

Tabell 3.2 – I vilken omfattning olika säkerhetsinitiativ påverkar olika delar i transportkedjan

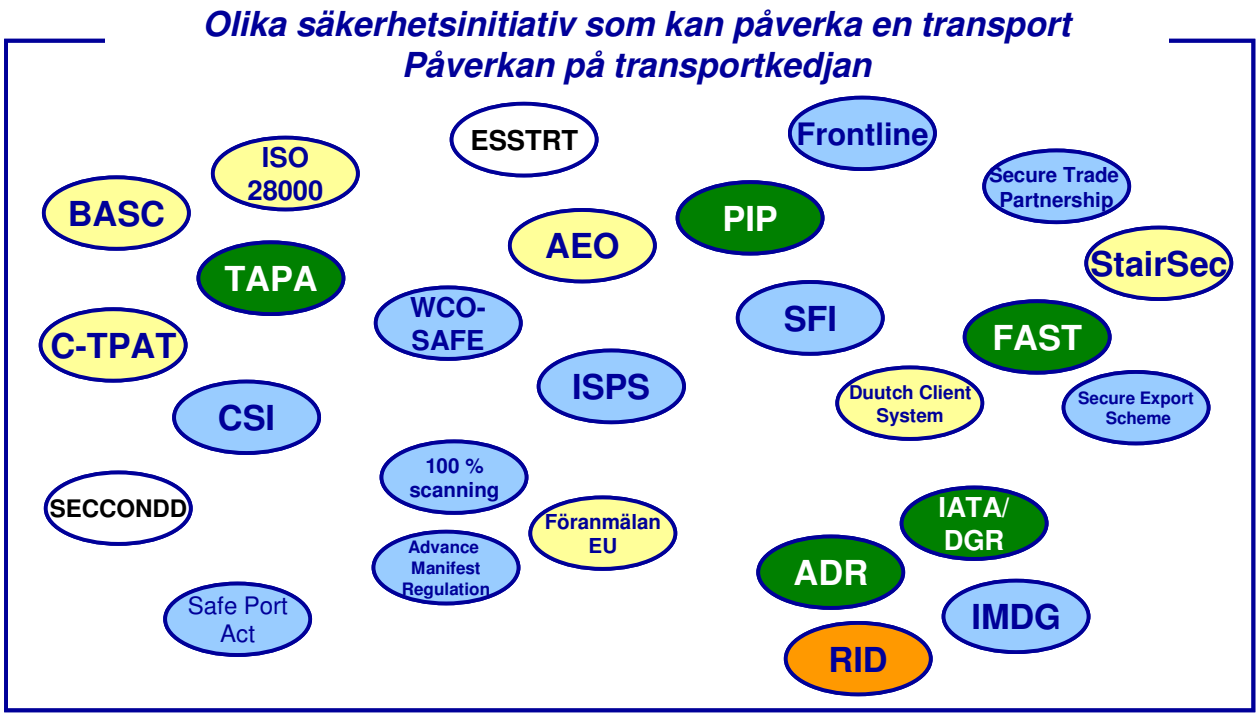


Bild 3.4 – Olika säkerhetsinitiativs påverkan på olika delar i transportkedja

9.1.3 Drivkraft

Det finns en mängd olika drivkrafter till att ta fram ett säkerhetsinitiativ. En analys av bakomliggande drivkrafter har gjorts av de 26 säkerhetsinitiativen. Drivkrafterna har delats in tre olika kategorier:

- Förenkling, effektivisering och standardisering
- Underlag till riskanalys
- Skydd och säkerhetskontroller

Förenkling, effektivisering och standardisering
Många av säkerhetsinitiativen har någon forma av förenkling, effektivisering och eller standardisering som sin tyngsta drivkraft. Vad som sedan menas med denna förenkling/effektivisering beror ofta på initiativtagaren. Tullmyndigheter vill effektivisera både det administrativa och fysiska tullhanteringen, politiska initiativ vill effektivisera landets säkerhet, privata initiativ vill förenkla handeln och transporter osv.

Underlag till riskanalys
Ett antal initiativ har drivkraften att skapa underlag till olika riskanalyser. Syftet är visserligen att effektivisera informationsflödet främst för tullmyndigheter för att utarbeta en strategi för vilka delmängder i det totala transportflödet som ska kontrolleras extra noggrant, men för transportkedjan i stort upplevs inte denna effektivisering snarare tvärtom.

Transportskydd och skyddskontroller
Ett antal säkerhetsinitiativ har drivkraften att på ett eller annat sätt öka transportskyddet med hjälp av olika typer av säkerhets- och eller skyddskontroller. Ett antal av initiativen har sitt ursprung i transport av farligt gods och har som syfte att förebygga tillbud och olyckor med farligt gods samt att rutiner finns om något ändå skulle hända.

Analys
I tabellen på nästa sida återfinns en sammanställning av de olika drivkrafterna bakom säkerhetsinitiativen. Där framgår det att 10 stycken av initiativen har drivkraften att förenkla effektivisera eller standardisera, 10 stycken har transportskydd eller säkerhetskontroller som främsta drivkraft medan det är 4 initiativ som har drivkraften att skapa underlag till riskanalyser.

Säkerhetsinitiativ	Förenkling, effektivisering och standardisering	Underlag till riskanalys	Transportskydd och skyddskontroller
100 % scanning			x
ADR			x
AEO	x		
BASC	x		
CSI			x
C-TPAT	x		
Dutch Client System		x	
ESSTRT			
FAST	x		
Frontline	x		
Föranmälan EU		x	
Föranmälan USA		x	
IATA/DGR			x
IMDG-kod			x
ISO 28000:2007	x		
ISPS-kod			x
PIP	x		
RID			x
SAFE Port Act		x	
SECCONDD			
Secure Exporte Scheme	x		
Secure Trade Partnership	x		
SFI			x
StairSec	x		
TAPA			x
WCO-SAFE	x		

Tabell 3.3 – Drivkrafter för olika säkerhetsinitiativ

Två av initiativen (ESSTRT och SECCOND) har inte kategoriserats då de inte är fullt utvecklade säkerhetsinitiativ utan istället är dels en studie (ESSTRT) respektive ett forskningsprojekt (SECCOND).

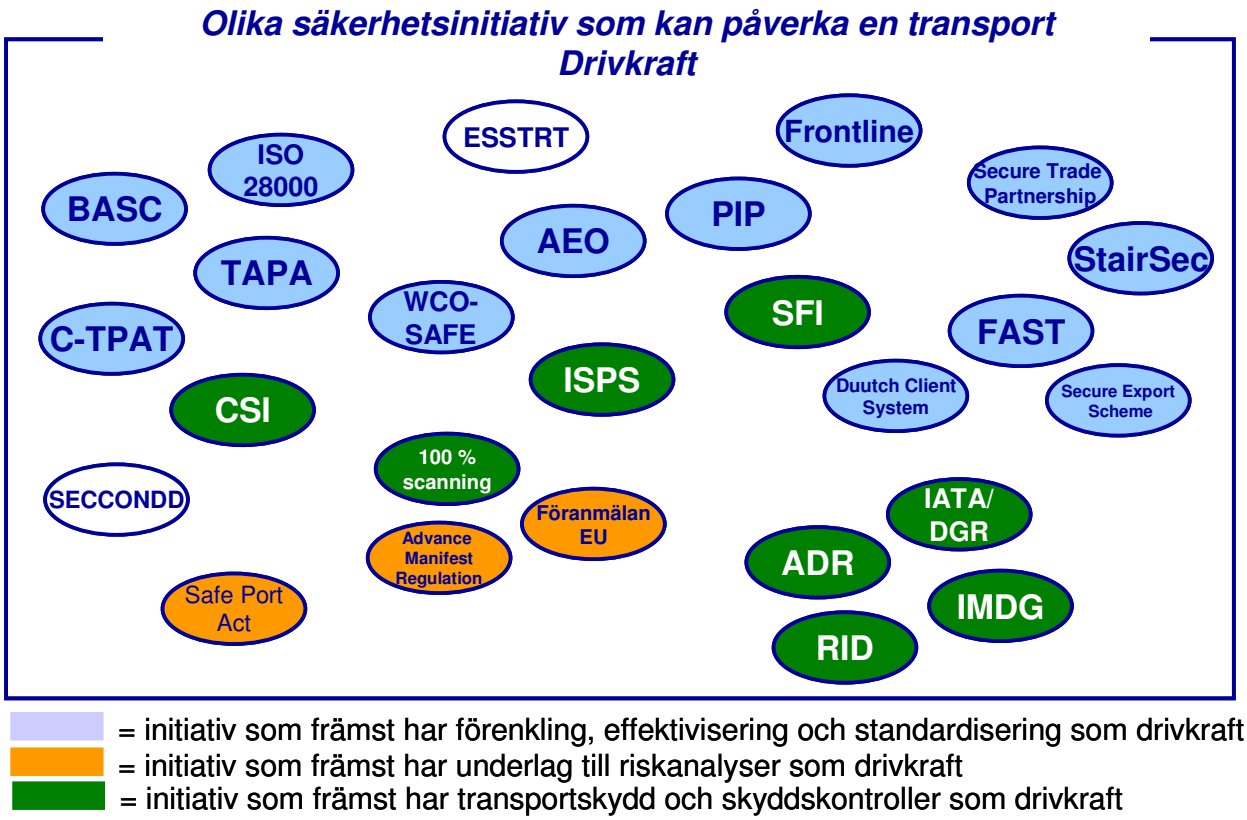


Bild 3.5 – Drivkrafter för olika säkerhetsinitiativ

9.1.4 Säkerhetshot som förebyggs/bekämpas

De olika säkerhetshoten är indelade i fem grupper på samma sätt som i projekts första fas:

- Terrorism
- Smuggling
- Trafficking
- Stöld
- Skadegörelse

Terrorism
Med säkerhetshotet terrorism avses det systematiska användandet av våld eller förstörelse, särskilt mot civila mål, för att med hjälp av rädsla tvinga fram politiska eller andra typer av förändringar.

Smuggling
Med smuggling i detta projekt avses införsel och utförsel av varor från eller till en stat, som sker i strid mot statens lagstiftning

Trafficking
Med trafficking i detta projekt avses införsel och utförsel av personer från eller till en stat, som sker i strid mot statens lagstiftning

Stöld
I projektet är stöld begränsat till stöld av gods och/eller lastbärare med eller utan transportmedel.

Skadegörelse
I projektet är skadegörelse begränsat till skadegörelse av gods, lastbärare, transportmedel och/eller aktuella terminaler.

Analys
En analys har gjorts vilka säkerhetshot som de 26 olika initiativen täcker. I denna analys kan ett säkerhetsinitiativ täcka ett eller flera säkerhetshot.

Resultatet blev att 22 av 26 initiativen helt eller delvis täcker terrorism, 14 stycken täcker smuggling, 6 stycken stöld, 5 stycken skadegörelse och 4 av säkerhetsinitiativen tar helt eller delvis upp trafficking.

Av de 26 initiativen är bedömningen att tre av dem mer eller mindre täcker samtliga fem säkerhetshot. Dessa initiativ är AEO, Frontline och WCO-SAFE.

Säkerhetsinitiativ	Terrorism	Smuggling	Trafficking	Stöld	Skade-görelse
100 % scanning	x				
ADR	x				
AEO	x	x	(x)	x	x
BASC		x			
CSI	x				
C-TPAT	x				
Dutch Client System	x	x			
ESSTRT	x				
FAST	x	x			
Frontline	x	x	x	x	x
Föranmälan EU	x	x			
Föranmälan USA	x	x			
IATA/DGR	x				
IMDG-kod	x				
ISO 28000:2007	x	x			
ISPS-kod	x				
PIP	x	x	x	x	
RID	x				
SAFE Port Act	(x)	x			
SECCONDD	x	x		x	
Secure Exporte Scheme		x			x
Secure Trade Partnership	x				
SFI	x				
StairSec		x			
TAPA				x	(x)
WCO-SAFE	x	x	x	x	x

Tabell 3.4 – Vilka säkerhetshot som olika säkerhetsinitiativ täcker

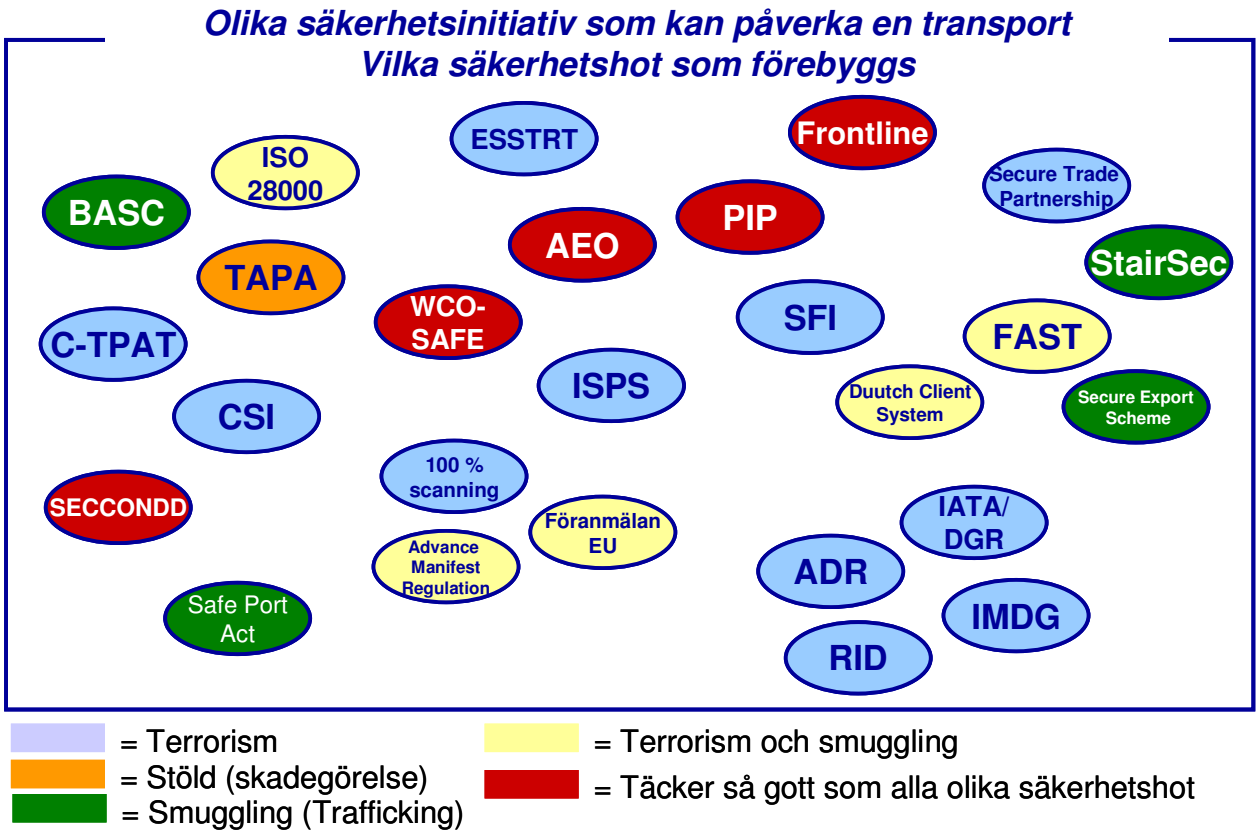


Bild 3.6 – Vilka säkerhetshot som olika säkerhetsinitiativ täcker

9.2 Val av säkerhetsinitiativ

I avsnitt 3.1 görs ett antal avgränsningar med målet att göra ett urval av säkerhetsinitiativen för att i första hand finna dem som berör kombitransporter inom EU, då det är ett övergripande mål för V-FUD SirC. I tabell 3.5 finns en sammanfattning av vilka avgränsningar som följer det övergripande målet som passar in på de olika säkerhetsinitiativen.

Säkerhetsinitiativ	Avgränsning				
	Geografisk	Påverkan på trpkedjan	Drivkraft	Inblandade säker-hetshot	Antal som täcker målen
100 % scanning					
ADR	X				1
AEO	X	X	X	X	4
BASC		X	X		2
CSI					
C-TPAT					
Dutch Client System		X	X		2
ESSTRT	X	(X)	X		2
FAST					
Frontline			X	X	2
Föranmälan EU	X	X	X		3
Föranmälan USA					
IATA/DGR	X				1
IMDG-kod	X				1
ISO 28000:2007	X	X	X	X	4
ISPS-kod	X				1
PIP			X		1
RID	X				1
SAFE Port Act					
SECCONDD	X	(X)		X	2
Secure Exporte Scheme			X		1
Secure Trade Partnership			X		1
SFI					
StairSec		X	X		2
TAPA	X				1
WCO-SAFE	X	X	X	X	4

Tabell 3.5 – Vilka säkerhetsinitiativ täcker bäst de övergripande målen

Förklaring till markeringar i tabell 3.5:

Geografisk	Initiativ som är minst verksamma inom Europa
Påverkan på transportkedjan	Initiativ som har stor eller viss påverkan på en kombitransportkedja
Drivkraft	Drivkraften är förenkling, effektivisering eller standardisering
Inblandade säkerhetshot	Minst 3 av de 5 säkerhetshoten täcks av initiativet

Sammanfattningen i tabell 3.5 visar att tre av säkerhetsinitiativen uppfyller samtliga 4 avgränsningar; AEO, ISO28000 och WCO-SAFE. Av dessa har framför allt AEO och WCO-SAFE nära kopplingar till varandra. Eftersom AEO är ett initiativ från Europaparlamentet (och tullmyndigheterna inom EU) plockas WCO-SAFE bort inför en närmare granskning. Detta ger följande urval i första hand:

AEO Med Europaparlamentet som initiativtagare och med en drivkraft att effektivisera och ge en snabb återhämtning vid incidenter samt generellt öka säkerheten i hela logistikkedjan täcker AEO samtliga avgränsningar inom detta projekt.

ISO28000 En globalt spridd standard som arbetar med de flesta säkerhetsfrågorna inom logistikkedjan och även inom avgränsningarna för detta projekt.

För att få referenser och möjlighet till jämförelser till andra initiativ väljs dessutom ytterligare tre säkerhetsinitiativ ut:

C-TPAT C-TPAT är begränsat till framför allt gods som importeras till USA men tas med som en referens med tanke på att en hel del gods som transporteras i kombikedjor inom Europa förr eller senare ska exporteras till USA.

ISPS-koden Allt gods som transporteras på sjön påverkas av ISPS-koden. ISPS-koden är dessutom det första initiativet som kom i drift efter händelserna i New York den 11 september 2001.

TAPA TAPA är ett intressant initiativ eftersom det är företag, verksamma inom produktion och tranporter, som är initiativtagare och inte någon myndighet eller standardiseringsorganisation.

Dessa fem initiativ beskrivs närmare i nästa avsnitt.

Detta avsnitt avslutas med en kort sammanfattning i tabellform av de olika säkerhets-initiativens geografiska spridning, initiativtagare, inriktning, drivkrafter, säkerhetshot som påverkas samt vilka delar i transportkedjan som påverkas.

Säkerhetsinitiativ	Geografiskt område	Initiativtagare	Inriktning/ Drivkraft	Säkerhetshot som påverkas	Påverkan på tranportkedjan								
					Avs.	LV-term	LV-trp	Kombi-term	Kombi-trp	Jvg-trp	Hamn-term	Sjötrp	Mott.
100 % scanning	USA	USA:s kongress	Lagkrav på säkerhetskontroll	Förhindra terrorism	x						x	x	
ADR	Europa	Expertkommitté i FN:s regi	Transportskydd av farligt gods	Förhindra terrorism	x	x	x	x	x		x	x	x
AEO	EU	EU-parlamentet och tullmyndigheter	Certifiering av aktörer i transportkedjan	Generell förbättring av säkerhet i logistikkedjan	x	x	x	x	x	x	x	x	x
BASC	Latinamerika/ Karibien	Privata företag	Främja säkerhet i transporter	Att genom samarbete motverka främst smuggling	x	x	x	x	x	x	x	x	x
CSI	USA	U.S. Customs an Border Protection (CBP)	Säkerhetskontroll i utländsk hamn av gods efter riskanalys	Förhindra smuggling och terrorism	x						x	x	
C-TPAT	USA	U.S. Customs an Border Protection (CBP)	Genom förebyggande arbete öka säkerheten i transportkedjan	Förhindra terrorism	x	x	x	x	x	x	x	x	x
Dutch Client System	Nederländerna	Holländska tullen	Effektivisera tullarbete och fokusera på gods med hög risk	Förhindra smuggling och indirekt terrorism	x	x	x	x	x	x	x	x	x
ESSTRT	Europa	Europeiska kommissionen	Analysera terroristhot och ta fram lösningar	Förhindra terrorism (inom EU)									

Säkerhetsinitiativ	Geografiskt område	Initiativtagare	Inriktning/ Drivkraft	Säkerhetshot som påverkas	Påverkan på tranportkedjan								
					Avs.	LV-term	LV-trp	Kombi-term	Kombi-trp	Jvg-trp	Hamn-term	Sjötrp	Mott.
FAST	USA	USA, Kanada och Mexicos tullmyndigheter	Förenkla transport av gods mellan länderna	Förhindra smuggling och indirekt terrorism		x	x						x
Frontline	Australien	Australian Customs Service	Förenkla och effektivisera tullarbetet	Försvåra kriminell aktivitet såsom smuggling, trafficking och pengatvätt	x						x	x	x
Föranmälan EU	EU	Europeiska kommissionen	Informationskrav som ger underlag till riskanalyser	Försvåra kriminell aktivitet över EU:s yttre gränser	x	x	x	x	x	x	x	x	
Föranmälan USA	USA	USA:s kongress	Informationskrav som ger underlag till riskanalyser	Försvåra kriminell aktivitet och terrorism	x						x	x	
IATA/DGR	Globalt	IATA med FN:s rekommendationer som underlag	Transportskydd av farligt gods	Förhindra terrorism	x	x	x						x
IMDG-kod	Globalt	IMO med FN:s rekommendationer som underlag	Transportskydd av farligt gods	Förhindra terrorism	x	x	x				x	x	x
ISO 28000:2007	Globalt	Organisationer anslutna till ISO	Standardisering av säkerheten i transportkedjan	Skapa en standard för att bekämpa smuggling, piratkopiering och terrorism	x	x	x	x	x	x	x	x	x

Säkerhetsinitiativ	Geografiskt område	Initiativtagare	Inriktning/ Drivkraft	Säkerhetshot som påverkas	Påverkan på tranportkedjan								
					Avs.	LV-term	LV-trp	Kombi-term	Kombi-trp	Jvg-trp	Hamn-term	Sjötrp	Mott.
ISPS-kod	Globalt	International Maritme Organization IMO	Krav på kontroller och skyddsåtgärder	Förhindra terrorism			x	x	x	x	x	x	
PIP	Kanada	CBSA – Canada Border Services Agency	Effektivisera tullarbetet och höja säkerheten I logistikkedjan.	Förhindra organiserad brottslighet främst smuggling och indirekt terrorism		x	x						
RID	Europa	Expertkommitté i FN:s regi	Transportskydd av farligt gods	Förhindra terrorism	x		x	x	x	x			x
SAFE Port Act	USA	USA:s kongress	Grunden för många av USA säkerhetsinitiativ för att öka säkerheten i hamnar	Försvåra kriminell verksamhet främst smuggling och indirekt terrorism	x						x	x	
SECCONDD	Globalt	Thales Research and Technology (UK) Ltd, Selex Communications S.p.A, Cotecna Inspection Ltd, HM revenue and Customs och CEN	Forskning för att ta fram "säkra" containers	Förhindra stöld, smuggling terrorism									

Säkerhetsinitiativ	Geografiskt område	Initiativtagare	Inriktning/ Drivkraft	Säkerhetshot som påverkas	Påverkan på tranportkedjan								
					Avs.	LV-term	LV-trp	Kombi-term	Kombi-trp	Jvg-trp	Hamn-term	Sjötrp	Mott.
Secure Exporte Scheme	Nya Zeeland	New Zealand Customs Service	Förbättra säkerheten i logistikkedjan	Förhindra smuggling och indirekt sabotage och terrorism	x	x	x	x	x	x	x	x	x
Secure Trade Partnership	Singapore	Singapore Customs	Förbättra säkerheten i logistikkedjan	Förhindra terrorism	x						x	x	
SFI	USA	U.S. Customs and Border Protection (CBP)	Lagkrav på säkerhetskontroll	Förhindra terrorism							x	x	
StairSec	Sverige	Svenska Tullverket	Effektivisera tullarbetet och höja säkerheten I logistikkedjan	Förenkling och kvalitetssäkring av tullhantering för att hindra smuggling	x	x	x	x	x	x	x	x	x
TAPA	Globalt	Privata företag	Standardisering och informations-spridning	Förhindra stöld	x	x	x						x
WCO-SAFE	Globalt	World Customs Organization (WCO)	Att öka säkerheten och förenkla för den internationella handeln	Underlätta handel mellan länder men samtidigt öka säkerheten i transportkedjan	x						x	x	x

9.3 **Tabell 3.6 – Sammanfattning av olika säkerhetsinitiativ**

10 Beskrivning av utvalda säkerhetsinitiativ

I tillägg till den översiktliga förklaringen som presenterats för flertalet betydelsefulla säkerhetsinitiativ kommer detta kapitel gå in lite på djupet för valda initiativ.

Slutligen i denna Fas 3 kommer en jämförelse göras mellan säkerhetsinitiativen för att belysa likheter, skillnader och eventuella motsägelser.

10.1 AEO, Authorized Economical Operators

10.1.1 Inledning

AEO utgör en del i CSP, Customs Security Programme, som är en beteckning för de åtgärder kommissionen föreslog till Europaparlamentet i slutet av 2003. Den andra delen är initiativet ”föranmälan EU”.

Även om Europaparlamentet antog reglerna om AEO är det i praktiken tullmyndigheterna inom den europeiska gemenskapen som praktiskt implementerar initiativet. En viktig del i att införa AEO är att harmonisera sättet på vilket tullmyndigheterna i olika länder certifierar företag som ansöker om AEO-status.

10.1.2 Harmonisering

Målet är att genom certifiering av aktörer förbättra säkerheten i leveranskedjan. I utvecklingen av AEO har det varit ett grundläggande önskemål att, i den mån det varit möjligt, harmonisera ramverket med WCO SAFE, ISO 28000 samt andra redan existerande säkerhetsstandarder för sjö- och flygtransporter.

Samstämmigheten med WCO SAFE har ansetts ytterst viktig då WCO som organisation står bakom 99 procent av den globala handeln. Det innebär att de regler och rekommendationer, vilka beslutas om i WCO, blir bestämmande för i princip alla kommersiella internationella transporter. Utan den hade en aktörs AEO-status inte blivit lika slagkraftig i det internationella världshandelssystemet.

10.1.3 Transportslag

De flesta säkerhetsinitiativ fokuserar på ett transportslag i hela logistikkedjan som många gånger består av både väg-, kombi- och sjötransport. Som exempel ligger fokus för de amerikanska initiativen såsom C-TPAT, CSI, SFI mfl. på containertrafik till sjöss gällande import till USA.

AEO är mer generellt utformat och syftar till en förbättrad säkerhet i hela logistikkedjan, på det globala planet, både import och export. Det medför också att riktlinjerna måste vara anpassningsbara för att passa alla transportslag.

10.1.4 Certifiering

Alla aktörer inom den europeiska unionen kan erhålla AEO-status och därmed ha rätt till vissa förmåner i tullförfarandet om vissa krav uppfylls. AEO kriterierna är enligt AEO guidelines:

- *an appropriate record of compliance with customs requirements*

- *a satisfactory system of managing commercial and, where appropriate, transport records, which allows appropriate customs controls*
- *proven financial solvency and*
- *where applicable, appropriate security and security standards*

I AEO Guidelines[56] finns en omfattande enkät för att hjälpa den certifierande aktören (företaget som tillhandahåller expertis i certifieringsprocessen), tullmyndigheten, och det ansökande företaget som önskar erhålla AEO-status att bedöma om kriterierna uppfyllts.

Det ansökande företaget behöver bara ge svar på de områden som är relevanta i dess situation och ej heller ge information tullmyndigheten redan känner.

Enkäten/frågeformuläret är uppdelad i sektioner och undersektioner. Sektionerna är:

- *Company's information*
- *Compliance record*
- *The applicants accounting and logistical system*
- *Financial solvency*
- *Safety and security requirements*

Det bör noteras att alla kriterier inte behöver uppfyllas för alla aktörer i logistikkedjan utan kraven skiljer mellan tillverkare, exportör, fraktförmedlare, lagerföretag, tullagent, åkeri, importör. Det ser ut som följer:

4.01.	**Indicator**	**Risk description**	**Points for attention**	**References to international standards**
	Beteckning av bedömt område	Vad är risken om kriteriet inte uppfylls	Områden och frågor som bör belysas och besvaras	Om det finns någon referens till en annan standard anges denna

Följande kommer ges några utvalda exempel från varje sektion som ger en bild av säkerhetsinitiativet AEO.

10.1.4.1 Company's information

Sektionen med företagsinformation behandlar:

- Grundläggande företagsinformation såsom omsättning, lagerkapacitet, inköp av material från utlandet, försäljning till utlandet m.m.
- Statistik för tullärenden såsom ursprungsland för importerat gods m.m.

Exempel grundläggande företagsinformation:

[56] Authorised Economic Operators – Guidelines, European Commision Customs Policy TAXUD/2006/1450

1.01.	Indicator	Risk description	Points for attention	References to international standards
5.	Goods received in customs or fiscal warehouse		Provide an estimate of the volume of the goods received in customs or fiscal warehouse expected in the next 2 years.	

10.1.4.2 Compliance record

Denna sektion behandlar hur väl aktören har följt gällande tullbestämmelser och dess relation till myndigheten.

Det ansökande företag, dess ledning, den ansvarige för tullärenden och den juridiska representanten i tullhanteringen får inte ha begått en allvarlig överträdelse av gällande bestämmelser inom en tre års period. Undantag kan göras om överträdelsen inte är relevant i sett till antal hanterade ärenden.

Exempel på samarbete med tullmyndighet:

2.01.	Indicator	Risk description	Points for attention
4.	Customs compliance	Inadequate awareness of breaches against customs rules	Has the applicant established procedures on disclosing irregularities to the relevant governmental agencies? Describe the routines for handling over information to Customs where criminal activity is suspected?

10.1.4.3 The applicants accounting and logistical system

Några exempel ges nedan för vilka kriterier som finns inom sektionen.

Ett fullvärdigt system ska finnas för att hantera bokföring av handelstransaktioner och transportdokumentation.

Exempel på granskningsmöjlighet:

3.01.	Indicator	Risk description	Points for attention	References to inter-national standards
1.	Level of access for competent authorities	- Inability to readily undertake an audit due to the way in which the applicant's accounting system is structured - Lack of the control over the system's security and access	- Customs authorities shall have access to applicant's records for control purposes including summary decleration as required. - Are an audit trail for fiscal and/or customs purposes available?	ISO 9001:2001, section 6.3

Aktörens organisation ska vara anpassad för att administrativt korrekt hantera mängden gods och ha interna kontrollsystem som upptäcker illegala och/eller avvikande transaktioner.

Därutöver ska verksamhetens anställda vara införstådda med att misstänkta händelser ska rapporteras in till tullmyndigheten. Det kan vara underlig godsdokumentation, onormala förfrågningar från extern part om sändelser, förstörda eller angripna sigill m.m.

Elektronisk information ska skyddas väl:

3.07.	Indicator	Risk description	Points for attention	References to inter-national standards
1.	Certification standards for securing computerised enviroment	Unauthorized access and/or introsion to the economic operator's computer systems	Are any existing certification standards applied for securing computer system?	ISO 17799:2005 ISO 27001:2005

10.1.4.4 Financial solvency

Erhållande av AEO-status kräver att aktören har god finansiell stabilitet med huvudsyftet att garantera betalning av tullavgifter. Den certifierande parten, tullmyndigheten, kan på egen hand analysera aktörens balansräkning och finansiella transaktioner alternativt kan företaget själv tillhandahålla uppgifterna.

Kraven gör bland anat gällande att aktören inte har varit sen med betalningarna de senaste tre åren. Exempel från AEO Guidelines:

4.01.	Indicator	Risk description	Points for attention
1.	Insolvency	Non-compliant behaviour	Check and analyse the balance and financial movements of the applicant to analyse the applicant's ability to pay their legal debts. In most cases the banking relation of the applicant will be able to report on the financial solvency of the applicant.

10.1.4.5 Safety and security requirements

Sektionen beskriver de säkerhetskrav som måste uppfyllas av en aktör som söker AEO-status. Det innefattar både administrativa rutiner och fysisk säkerhet. Med en god fysisk säkerhetsnivå garanteras en hög säkerhet för hela logistikkedjan även om bra rutiner på det administrativa planet ytterligare kan förstärka säkerheten men framförallt identifiera och upptäcka misstag som gjorts.

Aktören ska i sin policy visa en hög medvetenheten om säkerhetsåtgärder internt i företaget och i affärer med kunder, leverantörer med flera.

Exempel ges från varje delsektion i ”Safety and security requirements”. Noteras bör att kriterierna är mycket omfattande och finns att inhämta i sin helhet i refererad AEO Guidelines[57].

Första delsektionen *Security assessment conducted by the economic operator* består av påståenden och frågor som ska hjälpa aktören som söker AEO-status att identifiera den egna verksamhetens risker och hot. En självbedömning av verksamheten är inte ett krav i AEO certifieringsprocessen men är det i exempelvis enligt ISPS-koden.

Exempel på utvärderingsfrågor:

5.01.	**Indicator**	**Risk description**	**Points for attention**	**References to inter-national standards**
1.	Self assessment	Inadequate safety and security awareness	What kind of safety and security risks or dangers have you identified	ISO 28001:2006, section A.4.2 ISPS Code
3.	Internal control procedures	Inadequate control within the applicant over safety and security issues	Are there any existing documented security routines and how are they communicated to the personnel and other people visiting the company?	ISO 28001:2006, section A.3.3, A.4.2 ISPS Code

Andra delsektionen *Entry and access to premises* behandlar krav på tillgång till verksamhetens område. Generellt ska byggnadens skalskydd vara utformad på ett sådant sätt att ett rimligt motstånd ges mot intrång. Kontroll av vilka personer som har tillgång till området ska ske.

5.02.	**Indicator**	**Risk description**	**Points for attention**	**References to inter-national standards**
2.	Standard operating procedures in case of intrusion	No proper action if intrusion has been discovered	The applicant should have established procedures to respond when an unauthorized intruder has been discovered on the premises.	ISO 28001:2006, section A.3.3 ISPS Code

Physical security består av kriterier gällande ”fysiska” säkerhetsåtgärder. Det är krav på övervakning av portar, belysning, hantering av nycklar etc.

Krav finns på att verksamhetens perimeterområdet regelbundet kontrolleras så att säkerhetsskyddet är intakt.

[57] Authorised Economic Operators – Guidelines, European Commision Customs Policy TAXUD/2006/1450

5.03.	Indicator	Risk description	Points for attention	References to international standards
2.	Gates and gateways	Existance of gates or gateways which are not monitored	Identify all gates or gateways at the premises. When gates or gateways are not locked they should be manned or guarded with alternative access monitoring or control measures	ISO 28001:2006, section A.3.3 ISPS Code

En mycket viktig del i att förbättra den globala transportkedjans säkerhet är att förhindra och garantera godsenheters intakthet. Påverkan på dessa behöver inte alltid inträffa under transportens gång utan enheten kan manipuleras redan innan den lämnar avsändarens område.

Delsektion 4 *Cargo Units* behandlar detta med fokus på säkerställande av godsenheters intakthet. Krav på bland annat att:

- Åtkomst till gods ska kontrolleras med mål att förhindra obehörigas tillgång till godsenheter
- Gods ska övervakas alternativt hållas inlåst
- Godkända ISO-sigill ska användas
- När tillämpbart ska inspektion göras av enhet
- Att en handlingsplan finns när manipulation av gods upptäcks se exempel från AEO Guidelines nedan:

5.04.	Indicator	Risk description	Points for attention	References to international standards
5.	Standard operating procedures in case of intrusion and/or tampering with cargo units	No proper action if unauthorized access or tampering has been discovered	The applicant should have appropriate procedures laid down on what measures should be taken when an unauthorized access or tampering is discovered	ISO 28001:2006, section A.3.3

Enligt delsektion 5 *Logistical processes* ska den typ av transport den AEO-status ansökande aktören använder identifieras. För utgående gods bör undersökas om det anlitade transportbolaget/åkeriet är kontrollerat med avseende på de säkerhetsrutiner som används och om de är certifierade enligt någon erkänd standard.

Om den ansökande aktören inte alltid är slutmottagare för allt gods är det viktigt att rutiner finns för inkommande gods enligt undersektion *Incoming goods*. Säkerheten kan inte garanteras även om leveransen kommer från en känd aktör. Gods kan ha manipulerats under transport.

Exempel är åverkan på sigill:

5.07.	Indicator	Risk description	Points for attention	References to international standards
5.	Sealing of incoming goods	Lack of control of reception of goods which is not registered in a logistical system which might pose a safety or security risk	At reception of the goods, the integrity of seals should be checked. Where relevant the applicant should have routines to seal incoming goods	ISO 28000:2006, section A.3.3 ISO 17712

Rutiner ska finnas för hur gods mottages speciellt det gods som inte redan är registrerat i logistiksystemet enligt AEO Guidelines nedan:

5.07.	Indicator	Risk description	Points for attention	References to international standards
1.	Routines for checking incoming transport	Lack of control of reception of goods which is not registered in a logistical system which might pose a safety or security risk	Where appropriate the applicant should establish routines: - Appointing staff responsible of receiving the driver and goods at arrival - Comparing the goods with the accompanying transport documents and customs papers	ISO 9001:2001, section 6.2.2 ISO 28001:2006, section A.3.3

Ytterligare exempel på krav under *Incoming goods*:

- Rutiner ska finnas för verifiering av att eventuella överenskommelser om säkerhetsarrangemang med utländska samarbetspartners och leverantörer följs. Personalen ska vara informerad om dessa.
- Gods ska bara kunna levereras till godsmottagningen.
- Gods ska lagras och förvaras på område avsett för detta.

Delsektion 8 *Storage of goods* behandlar mer i detalj hur gods ska förvaras. Exemplet nedan från AEO Guidelines är det enda kriteriet som refererar till TAPA:s standard. Standarden är främst inriktad på säkerhet i hög-värdes transportkedjor och enligt AEO kriteriet ska inte olika typer av gods blandas.

Annars rör kriterierna mest kontroll av tillgång till gods. Gods ska förvaras på korrekt plats och åtkomst till område ska regleras.

5.08.	Indicator	Risk description	Points for attention	References to inter-national standards
3.	Separated storage of different goods	Un-authorized substitution of goods and/or tampering with goods	Where appropriate different types of goods should be seperated, e.g. foreign, domestic, high-value goods, hazardous goods etc (see also 5.06.1). The location of storage should be registered in the logistical administration, as soon as the goods are arrived in the storage location.	TAPA

För aktörer i logistikkedjan som har verksamhet inom produktion finns kriterier som reglerar hur godset/produkten ska skyddas i produktionsledet. Riskerna är framförallt manipulering av produkt för att användas i smugglingssammanhang. Nivån på säkerhetsrisken är delvis beroende på vilken produkt som tillverkas men desto viktigare är hur den färdiga produkten packas.

AEO-riktlinjerna gör därför gällande bland annat att tillträde till produktionsutrymmena ska kontrolleras. Om delar av produktionen sker hos underleverantör måste även denna vidta lämpliga säkerhetsåtgärder.

Efter packning av produkt försämras ofta kontrollmöjligheterna för godsets innehåll avsevärt. Det är därför av yttersta vikt att, om packningen utförs av en extern part, denna har säkerhetsåtgärder i bruk i nivå med den AEO certifierade aktören. Ansvaret för att se till att de uppfylls ligger hos beställaren. Ett exempel på kriterie som är unikt för AEO:

5.09.	Indicator	Risk description	Points for attention	References to inter-national standards
6.	Quality inspection	Incomplete control over the flow of goods	If a quality inspection exists for the goods, which can be an additional element to ensure the security integrity of the goods.	

Ett av de absolut viktigaste områdena när det gäller säkerheten i den totala logistikkedjan är rutinerna vid lastning. Det gäller framförallt aktörer som hanterar stora mängder gods från olika mottagare det vill säga logistik-, combi- och hamnterminaler.

AEO-fokuserar på alla delar i logistikkedjan till skillnad från de flesta andra säkerhetsinitiativen globalt sätt som nästan uteslutande är inriktade på en ökad säkerhet för sjötransporter där hamnterminalerna är en mycket viktig del.

Kriterierna för lastning finns i delsektion 10 *Loading of goods*.

Om last/gods lämnas oövervakat ökar risken för sabotage och manipulering av gods och/eller godsenheter. Det regleras i följande exempel från riktlinjerna:

5.10.	Indicator	Risk description	Points for attention	References to international standards
3.	Supervision over loading of goods	Lack of supervision of loading of goods	Personnel should be assigned to supervise the loading of goods. It should be avoided that outgoing goods could be loaded or left behind in unsupervised. The applicant should identify procedures avoiding	

Andra krav gällande rutiner för lastning är:

- Personal ska regelbundet hållas informerade om vilka säkerhetsåtgärder som finns och vad som krävs för att möta dessa.
- Rutiner ska finnas för hur utgående gods förseglas och hur detta kontrolleras i processerna.
- Klara processvägar ska vara införda för att hantera upptäckter av avvikande gods (som skiljer sig från vanligtvis hanterat gods och/eller väcker misstänksamhet).

Delsektion 11 *Security requirements business partners* behandlar vilka åtgärder den sökande aktören ska ha vidtagit gällande dennas affärspartners. I CCIP (Customs Code Implementing Provisions) artikel 14k (1) (e) står:

The area shall be considered to be appropriate if the applicant has implementet measures allowing a clear identification of his business partners in order to secure the international supply chain.

Vidare konstateras att en aktör bara är ansvarig för sin del av logistikkedjan. Det innebär följaktligen att lättnader i tullhantering etc. enligt AEO endast gäller aktören med AEO-status.

Avgörande för säkerheten i ett företag är de som utför jobben och därmed arbetar med införda rutiner och processer i den kontinuerliga verksamheten. Det är därför av största vikt att de anställda som individer inte utgör en säkerhetsrisk. Innan anställning ska en bakgrundskoll göras i den mån de nationella lagarna tillåter. Tillfälligt anställda och inhyrd personal utgör idag en väsentlig del av arbetskraften i företag, speciellt inom många av de näringar där transportkedjorna är som mest utsatta (lagerterminaler osv.). Enligt AEO Guidelines:

5.12.	Indicator	Risk description	Points for attention	References to international standards
4.	Safety and security requirements for temporary personnel	Infiltration of staff that could compose a security risk	The applicant should have security requirements in place regarding the use of temporary personnel	ISO 28001:2006, section A.3.3

Sista delsektionen *External services* under sektion *Safety and security requirements* fortsätter på linjen med insider-/infiltrationsrisker:

5.13.	Indicator	Risk description	Points for attention	References to international standards
1.	External services	Infiltration of staff that could compose a security risk	In case that services are outsourced, i.e.; transportation, security guards, cleaning, maintenance; security demands should be incorporated in the contractual arrangements made with the external companies.	ISO 28001:2006, section A.3.3

10.1.4.6 Typ av certifiering

Certifiering enligt AEO (Authorised Economic Operators) kan erhållas enligt:

- *Customs Simplifications* – krävs i princip uppfyllande av kriterierna som specifierar den administrativa hanteringen av tullprocesserna samt att aktören följt gällande tullbestämmelser. Sektionerna är *compliance record, the applicants accounting and logistical system* och *financial solvency*.

- *Security and Safety* – kriterierna enligt sektion *safety and security requirements* och alla delsektioner ska vara uppfyllda. Dessa rör främst krav för att säkerställa godsets korrekthet dvs. att ingen manipulering skett m.m.

- *Customs Simplifications / Security and Safety* – alla kriterier ska uppfyllas

10.1.4.7 Kriterier för olika aktörer

Alla kriterier i respektive sektion i AEO-Guidelines är inte tillämpbara för de olika aktörerna i en logistikkedja. Uppdelningen är logisk så till vida att exempelvis en exportör till sin definition inte har någon tillverkning och därmed gäller inte kriterierna under delsektion *production of goods*. Liknande för övriga aktörer.

I riktlinjerna är aktörerna uppdelade enligt: Tillverkare, exportör, speditionsfirma, lagerföretag, tullagent, fraktföretag och importör.

Samma resonemang är tillämpbart för aktörer som driver flera delar i en logistikkedja. Exempelvis om en exportör även transporterar gods måste kriterierna i AEO-Guidelines uppfyllas för både ”exportören” och ”speditionsfirman”.

10.1.5 Förmåner

En aktör som uppfyller kraven för certifiering och erhåller AEO-status kommer bidra till den globala leveranskedjans säkerhet. Tullmyndigheterna kan omfördela resurser till att arbeta mer fokuserat med kontroller av hög-risk gods vilket försvårar smuggling och minskar risken för terroristattacker.

En AEO-status aktör bidrar till ett säkrare samhälle men att införa och följa respektive säkerhetskrav kan vara relativt omfattande och innebära investeringar i både rutiner och anläggningar.

Förmåner för AEO-aktör:

- Färre kontroller av gods och tullhandlingar
- Prioritering vid genomförande av kontroll
- Möjlighet att önska plats för kontroll
- Användande av förenklade summariska in- och utförseldeklarationer i samband med import och export.

10.2 TAPA

10.2.1 Inledning

TAPA, The Technology Asset Protection Association, är en sammanslutning av företag verksamma inom produktion och transport av högvärdigt gods. Föreningen grundades 1997 i Nord Amerika av Intel, Compaq, Sun mfl. och var inledningsvis främst riktad mot tillverkare i högteknologiska branscher som kände ett behov att motverka de ökande säkerhetsriskerna och då framförallt stöld.

Under senare delen av 90-talet exploderade utvecklingen av teknisk utrustning. I takt med teknikutvecklingen blev utrustningen allt attraktivare för den kriminella marknaden med radikalt ökade antal stölder som följd.

TAPA för samman tillverkande företag, transportfirmor, polisen och andra intressenter med mål att minska förlusterna i de internationella logistikkedjorna. Visionen är en global säkerhetsstandard.

10.2.2 Transportslag

Unikt för TAPA som säkerhetsinitiativ är inriktningen mot lastbilstransporter och att säkerhetshotet som främst ska förebyggas är stöld. Det beror på att det bakomliggande intresset är minskade ekonomiska förluster och inte primärt en förbättrad säkerhet i den globala transportkedjan.

10.2.3 Initiativ

TAPA står bakom säkerhetsinitiativen IIS, FSR och TSR där FSR är det mest globalt erkända.

10.2.3.1 Freight Security Requirements (FSR)

FSR reglerar vilka krav som ställs på de olika aktörerna i transportkedjan för säkra transporter och lagring både sett till inre och yttre säkerhet. Kraven i FSR är uppdelade efter klassning och är konkreta regler för hur säkerhetssystemen bör vara utformade i de olika delarna i transportkedjan. Exempel på några specifikationer för ”visuell” säkerhet är; CCTV övervakning över lastbryggor och passerkontroll för anställda och besökare.

Utöver den ”visuella” säkerheten finns krav för hur processerna ska hanteras gällande dokumenthantering avseende bland annat; rapportering av förlorat gods och att bara nödvändig information om hanterat gods ges till inblandade parter. FSR reglerar också personalens tillgång till ”känsligt” gods. Exempelvis bör allt tillträde till lokal där gods hanteras enligt FSR vara begränsat till enbart berörd personal.

10.2.3.2 Trucking Security Requirements (TSR)

TSR är en detaljerad kravspecifikation, baserad på FSR, som är ämnad för lastbilstransporter. Exempelvis finns instruktioner för hur lastbilar och last ska skyddas från stöld och inbrott med larm- och spårningsutrustning etc. Specificerat finns därutöver krav på: personalkontroll, rapportering om tillbud väl inträffar, hur parkering bör ske för minskad risk, att en handlingsplan finns m.m.

10.2.3.3 Incident Information Service (IIS)

Initiativet IIS är ett samarbete som bygger på informationsutbyte medlemmarna emellan samt myndigheter gällande kriminalitet inom området. Information om en incident samlas i en central kunskapsbas vilket underlättar undersökning och uppklarande av aktuellt brott men används också i förebyggande syfte med mål att minska riskerna.

Vetskapen om brott blir tillgänlig för medlemsföretag och en riskbedömning utgående från den egna verksamheten kan göras. Ytterligare en fördel med IIS är att informationen om en stöld snabbt blir känd i branschen vilket kan förbättra chanserna att hitta det stulna. Informationen i IIS hjälper medlemsföretag och myndigheter att göra statistiska riskbedömningar.

10.2.4 Ingående om Freight Security Requirements

Följande kommer en förklaring av FSR mer ingående med grundläggande principer och exempel på konkreta säkerhetsåtgärder.

10.2.4.1 Inledning

Målet med FSR, Freight Secure Requirements, är att skydda medlemmarnas tillgångar i den globala transportkedjan från främst stöld.

I direktiven för FSR specificeras den lägsta acceptabla säkerhetsnivån som ska vara uppfylld genom hela logistikkedjan. Som medlem i TAPA agerar du oftast som köpare när det gäller transporter och det är under de externa transporterna nästan uteslutande all stöld eller stöldförsök genomförs. Det är därför av största vikt att också alla underleverantörer av transporttjänster eller däri inblandade aktörer har en hög säkerhetsnivå. Enligt TAPA:s riktlinjer för FSR;[58]

The FSR outlines the process and specification for Suppliers to attain TAPA certification for their facilities and transit operations. It is the intention of TAPA members to select Suppliers that meet or exceed TAPA certification requirements.

Eftersom TAPA är ett initiativ som skapats och som drivs av privata aktörer är deras vision inte att förbättra den egna verksamhetens säkerhet utan deras samarbetspartners för att på så sätt öka säkerheten i ingående transporter från underleverantörer och i den utgående leveranskedjan till kunder. Det juridiska ansvaret för godset ligger hos leverantören av transporttjänster och dennas eventuella partners men det är av TAPA medlemmens högsta intresse att leveranser av in- och utgående gods går enligt plan. En stöld eller stöldförsök medför, förutom de ekonomiska aspekterna, försenade eller uteblivna leveranser något som kan drabba aktörernas relation till varandra och deras fortsatta samarbete.

10.2.4.2 Avtal med leverantör

FSR refereras till i varje avtal mellan TAPA medlemmen och dess leverantörer av transporttjänster med syftet att säkerställa att säkerhetsåtgärderna implementeras.

[58] TAPA, Freight Suppliers Minimum Security Requirements 2005

Kraven i FSR ska tillämpas globalt – i transporter till och från alla nationer och kontinenter.

Det är, som grundprincip, transportören själv som står för certifieringen och de resurser det kräver.

För en TAPA medlems anlitade transportaktör gäller bland annat att;

- Redovisa en handlingsplan vilken belyser de områden i verksamheten som inte uppfyller FSR och presentera hur det ska åtgärdas. Transportaktören har 60 dagar från kontraktsdatum med TAPA medlem för implementering.

- Alla transportaktörens anläggningar som ska hantera godset enligt kontraktet ska nå upp till säkerhetskraven inom 60 dagar.

- Transportköpare (TAPA ansluten) ska informeras om av transportaktören identifierade säkerhetsrisker även om dessa går utanför kriterierna i FSR riktlinjerna.

- Om något av kriterierna på grund av verksamhetens uppbyggnad inte kan uppfyllas eller om en motsvarande säkerhetsåtgärd används kan dispens erhållas från TAPA. En bedömning görs i varje fall av en oberoende granskningsaktör.

10.2.4.3 Säkerhetsorganisation

För att säkerställa avtalets efterlevnad med avseende på Freight Security Requirements ska transportaktören utse en ansvarig för FSR som håller kontakten med transportköparens representant. Transportaktörens ansvarige;

- Har ansvaret för att kraven i FSR efterlevs.

- Har relevant bakgrund och besitter kompetens inom området.

- Ska utse en representant / representanter med ansvar för varje geografiskt område där kontraktet tillämpas.

Transportaktören ska därutöver utse en ansvarig för att utreda eventuella förluster av den TAPA anslutna transportköparens gods. Kan vara samma person som den ansvarige för regelefterlevnaden.

10.2.4.4 Riskbedömning och granskning

Köparen (TAPA anslutna transportköparen) har rätt att genomföra riskbedömningar av transportaktörens lokaler som används för hantering och förvaring av köparens gods. Granskning får ske oplanerat med ett dygns förvarning.

Transportaktören är dessutom skyldig att själv granska den egna verksamheten med syftet att säkerställa efterlevnad av FSR kriterier.

Om köparen eller dess anlitade part för granskning upptäcker brister i hanteringen av gods enligt FSR kan denna utfärda en SCAR (Supplier Corrective Action

Requirement) som innehåller anmärkningar på säkerheten. Den granskade transportköparen måste besvara och åtgärda bristerna enligt SCAR.

10.2.4.5 Certifieringsprocess för lager- och lastbilsfaciliteter

Den av TAPA aktören anlitade transportaktörens faciliteter klassificeras i certifieringsprocessen till en av tre nivåer där A är den högsta säkerhetsnivån. Om transportaktören ska hantera ”TAPA gods” i lager inte tidigare använd för ändåmålet och därmed inte godkänd måste dessa certifieras / klassificeras.

Transportaktören i samarbete med den TAPA certifierade granskaren måste genomföra en klassningsbedömning över säkerhetskrav inom 30 dagar från det att kontrakt om transporttjänster skrivits.

Utgångspunkt för granskningen är TAPA:s granskningsformulär. Kraven för respektive område är uppdelade i nämnda tre säkerhetsnivåer. Vissa kriterier är absoluta krav för att uppfylla en viss säkerhetsnivå (se **M** i exempel nedan) medan övriga kriterier (se **R** i exempel nedan) används för en helhetsbedömning där en slutlig poäng beräknas för den totala säkerhetsnivån.

10.2.5 Kriterier för certifiering enligt TAPA

Kriterierna är utarbetade av experter inom företagssäkerhet och logistik och är baserad på verkliga tillbud inom transportbranschen.

Följande kommer presenteras, exempel från FSR specifikationerna både för säkerhet i den ”fasta” verksamheten *Supplier Facility Requirements* och transportsäkerhet *Truck Freight Security Requirements*.

10.2.5.1 Supplier Facility Requirements

Transportaktörens faciliteter för hantering och förvaring av transportköparens gods ska ha en god generell säkerhetsnivå med bra perimetersäkerhet (exempelvis stängsel), alarmsystem, kameraövervakning. Verksamheten ska inte vara placerad i område med erkänt hög brottslighet.

Perimeter Security listar kriterier för kameraövervakning, belysning, alarmsystem, fönster, dörrar, portar m.m. Utvalda exempel nedan;

Security Requirements	**Applicable to Final Classification**		
R = Requirement **M** = Mandatory Requirement to pass	A	B	C
1.2. CCTV Systems			
1.2.1 CCTV external coverage of shipping and receiving yard, including entry / exit point, to cover movement of vehicles and people	**M**		
1.2.2 CCTV coverage of all external dock area	**M**	**M**	**M**
1.3. Lightning			
1.3.2 Dock doors illuminated externally at night	**R**	**R**	**R**

1.5. Perimeter windows, doors & other openings 1.5.1 Any windows or other openings in warehouse walls/roof must be secured by steel bars/mesh (or any other material that would harden opening to burglary)	**R**	**R**	

Access Control – Office Area listar kriterier för åtkomst till kontorsytor. Utvalda exempel nedan;

Security Requirements **R** = Requirement **M** = Mandatory Requirement to pass	**Applicable to Final Classification** A	B	C
2.1. Office Entrances			
2.1.1 Visitor office access points controlled	**R**		
2.1.2 All office access points controlled	**M**	**M**	
2.1.3 Access control processes both during and outside normal operating hours to ensure access is granted only for authorized supplier employees and visitors	**R**	**R**	**M**

Facility Dock/Warehouse listar kriterier för åtkomst till lagerytor bland annat gällande hur högvärdesgods ska förvaras, kameraövervakning m.m. Utvalda exempel nedan;

Security Requirements **R** = Requirement **M** = Mandatory Requirement to pass	**Applicable to Final Classification** A	B	C
3.3. High value storage area			
3.3.2 Restricted-access, caged/vault area for assets on site more than 6 hours: High-grade security mesh, chain-link, or hard-wall, including top/roof; CCTV, pad-locked		**M**	**R**
3.5. CCTV coverage			
3.5.1 Internal docks covered by CCTV	**M**	**M**	**M**

Security Systems listar krav på använda säkerhetssystem. Utvalda exempel nedan;

Security Requirements **R** = Requirement **M** = Mandatory Requirement to pass	**Applicable to Final Classification** A	B	C
4.2. Intruder alarm system			
4.2.1 Minimum of 60 days records on system alarms	**R**	**R**	
4.4. Card access system			
4.4.1 Minimum 60 days records on system transactions	**R**	**R**	
4.4.2 Restricted access to system functions	**R**	**R**	

4.5. Security system maintenance 4.5.1 Preventative maintenance plan in place to routinely test and service access control and alarm systems	**R**	**R**	**R**

Security Procedures listar krav på olika processer med koppling till hantering av TAPA medlemmens gods och andra säkerhetskrav av mer allmän karaktär. Utvalda exempel nedan;

Security Requirements	**Applicable to Final Classification**		
R = Requirement **M** = Mandatory Requirement to pass	A	B	C
5.1. Adequate documented security procedures 5.1.2 Process for timely reporting of incidents of lost or missing Buyer's assets. Incidents to be reported by the Supplier to the Buyer within 12 hours for missing assets	**R**	**R**	**R**
5.1.5 Security awareness training (including robbery resonse training) for all dock, warehouse, Security and reception employees			
5.1.15 Personal containers (defined as lunch box, backpacks, coolers, purses etc.) are controlled in the warehouse	**R**	**R**	
5.2. Background checks (vetting) within constraints of Local country laws 5.2.1 Criminal history checks in place encompassing 5-year criminal history and employment check (vetting within constraints of local county laws).	**M**	**M**	**M**
5.3. Terminated employees & contractors procedure 5.3.1 Termination procedures in place for employees and contractors, ensuring return of ID's, access cards, keys and other sensitive information	**R**	**R**	**R**

10.2.5.2 Truck Freight Security Requirements

Truck Freight Security Requirements behandlar de kriterier som berör fysisk transport av gods till och från anläggning. Det berör trailersäkerhet, spårbarhet vid stöld, förarträning för att hantera nödsituationer m.m.

Standard Truck Security Requirements listar främst krav på säkerhetssystem för transportbärare/lastbil. Utvalda exempel nedan;

Security Requirements	**Applicable to Final Classification**		
R = Requirement **M** = Mandatory Requirement to pass	A	B	C
6.1. Adequate cargo truck security devices installed 6.1.1 Solid-top, hard-sided, locked cargo doors or reinforced soft-sided trailer	**R**	**R**	**R**

6.1.2. Security tamper evident seals for trucks carrying Buyer only shipments	**R**	**R**	**R**
6.1.5 Written contingency plans in place for reporting unscheduled events (i.e. stops, delays, route deviation)	**R**	**R**	**R**
6.3. Loading/unloading			
6.3.1. Proof of shipping and receiving records	**R**	**R**	**R**

Enhanced Security Requirements listar tuffa säkerhetskrav som gäller främst för det högsta certifieringssteget. Utvalda exempel nedan;

Security Requirements	**Applicable to Final Classification**		
R = Requirement **M** = Mandatory Requirement to pass	A	B	C
8.1. Driver training			
8.1.1 Supplier to provide robbery response training, detailing safe and secure actions to be taken during the event driver is threatened. Details of training are to be available to Buyer	**R**	**R**	
8.1.2 Security Awareness training provided to drivers on mitigating risk. Details of training are to be available to buyer	**R**		
8.2. Truck escorts (armed where local law permits) Cost shall be borne by Buyer			
8.2.1 Capability to provide overt and covert escorts with real time communications to base and local police; written documentation in place	**R**		
8.3. Vehicle tracking – subject to availability and negotiated between Buyer and Supplier			
8.3.1 GPS or similar technology installed on all vehicles transporting Buyer's assets	**R**		

10.2.6 Förmåner

FSR, Freight Security Requirements, är ett initiativ för att förbättra säkerheten i den globala logistikkedjan skapat av en sammanslutning av privata aktörer. Målet är att minska antalet tillbud för det "egna" transporterade godset främst avseende stöld. Det är TAPA medlemmens samarbetspartners, avseende transport och förvaring av gods, som ska uppfylla TAPA kriterierna för att minska antalet tillbud med kundens gods. TAPA medlemmarnas intention är att välja aktörer som uppfyller eller överträffar kraven, och om inte, specificera i leverantörskontraktet att nödvändiga säkerhetsåtgärder införs.

En TAPA certifiering innebär inga statliga myndighetsförmåner i likhet med exempelvis tullättnaderna i AEO. En certifiering påvisar däremot en hög allmän säkerhetsnivå hos logistikaktören vilket är positivt även i andra upphandlingar med kunder som inte är TAPA medlemmar.

10.3 ISO 28000

10.3.1 Inledning

ISO 28000 är en standard utarbetad för att öka säkerheten i det globala logistiksystemet. Standarden är inriktad på att ge övergripande riktlinjer och rekommendationer av frågor gällande säkerhetsarbetet. Målet är bättre koll på flödena av gods, smugglingsbekämpning samt förhindra terrorattacker.

ISO 28000 är fokuserat, likt andra ISO standarder, på hur ledning- och kontrollprocesser och system ska utformas och tillämpas. Det finns inga, som bland annat för säkerhetsinitiativet AEO och TAPA, kriterier för hur den fysiska säkerheten ska vara utformad såsom övervakningskameror, skalskydd, inpasseringssystem o.s.v.

10.3.2 Harmonisering

ISO, International Organization for Standardization, är en organisation som arbetar med standardiseringsfrågor på en internationell nivå. ISO utgörs av de nationella standardiseringsorganisationerna varav varje land får representeras av en nationell organisation.

Inom EU bedrivs standardiseringsarbetet av CEN, European Committee for Standardization, som har som mål att harmonisera standardiseringsarbetet i unionen. Nationella standarder ska överges till förmån för motsvarande CEN standard om inga giltiga skäl finns gällande den egna nationens lagstiftning.

CEN samarbetar med ISO med mål att harmonisera och förenkla redan existerande regler och standarder i syfte att skapa en mer global standard för säkerhet i leveranskedjan.

10.3.3 Transportslag

Standarden ISO 28000 är mycket generellt utformad. Den är tillämpbar för både mindre och större verksamheter inom tillverkning, lager, hantering och transport av gods.

ISO 28000 riktar sig således till alla aktörer inom skilda branscher men med ett gemensamt mål – en vilja att utarbeta, införa och förbättra hur säkerhetsfrågorna hanteras, samt bedriva processerna enligt en given standard som kan hänvisas till i upphandlingar med leverantörer och kunder.

10.3.4 Certifieringsprocess

Certifieringsprocessen för ISO 28000 består av tre steg;

- **Steg 1:** Utvärdering av verksamhet
- **Steg 2:** Implementering av förbättringsåtgärder
- **Steg 3:** Granskning av oberoende part

10.3.4.1 Utvärdering av verksamhet

Målet med det första steget i certifieringsprocessen, utvärderingen av verksamheten (The Site Assessment Stage), är att analysera hur väl det existerande systemet uppfyller kraven i ISO 28000 och vad som behöver åtgärdas för överensstämmelse.

Fokus ligger på tre områden;

- Granskning av dokumentation
- Genomgång av använda processer
- Undersökning av vilka åtgärder som är på plats för den ”fysiska” säkerheten

10.3.4.2 Implementering av förbättringsåtgärder

Utvärderingen ger en tydlig bild av vad som behöver förbättras för att visa överensstämmelse med ISO 28000.

Förbättringsåtgärder införs och aktören är redo för granskningen av en oberoende part.

10.3.4.3 Granskning av oberoende part

Ett certifieringsgodkännande görs av en oberoende part. Granskningsprocessen tar minst tre månader varav själva bedömningen uppskattningsvis tar drygt en vecka.

Efter erhållande av certifiering enligt ISO 28000 kommer aktören årligen granskas och tre år efter godkännande måste aktören på nytt certifieras.

10.3.5 Generella certifieringskrav

Generellt gäller, enligt ISO 28000 standarden, att:

The organization shall establish, document, implement, maintain and continually improve an effective security management system for identifying security threats, assessing risks and controlling and mitigating their consequences.[59]

Vidare ska aktören kontinuerligt förbättra och effektivisera arbetet enligt samtliga kriterier.

Certifieringskraven är uppdelade i fem områden och följande ges några exempel från respektive område.

10.3.5.1 Security management policy

Generellt gäller att aktören ska utarbeta, införa eller redan ha på plats en övergripande ”security management policy” erkänd av företagets ledning. Den ska bland annat;

- *be consistent with other organizational policies*
- *be appropriate to the threats to the organization and the nature and scale of its operations*
- *be documented, implemented and maintained*

[59] Specification for security management systems for the supply chain, International Standard ISO 28000

- *be communicated to all relevant employees and third parties including contractors and visitors with the intent that these persons are made aware of their individual security management-related obligations*

10.3.5.2 Security risk assessment and planning

Följande är några exempel från sektionen *Security risk assessment and planning:*

Security risk assessment gör gällande att aktören ska ha processer för att identifiera och bedöma hot mot säkerheten. Utvalda exempel följer;

- *physical failure threats and risks, such as functional failure, incidental damage, malicious damage or terrorist or criminal action*
- *natural enviromental events (storm, floods, etc.), which may render security measures and equipment ineffective*
- *factors outside of the organization's control, such as failures in externally supplied equipment and services*

Legal, statutory and other security regulatory requirements innehåller följande två punkter;

- *to identify and have access to the applicable legal requirements and other requirements to which the organization subscribes related to its security threat and risks, and*
- *to determine how these requirements apply to its security threats and risks*

10.3.5.3 Implementation and operation

Följande är några exempel från sektionen *Implementation and operation* i certifieringskraven:

Structure, authority and responsibilities for security management behandlar att;

The organization shall establish and maintain an organizational structure of roles, responsibilities and auhtorities, consistent with the achievement of its security management policy, objectives, targets and programmes.

Utvalda exempel följer;

- *appointing (a) member(s) of management with the necessary authority to ensure that the objectives and targets are implemented*
- *ensuring any security programmes generated from other parts of the organization complement the security management system*
- *communicating to the organization the importance of meeting its security management requirements in order to comply with its policy*
- *ensuring security-related threats and risks are evaluated and included in organizational threat and risk assessments, as appropriate*

Competence, training and awareness behandlar kriterier som gäller för de ansvariga för utformning, genomförande och ledning av den säkerhetsutrustning respektive processer som används. Dessa ska vara kvalificerade för uppgiften avseende utbildning och erfarenhet. Några exempel följer;

- *the importance of compliance with the security management policy and procedures, and to the requirements of the security management system*
- *their roles and responsibilities in achieving compliance with the security management policy and procedures and with the requirements of the security management system, including emergency preparedness and response requirements*

10.3.5.4 Checking and corrective action

Följande är några exempel från sektionen *Checking and corrective action* vilken behandlar hur själva säkerhetsprocesserna ska mätas avseende dess effektivitet, hur utvärdering ska ske m.m.

Security performance measurement and monitoring ger kriterier för hur säkerhetsprocessystemet ska övervakas, dess effektivitet m.m. Utvalda exempel;

- *monitoring the extent to which the organization's security management policy, objectives and targets are met*
- *proactive measures of performance that monitor compliance with the security management programs, operational control criteria and applicable legislation, statutory, and other security regulatory requirements*

System evaluation specificerar hur system ska utvärderas;

The organization shall evaluate security manangement plans, procedures, and capabilities through periodic reviews, testing, post-incident reports, lessons learned, performance evaluations, and exercises…

The organization shall periodically evaluate compliance with relevant legislation and regulations, industry best practices, and conformance with its own policy and objectives.

Security-related failures, incidents, non-conformances and corrective and preventive action ger krav på att processer ska finnas för;

- *evaluating and initiating preventive actions to identify potential failures of security in order that may be prevented from occuring*
- *the investigation of security-related; failures including near misses and false alarms, incidents and emergency situations, non conformance*
- *taking action to mitigate any consequences arising from such failures, incidents or non-conformances*

10.3.6 Metod för uppfyllande av mål

För att uppfylla kraven för certifiering och kontinuerligt i den löpande verksamheten kunna upprätthålla kraven för ISO 2800 är standarden baserad på PDCA metoden. PDCA är en förkortning på Plan-Do-Check-Act och den kan kort förklaras som;

- Plan: identifiera och definiera vilka åtgärder som måste införas för att uppfylla önskade mål gällande säkerheten.
- Do: genomför åtgärder enligt punkt 1.
- Check: följ upp genomförda åtgärder och säkerställ att de definierade målen uppfyllts enligt säkerhetspolicyn.
- Act: gör kontinuerliga förbättringsåtgärder av säkerhetsledningssystemet.

10.3.7 Fördelar

Införande av processer enligt kraven i ISO 28000 kan förbättra aktörens verksamhet på mer än säkerhetsområdet eftersom certifieringskriterierna är mycket allmänt utformade och omfattar många generella handlingsprocesser när det gäller styrning, ledning, kontroll m.m.
Direkta fördelar kan förutom ökad säkerhet i logistikkedjan bli exempelvis;

- Ökad omsättning
- Förbättrad effektivitet i logistikkedjan
- Bättre kontroll och ledning över lager och -aktiviteter
- Minskning av de mänskliga felen

Certifiering enligt ISO 28000 ger fördelar gentemot konkurrerande aktörer eftersom;

- Aktören konkret kan påvisa att säkerheten inom logistikkedjan tas på allvar
- Hög säkerhetsnivå
- ISO 28000 är erkänd av säkerhetsinitiativet AEO, Authorized Economical Operators, samt U.S. Customs and Border Protection och är därmed en bra grund för certifiering enligt dessa

10.4 C-TPAT

10.4.1 Inledning

C-TPAT, Customs-Trade Partnership Against Terrorism, infördes som ett initiativ av CBP för att öka säkerheten efter terroristattacken 9/11 2001 genom att förbättra säkerheten i den globala leveranskedjan. Målet är att förhindra terrorister och vapen att smugglas in i USA. Till skillnad från traditionellt tullarbete bygger C-TPAT på ett utökat samarbete mellan CBP och de företag vilka utgör navet i den omfattande importen av varor till USA.

Med tanke på volymen av importerat gods är CBP tvunget att hitta metoder att kombinera en omfattande och noggrann kontroll men samtidigt uppehålla en effektivitet i varuflödet genom gränskontrollerna.

Strategin är att jobba alltmer förebyggande innan godset anländer fysiskt till gränskontrollen bland annat genom att tidigt analysera tillgänglig information och rikta in aktiviteten på gods som bedöms ha hög risk. Fokus från CBP sida är att involvera företag i samarbetet vilka hanterar stora volymer gods men med låg risk.

Fokus i C-TPAT initiativet är att låta företagen bli än mer involverade i att säkerställa hela transportkedjan genom omfattande arbete med den passiva säkerheten och därmed underlätta tullens arbete. Som ett led i detta bör samarbetet mellan importör (i USA) och exportör fördjupas med mål att öka kontrollen av det egna godset med avseende bland annat på att försvåra att lasten ändras eller manipuleras innan sändning och under transportens gång.

10.4.2 Kopplingar

C-TPAT har kopplingar till The Security and Accountability for Every Port Act, SAFE, som är en lag som trädde i kraft år 2006 och var Bush administrationens respons på det ökade terroristhotet. Innebörden i SAFE Port Act är att varje hamn har ansvarsskyldighet för den egna och landets säkerhet. Lagen är grunden till många av de amerikanska säkerhetsinitiativen och det utvecklande arbetet inom den marina säkerheten bedrivs av the Department of Homeland Security (DHS).

10.4.3 Harmonisering

Inom ramen för C-TPAT har U.S. Customs and Border Protection hittills ömsesidigt erkänt Nya Zealand, Canada och Jordaniens säkerhetsarbete. Målet är en global koordinering av säkerhetsarbetet och initiativen med syfte att skapa en säker global logistikkedjan.

10.4.4 Transportslag

Inriktningen på säkerhetsarbetet under C-TPAT är kontroll av godsimport till USA gällande alla transportslag.

Exempelvis transporterades 11 miljoner lastbilscontainers över gränserna 2008 varav en fjärdedel kontrollerades. 2,7 miljoner containers passerade gränserna med tåg med

en kontrollfrekvens på nio av tio och med containerfartyg ankom 11 miljoner st där drygt en av varje 33:e container kontrollerades.[60]

10.4.5 Certifieringsprocess

Detta projekt, Protected – Security i kombitransporter, är begränsad till en utredning om hur kombitransporter inom Europa påverkas av valda säkerhetsinitiativ. Kriterierna i C-TPAT är tillämpbara för olika aktörer. Exempel kommer att tas från certifieringskriterierna för utländska tillverkare med hänsyn till rapportens begränsningar och för att vara av nytta i senare faser.

Kriterierna i C-TPAT är minimikrav som måste uppfyllas för certifiering och erhållande av de grundläggande förmånerna. Den högsta nivån av lättnader i tullförfarandet ges till de aktörer som vida överträffar grundkraven och visar en seriositet i säkerhetsarbetet.

Målet med grundkraven i C-TPAT är att vara en utgångspunkt för aktörer att förbättra säkerheten i logistikkedjan och minska risken för stöld och smuggling i legitimt gods som kan användas för exempelvis terrorism.

En utvärdering ska årligen göras av den certifierade aktören för att säkerställa att kraven i C-TPAT följs och när säkerhetsläget bedöms som allvarligt.

Följande ges utvalda exempel från certifieringskraven, **Minimum-Security Criteria for C-TPAT Foreign Manufacturers**, för utländsk tillverkare. Utländsk syftar till aktör utanför USA.

10.4.5.1 Business Partner Requirement

Samarbetspartners måste väljas enligt etablerade riktlinjer och processer.

Security Procedures gör gällande att för samarbete med aktörer som inte är C-TPAT certifierade krävs att dessa uppfyller motsvarande säkerhetsnivå;

For those business partners not eligible for C-TPAT certification, the foreign manufacturer must require that their business partners to demonstrate that they are meeting C-TPAT security criteria via written/electronic confirmation…

Based upon a documented risk assessment process, non-C-TPAT eligible business partners must be subject to verification of compliance with C-TPAT security criteria by the foreign manufacturer.

"Utländsk tillverkare" ska också se till att eventuellt anlitade underleverantörer för transporttjänsterna (ex. åkeriet) i sin tur inte anlitar icke C-TPAT certifierade företag och att dessa aktörer har tillräckliga säkerhetsåtgärder/-processer på plats framförallt där lastning av gods sker.

[60] A Guide To Program Benefits, U.S. Customs and Border Protection C-TPAT Program, Office of Field Operations

10.4.5.2 Container and Trailer Security

Generellt för container- och trailersäkerhet gäller att;

Container and trailer integrity must be maintained to protect against the introduction of unauthorized material and/or persons. At the point-of-stuffing, procedures must be in place to properly seal and maintain the integrity of the shipping containers and trailers.

Container Inspection processer måste finnas för hur containers fysiska integritet ska undersökas. Det ska göras innan packning av densamma och kontroll ska göras av lås samt alla sidor och underrede.

Container and Trailer Storage specificerar krav på förvaring;

Containers and trailers under foreign manufacturer control or located in a facility of the foreign manufacturer must be stored in a secure area to prevent unauthorized access and/or manipulation. Procedures must be in place for reporting and neutralizing unauthorized entry into containers/trailers or container/trailer storage areas.

10.4.5.3 Physical Access Controls

Otillbehörligt tillträde till verksamhetens lokaler måste förhindras. Exempelvis måste alla anställda, besökare, varulämningar osv. vid passage in på område, identifieras.

Visitors *must present photo identification for documentation purposes upon arrival. All visitors should be escorted and should visibly display temporary identification.*

Deliveries (including mail) ställer krav på att alla leveranser ska identifieras med avseende på riktigheten. Dessutom gäller att:

Arriving packages and mail should be periodically screened before being disseminated.

10.4.5.4 Personnel Security

Rutiner måste finnas för att vid nyanställning och kontinuerligt undersöka personalens bakgrund och om eventuella privata förehavanden strider mot aktörens säkerhetspolicy. För bakgrundskontroll finns följande krav:

Background Checks / Investigation *consistent with foreign regulations, background checks and investigations should be conducted for prospective employees. Once employed, periodic checks and reinvestigations should be performed based on cause, and/or the sensitivity of the employee's position.*

10.4.5.5 Procedural Security

Rutiner måste finnas för att garantera att säkerheten i hantering, transport och lagring av gods är god och att därtill hörande processer håller en hög säkerhetsnivå.

Documentation Processing gör gällande att rutiner ska finnas för att säkerställa att all information rörande transporten av gods är komplett, riktig och skyddad mot manipulation och förlust.

Shipping and Receiving av gods ska noga kontrolleras enligt kraven;

Departing cargo being shipped should be reconciled against information on the cargo manifest. The cargo should be accurately described, and the weights, labels, marks and piece count indicated and verified. Departing cargo should be verified against purchase or delivery orders. Drivers delivering or receiving cargo must be positively identified before cargo is received or released. Procedures should also be established to track the timely movement of incoming and outgoing goods.

10.4.5.6 Physical Security

Verksamhetens anläggningar måste ha ett utbyggt skalskydd för att hindra oauktoriserat tillträde. Det innefattar: staket runt område, portar till område, regler för parkering av privata bilar i närhet till godshantering, allmän säkerhetsstruktur på byggnad, lås till samtliga öppningar till område och byggnader, god belysning med fokus på område och byggnads skalskydd samt alarm och videoövervakningssystem. Några utvalda exempel följer;

Fencing krav specificerar följande:

Perimeter fencing should enclose the areas around cargo handling and storage facilities. Interior fencing within a cargo handling structure should be used to segregate domestic, international, high value, and hazardous cargo. All fencing must be regulary inspected for integrity and damage.

Alarm Systems and Video Surveillance Cameras *should be utilized to monitor premises and prevent unauthorized access to cargo handling and storage areas.*

10.4.5.7 Information Technology Security

System ska finnas för upptäckande av felaktig access och manipulering av datasystem och dess innehåll av affärsinformation.

Därutöver ska IT rutiner och processer vara införda för att garantera en säker IT miljö exempelvis rutiner för lösenordsbyte m.m.

10.4.5.8 Security Training and Threat Awareness

Ett aktivt deltagande i säkerhetsarbetet från de anställda men framförallt en uppmärksamhet på riskerna/riskområdena beskrivs följande;

A threat awareness program should be established and maintained by security personnel to recognize and foster awareness of the threat posed by terrorists and contraband smugglers at each point in the supply chain. Employees must be made aware of the procedures the company has in place to adress a situation and how to report it. Additional training should be provided to employees in the shipping and receiving areas, as well as those receiving and opening mail.

Additionally, specific training should be offered to assist employees in maintaining cargo integrity, recognizing internal conspiracies, and protecting access controls. These programs should offer incentives for active employee participation.

10.4.6 Förmåner

Beskrivningen av C-TPAT fokuserar i rapporten på hur en utländsk tillverkare påverkas bland annat när det gäller vilka säkerhetskriterier som är tillämpliga.

De konkreta förmånerna för en utländsk tillverkare att certifieras enligt C-TPAT är mycket få eftersom dessa främst är riktade mot importörer i USA. I en uppföljningsundersökning[61] gjord 2007 för att analysera konsekvenserna av införandet av C-TPAT konstateras att den främsta motivationen för en icke-importör är att det krävts av en samarbetspartner.

10.4.7 Fördelar för importör

Förmånerna för en certifierad importör i USA är enligt undersökningen[62] bedömd av deltagarna betydelse för deras verksamhet;

1. *Reduce time and cost of getting cargo released by CBP* (CBP, Customs and Border Protection)

För C-TPAT certifierade aktörer förkortas den tid CBP behöver när kontroll av godstransport väl genomförs. Det minskar risken för förseningar i den fortsatta transporten och därmed eventuella ekonomiska konsekvenser.

2. *Reduce time in CBP secondary cargo inspection lines*
3. *Improve predictability in moving goods and services across borders*
4. *Reduce penalties*
5. *Generate significant opportunities for cost avoidance*
6. *Improve security for workforce*
7. *Reduce cargo theft and pilferage*

Detta är i högsta grad även tillämpligt för den utländska tillverkaren. Den egna verksamhetens säkerhet förbättras eller i varje fall certifieras.

8. *Access to FAST program*

[61] Customs-Trade Partnership Against Terrorism Cost/Benefit Survey, CSR Center for Survey Research & Weldon Cooper Center for Public Service, 2007
[62] Customs-Trade Partnership Against Terrorism Cost/Benefit Survey, CSR Center for Survey Research & Weldon Cooper Center for Public Service, 2007

10.5 ISPS

10.5.1 Inledning

ISPS-koden är IMO:s (International Maritime Organizations) svar på den ökade hotbilden efter händelserna den 9/11 i USA. Risken för terroristattacker blev plötsligt ett verkligt hot mot transportnäringen världen över. Kort efter händelserna beslutade IMO att försöka definiera vilka åtgärder som bör införas för att förebygga att en liknande händelse inträffar inom sjöfarten och vilket tillvägagångssättet skulle vara. ISPS påverkar främst hamnar, rederier och fartyg.

Syftet med ISPS-koden är:

- *to establish an international framework involving co-operation between Contracting Governments, Government agencies, local administrations and the shipping and port industries to detect/assess security threats and take preventive measures against security incidents affecting ships or port facilities used in international trade*
- *to establish the respective roles and responsibilities of all these parties concerned, at the national and international level, for ensuring maritime security*
- *to ensure the early and efficient collation and exchange of security related information*
- *to provide a methodology for security assessments so as to have in place plans and procedures to react to changing security levels*
- *to ensure confidence that adequate and proportionate maritime security measures are in place*

ISPS-koden är utformad för att vara ett grundläggande krav med rekommendationer, sett på ett globalt plan, som således utgör en minimal säkerhetsnivå vilket alla länder bör uppfylla. Det är ländernas individuella ansvar att med ISPS som utgångspunkt göra bedömningar om vilka säkerhetsåtgärder som krävs för tillfället och kommunicera dessa till berörda parter såsom fartyg och hamnar.

Koden antogs 2002 av *the Conference of Contracting Governments to the International Convention for the Safety of Life at Sea* och togs i kraft juli 2004 och finns som ett tillägg i SOLAS konventionen (Safety of Life at Sea) och är därmed obligatorisk för de till SOLAS 148 tillhörande staterna. Globalt följer däremot 167 länder ISPS koden.

ISPS består både av krav och frivilliga rekommendationer. Riskbedömningar måste göras i varje enskilt fall där det fastslås vilka åtgärder som är nödvändiga. Det är ett ramverk för att bedöma risker och tillhandahåller sätt på hur sårbarheten kan minskas. Fartyg och hamnar måste, efter ISPS-kodens införande, visa på att ett korrekt tillvägagångssätt används i bedömningen av risker.

Koden omfattar kortfattat följande kravområden som kommer utvecklas längre fram i rapporten under avsnittet *Certifiering*;

- Att information avseende hot mot säkerheten samlas in och utvärderas
- Utbyte av sådan information stater emellan
- Att resurs för larmning finns vid hot mot säkerheten

- Obehöriga ska förhindras tillträde till fartyg, hamnar och skyddsområden
- Likaså vapen, explosiva medel m.m.
- Fartyg och hamnar ska ha skyddsplaner och att personal är utbildade och övade i dessa

10.5.2 Kopplingar

En koppling till ISPS är EU:s förordning *om förbättrat sjöfartsskydd på fartyg och i hamnanläggningar*[63]. Den har som mål att *skyddet för de medborgare som utnyttjar dessa* (fartygetstransport för gods eller persontrafik) *samt miljöskyddet bör alltid säkerställas inför de hot som utgörs av avsiktliga olagliga handlingar, såsom terroristattacker, sjöröveri eller andra liknande handlingar*. Förordningen innefattar i princip samma krav som ISPS-koden där delar är obligatoriska för EU:s medlemsstater.

10.5.3 Transportslag

Varje fartyg, hamn och rederi ska utarbeta och införa säkerhetsplaner som ska respondera mot respektive säkerhetsnivå och tydligt specificera nödvändiga åtgärder för att upprätthålla säkerheten vid incidenter.

Fartyg som berörs är;

- Passagerarfartyg
- Lastfartyg med en bruttovikt på minst 500 ton
- Mobila offshoreborrenheter

Samt hamnar som betjänar fartygen.

10.5.4 Fastställande av säkerhetsnivå

Enligt tidigare är det ländernas individuella ansvar att, med riktlinjerna och kraven i ISPS som utgångspunkt, kontinuerligt eller vid ett förändrat säkerhetsläge nationellt eller internationellt göra bedömningar om vilka säkerhetsåtgärder som krävs för tillfället och kommunciera dessa till berörda parter såsom fartyg och hamnar.

I ISPS-koden del B paragraf 4.8 beskrivs hur fastställande av skyddsnivå bör ske:

Den fördragsslutande staten bör vid fastställande av skyddsnivå ta hänsyn till allmän och specifik information om hot. Den fördragsställande staten bör fastställa den skyddsnivå som skall gälla för fartyg och hamnanläggningar till en av följande tre nivåer:

- *Skyddsnivå 1: normal, den skyddsnivå på vilken fartyg och hamnanläggningar normalt arbetar.*
- *Skyddsnivå 2: förhöjt skydd, den skyddsnivå som skall gälla så länge det föreligger en förhöjd risk för säkerhetstillbud.*
- *Skyddsnivå 3: exceptionell, den skyddsnivå som skall gälla under den tid då det föreligger en sannolik eller överhängande risk för säkerhetstillbud.*

[63] Europaparlamentets och rådet förordning EG nr 725/2004, *om förbättrat sjöfartsskydd på fartyg och i hamnanläggningar*, 2004

I Sverige gäller enligt sjöfartsinspektionens tillsynsenhet (nu tillhörande transportstyrelsen) beslut:[64]

Sjöfartsskydd – Åtgärder vid beslut om höjning av skyddsnivåer

Grundregeln i lagstiftningen är att Rikspolisstyrelsen, genom Rikskriminalpolisen, efter att ha hört Sjöfartsinspektionen och Kustbevakningen ska besluta om skyddsnivån för sjöfarten…

Vid en ändring av skyddsnivån ska myndighetens beredskapsinspektörer vidta följande åtgärder gällande hamnanläggningar, svenska fartyg samt utländska fartyg på svenskt territorialvatten:

- *Kontakta berörda hamnanläggningars skyddschefer och meddela att skyddsnivån höjts. Det kan gälla en eller flera anläggningar i samma inspektionsområde.*
- *Kontakta skyddscheferna på rederierna för de svenska fartygen och meddela att skyddsnivån höjts. I detta fall kan ett eller flera rederier vara berörda. Det är i första hand rederiet som ska meddela sina fartyg.*
- *…ett NAVTEX[65] meddelande med följande innehåll "The Swedish Government has decided that all ships in Swedish ports or in Swedish territorial waters about to enter a Swedish port shall apply security level X"*

10.5.5 Säkerhetsnivåer

I ISPS-koden finns tre säkerhetsnivåer för fartyg respektive hamnar vars innehåll kommer specifieras mer ingående längre fram. Först ges en överblick över dess innebörd[66];

10.5.5.1 Fartyg

Skyddsnivåer på fartyg

Ett fartyg ska leva upp till de skyddsnivåer som meddelas från den egna staten eller av den staten man befinner sig i.

På *skyddsnivå 1* ska skyddsarbete ombord utföras på rätt sätt, kontroll ske av personer som går ombord och deras tillhörigheter, bevakning göras av skyddsområden så att endast behöriga personer får tillträde dit, övervakning ske av däck, lasthantering och företagets förråd samt ska det ses till att skyddskommunikation är upprättad.

På *skyddsnivå 2 och 3* utökas nivån på kontroller och de utökade skyddsåtgärderna ska finnas beskrivna i fartygets skyddsplan.

När myndigheten fastställer att skyddsnivån 2 eller 3 ska gälla, ska fartyget bekräfta att instruktioner om ändrad skyddsnivå mottagits. Beroende på vilken situation

[64] Sjöfartsinspektionen, *Sjöfartsskydd – Åtgärder vid beslut om höjning av skyddsnivåer*, CI-beslut NR 1/2006
[65] NAVTEX är ett internationellt system för att sända ut navigationsvarningar samt väder- och isinformation till fartyg.
[66] Överblicken är hämtat från MariTerms genomgång av ISPS koden, *ISPS CODE Your Key To Security*

fartyget befinner sig i ska fartygets och aktuella hamnars skyddschefer samarbeta och samordna lämpliga åtgärder.

Fartygets skyldigheter

Ett fartyg ska uppfylla de skyddsnivåkrav som gäller för aktuell hamn och ska utan onödig fördröjning anpassas till eventuell ändring av högre skyddsnivå. Om fartyget inte uppfyller aktuella krav, ska fartyget informera lämplig myndighet innan fartyg/hamnsamverkan inleds eller innan hamnen anlöps.

10.5.5.2 Hamn

En hamnanläggning är en plats där, enligt beslut från ansluten stat eller utsedd myndighet, fartyg/hamnsamverkan pågår. Detta inkluderar, när så är tillämpligt områden för ankring, väntekajer och insegling från sjösidan.

I princip är det samma krav på en hamn som för ett fartyg i fråga om att skapa skydd för den egna anläggningen och ha kontroll över vad, vilka och hur gods, fartyg och människor kommer till och in i hamnen. En hamn ska arbeta på den skyddsnivå som fastställs av den anslutna stat inom vars territorium hamnen ligger. Skyddsåtgärder och skyddsprocedurer ska tillämpas i hamnen så att det blir minimala störningar eller förseningar för passagerare, fartyg, besättning, besökare, godstransporter och service.

Skyddsnivåer i hamnen

På *skyddsnivå 1* ska i alla hamnanläggningar ett antal åtgärder vidtas för att identifiera och vidta förebyggande åtgärder mot säkerhetstillbud. Åtgärderna är att kontrollera tillträdet till hamnanläggningen, att säkerställa att hamnanläggningens alla sjöfartsskyddsuppgifter utförs och att kommunikation i sjöfartsskyddsfrågor snabbt finns till hands. Vidare ska hamnanläggningen (inklusive ankarplatser och områden för förtöjning), lasthanteringen, hantering av fartygets förråd och områden med begränsat tillträde övervakas för att säkerställa att endast behöriga personer får tillträde.

På *skyddsnivå 2 och 3* ska ytterligare skyddsåtgärder, som specifieras i hamnanläggningens skyddsplan, införas för varje typ av verksamhet.

På *skyddsnivå 3* ska hamnanläggningen dessutom bemöta och genomföra skyddsinstruktioner från den stat inom vars territorium hamnanläggningen ligger.

10.5.6 Skyddsplan

En överblick ges följande av innebörden av en skyddsplan för fartyg respektive hamnar.[67]

[67] Överblicken är hämtat från MariTerms genomgång av ISPS koden, *ISPS CODE Your Key To Security*

10.5.6.1 Fartyg

Fartygets skyddsutredning

En skyddsutredning måste göras på fartyget för att man ska kunna sammanställa och uppdatera fartygets skyddsplan. Rederiets skyddschef ser till att fartygets skyddsutredning utförs i enlighet med ISPS koden. Skyddsutredningen ska omfatta en skyddsinspektion

ombord och bland annat innehålla identifiering av befintliga skyddsåtgärder, skyddsprocedurer och skyddsinsatser, identifiering och utvärdering av vilken verksamhet ombord som är viktigast att skydda samt identifiering av tänkbara hot mot fartygets verksamhet och sannolikheten för att de uppkommer.

Fartygets skyddsplan

Ett fartygs skyddsplan är en plan med åtgärder ombord på fartyget, avsedda att skydda personer ombord, last, lasttransportenheter, fartygets förråd och fartyget självt från riskerna vid ett säkerhetstillbud. Alla fartyg ska ha sin skyddsplan ombord och planen ska innehålla instruktioner hur man agerar i de tre olika skyddsnivåerna.

Skyddsplanen ska utarbetas i enlighet med ISPS koden och skrivas på fartygets arbetsspråk. Om fartygets arbetsspråk inte är engelska, franska eller spanska ska det finnas en översättning av planen till något av dessa språk.

Skyddsplanen ska bland annat behandla åtgärder som förhindrar att vapen, farliga ämnen och farliga anordningar avsedda att användas mot människor, fartyg eller hamnar tas ombord på fartyget, åtgärder som förhindrar obehörigt tillträde till fartyget och dess skyddsområden och skyddsåtgärder på skyddsnivå 2 och 3. Planen ska även behandla tillvägagångssätt vid evakuering i händelse av hot eller brott mot säkerheten, arbetsuppgifter för ombordpersonal som tilldelats skyddsansvar och annan ombordpersonal i fråga om skyddsaspekter samt
procedurer för utbildning och övningar kopplade till planen, för koppling till hamnens skyddsverksamhet och för rapportering av säkerhetstillbud.

Planen ska skyddas mot obehörigt tillträde och avslöjande och ska under normala omständigheter inte inspekteras av tjänstemän auktoriserade av ansluten stat.

10.5.6.2 Hamn

Hamnens skyddsutredning

En skyddsutredning motsvarande den som görs på fartyg ska genomföras på en hamnanläggning. Skyddsutredningen görs för att kunna sammanställa och uppdatera hamnens skyddsplan.

Skyddsutredningen ska bland annat innehålla identifiering och utvärdering av viktiga tillgångar och den infrastruktur som är viktig att skydda, identifiering av tänkbara hot mot egendom och infrastruktur och sannolikheten för att hoten ska förverkligas samt identifiering, urval och prioritering av motåtgärder.

Hamnens skyddsplan

En hamns skyddsplan ska utarbetas baserad på hamnens skyddsutredning. Planen ska innehålla föreskrifter för de tre skyddsnivåerna.

Planen ska skrivas på det arbetsspråk som används i hamnen och ska bland annat omfatta åtgärder för att hindra vapen, farliga ämnen och anordningar avsedda att användas mot

människor, fartyg och hamnar, från att införas i hamnanläggningen eller ombord på fartyg, för att hindra obehörigt tillträde till hamnen, fartyg som är förtöjda i hamnen och till skyddsområden inom anläggningen och åtgärder som effektivt säkerställer lastens och lasthanteringsutrustningens säkerhet i hamnen. Vidare ska planen omfatta procedurer för evakuering i händelse av hot eller brott mot säkerheten, för samverkan med fartygens skyddsverksamhet och för åtgärder i händelse av skyddslarm ombord på fartyg som ligger i hamnen. Procedurer ska också finnas för att underlätta för personalbyten och för besättningen att gå i land, samt för besökare att komma till fartyget, inklusive representanter från sjöfartens
välfärdsorganisationer och fackföreningar och för åtgärder vid eventuella skyddsinstruktioner som den anslutna stat, inom vars territorium hamnen ligger, utfärdar vid skyddsnivå 3.

10.5.7 Specificerade krav för fartyg

Följande kommer ges utvalda exempel på de ingående kraven i ISPS-koden och de rekommendationer som finns för hur dessa krav ska uppfyllas.

Exemplen är uppdelade i respektive säkerhetsnivå. För nivå två gäller även kraven för nivå ett och för den högsta nivån, nivå tre, är kraven för både första och andra nivån obligatorium.

De exakta kraven för varje säkerhetsnivå specifieras i fartygets skyddsplan. De krav som citeras från ISPS Coden i följande avsnitt är exempel på vad skyddsplanen *kan* innehålla för respektive säkerhetsnivå.

10.5.7.1 Access to the ship

Specificerar rutiner för att förhindra obehörigt tillträde till fartyg. Något som kan få allvarliga konsekvenser om fripassagerarna inte upptäcks i tid.

Några exempel ges från respektive säkerhetsnivå.

Security level 1

Kan bland annat innebära följande;

Checking the identity of all persons seeking to board the ship and confirming their reasons for doing so by checking, for example, boarding passes, work orders, etc

Providing security briefings to all ship personnel on possible threats, the procedures for reporting suspicious persons, objects or activities and the need for vigilance

Security level 2

Kan innebära i tillägg till kriterierna på nivå 1;

Assigning additional personnel to patrol deck areas during silent hours to deter unauthorized access

Establishing a restricted area on the shore side of the ship, in close co-operation with the port facility

Carrying out a full or partial search of the ship

Security level 3

Följande kan vara åtgärder som genomförs om den högsta säkerhetsnivån fastställs;

Granting access only to those responding to the security incident or threat thereof

Evacuation of the ship

10.5.7.2 Restricted areas on the ship

Skyddade områden införs med mål att skydda eventuella passagerare, hamnpersonal eller myndighetspersoner men också för att skydda känsliga utrymmen på fartyg och skydda gods från manipulation (exempelvis smuggling och terrorism).

Känsliga utrymmen kan vara; bryggan, maskinrum, övervakningsrum, luftcirkulationssystem, dricksvattentankar, hytter m.m.

Security level 1

Fartygets skyddsplan kan innehålla följande åtgärder för att skydda fartygets skyddade områden för, av myndigheter bestämda, säkerhetsnivå 1;

Locking or securing access points

Using automatic intrusion-detection devices to alert the ship's personnel of unauthorized access

Security level 2

Continuously monitoring surveillance equipment

Dedicating additional personnel to guard and patrol restricted areas

Security level 3

Setting up of additional restricted areas on the ship in proximity to the security incident, or the believed location of the security threat, to which access is denied

Searching of restricted areas as part of a search of the ship

10.5.7.3 Handling of cargo

Kriterier för godshantering ska finnas i fartygets skyddplan för att förhindra att gods manipuleras och att inget gods som inte ska transporteras med fartyget finns i lasten.

Generellt gäller att allt gods ombord ska kunna identifieras (att enheten är legitimt gods) och att ingen manipulation ska kunna ske av lastat gods.

Security level 1

Routine checking of cargo, cargo transport units and cargo spaces prior to, and during, cargo handling operations

Checks to ensure that cargo being loaded matches the cargo documentation

Checking of seals or other methods used to prevent tampering

Security level 2

Detailed checking of cargo, cargo transport units and cargo spaces

Intensified checks to ensure that only the intended cargo is loaded

Increased frequency and detail in checking of seals or other methods used to prevent tampering

Security level 3

Suspending the loading or unloading of cargo

Verifying the inventory of dangerous goods and hazardous substances carried on board, if any, and their location

10.5.7.4 Monitoring the security of the ship

Fartygets säkerhetåtgärder (exempelvis områden med begränsat tillträde) måste kunna övervakas och förutsättningar för det kan vara; ljussättningen, vakter, automatiska system för att upptäcka inkräktare och övervakningsutrustning.

Generellt gäller exempelvis att vid användande av automatiska system för upptäckande av inkräktare att larmsignalen ska vara upptäckbar i områden på fartyget som alltid är bemannade eller kontinuerligt är övervakade.

Security level 1

Exempel från belysningskrav;

The ships's deck and access points to the ship should be illuminated during hours of darkness and periods of low visibility while conducting ship/port interface activities or at a port facility or anchorage when necessary.

The ship's personnel should be able to detect activities beyond the ship, on both the shore side and the water side

Coverage may be provided through co-ordination with the port facility

Security level 2

Increasing the frequency and detail of security patrols

Assigning additional personnel as security look-outs

Increasing the coverage and intensity of lightning or the use of security and surveillance

Security level 3

Switching on of all lightning on, or illuminating the vicinity of, the ship

Initiation of measures, including the slow revolution of the ship's propellers, if practicable, to deter underwater access to the hull of the ship

10.5.8 Specifierade krav för hamnar

På motsvarande sätt som för fartyg ska hamnar ha en utarbetad skyddsplan som ska specifiera vilka åtgärder som *kan* införas under respektive säkerhetsnivå.

Skyddsplanen ska ta upp följande områden; fysisk säkerhet (perimetersäkerhet osv.), personalsäkerhet, kommunikationsutrustning, transportinfrastruktur, m.m.

Funktioner att skydda kan vara;

- accesspunkter (portar, tillfartsentréer), ankarplatser
- godsterminaler, -lagerområden, -hanteringsutrustning
- kommunikationsutrustning (radiotrafik, telefoni, nätverk)
- hamntrafik managementsystem och navigationshjälp
- energi- och vattenförsörjning
- interna vägar och järnvägsnät

- diverse säkerhet och övervakningssystem

Hoten mot en hamns säkerhet är många och diversifierade. Hamnens skyddplan ska utvärdera eventuella hot mot den aktuella hamnen säkerhet och förmågan att upprätthålla verksamhet.

Det kan vara;

- förstörelse av hamn eller fartyg förtöjt i hamn på grund av sabotage, skadegörelse, sprängning m.m.
- kapning av fartyg
- manipulering av gods, fartygsutrustning, m.m.
- obehörigt tillträde till fartyg exempelvis i form av fripassagerare
- smuggling av vapen, massförstörelsevapen, m.m.
- användande av fartyg som vapen
- attacker på hamnområde med kärn-, biologiska- eller kemiska vapen

Följande kommer ges utvalda exempel från några områden där det ska specificeras åtgärder för respektive säkerhetsnivå.

10.5.8.1 Access to the port facility

Skyddsplanen ska behandla åtgärder för att skydda alla hamnens accesspunkter. Exempel följer för respektive säkerhetsnivå;

Security level 1

At security level 1, the PFSP should establish the control points where the following security measures may be applies:

Checking identity of all persons seeking entry to the port facility in connection with a ship, including passengers, ship's personnel and visitors, and confirming their reasons for doing so by checking, for example, joining instructions, passenger tickets, boarding passes, work orders, etc

Checking vehicles used by those seeking entry to the port facility in connection with a ship

Identification of any access points not in regular use, which should be permanently closed and locked

Security level 2

Assigning additional personnel to guard access points and patrol perimeter barriers

Limiting the number of access points to the port facility, and identifying those to be closed and the means of adequately securing them

Denying access to visitors who are unable to provide a verifiable justification for seeking access to the port facility

Using patrol vessels to enhance water-side security

Security level 3

Suspension of access to all, or part, of the port facility

Granting access only to those responding to the security incident or threat thereof

Evacuation of all, or part, of the port facility

10.5.8.2 Restricted areas within the port facility

Restricted areas, skyddade områden, kan vara; land- och vattensida i direkt anslutning till fartyg, ombordstigningsområden, lastningsområden, områden där säkerhetsinformation

förvaras, områden där farligt gods hanteras/förvaras, förvaringsutrymmen för övervakningsutrustning m.m.

Security level 1

Providing passes which must be displayed to identify individual's entitlement to be within the restricted area

Clearly marking vehicles allowed access to restricted areas

Providing automatic intrusion-detection devices, or surveillance equipment or systems to detect unauthorized access into, or movement within, restricted areas

Security level 2

Further restricting access to the restricted areas and movements and storage within them

Enforcing restrictions on access by unauthorized craft to the waters adjacent to ships using the port facility

Security level 3

Setting up of additional restricted areas within the port facility in proximity to the security incident, or the believed location of the security threat, to which access is denied

Preparing for the searching of restricted areas as part of a search of all, or part, of the port facility

10.5.8.3 Handling of cargo

Kriterierna är till för att förhindra manipulering av gods och att inget icke accepterat/illegitiment gods lastas ombord fartyg eller förvaras i hamnområde.

Följande är exempel från respektive säkerhetsnivå;

Security level 1

Checks to ensure that cargo entering the port facility matches the delivery note or equivalent cargo documentation

Checking of seals and other methods used to prevent tampering upon entering the port facility

Security level 2

Intensified checks, as appropriate, to ensure that only the documented cargo enters the port facility, is temporarilty stored there and is then loaded onto the ship

Increased frequency and detail in checking of seals and other methods used to prevent tampering

Security level 3

Restriction or suspension of cargo movements or operations within all, or part, of the port facility or specific ships

Verifying the inventory of dangerous goods and hazardous substances held within the port facility and their location

10.5.8.4 Monitoring the security of the port facility

Hamnorganisationen ska ha resurser för att övervaka området, anslutande områden (såväl land som vatten), fartyg och områden omslutande fartyg oberoende av väderförhållande och tid på dygnet. Övervakningen kan innefatta användande av; belysningssystem, säkerhetsvakter, kameraövervakning, larm m.m.

För respektive säkerhetsnivå kan gälla enligt hamnens skyddplan;

Security level 1

Observe access points, barriers and restricted areas

Allow port facility security personnel to monitor areas and movements adjacent to ships using the port facility, including augmentation of lighting provided by the ship itself

Security level 2

Increasing the coverage and intensity of lightning and surveillance equipment, including the provision of additional lightning and surveillance coverage

Assigning additional security personnel to monitor and patrol

Security level 3

Switching on all lightning within, or illuminating the vicinity of the port facility

Switching on all surveillance equipment capable of recording activities within, or adjacent to, the port facility

Maximizing the length of time such surveillance equipment can continue to record

10.5.9 Förmåner

ISPS-koden är ett obligatorium för de fartyg, rederier och hamnar som har sin verksamhet i en nation som är ansluten till IMO. Inga direkta förmåner finns därmed inte med koppling till ett godkännande enligt koden.

Däremot anser, enligt en rapport från UNCTAD, en majoritet av de tillfrågade hamnkontoren att ISPS-koden haft en övergripande positiv effekt på verksamheten[68] framförallt gällande;

ökat riskmedvetande, effektivisering av processer, standardiserad riskbedömning och en generell förbättring av verksamhetsutövandet.

För många hamnar har uppfyllande av ISPS-koden krävt antagande av nya och ytterligare rutiner (div. säkerhetsprocesser) men kodens krav har trots detta mötts utan större problem.

[68] United Nations Conference on Trade and Development, *Maritime Security: ISPS Code Implementation, Costs and Related Financing*, 2007

11 Utvärdering av olika säkerhetsinitiativ

AEO, C-TPAT, TAPA, ISPS och ISO är de säkerhetsinitiativ som valts för den mer ingående beskrivningen i denna fas 3. Kraven för certifiering är i de beskrivna initiativen omfattande och på grund av det har bara utvalda exempel på kriterier presenterats. Följande är en översiktlig jämförelse mellan de utvalda säkerhetsinitiativen.

Den första jämförelsetabellen behandlar generella egenskaper såsom; initiativtagare, vilket säkerhetshot som primärt ska förebyggas, vilka transportslag som berörs. I den andra jämförelsetabellen jämförs de ingående kriterierna för certifiering. Eftersom formuleringarna och den exakta innebörden av certifieringskraven säkerhetsinitiativen emellan inte är lika har dessa formulerats något mer generellt vilket därigenom möjliggör jämförelse.

11.1 Jämförelse mellan utvalda säkerhetsinitiativ

11.1.1 Generell jämförelse

	AEO	C-TPAT	TAPA	ISPS*	ISO
Allmänt om certifiering					
Erhållande av direkta förmåner i tullhantering	x				
Tillgänglig för aktörer globalt	x	x	x	x	x
Statlig eller överstatlig initiativtagare	x	x			
Inriktning på gods					
Globalt gods			x	x	x
Import till USA		x			
Import och export EU	x				
Säkerhetshot som primärt ska förebyggas					
Terrorism	x	x		x	x
Stöld	x		x		
Smuggling	x			x	x
Trafficking	x				
Transportslag					
Lastbilstransporter	x	x	x		x
Tåg	x	x			x
Flyg	x	x			x
Fartyg	x	x		x	x
Kopplingar till utvalda initiativ					
AEO			x		x
C-TPAT					
TAPA	x				
ISPS					

11.1.2 Jämförelse av kriterier[69]

	AEO	C-TPAT	TAPA	ISPS*	ISO
Lokaler och områden					
Skydd av lokaler (perimetersäkerhet såsom stängsel, lås osv.)	x	x	x	x	x
Övervakning av lokaler (exempelvis kameraövervakning)		x	x	x	x
Bemanning eller bevakning av olåsta portar och accesspunkter till område	x	x	x	x	
Tillträdeskontroll	x	x	x	x	x
Godshantering					
Användande av tekniska lösningar för att hindra olovligt handhavande av gods (användning av högsäkerhetssigill, utrustning för stillastående fordon m.m)		x	x	x	
Rutiner för kontroll av inkommande gods med avseende på att gods är registrerat i logistiksystemet	x	x	x	x	x
Kontroll av sigill på inkommande gods	x	x		x	x
Separat förvaring av olika typer av gods (exempelvis utländskt-, högvärdes-, farligt gods m.m.)	x	x	x		x
Användande av tekniska lösningar för att spåra/följa gods					
Kvalitétsinspektion av packning (om denna sker hos extern part)	x				x
Lastning av gods					
Övervakning under lastning av gods i lastbärare av aktörens personal	x		x		
Rutiner för hur utgående gods förseglas och hur detta kontrolleras	x				x
Kontroller över att gods som lastas matchar godsdokumentation		x	x	x	
Personal					
Rekrytering och avveckling av personal (bakgrundskontroller, intervjuer med personal som lämnar företaget osv.)	x	x	x		x
Utbildning av personal (fortlöpande utbildning i säkerhetsfrågor, riskmedvetande osv.)	x	x	x		x
Informationsspridning (intern och extern information om företagets/aktörens säkerhetsrutiner)		x		x	x
Informationssäkerhet					
Kvalitetssäkring för data och informationssystem		x			x
Skydd av affärsinformation	x	x	x		x
Informationsutbyte med tullmyndigheterna	x	x			x
Nätverk och affärssystem					
Säkerhetshanteringssystem (definierade och dokumenterade säkerhetsförfaranden, interna och externa säkerhetsrevisioner osv.)	x	x			x
Utvärderingssystem för affärspartners (leverantörer, samarbetspartners, kunder)		x	x		x
Etablering av samarbete med tullmyndigheter eller andra myndigheter som utövar gränskontroller. Förfarande för att anmäla avvikelser eller olaglig aktivitet.	x	x	x	x	x

* Skyddplanerna för fartyg och hamn kan variera med avseende på exakta krav på åtgärder.

[69] Inspiration och formuleringar lånade från Kommerskollegium, *Säkerhet i leveranskedjan: Hur påverkas handeln av det ökade antalet säkerhetsinitiativ*, 2008. Uppgifterna är kompletterade

11.1.3 Förklaring av punkter i jämförelse

Följande avsnitt ger en förklaring av vissa jämförelsekriterier. Jämförelsen säkerhetsinitiativen emellan för några av dessa punkter diskuteras vidare i *diskussion av jämförelse*.

11.1.3.1 Generell jämförelse

Erhållande av direkta förmåner i tullhanteringen behandlar frågan om en certifierad aktör erhåller någon form av konkreta lättnader i tullhanteringen det kan exempelvis vara minskat antal godskontroller.

Statlig eller överstatlig initiativtagare är exempelvis USA:s kongress eller EU parlamentet. Alternativet är en sammanslutning av nationella intressen som IMO (International Maritime Organization), ISO (International Organization för Standardization) eller en sammanslutning av privata företag med samma intressemål.

Inriktning på gods syftar på om säkerhetsinitiativet är begränsat till att gälla gods med en specifik destination eller skeppningsplats. Globalt gods har obestämd transportväg därmed inte sagt att allt gods påverkas utan bara det gods som skickas mellan två länder vilka (ett av länderna eller båda) har erkänt säkerhetsinitiativet.

Säkerhetshot som primärt ska förebyggas kan vara terrorism, stöld, smuggling och/eller trafficking. Det bör noteras att det ena kan förutsätta det andra. I fallet med terrorism så kan det mycket väl innefatta även smuggling av exempelvis WMD (Weapons of Mass Destruction). Motsvarande så innebär förebyggande av smuggling att även terroristhandlingar motverkas.

Transportslag kan vara; lastbils-, tåg, flyg eller fartygstransporter. En komplett logistikkedjan innefattar emellertid oftast flera transportslag varför säkerhetsåtgärder inriktade på ett av dessa får positiva konsekvenser för säkerheten på efterföljande transportslag. Exempelvis åtföljs en sjötransport nästan alltid av transport med lastbil eller järnväg.

11.1.3.2 Jämförelse av kriterier

Skydd av lokaler är perimetersäkerhet vilket innebär skydd av område där aktör har sin verksamhet och skydd av själva byggnaderna. Det sker med exempelvis stängsel, grindar, vaktkurer med bommar, övervakning med teknisk utrustning såsom kameraövervakning, larm m.m. När det gäller ISPS-koden syftar denna till skydd av hamnområde samt skydd av fartyg.

Tillträdeskontroll är kontroll av accesspunkter (ingångar till byggnad eller ombordstigning på fartyg). Det kan ske genom kontroll av ID-kort, boardingpass, anledning till besök m.m. Kan vara digitalt inpasseringssystem.

Användande av tekniska lösningar för att hindra olovligt handhavande av gods, vilket innebär att för att förhindra kriminell manipulation av legitimt gods, använda tekniskt utrustning för att begränsa möjligheten till åtkomst av gods eller godsenhet. Exempelvis kan containers utrustas med sigill som kraftigt begränsar möjligheten att öppna en container utan att det upptäcks genom påverkat sigill vid exempelvis tullkontroll av container.

Rutiner för kontroll av inkommande gods med avseende på att gods är registrerat i logistiksystemet innebär i princip att allt inkommande gods ska vara önskat från mottagare. Med anledning av det är det därmed per automatik oftast inregistrerad i aktörens logistiksystem. Inkommande gods ska därför kontrolleras mot uppgifter på registrerat gods. Detta är givetvis av yttersta vikt för aktörer inom vidaretransport av gods såsom hamnar där inkommande gods skickas för vidare transport på exempelvis fartyg.

Kontroll av sigill på inkommande gods ska ske för att säkerställa att gods inte har manipulerats under transporten. Den legitima godsenheten kan ha använts för transport av illegitimt gods eller eventuellt ha utsatts för stöld.

Separat förvaring av olika typer av gods innebär att gods med högt värde eller farligt gods ska förvaras separerat från ”vanligt gods”. Detta för att bättre kunna kontrollera tillgången till godset och därmed kunna garantera högre säkerhetsnivå.

Användande av tekniska lösningar för att spåra/följa gods kan exempelvis vara smarta containers (se exempelvis säkerhetsinitiativet SECCONDD i fas 2) där berörda parter kan göra icke visuella kontroller under containerns transportväg. Det ska också vara möjligt att kontrollera aktuell position, vart container varit och vart den är på väg.

Kvalitétsinspektion av packning innebär att godsets packning ska kontrolleras om denna utförts hos en extern leverantör som inte är certifierad enligt aktuellt säkerhetsinitiativ.

Övervakning under lastning av gods i lastbärare av aktörens personal innebär att den certifierade aktörens personal (chaufför som tillhör den certifierade aktören) ska bevaka lastning av gods i lastbärare om detta är möjligt under givna omständigheter.

Rutiner för hur utgående gods förseglas och hur detta kontrolleras i processen att packa och skicka gods. Det ska kontrolleras att exempelvis godsenheterna är förseglade på korrekt sätt och med godkända sigill men framförallt att det görs.

Kontroller över att gods som lastas matchar godsdokumentation innebär att kontroll ska ske så att korrekt gods skickas iväg. Kan annars förutom leveransförseningar medföra problem i tullhanteringen.

Rekrytering och avveckling av personal ska ske enligt bestämda processer som bland annat bör involvera bakgrundskontroll avseende brottsligt förflutet, kontakt med kriminella nätverk osv. i den mån det är möjligt (med tanke på nationella regler).

Utbildning av personal innebär att aktörens personal ska erhålla relevant utbildning i säkerhetsfrågor gällande exempelvis hot mot företagets verksamhet, allmänt riskmedvetande och hur eventuella incidenter ska hanteras.

Informationsspridning ska ske internt och externt till aktörens samarbetspartners om bland annat vilka säkerhetsrutiner som ska följas.

Kvalitetssäkring för data och informationssystem innebär att lagring av fullständig data om försändelser ska ske, införande av felfria dokumentationsprocesser m.m.

Skydd av affärsinformation innebär förfaranden för lagring och handhavande av data som förhindrar obehörigt tillträde och användning.

Informationsutbyte med tullmyndigheterna innefattar; att komplett och korrekt information ska kunna ges inom önskad tid till myndigheter när så begärs, att förhandsanmälansreglerna följs osv.

Säkerhetshanteringen avser hanteringen exempelvis till godset hörande tulldokument. Processerna för att hantera informationen ska vara väl definierade och dokumenterade och dess efterlevnad ska garanteras. Det kan bland annat ske genom interna och externa säkerhetsrevisioner.

Utvärderingssystem för affärspartners innebär att logistikkedjans säkerhet ska garanteras även när det gäller den certifierade aktörens affärspartners. Exempelvis kan en godsenhet paketeras hos en extern samarbetspartners och skickas till kund. Säkerhetsrutinerna hos affärspartnern måste hålla samma nivå som för den certifierade aktören.

Etablering av samarbete med tullmyndigheter eller andra myndigheter som utövar gränskontroller innebär att den certifierade aktören förutom att uppfylla krav gällande tullhanteringen dessutom exempelvis anmäler misstänkt kriminell aktivitet även om denna inte drabbar aktören själva.

11.1.4 Diskussion om generell jämförelse

Allmänt om certifiering
I jämförelse mellan AEO och ISO angående vad respektive standard har för avsikt att uppnå med certifiering, är det viktigt att poängtera från vilken grund standarderna har byggts upp. Olika standarder har olika utgångspunkter och detta medför att åtgärder prioriteras olika beroende på standardens syfte.

AEO är den europeiska gemenskapens åtgärdspaket för att öka säkerheten i transportkedjan och förenklad tullhantering utgör ett av standardens grundläggande mål. Anledningen till detta hör samman med att det är Europaparlamentet och nationella tullmyndigheter som är initiativtagare, där förenkling innebär att statliga resurser kan koncentreras till gods med ökad hotbild istället för att avsättas till fler godstransportkontroller. Huruvida ett certifierande verkligen leder till förenklad tullhantering bör dock ställas i relation till det merarbete som certifieringen innebär. Enligt standarden så kan gods som är kvalitetssäkrat undvika kontroll men samtidigt måste mer uppgifter angående godset lämnas in till aktuellt Tullverk, arbetsbesparingen i sin helhet skulle därför kunna ifrågasättas. Denna problematik föreligger inte inom certifiering enligt ISO 28000, då denna standard inte prioriterat några åtgärder för att effektivisera och förenkla tullhanteringen.

Certifiering enligt AEO sker efter att en utförlig ansökningshandling har inskickats och godkänts av Tullverket medan certifieringen enligt ISO 28000 kan utfärdas efter att en utvärdering av verksamheten genomförts och godkänts av auktoriserad ISO-handläggare. Både AEO och ISO standarderna är globalt tillgängliga för de aktörer som väljer att uppfylla kraven för respektive standard.

Inriktning på gods
En inskränkning som kan ha betydande inverkan i möjligheten för en standard att få god genomslagskraft är de globala begränsningar som i förekommande fall görs gällande. Transporter är av sin natur förknippade med förflyttningar och detta medför att en lastbärare bör ha internationell rörlighet för att kunna transporteras effektivt mellan länder, utan orimlig arbetsinsats. I detta perspektiv kan det spekuleras i huruvida standarder som inte är kompatibla på globala transporter, inskränker möjligheten till att bli erkända i större omfattning. Detta gäller framförallt AEO vars utgångspunkt är att endast transporter som importeras och exporteras till och från EU är tillämpbara för certifiering enligt AEO. Denna begränsning föreligger inte avseende ISO 28000, där certifiering kan ske av alla globala transporter oberoende av något enskilt kontinentalintresse. Det ska dock påpekas att AEO är harmoniserad med både WCO-SAFE samt ISO 28000, vilket i praktiken innebär att inskränkningen i tillämpbarhet kan anses vara av mer marginell karaktär än för standarden som enskilt objekt.

Varje standardinitiativ har sina respektive för- och nackdelar och det kan därför vara svårt att utesluta en standard enbart på grund av särskilda begränsningar, likt den globala tillämpbarheten. I vissa fall kan det även vara så att något val inte är aktuellt till följd av att en standard är tvingande och på så vis inte möjlig att förhandla bort. Detta är exempelvis fallet med C-TPAT och ISPS, där varje transport i det första fallet ska uppfylla de kriterier som USA ställer avseende import samt att varje transport i det senare fallet ska uppfylla de kriterier som gäller för hamnverksamhet och transport med fartyg. Uppfyller transporterna inte dessa kriterier så ges per automatik inget tillträde till endera restriktionsområdet. På samma sätt är restriktioner för transporter som sker i enlighet med AEO samt ISO 28000, endast gällande om ett frivilligt beslut tagits om att standardinitiativen ska tillämpas på transporten, detta utgör därför inget tvingande åtagande gentemot transportören.

Säkerhetshot som primärt ska förebyggas
Standardiseringsprocesser på global nivå bedrivs oftast av privata organisationer där bakgrunden till standarden till stor del beror på de intressen som organisationen företräder. Det förekommer dock att initiativ till upprättande av en ny standard tas genom statligt engagemang, där drivkraften i dessa fall kan skilja sig mot kraften som driver de privata organisationerna. I fråga om säkerhet innebär detta att olika aktörer kan värna om olika skyddsintressen och för att förstå förhållandet mellan uttrycklig åtgärd i standarden och bakomliggande orsak, bör initiativtagarnas inbördes avsikter iakttas.

I en jämförelse mellan AEO och ISO 28000, i avseende att klargöra vilka säkerhetshot som har prioriterats för respektive standard, förefaller det naturligt att den statliga drivkraften i AEO är att skydda de nationella intressena mot terrorism, smuggling och trafficking. Med hjälp av AEO-certifierade transporter blir det lättare att kontrollera de

skyddsintressen som nationella stater har i att minska oron och kriminaliteten i samhället. Vad som dock ska noteras är att åtgärder mot terrorism och smuggling även beaktas av ISO 28000, trots att ingen statlig funktion är inblandad. Liknande företeelse görs inte gällande i TAPA där huvudsyftet är att prioritera åtgärder mot förekomsten av stöld, vilket med stor sannolikhet beror på initiativtagarna bakom standarden som består av representanter för gods- och transportägarna. Det är därför inte förvånande att åtgärder mot terrorism inte görs gällande då intresset av att göra godset mindre stöldbegärligt är högre än intresset att försöka minska risken för genomförandet av en terroristhandling.

Transportslag
Transporter blir alltmer internationella och för att tillgodose de olika transportslagens respektive fördelar har intermodala transporter blivit allt vanligare. Dessa transporter kräver dock att den lastbärare som används ska ha förmågan att på ett effektivt sätt omlastas mellan de olika transportmedlen. Containern är i detta sammanhang en av de mest tillämpbara lastbärarna.

Även om en lastbärare har fysisk förmåga att ingå i det intermodala flödet kan standardinitiativ som endast förhåller sig till ett transportslag medföra konsekvenser då en intermodal transportkedja ska konstrueras. Detta är fallet då ISPS, via sin tvingande funktion, framkallar ett minimikrav som andra ej tvingande standarder måste uppfylla för att på så sätt ej emotsätta sig den tvingande regleringen. Eftersom både AEO och ISO 28000 uppfyller kraven för fartygstransporter så måste således ISPS vara speglad i dessa standarder, därtill finns inga hinder för att ytterligare utöka säkerhetskriterierna för dessa transporter. Problemet med reglering av den här karaktären uppstår dock i fall då ett nytt tvingande initiativ kommer till stånd och som ställer orimligt högre krav än vad motsvarande standarder har angivit i sina kriteriegrunder. I dessa fall måste en genomgripande anpassning ske för alla initiativ som ej uppfyller dessa krav, på så sätt kan en länk i kedjan påverka säkerhetskriteriet för hela transportkedjan.

Både AEO och ISO 28000 uppfyller kraven för samtliga fyra huvudtransportslag och i sin helhet innebär detta god täckningsförmåga avseende möjlighet till global och intermodal tillämpning. Det kan dock förekomma att skillnader mellan standarderna görs gällande på en mer detaljerad nivå och en vidare jämförelse kring detta kräver en alltför djupgående analys, varför detta därför lämnas utan avseende.

11.1.5 Diskussion om jämförelse av kriterier

Lokaler och områden
En av de viktigaste och mest betydelsefulla åtgärder som kan vidtas för att minska risken för otillbörligt tillträde till områden som ska säkras, är att bygga upp fysiska hinder som försvårar tillgängligheten för utomstående. Denna åtgärd motverkar alla säkerhetshot som presenterats i denna rapport men utgör ingen definitiv säkerhetslösning, varför fysiska hinder därför ska tillämpas i kombination med annat säkerhetsarbete.

Med hänsyn till att fysiskt skydd utgör en primär åtgärd för att minska säkerhetshoten, är det inte förvånande att samtliga standarder som valts för jämförelse i denna delfas prioriterar arbete som fokuserar på det fysiska skyddet. Till detta hör även att tillträdespunkter till det område som täcks av säkerhetsbestämmelser, måste tillämpa kontroll över de personer som passerar dessa punkter för att därmed bekräfta om dessa är behöriga att beträda området eller ej. Dessa två faktorer är tätt sammankopplade och de bör därför tillämpas i samverkan med varandra för att inte riskera att säkerhetsluckor byggs upp inom befintliga säkerhetslösningar.

Ett grundproblem i allt arbete som görs för att tillgodose en god säkerhetsnivå är att det alltid är svårt att förutsäga vilka säkerhetsrisker som den egna personalen står för. Andelen insiderbrott är relativt hög och därför inte en försumbar del av de hot som en aktör kan utsättas för. Det är därför viktigt att åtgärder även riktas mot att förebygga risker inom den egna organisationen. En sådan åtgärd kan vara att övervaka de aktiviteter som sker inom den aktuella verksamheten, för att på så sätt upptäcka misstänkta säkerhetsöverträdelser. Bakgrunden till detta är att personer som är behöriga att få tillträde till det aktuella säkerhetsområdet per automatik inte nekas tillträde, varvid det kan vara svårt att kontrollera om denna behöriga person medvetet åsidosätter gällande regler som faller inom eller utom ramen för sin befogenhet. En kontrollfunktion kan med god effektivitet utföras med hjälp av kameraövervakning och en sådan ständig kontroll kan fungera i preventivt syfte samtidigt som funktionen kan vara reparativ i fall då det ska fastslås hur överträdelsen kunde genomföras. Det kan därför i sammanhanget noteras att AEO saknar denna funktion samtidigt som övriga standarder presenterade i denna rapport prioriterar denna åtgärd.

Godshantering
Investeringar i att utveckla och underhålla säkerhetssystem kan många gånger vara kostsamma, samtidigt kräver olika typer av gods olika nivåer av säkerhetsarrangemang. Gods med högt värde kan i detta sammanhang vara mer attraktivt för stöld än gods med lågt värde, varvid säkerheten kring det förstnämnda troligen kräver ett bättre skydd än för det sistnämnda. Genom att selektera gods utefter denna princip så kan säkerhetsnivån anpassas till rådande förhållande, vilket också möjliggör kostnadsbesparingar. Denna metod är inte enbart tillämplig för kategorisering efter godsvärde då även andra aspekter kan ligga till grund för säkerhetsbedömningen, till dessa aspekter hör bl.a. skyddet kring farligt respektive ofarligt gods. Metoden är relativt välrepresenterad bland standarderna som behandlats i denna rapport.

Vad gäller risken för terroristaktiviteter så är denna att betrakta som relativt låg om flödet av certifierade lastbärare ligger till grund för bedömningen kring godshanteringen. Att lastbärare som lastats på ett säkerhetsfullvärdigt sätt med efterföljande plombering och kontroll vid ankomst, skulle vara manipulerade för användning i en terroristaktion, är inte sannolikt. Detta gäller under förutsättning att varje enskilt säkerhetsmoment genomförs enligt gällande regelverk, så att inga säkerhetsluckor uppstår. Risken för terroristaktiviteter inom transportkedjan är däremot desto större om lastbärare som inte ska ingå i transportflödet ändå lyckas etablera sig inom densamma. Okända lastbärare av den här karaktären måste identifieras i ett tidigt skede för att på så sätt kunna fastställa innehåll och vem som är ansvarig för enheten. Denna identifikation bör göras genom att det enbart är gods som överensstämmer med registrerade enheter i logistiksystemen, som ges tillträde till området, och där övriga enheter förbjuds fortsatt transport för att istället genomgå en grundlig undersökning. Detta är en ytterst primär åtgärd för att minska risken för att oidentifierat gods ska kunna få tillträde till transportkedjan, vilket följs av att metoden används av samtliga standarder i denna del.

Lastning av gods
Oavsett hur säkerhetsarrangemangen är utformade i syfte att motverka hotet mot den egna verksamheten så är det vid hanteringen av gods och lastbärare som den kritiska punkten uppstår för när en hotbild mot transportkedjan kan införlivas. En lastbärare som prepareras eller utsätts för en handling som strider mot de säkerhetsregler som gällande standard föreskriver, och som ej upptäcks, blir genom standardens lättnadsfördelar svår att identifiera i ett senare skede efter att lastbäraren förslutits och lämnat avsändaren.

Det är anmärkningsvärt att AEO inte har rutiner för att kontrollera att det gods som lastats i en sedermera förseglad lastbärare, överensstämmer med den godsspecifikation som blivit deklarerad i godsmanifestet. Detta med anledning av att standarden bl.a. har till syfte att minska risken för stöld och där en kontrollfunktion mot manifestet med största sannolikhet hade fått genomslag i arbetet med att försöka upprätthålla denna målsättning. Det framgår samtidigt att standarden ålägger en viss del av denna kontrollfunktion på aktörens personal, som därmed ska övervaka lastningen och därtill meddela om oegentligheter förekommer. Bristen med ett sådant upplägg, utan att använda ytterligare säkerhetsnivåer med tillsyn över kontrollfunktionen, är att systemet blir utsatt för risken att aktören själv medverkar till att bryta mot regelverket, risken för insiderbrott ökar. Tillsyn över kontrollfunktionen verkställs i praktiken endast genom TAPA, som därmed tar ytterligare steg mot att öka säkerheten.

Både AEO och ISO har skapat reglering kring hur lastbäraren ska säkras och förseglas efter det att godset har lastats ombord. Detta är samtidigt den enda kontrollfunktion som ISO tillhandahåller vid godshanteringen och det kan därför spekuleras i att standarden till stor del litar på de säkerhetsåtgärder som i övrigt har vidtagits hos avsändaren, och att någon ytterligare funktion därför ej är nödvändig för att minska otillbörligt handlande vid lastningen. Det ska samtidigt påpekas att ISO inte har för avsikt att förebygga stöld i den omfattning som både AEO och TAPA föreskriver. AEO och ISO beaktar dock risken för att lastbäraren manipuleras efter utleverans hos avsändaren och det finns därför rutiner för hur lastbärarens intakthet ska kontrolleras hos mottagaren.

Personal
Alla säkerhetsstandarder bygger i varierad utsträckning på att ett förtroende ges till dem som har till uppgift att upprätthålla säkerheten. Detta följer av problematiken att det annars skulle vara svårt att fullfölja de uppgifter som ett företag har åtagit sig gentemot kund, då vissa arbetsmoment i förekommande fall kan behöva utföras av en människa. Risken finns dock alltid för att en person brister i sitt förtroende, vilket kan få till följd att ett säkerhetshot realiseras. I förebyggande syfte finns det därför särskilda principer för hur personalsäkerheten ska hanteras, vilket regleras i varierad utsträckning under varje gällande standard.

Den mest primära åtgärd som bör vidtas för att minimera risken för att anställd personal bryter mot de säkerhetsregler som en arbetsplats har vidtagit, är att genomföra en grundlig personanalys av de kandidater som ingår i en eventuell rekryteringsprocess. Genom att undvika att anställa personer som uppvisar tendens till att vara olämpliga för att förvalta förtroende på ett ansvarsfullt sätt, har en grund lagts till att med tiden också kunna införa ett mer utvecklat säkerhetsarbete. Ett annat problem som är kopplat till personalsäkerheten är den brist på kompetens som kan förekomma i fall då otillräckliga resurser har lagts på utbildning. En sådan brist kan exempelvis uppkomma om en nyanställd person inte får den introduktionskurs som krävs för att kunna förstå företagets säkerhetsarbete och den anställdes förpliktelser, eller om företaget brister i den fortlöpande utbildningen kring nya rutiner och säkerhetshot som påverkar verksamheten.

I många standardinitiativ utgår man från en förutbestämd rutin som påverkas först om en ändring eller komplettering införs till de redan existerande bestämmelserna. Det förekommer dock i vissa standarder, däribland ISPS, att förutbestämda rutiner tillämpas först när omständigheterna ändras i sådan omfattning att högre alternativt lägre säkerhetsåtgärder måste eller bör vidtas. När olika säkerhetsrutiner gäller för skilda situationer är det viktigt att information om ändrad säkerhetsstatus förmedlas till de personer/aktörer som ska anpassa åtgärderna efter gällande rutin. Detta kan ske både internt och externt. Kravet på god informationsspridning är som mest relevant i standarder som ska förebygga terrorism då hotbilden för angrepp av denna karaktär oftast är oförutsägbar, vilket därav kräver snabba insatser.

Informationssäkerhet
Säkerhetsarbete bygger till viss del på att skapa osäkerhet hos den som planerar att genomföra en oärlig handling, vilket i förekommande fall också kan utgöras av kriminell verksamhet. Osäkerhet kring vilka åtgärder som inkräktaren kan komma att behöva möta till följd av handlingen innebär således ett övertag för den som vidtagit åtgärderna. Detta kan exempelvis vara fallet då en övervakningskamera fångar upp en bildsekvens utan att personen som förekommer på inspelningen är medveten om detta. En sådan ovisshet och omedvetenhet kan både verka i förebyggande syfte genom att avskräcka personen från att begå handlingen, alternativt utgöra bevismaterial om handlingen trots detta ändå utförs. Med bakgrund av detta är det därför av stor betydelse att information kring vilka säkerhetssystem som används samt hur dessa fungerar, inte ska kunna användas av obehöriga.

Utöver behovet av att säkerställa skyddet kring information om verksamma säkerhetssystem är det också viktigt att andra informationskällor säkras mot

otillbörligt utnyttjande. Till sådan information hör exempelvis uppgifter som är kopplade till den affärsmässiga delen av företagets verksamhet, där information om företagets kundrelationer kan utgöra ett sådant exempel. Eftersom uppgifter av denna karaktär skulle kunna utnyttjas i samband med en kriminell handling, däribland smuggling, är det inte enbart av vikt för företaget att sådana uppgifter förvaras åtskilda från obehöriga. Informationsspridning kan komma att underlätta genomförandet av kriminella handlingar och med bakgrund av det så är åtgärder för att förhindra sådan spridning, prioriterade av flertalet standarder.

Att den information som avsändaren har lämnat till transportören ska vara den information som presenteras när godset levereras till mottagaren, är också av stor betydelse. För att kunna säkerställa tillförlitligheten i detta informationsflöde är det viktigt att hanteringen av information är kvalitetssäkrad enligt vad respektive standard föreskriver. Det är dock anmärkningsvärt att det endast är ISO och C-TPAT som har prioriterade åtgärder för hur denna kvalitetssäkring ska genomföras.

Nätverk och affärssystem
Till transportkedjan är många aktörer knutna och i fråga om säkerhetsarbete så är det den gemensamma säkerhetsnivån som avgör hur säkert ett transportflöde i realiteten är. Detta kan beskrivas som beroendet till den del som utgör den svagaste länken, där säkerheten aldrig kan bli högre än vad som motsvarar denna lägstanivå. Att kontrollera och utvärdera den gemensamma säkerhetsnivån är därför betydande när det gäller att identifiera säkerhetsluckor, vilka i annat fall kan bli föremål som inkörsport till aktiviteter som i övrigt ska täckas av åtgärderna i respektive standard. Denna grundprincip kan antas utgöra en primär åtgärd för att förebygga skyddsintrång och det ska därför tas i beaktande att exempelvis AEO inte prioriterar detta arbete. I denna situation måste AEO ha en tilltro till att de aktörer som är knutna till transportkedjan också uppfyller sina åtaganden, utan att något formellt system finns för att utvärdera den övergripande säkerhetsnivån mellan aktörerna.

FAS 4 – Avslutande rekommendationer och slutsatser

12 Rekommendationer av olika säkerhetsinitiativ

Säkerhetsbranschen har under de senaste åren expanderat kraftigt vad gäller utvecklingsarbetet kring nya säkerhetsstandarder. Detta har till stor del följts av den förändrade hotbild som världen har skådat alltsedan terroristattackerna mot USA den 11:e september 2001, vilket skapat underlag för både affärsmässiga och statliga säkerhetsinitiativ. Problematiken med denna utveckling kan dock anses bestå i bristen av samverkan, vilket skapar svårigheter i fall då flera transportslag ska bidra till bildandet av en komplett transportkedja. Detta kan i förekommande fall leda till att helhetsbilden kring den samlade säkerhetsbilden längs kedjan blir svårare att förutse, vilket beror på konsekvensen av att enskilda aktörer kan behöva särskild certifiering enbart för att täcka säkerhetsriskerna inom dennes verksamhet.

Eftersom säkerhetsnivån kan skilja mellan olika verksamheter inom transportkedjan, men där den gemensamma länken är flödet av transporter, medför nivåskillnader att hela kedjan kan påverkas. På detta sätt kan en transportbärare tvingas att anpassa säkerhetstillämpningarna efter den del av kedjan som kräver de största åtgärderna. Förberedelser inför detta kan därför komma att behöva göras redan i det skede då transportbäraren lämnar avsändaren, något som kräver god tillförlitlighet i de informationsflöden som sker mellan de olika aktörerna.

12.1 Sammanställning över transportkedjans olika aktörer

För att klargöra hur transportkedjan påverkas genom införandet av olika standarder måste en sammanställning över de olika aktörerna genomföras. Detta är en viktig del i arbetet med att finna effektiva lösningar som kan minska risken för överdimensionering och därigenom kostnadsbilden för säkerhetssystemet.

12.1.1 Avsändare

Det är hos avsändaren som den största säkerhetsrisken föreligger eftersom gods ofta packas på ett sådant sätt att en kontroll av godsinnehåll kan bli svår att genomföra i ett senare skede. En godsenhet, exempelvis en container, lastas från bakre väggen och ut mot dörrarna med minsta möjliga fria utrymme. Detta medför att transportkostnaden minskar samt att en kompakt packning är att föredra utifrån lastsäkringssynpunkt, genom minskat antal godsskador.

Illegitimt gods som lastas i en legitim transportenhet från en av tullmyndigheterna erkänd aktör löper mycket liten risk att upptäckas. Därför är det av högsta vikt att ett sådant scenario undviks, vilket enklast görs genom att i så stor utsträckning som möjligt garantera säkerheten hos avsändaren alternativt den samarbetsaktör som utför packningen.

Vid packningen krävs försäkran om att gods som packas inte har manipulerats, vilket kan vara mycket svårt. Sådan kontroll utförs genom visuell undersökning av godsets intakthet men också med hjälp av godsdeklarationen, det vill säga dokumentet som fastställer om godset stämmer överens med fraktsedeln/deklarationen eller ej. Vad som anses utgöra intakt gods följer av överensstämmelse avseende vikt, volym, mått, och godsets beskaffenhet och dessa krav är särskilt betonade i C-TPAT, TAPA och ISPS.

På många industrier sker packning och lastning av gods utav en extern part samtidigt som annan aktör ansvarar för själva transporten. I dessa fall utgör själva lastningen ett riskmoment då illegitimt gods kan sammanblandas med gods som är legitimt. Godset måste därför kontrolleras med avseende på hur det överensstämmer med dokumentationen och personal från den certifierade transportören måste därför övervaka lastningen i den mån det är möjligt. Dessa krav återfinns i AEO samt TAPA.

Vid slutförd lastning, av extern part eller transportören själv, måste transportenheten förseglas under kontrollerade former. Detta för att säkerställa att enheten inte öppnas eller riskerar manipulation innan den nått fram till mottagaren, alternativt under legitim kontroll av tullmyndighet. Försegling sker med hjälp av högsäkerhetssigill och rutiner för hur detta ska ske samt hur kontroll ska utföras, framgår genom kriterier i både AEO och ISO 28000.

Den personal som utför nämnda moment måste vara kontrollerad med avseende på kriminellt förflutet, aktuella kontakter med kriminella nätverk och liknande företeelser (krav i AEO, C-TPAT, TAPA, ISO 28000). I annat fall är risken att dessa personer utnyttjar sin position i syfte att smuggla illegitimt gods i legitima godsenheter. Skulle så ske är sannolikheten för upptäckt mycket liten eftersom alla säkerhetsrutiner utåt sett kan anses vara uppfyllda.

12.1.2 Terminaler

I detta avsnitt redovisas de fyra ”terminallänkarna” inom den intermodala transportkedjan tillsammans eftersom de besitter liknande förhållanden och förutsättningar. De fyra länkarna är:

- Landsvägterminal (typ Schenker)
- Kombiterminal (typ CargoNet)
- Järnvägsterminal (typ Green Cargo)
- Hamnterminal (typ Göteborg Hamn)

Terminaler kan i dess helhet jämföras med förutsättningarna som gäller för avsändaren, med undantaget att ökad informationssäkerhet troligen skulle bidra till en bättre säkerhetsmiljö. Enligt en uppskattning som polisen har genomfört i projektfas 1 är minst 30% av brotten insiderrelaterade.

I de flesta fall hanteras externt gods på terminalerna samtidigt som både intern och extern personal uppenbarar sig på terminalområdet. Detta ställer ofta höga krav på tillträdeskontroll, övervakning, bevakning och skydd av lokaler och område. Dessa krav återfinns i varierad omfattning i samtliga säkerhetsinitiativ. Här återfinns bland annat renodlade och fysiska säkerhetsinvesteringarna såsom staket, lås, larm, bevakning och kameraövervakning. Dessa investeringar ger god brottspreventiv effekt och verkar som motivationssänkare av en potentiell gärningsman. Statistiken från fas 1 påvisar dock att det är i de terminalnära skedena som de flesta säkerhetshoten uppstår, det vill säga just innan eller just efter godset har varit på en terminal. Sker mellanlagring, ompackning och/eller omlastning av gods till nya lastbärare ställs i princip samma krav på godshantering och lastning av gods som för avsändare.

Den interna personalen på den terminal som hanterar godset måste vara kontrollerad med avseende på kriminellt förflutet, aktuella kontakter med kriminella nätverk och liknande (krav i AEO, C-TPAT, TAPA, ISO 28000). Då andelen extern personal troligtvis är högre än hos exempelvis en avsändare gäller dock för den interna personalen att vara informerad och observant på att inget illegitimt gods hamnar i legitima godsenheter. I projektets fas 1 konstaterades det att personal med stärkt status kan ge god effekt på säkerheten. Tanken är att ”Trivs jag på arbetet och är stolt över min arbetsgivare är jag i allra högsta grad med och skyddar detsamma”.

Det är inte enbart den fysiska hanteringen av gods som åläggs krav, den administrativa hanteringen av dokument och information är också viktig för att försvåra att gods eller lastbärare manipuleras. En metod för att öka säkerheten i denna del är att kvalitetssäkra data och informationssystem, vilket krävs i C-TPAT och ISO 28000, och/eller skydda affärsinformation, krav enligt AEO, C-TPAT, TAPA, ISO 28000, vilka gemensamt kan bidra till att ingen otillbörligen kommer över information om godset eller aktuell lastbärare.

12.1.3 Landtransporter

I detta avsnitt redovisas de tre ”transportlänkarna” inom den intermodala transportkedjan på land tillsammans eftersom de besitter liknande förhållanden och förutsättningar. De tre länkarna är:

- Landsvägtransport (Distribution/Fjärrtransport)
- Kombitransport
- Järnvägstransport

I fas 1 konstaterades det att för hot som uppkommer till följd av transportarbete finns det många åtgärder att vidta. Framförallt påvisas det i polisens statistik att 81 % av brotten är riktade mot oskyddade transporter, kapellskärning alternativt stöld ur olåst trailer/lastbil. Problemen inträffar oavsett om det som avses är antingen väg- eller järnvägstransport, där problemen kan översättas till situationer då godset står still, befinner sig på ett stickspår eller en rastplats utefter ett vägstråk. Således skulle ett fysiskt skydd av lastbärare utgöra ett effektivt skydd för att minska riskerna i denna del av transportkedjan. Krav på exempelvis högsäkerhetssigill, utrustning för stillastående fordon, spårutrustning för gods samt lastbärare eller liknande, återfinns i C-TPAT, TAPA (endast landsväg) samt till viss del även i ISPS (endast gods som ska eller har transporterats på sjön). Beräkningar i fas 1 påvisar att låsta/skyddade lastutrymmen i sammanhanget inte är oskäligt kostsamma.

Att illegitimt gods placeras i legitima lastbärare utgör en risk även under landtransporter, men risken får trots detta anses som relativt låg. Dock gäller samma krav som för avsändare samt terminalhantering, avseende hantering av gods, rutiner kring personal samt rutiner för att hantering av data och information. Utbildning och information till medarbetare i hela kedjan är en god metod för både riskbedömningar och undvikande av kända riskområden.

12.1.4 Sjötransport

För sjötransporter har den internationella sjöfartorganisationen tagit fram säkerhetsinitiativet ISPS som ställer krav för transporter av gods till sjöss. Uppfylls kraven i ISPS uppfylls även de flesta kraven i andra initiativ såsom AEO, C-TPAT och ISO 28000. Inom ISPS åläggs stort fokus på övervakning, bevakning och tillträdeskontroll av både fartyg och hamnanläggningar. När godset väl är ombord är kraven på övervakning i regel lägre.

En viktig detalj som skiljer ISPS från de andra initiativen är att den utgår från olika skyddsnivåer utifrån vilken hotbild som föreligger gentemot fartyg respektive hamnanläggning. Ökar hotbilden så ökar samtidigt även kraven på de rutiner som ska träda i kraft för att hantera hotbilden. Sådana åtgärder anpassas därför till rådande skyddsnivå. En del som ISPS inte täcker lika väl som de andra initiativen är dock hanteringen och skydd av data och information.

Sett ur ett nationellt perspektiv är sjötransporter det område som åtnjutit mest kapital för utveckling av säkerhetsskydd (uppskattat värde per enhet) och orsaken till detta är ISPS kodens införande. I fas 1 konstaterades det samtidigt att skadekostnaderna för exempelvis stöld och skadegörelse i hamnanläggningar, är mycket låga efter dessa investeringar.

12.1.5 Mottagare

I fas 1 presenterades statistik som visade att den största risken som återfinns hos mottagaren är risken för bedrägeri och godsstöld. Således skulle ett gott skydd kunna uppnås genom utveckling av det så kallade logiska skyddet, det vill säga fastställa att goda rutiner finns för gods- och personalhanteringen, vilka i stort ska motsvara de krav som ställs på avsändare.

Eftersom transporten redan är genomförd blir det hos mottagaren som en hotbild kan uppstå, exempelvis genom att godset i en mottagen lastbärare utgör ett hot eller en risk för mottagarens personal och/eller anläggning samt omgivning. Det är därför viktigt att kontrollera att mottaget gods överensstämmer med tillhörande fraktdokument samt att godset eller lastbäraren inte är manipulerade. Krav på rutiner för mottagningskontroll finns i samtliga aktuella säkerhetsinitiativ. I TAPA finns dock inget krav på kontroll av sigill.

12.2 Rekommendationer kring säkerhetsinitiativ i olika delar av transportkedjan

Det växande utbudet av tillgängliga säkerhetsinitiativ skapar problematiska beslutsprocesser i fall då en organisation ska genomgå certifiering för ökad säkerhet. Beslut av denna karaktär grundas ofta på kundens krav över säkerhetsinsatser som företaget måste uppfylla för att affärsrelationen ska bestå. Förutom ekonomiska insatser krävs också stor kunskap och mycket arbete om rätt beslut ska fattas till rätt kostnad. Det är samtidigt inte möjligt att ge generella riktlinjer för vilka standarder som är tillämpliga för respektive aktör i transportkedjan. Detta är en unik frågeställning som i hög grad beror på de förutsättningar som är aktuella i varje enskilt fall. Trots detta så kan man dock urskilja vissa kriterier som kan utgöra en bas för beslutsfattande, där en sådan grund kan användas som utgångspunkt till fördjupning med fokus mot mer organisationsspecifika krav. Mallen för detta innehåll presenteras i följande delavsnitt.

För att på ett enkelt sätt kunna jämföra investeringskostnaderna för respektive åtgärd i varje individuell del av transportkedjan, har nedanstående poängsystem använts baserat på de uppgifter som framgår av fas 1 ”Motåtgärder i delar av transportkedjan”. Maximal kostnad ger 6 poäng och minimal kostnad ger 0 poäng.

	Låg	**Medel**	**Hög**	
Logiskt skydd	0	1	2	
Elektroniskt skydd	0	1	2	
Fysiskt skydd	0	1	2	
Summa	**0**	**3**	**6**	**Poäng**

12.2.1 Avsändare/mottagare

Eftersom godsets ägare både kan utgöras av den som mottar och den som avsänder gods, föreligger samma förutsättningar för mottagarens certifieringsgrund som för användarens. Det är med bakgrund av detta inte nödvändigt att särskilja vilka kriterier som är av väsentlig betydelse för respektive part och innehållet i följande avsnitt kan därför användas gemensamt trots att beskrivningen utgår från avsändaren.

Avsändaren representeras i de flesta fall av den aktör som initierar ett transportflöde, dvs. från punkten där transportarbetet inleds. Beroende på var i värdekedjan (produktens förädlingsgrad) som transporten ska utföras så innebär detta att avsändaren kan anta olika karaktärer. En basindustri som utvinner metaller för fortsatt förädling är i detta perspektiv i regel den första avsändaren i leveranskedjan medan en återförsäljare av personbilar till konsumenter är avsändare som tillhör den övre delen av samma värdekedja. Att fastställa avsändarens plats i värdekedjan kan vara en primär åtgärd att vidta för att bedöma vilka risker som är förknippade med den specifika organisationen. I sammanhanget kan kategorisering mellan hög- och lågvärdigt gods därför ha en avgörande betydelse för bedömningen kring hur

stöldbegärligt det aktuella godset är och därmed vilket standardinitiativ som är mest tillämpligt.

Då avsändaren i regel representeras av varuägaren, alternativt en aktör som har särskilt varuintresse, bör vikten av att säkra godset mot handlingar som avser skadegörelse och stöld betonas. Samtidigt bör all annan aktivitet som resulterar i godsskador beaktas, med hänsyn till den helhetstäckande riskbedömningen.

Enligt de resultat som framkommit i fas 1 är risken för stöld då godset befinner sig hos avsändaren, lägre än den genomsnittliga sannolikheten. Detta följer troligen av att det är svårare att fullfölja ett stöldbrott, utan att bli upptäckt, då handlingen sker i avsändarens byggnad än om motsvarande handling hade utförts vid en obevakad terminal under transport. Investeringskostnaden för att förhindra brott av den här typen är samtidigt under medelkostnaden, 2 av 6 poäng enligt nedanstående tabell, vilket bör ställas i relation till den besparing som eventuellt följer av minskad stöldfrekvens. Vad som dock är viktigt att påpeka i sammanhanget är att avsändarens godsintresse inte avtar i samband med utleverans. Eftersom avsändaren har åtagit sig att leverera en vara av bestämd kvantitet och beskaffenhet, föreligger också ett intresse för att varan faktiskt blir felfritt levererad till mottagaren. Denna problematik kan i praktiken dock uttryckas på olika sätt, där det exempelvis är vanligt förekommande med skilda tillämpningar av diverse leveransvillkor (Incoterms), vilket i realiteten kan ge upphov till situationer då ansvaret för godset överlämnas till mottagaren redan då godset lämnat avsändaren. Oavsett hur parterna har utformat denna uppgörelse kring Incoterms så kan helhetsbilden dock betraktas som ett ömsesidigt intresse för att godset ska levereras felfritt. Detta är inte minst en viktig förutsättning för att kunna upprätthålla gynnsamma och välmående affärsrelationer.

	Låg	**Medel**	**Hög**	
Logiskt skydd	0	0	0	
Elektroniskt skydd	0	1	0	
Fysiskt skydd	0	1	0	
Summa poäng	**0**	**2**	**0**	**2**

Beroende på avsändarens affärsområde så kan godsets värde ha en avgörande betydelse för hur säkerhetsarbetet i transportkedjan ska utformas. Avsändaren har dessutom ofta rollen som initiativtagare till införandet av ett helhetstäckande säkerhetsarbete längs transportlänken, baserat på det godsintresse som tidigare beskrivits. I detta perspektiv så kan avsändare som representerar högvärdigt gods ha intresse av att tillgodose säkerhetsåtgärder mot stöld och skadegörelse, från utleverans hos avsändaren tills dess att godset levererats till mottagaren. Varje enskild aktör däremellan måste i en sådan situation certifieras enligt den standard som den aktuella aktören funnit mest lämplig, vilket inskränker möjligheten att använda aktörer som saknar denna certifiering. På samma sätt så kan det ekonomiska perspektivet innebära att avsändaren inte finner någon lönsamhet i att införa ett helhetstäckande

säkerhetsarbete för lågvärdigt gods, exempelvis bulkgods, utan i stället avgränsar säkerhetsarbetet till att endast omfatta den interna organisationen.

Som utgångspunkt i bedömningen av vilket standardinitiativ som är mest tillämpligt för avsändare, används nedanstående matris över de åtgärder som är av störst betydelse för dennes verksamhet. Kriterierna är baserade på de formuleringar som används i fas 3 – ”Jämförelse mellan utvalda säkerhetsinitiativ” och matrisen behandlar endast åtgärder som minskar risken för stöld och skadegörelse (säkerhetsrisker). C-TPAT och ISPS är exkluderade med hänsyn till deras alltför nischade karaktärer.

	AEO	TAPA	ISO
Kriteriegrund			
Säkerhetshot som primärt ska förebyggas - Stöld	X	X	
Skydd av lokaler	X	X	X
Övervakning av lokaler		X	X
Bemanning och/eller bevakning accesspunkter	X	X	
Tillträdeskontroll	X	X	X
Användande av tekniska lösningar för att hindra olovligt handhavande av gods		X	
Kontroll av sigill på inkommande gods	X		X
Övervakning under lastning av gods i lastbärare av aktörens personal	X	X	
Rutiner för hur utgående gods förseglas och hur detta kontrolleras	X		X
Kontroller över att gods som lastas matchar godsdokumentationen		X	
Rekrytering och avveckling av personal	X	X	X
Utbildning av personal (fortlöpande utbildning i säkerhetsfrågor, riskmedvetande)	X	X	X
Skydd av affärsinformation	X	X	X
Sammanställning – täckning av kriterier			
Summa	**10**	**11**	**8**

Enligt tabellen framgår det att TAPA täcker flest kriterier av de säkerhetsinitiativ som blivit utvalda för denna sammanställning. Det ska samtidigt påpekas att detta resultat troligen följer av att TAPA är anpassad till de förutsättningar som gäller för aktörer som har stark koppling till varuintresset. TAPA är på så sätt ett initiativ som ska förstärka dessa aktörers möjligheter till att försvara rätten till godset och därmed minska förekomsten av bland annat stölder. Ett tydligt exempel som illustrerar detta ändamål är användningen av särskilda lösningar för att försvåra möjligheten till

intrång i aktuell lastbärare, exempelvis med hjälp av högsäkerhetssigill, vilket TAPA är ensam om. Även kontroller för matchning mellan godsdokumentation är unik för TAPA.

Trots att TAPA kan anses vara den mest lämpliga standarden för tillämpning hos avsändare ska det noteras att det även finns begränsningar som kan påverka det slutliga valet av standard. En sådan begränsning kan exempelvis vara den brist på kompabilitet som TAPA har vad gäller tillämpning på intermodala transporter. TAPA är endast utvecklad för att hantera gods som transporteras med lastbilstransporter och detta försvårar kraftigt möjligheten till global distribution och längre regional transfereringar. Det är på så sätt svårt att få effektivitet i säkerhetsarbetet om godsdistributionens karaktär innebär att ytterligare certifiering måste ske för att täcka de brister som följer om det aktuella företaget också transporterar gods i det intermodala flödet. I detta perspektiv kan det därför spekuleras i huruvida det kan bli mer ekonomiskt lönsamt att istället tillämpa AEO, då denna certifiering skulle innebära att samtliga intermodala transportslag blir tillämpbara. Nackdelen med AEO kan dock å andra sidan bestå i bristen på förstärkta åtgärder mot intrång i aktuell lastbärare, exempelvis genom utebliven tillämpning av högsäkerhetssigill. AEO är samtidigt inte tillämpbart på globalt gods men eftersom standarden har koppling till WCO utgör detta i praktiken inte något överhängande problem.

Avsändaren bör genom detta resonemang överväga att antingen införa AEO eller TAPA, beroende på vilka kriterier som väger tyngst i respektive fall. Karaktären kring avsändarens verksamhet är därför avgörande i bedömningen av vilket av dessa bägge alternativ som har bäst förutsättningar för effektiv tillämpning. Steget mot att istället införa ISO 28000 anses vara alltför stort då denna standard inte föreskriver några direkta åtgärder för att minska risken för stöld eller handling som utgör motsvarande intrång på avsändarens godsintresse.

12.2.2 Landsvägsterminal

Landsvägsterminalen har en viktig uppgift att fylla i ett fungerande och effektivt distributionsnätverk. Transporter bygger i grunden på målsättningen att alla godsflöden ska kunna transporteras mellan alla tillgängliga platser fördelade på den globala arealen. Detta innebär samtidigt att även små flöden med låg transportintäkt ska kunna distribueras mellan punkter på samma sätt som flöden vilka ger stor förtjänst till transportören. Att transportera små godsvolymer till lågt pris skulle vara ekonomiskt omöjligt om förutsättningen skulle vara att detta gods i så fall skulle kräva direkt distribution, dvs. att en transportenhet hade krävts för varje enskild försändelse. Genom att konsolidera små försändelser på en gemensam plats så löser man detta problem, vilket sker genom att gods omlastas i syfte att bygga upp en större försändelse vilket i förlängningen medger ett effektivare flöde. Detta arbete sker bland annat i landsvägsterminalen och verksamheten utgör därför en viktig länk i arbetet med att upprätthålla god säkerhet i leveranskedjan.

Landsvägsterminalen är relativt utsatt för stöldangrepp men brottsfrekvens varierar beroende på vilken typ av terminal som beaktas. Typen av terminal kan ha stor inverkan på den hotbild som ligger till grund för antagande och det är i sammanhanget viktigt att skilja mellan dessa. Exempelvis finns det terminaler som endast hanterar

matvaror medan andra terminaler omlastar gods inom ramen för den ordinarie post- och speditionsdistributionen. Terminaler som hanterar det sistnämnda är troligen mer utsatta för stöldangrepp och på så vis krävs också mer resurser för säkerhetsarbete i denna typ av terminal. Det ska också påpekas att verksamhetens storlek i många fall också kan ha en betydande inverkan eftersom hög omsättning också skapar större utrymme för större investeringar. Terminaler som bedriver småskalig verksamhet har i detta perspektiv troligen mindre möjligheter till större säkerhetsåtgärder.

Den generella sannolikheten för att stöld ska inträffa i en terminal står i paritet med den genomsnittliga riskfaktorn för angrepp och det kan därför vara av betydelse att inte åsidosätta denna hotbild. Kostnaden för att försvåra sådana angrepp är dock något högre än genomsnittet, 4 av 6 poäng enligt nedanstående tabell, och det är därför viktigt att genomföra en noggrann kartläggning över vilka system som verkligen är användbara i den specifika situationen. Problemet med godsstölder på terminalområden har samtidigt blivit större de senaste åren och det är inte ovanligt att hela ekipage blir stulna. Ökad riskfaktor bör därför tas i beaktande när nya säkerhetssystem ska utarbetas. Det ska samtidigt påpekas att terminalanställd personal inte känner lika stor samhörighet med godset som för personal anställd hos tillverkaren, vilket ökar risken för stölder och sabotage.

	Låg	**Medel**	**Hög**	
Logiskt skydd	0	1	0	
Elektroniskt skydd	0	0	2	
Fysiskt skydd	0	1	0	
Summa poäng	**0**	**2**	**2**	**4**

Trots att terminalen inte har något direkt godsintresse så påverkar hög stöldfrekvens att motivationen att förlägga transportflödena via denna logistikpunkt blir lägre på sikt. Det bör därför ligga inom terminalens intresseområde att verksamheten inte är behäftad med sådan underdimensionerad säkerhet att dess kunder med tiden väljer andra transportvägar. Kostnaden för stulet gods täcks med största sannolikhet av gällande försäkringar men kostnaden för förlorade kundrelationer bör också vägas in i sammanhanget för att ge en verklig bild av hur underdimensionerad säkerhet påverkar verksamheten.

Risken för smuggling och skadegörelse ligger under den genomsnittliga risknivån och prioriteten bör därför i första hand riktas mot att bekämpa risken för stöld. För smuggling bör det dock betonas att någon direkt effekt på terminalverksamheten är svår att finna till följd av denna brottshandling. Smuggling innebär i praktiken endast att befintliga transportbärare och distributionsnätverk används för att genomföra ett brott som av sig självt inte påverkar systemet nämnvärt. Handlingen skulle kunna ses som ett parasitförhållande där terminalens verksamhet varken drar nytta eller lider av den handling som sker medan nyttoeffekten enkom är riktad mot dem som utför smugglingen. Att smuggling medges inom ett säkerhetssystem påvisar dock en brist som i sig kan vara av betydelse att uppmärksamma och därmed väsentlig att förhindra.

Som utgångspunkt i bedömningen av vilket standardinitiativ som är mest tillämpligt för landsvägsterminaler, används nedanstående matris över de åtgärder som är av störst betydelse för dennes verksamhet. Kriterierna är baserade på de formuleringar som används i fas 3 – ”Jämförelse mellan utvalda säkerhetsinitiativ” och matrisen behandlar endast åtgärder som minskar risken för stöld och skadegörelse (säkerhetsrisker). C-TPAT och ISPS är exkluderade med hänsyn till deras alltför nischade karaktärer.

	AEO	TAPA	ISO
Kriteriegrund			
Säkerhetshot som primärt ska förebyggas - Stöld	X	X	
Skydd av lokaler	X	X	X
Övervakning av lokaler		X	X
Bemanning och/eller bevakning accesspunkter	X	X	
Tillträdeskontroll	X	X	X
Användande av tekniska lösningar för att hindra olovligt handhavande av gods		X	
Rutiner för kontroll av inkommande gods med avseende på att gods är registrerat i logistiksystemet	X	X	X
Kontroll av sigill på inkommande gods	X		X
Separat förvaring av olika typer av gods	X	X	X
Övervakning under lastning av gods i lastbärare av aktörens personal	X	X	
Rutiner för hur utgående gods förseglas och hur detta kontrolleras	X		X
Kontroller över att gods som lastas matchar godsdokumentationen		X	
Rekrytering och avveckling av personal	X	X	X
Utbildning av personal (fortlöpande utbildning i säkerhetsfrågor, riskmedvetande)	X	X	X
Skydd av affärsinformation	X	X	X
Sammanställning – täckning av kriterier			
Summa	**12**	**13**	**10**

Eftersom tjänsteutbudet inom logistiksektor idag omfattar mer än att endast erbjuda transporter, måste även förutsättningarna för dessa tjänster vägas in i bedömningen av vilket standardinitiativ som är mest effektivt för det specifika fallet. För terminalen kan detta innebära att exempelvis tullhantering utgör en viktig del i terminalens verksamhet och standarder som förenklar detta arbete kan därför ha stor betydelse i det slutliga valet av standard. I detta perspektiv kan det därför vara väsentligt att poängtera de uppenbara tullhanteringsfördelar som erbjuds inom ramen för AEO, samt

att TAPA med högst poängsättning i tabellen ovan, inte erbjuder denna service. För terminaler med omfattande tullhantering kan denna faktor därmed utgöra ett viktigt avgörande för vilket standardalternativ som i förlängningen anses vara mest lämpligt.

Beroende på hur organisationen är uppbyggd kring den terminal som ska standardcertifieras, kan verksamhetens intressesfär påverkas av hur ansvaret för godset är fördelat mellan de olika aktörerna längs transportkedjan. Om terminalens åtaganden omfattar både omlastning och efterföljande transport så innebär detta att terminalaktörens intresseområde utvidgas till att även omfatta säkerhetsarbetet utanför terminalområdet. Situationer av denna karaktär är framförallt vanliga i större transportföretag med global utbredning. Konsekvensen av detta blir samtidigt att fler åtgärder måste utvecklas och eftersom risken för stöld är stor under landsvägstransporter bör företag som förbinder sig till sådana åtaganden, överväga att använda utökade säkerhetsåtgärder för att försvåra stöldangrepp. Användning av högsäkerhetssigill är en sådan åtgärd och det bör därför påpekas att det endast är TAPA som föreskriver krav kring detta.

TAPA brister i kompabiliteten med intermodala flöden, vilket försvårar möjligheten att tillämpa denna standard då terminaler ofta vidaretransporterar gods via andra transportslag längs transportkedjan. ISO 28000 föreskriver samtidigt inga åtgärder för att förhindra stölder och är därför av mindre intresse för landsvägsterminaler som även utför transportarbetet. I annat fall kan ISO 28000 vara ett alternativ, då stölder endast ska förhindras inom den interna organisationen.

12.2.3 Kombiterminal (Järnvägs- och kombiterminal)

Järnvägs- och kombitermialer utgör viktiga noder för att kunna anpassa transportflöden efter de transportslag som är mest lämpliga för respektive transportsträcka. Detta kan innebära att transporter med tillräcklig godsvolym över långa sträckor, lämpar sig bäst för distribution med järnväg då detta transportmedel kan genomföra distributionen med högre effektivitet. Problemet med dessa transporter är dock att järnvägsterminalen sällan ligger i nära anknytning till kunden, dvs. godsets avsändare respektive mottagare. Mellanliggande transporter med lastbil är därför nödvändiga för att göra godset tillgängligt för järnvägstransporten och utan omlastning hade effektivitetsanpassning inte varit möjligt. Med terminalens starka betydelse är det därför viktigt att säkerhetsnivån inte förändras i samband med att en transport övergår från en fas till en annan.

Liksom landsvägsterminalen så utsätts järnvägs- och kombiterminalerna för måttlig risk för stöldangrepp och kostnaderna för åtgärder är något över medelvärdet, 4 av 6 poäng enligt nedanstående tabell. Stöldrisken utgör troligtvis också ett större problem för järnvägsterminalerna eftersom gods vid dessa logistikpunkter omlastas mellan lastbärare, exempelvis mellan en järnvägsvagn och en containerenhet. Detta innebär att eventuella förseglingar bryts och att godset därmed blir tillgängligt på ett sätt som inte är möjligt i fall då lastbärare kan kontrolleras mot dess intakthet genom obruten försegling. Det blir därmed också svårare att försäkra huruvida godset överensstämmer med den kvantitet som ankom till terminalen, såvida metoder för kontroll av godsets överensstämmande med dokumentationen inte på nytt genomförs för efterföljande

transport. Detta kan vara fallet om ankommande gods med tåg tillämpar en standard som föreskriver sådan kontroll medan utgående transport med lastbil tillämpar en standard som inte föreskriver sådan kontroll. Gråzonen där emellan kan i praktiken underlätta för personer att genomföra stölder utan att det märks inom rimlig tid.

	Låg	Medel	Hög	
Logiskt skydd	0	1	0	
Elektroniskt skydd	0	0	2	
Fysiskt skydd	0	1	0	
Summa poäng	**0**	**2**	**2**	**4**

Som utgångspunkt i bedömningen av vilket standardinitiativ som är mest tillämpligt för kombiterminaler, används nedanstående matris över de åtgärder som är av störst betydelse för dennes verksamhet. Kriterierna är baserade på de formuleringar som används i fas 3 – ”Jämförelse mellan utvalda säkerhetsinitiativ” och matrisen behandlar endast åtgärder som minskar risken för stöld och skadegörelse (säkerhetsrisker). C-TPAT och ISPS är exkluderade med hänsyn till deras alltför nischade karaktärer.

	AEO	TAPA	ISO
Kriteriegrund			
Säkerhetshot som primärt ska förebyggas - Stöld	X	X	
Skydd av lokaler	X	X	X
Övervakning av lokaler		X	X
Bemanning och/eller bevakning accesspunkter	X	X	
Tillträdeskontroll	X	X	X
Användande av tekniska lösningar för att hindra olovligt handhavande av gods		X	
Rutiner för kontroll av inkommande gods med avseende på att gods är registrerat i logistiksystemet	X	X	X
Kontroll av sigill på inkommande gods	X		X
Separat förvaring av olika typer av gods	X	X	X
Övervakning under lastning av gods i lastbärare av aktörens personal	X	X	
Rutiner för hur utgående gods förseglas och hur detta kontrolleras	X		X
Kontroller över att gods som lastas matchar godsdokumentationen		X	
Rekrytering och avveckling av personal	X	X	X

Utbildning av personal (fortlöpande utbildning i säkerhetsfrågor, riskmedvetande)	X	X	X
Skydd av affärsinformation	X	X	X
Sammanställning – täckning av kriterier			
Summa	**12**	**13**	**10**

Angående stöldrisken så påverkas terminalernas beslut om motåtgärder av samma resonemang som för landsvägsterminalerna, dvs. huruvida järnvägs- och kombiterminalen även ansvarar för tidigare/efterföljande transporter. Detta avgör till stor del vilka resurser som terminalbolaget ålägger säkerhetscertifieringen och det finns i sammanhanget avgörande skillnader mellan de standarder som kan vara lämpliga i denna situation. Den största skillnaden utgörs av den brist i tillämplighet som TAPA har vad gäller möjligheten att använda standarden för andra transportslag än lastbilstransporter. Konsekvensen av detta är att standardens inskränkning gör det praktiskt omöjligt att få effektivitet i ett system där syftet med verksamheten är att sammanföra olika transportslag. Om TAPA skulle användas trots nackdelarna med ett sådant upplägg, skulle detta innebära ytterligare standardcertifiering för att täcka de säkerhetsluckor som uppstår då TAPA inte gäller. I detta perspektiv borde det därför vara mer effektivt att redan från början anpassa systemet efter en standard som täcker de områden som verksamheten kommer i kontakt med. AEO är i sammanhanget det standardalternativ som bäst uppfyller de krav som en operatör av järnvägs- och kombiterminaler bör ställa. ISO 28000 föreskriver inga åtgärder mot stöldangrepp och är därför inte lika lämplig att införa.

12.2.4 Hamnterminal

Tillskillnad från andra godsterminaler i transportkedjan så exponeras hamnen för stora globala säkerhetsrisker. Detta följer naturligt av sjöfartens internationella karaktär, vilket även ökar kraven på verksamma åtgärder för att försvåra genomförandet av tänkbara brottshandlingar. Hamnen är samtidigt unik i den utsträckning att verksamheten omsätter gods från samtliga av de huvudsakliga transportslagen, sjö, landsväg, och järnväg, och dess logistiska betydelse är därför att betrakta som mycket stor. Detta, i samband med den riskbild som föreligger, har givit upphov till den tvingande regleringen som gäller under den internationellt verkande ISPS-koden, vilken framförallt syftar till att minska risken för smuggling och terroristbrott i hamnar och ombord på fartyg. Regleringen fastställer genom sitt innehåll att samtliga hamnar och fartyg med verksamhet under IMO-ansluten stat, måste uppfylla de krav som koden kräver. Detta innebär bland annat att gods som inte uppfyller de certifieringskriterier som ISPS-koden föreskriver, i praktiken skall nekas tillträde och transport inom det aktuella restriktionsområdet. ISPS-koden inskränker på detta sätt samtidigt möjligheten till utformningen av de frivilliga standardalternativ som erbjuds, där samtliga av dessa standarder minst måste uppfylla ISPS-kodens krav om transport via fartyg ska kunna genomföras.

Med anledning av att sjöfartens hotbild i stora delar skiljer sig från de hot som andra terminaler utsätts för, är det viktigt att notera den skillnad som även finns mellan de angreppssätt som tillämpas för att förebygga de aktuella säkerhetsriskerna. I

jämförelse med landterminalerna innebär detta att resurser till större del riktas mot terrorism- och smugglingsförebyggande åtgärder, än mot bekämpningen av direkta hot riktade mot det specifika godset. Hamnterminalen agerar på detta sätt i allt större utsträckning som statligt filter för att stänga ute de risker som i annat fall skulle riktas mot samhället, om detta ställs mot de insatser som terminaler för landtransporter täcker. Utformningen av säkerhetsåtgärderna i varje enskild hamn har därför en betydande påverkan på graden av samhällsskydd, sett ur ett nationellt säkerhetsperspektiv.

Ur sannolikhetssynpunkt utgör smuggling det påtagligt största säkerhetshotet enligt resultat hämtad från fas 1, kapitel 3.2.4 om hamnterminalen. Risken för angrepp är högre än den genomsnittliga sannolikhetsfaktorn och stora investeringar har därför gjorts för att förbättra den övergripande säkerhetsnivån. Detta har till viss del resulterat i minskad brottfrekvens i svenska hamnar och det är därför troligt att även sannolikheten för smuggling kommer att minska framöver. I ett sådant perspektiv är det samtidigt troligt med en gradvis förflyttning av säkerhetshotet till andra delar av logistikkedjan, exempelvis landburna transporter, och kraven på säkerhetsåtgärder kan därmed komma att behöva utvecklas även inom dessa verksamheter. Detta resonemang är till stor del även tillämpligt för de hotbilder som omfattar trafficking och terrorism, förutsatt att resonemanget utelämnar sådana transporter som förutsätter interkontinentala sjötransporter, mot vilka förflyttning till landburna transporter ej är möjligt. På så sätt kommer det troligen vara fortsatt betydelsefullt med stark kontroll av viktiga internationella hamnfaciliteter, då hotbilden sannolikt inte kommer att minska i samma omfattning som för hamnar utan interkontinentala linjer.

Som utgångspunkt i bedömningen av vilket standardinitiativ som är mest tillämpligt för hamnterminaler, används nedanstående matris över de åtgärder som är av störst betydelse för dennes verksamhet. Kriterierna är baserade på de formuleringar som används i fas 3 – ”Jämförelse mellan utvalda säkerhetsinitiativ” och matrisen behandlar åtgärder som minskar risken för skadegörelse och andra säkerhetsrisker riktade mot hamnterminalen. C-TPAT och ISPS är exkluderade med hänsyn till deras alltför nischade karaktärer. ISPS är tvingande och på så sätt ej relevant med hänsyn till att hamnterminalen är beroende av andra transporter, vilka ISPS ej täcker. Frågeställningen utgår därför från att finna en standard som täcker även dessa transportslag.

	AEO	TAPA	ISO
Kriteriegrund			
Skydd av lokaler	X	X	X
Övervakning av lokaler		X	X
Bemanning och/eller bevakning accesspunkter	X	X	
Tillträdeskontroll	X	X	X

Rutiner för kontroll av inkommande gods med avseende på att gods är registrerat i logistiksystemet	X	X	X
Kontroll av sigill på inkommande gods	X		X
Separat förvaring av olika typer av gods	X	X	X
Rekrytering och avveckling av personal	X	X	X
Utbildning av personal (fortlöpande utbildning i säkerhetsfrågor, riskmedvetande)	X	X	X
Skydd av affärsinformation	X	X	X
Sammanställning – täckning av kriterier			
Summa	**9**	**9**	**9**

Hamnen har en särställning i den utsträckning att konkurrenssituationen ofta avviker från vad som normalt kännetecknar marknaden för landterminaler. Detta uttrycks genom att logistikflöden oftast byggs upp kring de noder och länkar som i kedjan medger den mest effektiva transporten, där bedömningen till stor del grundas på faktorer kring hamnens geografiska läge, aktuellt linjenät, fartygsfrekvens och typ av godshantering. För hamnens del skapar detta, i samverkan med låg hamntäthet, ökade möjligheter att etablera varaktiga kundrelationer samtidigt som konkurrensen mellan hamnar är lägre än för motsvarande förhållande mellan landterminaler. Detta resonemang skapar en snedfördelning som i stor omfattning kan gynna hamnverksamheten genom möjlighet till minskad ambition att införa effektiva säkerhetsrutiner. Om situationen däremot tar hänsyn till konkurrensen även mellan hamn- respektive landterminaler är situationen inte tillämplig och hamnen bör i detta perspektiv uttrycka hög säkerhetsambition för att framhålla konkurrenskraft gentemot landterminalerna. Hamnens position är i detta sammanhang inte lika unik.

Hamnen som enskilt objekt har relativt få egenintressen, motsvarande lastägarens intresse för leverans av felfri vara. I en sådan jämförelse är stölder samtidigt inte lika påtagliga i hamnterminaler som i terminaler för landtransporter, vilket i praktiken innebär minskat behov av skydd mot dessa säkerhetshot. Om hamnen utsätts för en ansenlig mängd stölder så bör detta ställas i relation till vilken skada som påförs hamnorganisationen, med hänsyn till hamnens unika position och ställning gentemot gods som måste transporteras med fartyg. Det är samtidigt inte vanligt att hamnterminalen tar ansvar för den del av transportarbetet som sker före respektive efter själva omlastningen på hamnområdet. Det är därför svårt att klargöra hur stor skada som hamnorganisationen lider genom en hög stöldfrekvens. Hoten om smuggling, terrorism och trafficking är på samma sätt inte tillräckligt riktade mot hamnen för att nämnvärt påverka ställningstagandet för ökat säkerhetsarbete. Vanligtvis så utnyttjar dessa aktiviteter endast hamnen som en passerpunkt för att möjliggöra ett syfte som finns bortom hamnens verksamhet. Undantaget kan vara i fall då hamnen i sig utgör måltavla för terroristbrott, vilket exempelvis är ett överhängande hot för internationellt viktiga hamn-noder. I dessa fall kan det därför finnas ett egenintresse för att skydda den egna organisationen mot angrepp. Detta gäller även för det mindre allvarliga brottet skadegörelse, till vilket bakgrunden också kan utgöra tillräckligt egenintresse för att resurser ska avsättas till motåtgärder. Kostnaderna för utveckling av fungerande säkerhetssystem får samtidigt betraktas som relativt höga, 4 av 6 poäng enligt nedanstående tabell.

	Låg	Medel	Hög	
Logiskt skydd	0	1	0	
Elektroniskt skydd	0	0	2	
Fysiskt skydd	0	1	0	
Summa poäng	**0**	**2**	**2**	**4**

Kombinationen av fördelaktig konkurrensnivå och brist på direkta egenintressen medför att hamnen per automatik har liten anledning till att avsätta resurser till aktiv utbyggnad av skyddsåtgärder. Detta försvåras till viss del av den tvingande reglering som på senare tid inneburit ökade krav på hamnterminalen, bland annat genom införandet av ISPS-koden, och betydelsen av resonemanget kan därför anses vara mindre mot bakgrund av de krav som idag kännetecknar branschen. Hamnen kan samtidigt inte isoleras från övriga logistikkedjan genom att endast uppfylla de krav som är absolut nödvändiga utifrån gällande lagstiftning eftersom transporter blir allt mer integrerade med varandra. Det ankommer därmed som ett indirekt krav på hamnen att förenkling och kompabilitet med intermodala flöden ska kunna tillämpas, i annat fall kan kunder på lång sikt välja andra distributionsvägar. Omfördelning möjliggörs genom anpassning till gällande förutsättningar och olika aspekter vägs i detta arbete mot varandra. Enligt resonemanget måste hamnen därför i de flesta fall täcka de krav som övriga transportbranschen kräver, trots att fördelarna för den enskilda hamnen kan vara marginella.

Enligt tabellen ovan så uppfyller de tre jämförbara standarderna lika många kriterier, kriterier med särskild betydelse bör därför selekteras för att öka möjligheten att bedöma vilken standard som är mest lämplig. Eftersom det är få skillnader i de faktiska åtgärdspaketen så är det av större vikt att bedöma helheten och den viktigaste aspekten i detta sammanhang består av den globala tillämpbarheten. Hamnen är en internationell aktör och genom att tillämpa en standard som både inskränker möjligheten till global distribution såväl som möjligheten till intermodala transporter, kan det blir svårt att erhålla effektivitet i säkerhetsarbetet. För global distribution är det endast TAPA samt ISO 28000 som direkt möjliggör dessa flöden. AEO kan via kopplingar till WCO antas kunna anpassas för global distribution men tillvägagångssättet är ej behandlat i detta projekt. För intermodalitet svarar både AEO samt ISO 28000 medan TAPA endast tillämpas på lastbilstransporter, vilket i praktiken utesluter möjligheten för standarden att bli gångbar för säkerhetscertifiering av hamnar. I ett annat perspektiv täcker samtidigt ISO 28000 samma säkerhetsrisker som ISPS och det är därför väsentligt att ifrågasätta värdet av att certifiera enligt ISO 28000 eftersom verksamheten ändå måste uppfylla kraven enligt ISPS. AEO, som även täcker stöld och trafficking, underlättar samtidigt tullhanteringen vilket kan vara av stor betydelse i valet av en standard som även syftar till att skapa effektivitet. AEO täcker därmed tillräckligt många kriterier för att utgöra intresse för hamncertifiering.

12.2.5 Landtransporter

Landsvägstransporter utgör en viktig länk i ett fungerande distributionssystem och inget annat transportslag kan i realiteten ersätta den flexibilitet och tillgänglighet som dessa transporter erbjuder. Andra transportslag är genom sin utformning beroende av att vägfordon i någon utsträckning genomför distribution både före och efter den del som sker med annat transportmedel, vilket i många fall utgörs av transporter till och från mottagare respektive avsändare. I detta perspektiv är järnvägstransporter begränsade eftersom distribution endast är möjlig för den sträcka som täcks av järnvägsnätet, det är därför sällan som dörr-till-dörr-leveranser kan uppfyllas enbart genom tillämpning av transport på järnväg. Kombinationen av olika transportslag skapar därmed krav på intermodalitet och med detta följer också krav på kompatibel och effektiv hantering av tillämpbart säkerhetsarbete, så att onödiga kostnader och merarbete undviks.

Både väg- och järnvägstransporter kan ske med olika typer av transportenheter och riskerna förknippade med respektive enhet kan variera kraftigt. Exempelvis så är gods som lastats i en gardintrailer betydligt mer tillgängligt än gods som lastats i en container, där valet av enhet till stor del kan baseras på värdet av det aktuella godset. Det är därmed svårt att på ett komplett sätt beskriva situationen för resonemanget kring standardcertifiering, eftersom transportörens godsinriktning är av stor betydelse i bedömningen av lämplig standard. Därtill måste förekomsten av internationell trafik ställas i relation till om transportören endast verkar på den nationella marknaden. Säkerhetshot som framförallt är förknippade med transportörens geografiska marknadsområde är trafficking och smuggling, där brottens natur förutsätter att egendom eller person förflyttas över landsgränser till länder där ett mervärde av förflyttningen kan realiseras. För inrikestrafik är dessa brott av mindre betydelse till följd av låg sannolikhetsgrad.

I fråga om säkerhetsarbete vad gäller transporter så skiljer detta sig från de säkerhetsåtgärder som kan tillämpas för fast anläggning. När lastbäraren väl har lämnat terminalområdet och inlett transporten är det med kraftig begränsning som säkerhetsåtgärder kan verkställas. För fast anläggning är det exempelvis vanligt med en kombination av olika åtgärder, där larm, fysiska hinder och övervakning förekommer i stor omfattning. För rörlig anläggning såsom lastbärare och transportfordon är det inte möjligt att tillämpa åtgärder av samma dignitet och med bakgrund av detta kan transporten därför betraktas som ett stort riskmoment, om jämförelse görs mot den del av logistikflödet då lasten befinner sig inom ett övervakat område. Även mellan väg- och järnvägstransporter finns det skillnader i fråga om hur stora säkerhetsrisker som lastbärarna utsätts för då dessa lämnar terminalområdet. För vägtransporter finns det i sammanhanget en klar fördel med chaufförens närvaro vilket möjliggör en bättre övervakningsfunktion än vad som är fallet för järnvägstransporter. Trots detta förekommer det situationer då godset är helt obevakat, både för väg- och järnvägstransporter, vilket framförallt inträffar i samband med vilotider för lastbilschaufförer och väntetider för järnvägshantering. Kostnaderna för åtgärder får samtidigt betraktas som låga, 1 av 6 poäng enligt nedanstående tabell.

	Låg	Medel	Hög	
Logiskt skydd	0	0	0	
Elektroniskt skydd	0	1	0	
Fysiskt skydd	0	0	0	
Summa poäng	**0**	**1**	**0**	**1**

Som utgångspunkt i bedömningen av vilket standardinitiativ som är mest tillämpligt för landtransportörer, används nedanstående matris över de åtgärder som är av störst betydelse för dennes verksamhet. Kriterierna är baserade på de formuleringar som används i fas 3 – ”Jämförelse mellan utvalda säkerhetsinitiativ” och matrisen behandlar åtgärder som minskar risken för stöld, skadegörelse och andra säkerhetsrisker riktade mot transportören. C-TPAT och ISPS är exkluderade med hänsyn till deras alltför nischade karaktärer.

	AEO	TAPA	ISO
Kriteriegrund			
Användande av tekniska lösningar för att hindra olovligt handhavande av gods (användning av högsäkerhetssigill, utrustning för stillastående fordon m.m.)		X	
Övervakning under lastning av gods i lastbärare av aktörens personal	X	X	
Rutiner för hur utgående gods förseglas och hur detta kontrolleras	X		X
Kontroller över att gods som lastas matchar godsdokumentationen		X	
Rekrytering och avveckling av personal	X	X	X
Utbildning av personal (fortlöpande utbildning i säkerhetsfrågor, riskmedvetande)	X	X	X
Skydd av affärsinformation	X	X	X
Sammanställning – täckning av kriterier			
Summa	**5**	**6**	**4**

Konkurrensen mellan landtransportörer är hård och i jämförelse med hamnterminalens förhållandevis unika position krävs att transportören åtminstone levererar en produkt som motsvarar vad transportköparen kan erhålla till samma pris av annan. Detta skapar ett stort egenintresse för upprätthållandet av en säkerhetsnivå som inte äventyrar transportägarens intresse av att få leverans av en felfri vara. Transportören representerar på så vis godsägaren under transporten och ska genom detta också vårda godset på ett sådant sätt att kundens önskemål inte åsidosätts. Det föreligger därför en direktrelation mellan godset, godsets ägare och transportören, en relation som inte ligger till grund om perspektivet istället riktas mot godsägaren och en eventuell

terminalaktör. I ett sådant perspektiv är det troligt att det ändå blir transportören som anses ansvarig i kundens bedömning av situationen, även om bristen är orsakad av terminalen och att det juridiskt också är denna part som blir rättsligt ansvarig. Problematiken innebär därför en subjektiv aspekt som transportören måste väga in i bedömningen av vilken säkerhetsnivå som det aktuella företaget bör tillämpa, för att inte riskera att förlora kunder till följd av säkerhetsluckor som i förlängningen drabbar transportköparen.

Det är uppenbart att det framförallt är stölder och skadegörelse som prioriteras ur transportörernas synvinkel och med bakgrund av detta så framträder TAPA som den starkaste standarden enligt tabellen ovan. TAPA täcker till stora delar samtliga av de kriterier som valts ut som särskilt betydelsefulla och det är samtidigt endast TAPA som täcker den förmodligen viktigaste åtgärden, användningen av högsäkerhetssigill. När denna används i kombination med en solid lastbärare såsom containers är det betydligt svårare för obehöriga att få tillgång till godset, vilket därtill är en av få verkningsfulla åtgärder som direkt försvårar intrång i enheter som annars förblir obevakade. För vägtransporter bör TAPA därför utgöra ett lämpligt alternativ i fall då den aktuella lastbäraren endast ska distribueras med lastbilstransporter.

För järnvägstransporter är TAPA inte en lämplig standard att använda till följd av att den enbart kan tillämpas för vägtransporter. Detta utesluter dock inte möjligheten att ändå använda högsäkerhetssigill för att kunna upprätthålla den godssäkerhet som standarden föreskriver, vilket i så fall bör ske i kombination med certifiering av någon av de återstående standarderna. AEO är i detta avseende ett intressantare alternativ mot bakgrund att tillämpningen även täcker hot som avser stöld, vilket inte täcks under ISO 28000. Detta utgör en så viktig grundförutsättning att det praktiskt sett inte finns någon egentlig anledning till att välja certifiering enligt ISO 28000. Bägge alternativen är dock kompatibla med intermodala flöden och i detta avseende brister däremot TAPA. Konsensus är därför att både väg- och järnvägstransporter som avser ingå i den intermodala logistikkedjan, bör överväga certifiering enligt AEO, såväl som järnvägstransporter bör överväga AEO framför ISO 28000 i alla förekomna fall.

12.2.6 Sjötransport

Sjötransportörer är i motsats till transportörer på land inte lika utsatta för intrång under själva distributionen. För väg- och järnvägstransporter är denna risk däremot ett stort problem eftersom lastbärare i regel är tillgängliga från dess att transportenheten avlastats hos avsändaren till dess att den levererats till mottagaren. För transporter med fartyg kan intrång av denna karaktär i princip endast genomföras via piratattacker, vilket i sig är väldigt ovanligt i fall då särskilt riskfyllda områden undviks. Riskmomenten föreligger därför i praktisk mening då fartyget befinner sig i hamn samt då lastnings- och lossningsarbete sker. Det är därför viktigt att analysera vilka säkerhetshot som kan uppkomma vid dessa situationer för att på så sätt även utvärdera vilka rutiner som ska skapas för att motarbeta dessa hotbilder.

De flesta transporter av förädlat gods till sjöss sker med containerfartyg och det är endast begränsade mängder som använder andra fartygstyper, vilket då främst utgörs av RoRo-fartyg över kortare sträckor på regional nivå. I fråga om stöldrisken så är det

dessa fartyg som är av intresse, främst med anledning av lastvärdet men också till följd godsets beskaffenhet. Andra godstyper som transporteras till sjöss omfattar till stora delar bulklaster och dessa lasttyper är varken högvärdiga eller särskilt stöldbegärliga. Fartygstypen har därför stor betydelse i bedömningen av vilken inriktning som säkerhetsarbetet ska ha och vilka hot som därmed ska förebyggas. Kostnaderna förknippade med säkerhetsutbyggnad anses dock vara mycket låga, 0 av 6 poäng enligt ovanstående beräkningsmodell.

	Låg	Medel	Hög	
Logiskt skydd	0	0	0	
Elektroniskt skydd	0	0	0	
Fysiskt skydd	0	0	0	
Summa poäng	**0**	**0**	**0**	**0**

Eftersom stölder och skadegörelse utgör en väldigt liten riskfaktor då fartyget befinner sig till havs är det sannolikt att det är andra risker som i sammanhanget bör tillägnas högre prioritet. Den påtagligt största riskfaktorn bedöms utgöras av smuggling, som står för en medelhög säkerhetsrisk, följt av riskerna för terrorism och trafficking som båda ligger under den genomsnittliga risknivån. Huruvida dessa brottshandlingar enskilt påverkar sjöfarten är svårt att fastställa men det är troligt att det liksom i andra fall endast utgör ett utnyttjande av det aktuella transportmedlet. Det är därför inte enkelt att bedöma på vilket sätt sjötransportören ska angripa dessa hotbilder. Det förekommer dock smuggling av exempelvis explosiva ämnen, vilket i sig kan utgöra ett hot som kan medföra skador på fartyg och besättning, om materialet av misstag detonerar. I dessa situationer finns det ett egenintresse av att skydda verksamheten mot sådana hotbilder. I praktiken har resonemanget kring smuggling och terrorism dock ingen betydelse då alla fartyg måste uppfylla de krav som gäller under ISPS-koden, förutsatt att fartyget seglar under en flaggstat som verkar under IMO. Frågan som dock bör ställas är om sjötransportören mot bakgrund av detta har något ytterligare intresse av att skydda sig mot dessa handlingar och därtill riskerna för stöld och skadegörelse.

Som utgångspunkt i bedömningen av vilket standardinitiativ som är mest tillämpligt för sjötransportörer, används nedanstående matris över de åtgärder som är av störst betydelse för dennes verksamhet. Kriterierna är baserade på de formuleringar som används i fas 3 – ”Jämförelse mellan utvalda säkerhetsinitiativ” och matrisen behandlar åtgärder som minskar risken för stöld, skadegörelse och andra säkerhetsrisker riktade mot transportören. C-TPAT är exkluderad med hänsyn till dess alltför nischade karaktär. ISPS-koden tas med i jämförelsen eftersom sjötransportören i praktiken agerar inom ett eget område och där kompabilitet med andra transportslag egentligen åligger hamnterminalen.

	ISPS	AEO	TAPA	ISO
Kriteriegrund				
Skydd av lokaler	X	X	X	X
Övervakning av lokaler	X		X	X
Bemanning och/eller bevakning accesspunkter	X	X	X	
Tillträdeskontroll	X	X	X	X
Användande av tekniska lösningar för att hindra olovligt handhavande av gods (användning av högsäkerhetssigill, utrustning för stillastående fordon m.m)	X		X	
Rutiner för kontroll av inkommande gods med avseende på att gods är registrerat i logistiksystemet	X	X	X	X
Kontroll av sigill på inkommande gods	X	X		X
Kontroll över att gods som lastas matchar godsdokumentationen	X		X	
Rekrytering och avveckling av personal		X	X	X
Utbildning av personal (fortlöpande utbildning i säkerhetsfrågor, riskmedvetande)		X	X	X
Informationsspridning (intern och extern information om företagets/aktörens säkerhetsrutiner)	X			X
Skydd av affärsinformation		X	X	X
Sammanställning – täckning av kriterier				
Summa	**9**	**8**	**10**	**9**

Genom situationen att sjöfarten måste uppfylla rutiner under tvingande regelverk, bör beslutet kring sjöfartens eventuella tilläggscertifiering grundas på frågeställningen om detta är nödvändigt eller om det är tillräckligt med tillämpning av ISPS-regelverket. I detta perspektiv kan det vara av stor vikt att bedöma på vilka grunder som de analyserade standarderna skiljer sig från varandra samt att avgöra hur stor betydelse dessa skillnader får.

Det är framförallt inom utbildnings- och personalområdet som ISPS avviker från de övriga standarderna och detta är anmärkningsvärt med tanke på de risker som en opålitlig besättning kan medföra. Stöldrisken orsakad av besättningen får i sammanhanget dock anses som låg mot bakgrund av att högsäkerhetssigill är obligatoriskt för fartyg som lyder under ISPS-koden. Risken för insiderrelaterad smuggling, terrorism och trafficking är i sammanhanget betydligt mer påtaglig men kan samtidigt försvåras genom strängare rutiner i hamnterminalen. Risken för terrorism ska dock anses vara av mer överhängande karaktär eftersom fartyget efter avgång inte befinner sig under någon nämnvärd kontrollfunktion, annat än vad som utgörs av besättningens egenkontroll. Aktiviteter såsom förberedelse till terroristbrott kan därför vara svåra att identifiera i tid.

TAPA är enligt tabellen ovan den standard som uppfyller flest av de utvalda kriterierna men med hänsyn till avsaknaden av kompabilitet med fartygstransporter, kan standarden inte utgöra något troligt underlag för certifiering av sjötransportörer. AEO brister samtidigt i den globala tillämpligheten vilket försvårar certifiering enligt denna standard, med hänsyn till sjöfartens internationella karaktär. AEO är dock sammankopplad med WCO och mot bakgrund av detta så bör den globala täckningen i praktiken inte utgöra något större problem. Det ska dock påpekas att denna del inte blivit tillräckligt analyserad i projektet för att på ett bra sätt kunna ge någon vägledning kring ett sådant upplägg. Det kan dock konstateras att AEO kompletterar ISPS-koden väl på de områden som ISPS brister och AEO bör därför kunna utgöra ett potentiellt alternativ om ytterligare steg ska tas mot förbättrad säkerhet. Framförallt utökas säkerheten mot stöldangrepp och trafficking, vilket varken täcks av ISPS-koden eller ISO 28000. I övrigt skapar ISO 28000 inga mervärden utöver AEO och de kriterier som redan är täckta av ISPS-koden. Certifiering enligt ISO 28000 medför därför en lägre säkerhetsnivå än i fallet då ISPS-koden kompletteras med certifiering enligt AEO. Det ska dock konstateras att det troligen kan räcka med att sjötransportören uppfyller de åtaganden som krävs ur den tvingande lagregleringen, då några direkta fördelar med utökad certifiering är svår att finna.

13 Slutsatser

Projektets syfte har under arbetets fortskridande genomgått en modifiering, något som har ansetts nödvändigt för att skapa en rapport som kan bidra med användbart innehåll till studiens intressenter. Detta har inneburit att projektet har frångått den initiala tanken om att skapa ett nytt regelverk för hantering av säkerhetsfrågor inom transportkedjan, till att istället försöka beskriva utbudet av de standarder som redan existerar. Projektet har därtill försökt belysa de säkerhetsstandarder som är mest relevanta för respektive aktör inom transportkedjan, samt vilka kriterier som dessa aktörer bör fokusera på. Bakgrunden till förändringsprocessen följer av att förutsättningarna för arbetet har ändrats över tid, vilket har skapat ett minskat behov av att fullfölja arbetet enligt det initiala syftet.

Olika motiv till att införa ett säkerhetsinitiativ

Olika aktörer prioriterar olika åtgärder för att minska riskerna inom ett för aktören viktigt område, vilket försvårar arbetet med en universellt fungerande standard med den helhetstäckande säkerheten i fokus.

Det har under projektet tydligt framgått att det finns intressekonflikter i de säkerhetsinitiativ som respektive standard förespråkar. Detta innebär i praktiken att olika intressenter prioriterar olika åtgärder i syfte att minska risken för intrång på de områden som respektive aktör framhåller som särskilt betydelsefulla. Ett system där säkerheten till viss del baseras på denna valfrihet skapar också försvårande omständigheter avseende det faktum att säkerhetsriskerna många gånger tillhör de länkar där säkerhetsåtgärderna är som lägst. Ett tydligt exempel som illustrerar denna problematik är i fall då intresset av att skydda gods mot stöld är viktigare än risken för att en transportbärare används för smugglingsändamål. Ett sådant system skapar säkerhetsluckor på grund av att en övergripande global standard saknas eller i vart fall inte är fullständigt utbyggd, vilket dock ska ställas i relation till de tvingande regler som till viss del täcker sådana brister, exempelvis ISPS för sjötransporter. Det bör däremot ifrågasättas hur tvingande reglering av denna karaktär faktiskt är anpassad till den hotbild som föreligger, så att säkerhetsnivån verkligen motsvarar de åtgärder som krävs för att minska säkerhetsriskerna. Det föreligger samtidigt en problemsituation då tvingande regelverk såsom ISPS, ställer krav på samtliga transporter som vid något skede ska hanteras inom ett ISPS-område. Det finns i detta sammanhang en uppenbar risk för att åtgärderna inom ett sådant regelverk är underdimensionerade för att inte påverka säkerhetsinsatserna i övriga transportskedjan i alltför hög grad.

För många säkerhetsinitiativ

Det stora antalet säkerhetsstandarder försvårar arbetet med att finna en gemensam överenskommelse inom vilket den övergripande säkerheten ska kunna harmoniseras.

Med bakgrund av det stora utbudet av säkerhetsstandarder så kan det konstateras att ytterligare initiativ till nyetableringar inte löser problematiken med ineffektiva

certifieringsprocesser. Det är i dagsläget för avancerat att på global nivå finna lösningar som är internationell såväl som nationellt verkningsfulla och arbetet med att tillgodose säkerheten kan samtidigt medföra höga kostnader. I förlängningen innebär detta både minskad säkerhet och förlorad effektivitet, där resultaten av dessa troligen skulle bli bättre genom konsolidering och minskning av antalet standarder. Detta är framförallt en viktig aspekt sett ur aktörernas perspektiv eftersom förenklad certifieringsprocess troligen också ger upphov till ökad ambition för certifiering. AEO är samtidigt ett exempel på standard som uppvisar tecken på att öka transparensen gentemot andra standarder, däribland WCO, TAPA, och ISO 28000. Detta kan vara ett första steg mot ett effektivare och mer globalt täckande säkerhetssystem. Fördelen med en individuellt verkningsfull standard är dock att en grundläggande säkerhetsnivå kan uppnås förhållandevis enkelt och med obehindrad global tillämpning, samtidigt kan utökad certifiering ske för verksamheter som är av särskild betydelse för aktören. Konsolidering i riktning mot en sådan standard skulle därför vara önskvärd.

Samverkan för bättre effektivitet

Myndigheter bör samarbeta på internationell nivå för att genomföra en översyn av effektiviteten i det nuvarande säkerhetssystemet. Det finns risk för att dagens konstruktion skapar ineffektiva säkerhetslösningar som i förlängningen verkar negativt på den globala säkerhetsnivån. Stater bör därför samverka för att på så sätt lämna förslag på hur effektivisering ska kunna uppnås.

Det råder stor brist på internationella samarbeten för att möjliggöra en effektivare utveckling av ett fungerande säkerhetsarbete på global nivå. Bristen på samverkan har troligen också gett upphov till den kraftiga expansionen av säkerhetsstandarder vilket med stor sannolikhet också har skapat försvårande procedurer för såväl certifiering som den dagliga verksamheten. Ett tydligt exempel som beskriver konsekvensen av utebliven internationell samverkan är de hårda regler som USA på kort tid försökt att implementera för fartygstransporter med USA som destination. Till dessa hör exempelvis 100%-scannning, vilket är en standard som ålägger en mycket stor arbetsbörda på de hamnar som trafikerar amerikanska farvatten och där det faktiska värdet av en sådan åtgärd inte är helt klargjord. Kontrasten mellan åtgärder av denna karaktär och åtgärder i den övriga internationella sjöfarten är mycket stor och samtidigt uppstår säkerhetshoten framförallt i de delar av kedjan där säkerheten är som lägst. Det är därför motiverat med internationell reglering som utjämnar denna snedfördelning och därmed möjliggör bättre resursfördelning, vilket troligen också minskar risken för över- kontra underdimensionerade säkerhetssystem.

Tillgripna godsvärdet ökar

Det är konstaterat att värdet på det gods som tillgrips inom transportkedjan ökar kraftigt, vilket påverkar kostnadsstrukturen och skadelidandet för varje enskilt tillfälle. Angreppen blir alltmer kännbara och troligen ökar detta ambitionen att förstärka skyddet gentemot verksamheten från utomstående..

Värdeökningen för den totala mängden tillgripet gods kan bero på ett antal faktorer. Under projektarbetet har det framkommit uppgifter om att Polisen infört nya rutiner

kring brottsrubriceringen av angrepp mot transportkedjan. Tidigare kamouflerades den verkliga kostnaden för dessa brott genom att det inte förekom någon separering mellan olika former av stölder. Genom förbättrad brottskodning är det därför numera möjligt att följa upp kostnadsbilden för varje enskilt angrepp riktat mot transportkedjan. Det har också framkommit uppgifter om att kunskapsbasen kring planering och tillvägagångssätt för angrepp har ökat bland kriminella, vilket med stor sannolikhet ökar precisionen och inriktningen av angreppet. En sådan inriktning är stölder av hela ekipage, något som i likhet med ökad kunskap troligen har bidragit till den senaste tidens stegring av det tillgripna godsets värde.

Säkerhetshotens betydelse för verksamheten

Transportbranschen upplever att det framförallt är stölder och skadegörelse som orsakar mest skada utifrån de säkerhetshot som blivit beskrivna i detta projekt.

Eftersom transportbranschen många gånger består av eller representerar de aktörer som besitter godsintresse, är det inte förvånande att säkerhetshot som avser stöld och skadegörelse är högt prioriterade av dessa aktörer. Branschen är samtidigt enig om att smuggling utgör ett problem men anser samtidigt inte att enskilda transportföretag ska lösa detta problem. Terrorism och trafficking är säkerhetshot som inte medför några kännbara konsekvenser för den enskilde aktören och åtgärder mot sådana angrepp prioriteras därför inte.

14 Förkortningar

ADR	European Agreement Concerning the International Carriage of Dangerous Goods
AEO	Authorized Economical Operators
BASC	The Business Alliance for Secure Commerce
BCS	Border Cargo Selectivity
CBP	U.S. Customs and Border Protection
CBSA	Canada Border Services Agency
CSI	Container Security Initive
C-TPAT	Customs Trade Partnership Against Terrorism
DGR	Dangerous Goods Regulations
DHS	Department of Homeland Security
DNDO	Domestic Nuclear Detection Office
ESSTRT	European High Level Study on Threats, Responses and Relevant Technology
FAST	Free and Secure Trade
FSR	Freight Security Requirements
IATA	The Air Transport Association
ICAO	International Civil Aviation Organization
IIS	Incident Information Service
IMDG	International Maritime Dangerous Goods Code
IMO	International Maritime Organization
ISO	International Organization for Standardization
ISPS	International Ship and Port Facility Security Code
PAPS	Pre Arrival Processing System
PIP	Partners In Protection
SFI	Secure Freight Initiative
SOLAS	Safety Of Life At Sea
STP	Secure Trade Partnership
TAPA	The Technology Asset Protection Association
TSR	Trucking Security Requirements
WMD	Weapons of Mass Destruction

15 Referenser

15.1 Publicerade källor

Bonander, Jesper & Wang, Mikael, *Nomadic Computing Towards Secure Cargo Transports*, 2004

Canada Border Services Agency's Evaluation Division, *Partners in Protection Evaluation Study*, 2006

Directorate General Enterprise and Industry Security Research, *Preparatory Action for Security Research SECCONDD*, 2005

ECMT, *Annual Report 2002*

Ekwall, Daniel, *Antagonistic Gateways in the Transport Network in a Supply Chain Perspective*, 2007

Ekwall, Daniel & Lumsden, Kenth, *Differences in Stakeholder Opinion Regarding Antagonistic Gateways Within the Transport Network*

ESSTRT Consortium, *New European Approach to Counter Terrorism*, 2006

European Commision, *Authorized Economic Operators Guidelines*, 2007

European Commision, *Proposal for a Regulation of the European Parliament and of the Council on Enhancing Supply Chain Security*, 2006

GAO, *The SAFE Port Act: Status and Implementation One Year Later*, 2007

Giermanski, Jim, *A different theory for 100 percent container scanning*, Security Info Watch, 2009

Herbert-Burns, Rupert, *Lloyd's handbook of maritime security*, 2008

Hinkelman, Edward G, *Dictionary of International Trade Handbook of the Global Trade Community*, 8th edition 2008

ISO, *Specification for security management systems for the supply chain ISO 28000*, First edition 2007

Kommerskollegium, *Säkerhet i leveranskedjan: Hur påverkas handeln av det ökade antalet säkerhetsinitiativ?*, 2008

Kvoten mellan den faktiska och den registrerade brottsligheten

Lloyds list, *U.S. Shippers Oppose 100 Percent Cargo Inspections*, 2009

MariTerm, *ISPS Code Your Key to Security*

Mazaheri, Arsham, *Impacts of the ISPS code on port activities*

McNicholas, Michael, *Maritime Security*, 2008

Nilsson, Per-Arne, *Polisens rapport om transportsäkerhet 2008,* Polismyndigheten i Västra Götaland

Riskhantering Akademin, *Godsvärdesanalys 2008,* Projekt Transportsäkerhet

Sarnecki, Jerzy, *Introduktion till kriminologi*

Schmitz, Michael, *WCO SAFE Framework of Standards, Fifth special meeting of the counter-terrorism committee*, 2007

Security Info Watch, *U.S Shippers Oppose 100 Percent Cargo Inspection*, 2009

Singapore Customs, *Secure Trade Partnership Guidelines and Criteria*, 2008

TAPA, *Freight Supplier Minimum Trucking Security Requirements*, 2008

Transek, *Brott mot yrkestrafik på väg*, 2006

U.S. Customs and Border Protection, *Container Security Initiative*, 2006

U.S. Customs and Border Protection, *C-TPAT A Guide To Program Benefits*, 2008

U.S. Customs and Border Protection, *Free and Secure Trade FAST Fact Sheet*, 2008

U.S. Customs and Border Protection, *Securing the Global Supply Chain*, 2004

U.S. Customs and Border Protection, *Written testimony of Ralph Basham*, 2007

Utevaron av olika skyddsåtgärder, logiska, fysiska eller elektroniska skydd

Wheeler, John, *Report on Airport Security*, 2002

World Customs Organization, *WCO SAFE Framework of Standards*, Juni 2007

15.2 Webbsidor

BASC, *www.wbasco.org*, 2010-04-27

Canada Border Services Agency, 2010-04-28
www.cbsa-asfc.gc.ca/media/release-communique/2008/2008-07-02-eng.html
www.cbsa-asfc.gc.ca/agency-agence/reports-rapports/ae-ve/2006/pip-pep-eng.html

CMP Canterbury join Customs' Secure Exports Scheme,
www.scoop.co.nz/stories/BU1002/S00283.html, 2010-06-17

CSI,
www.cbp.gov/xp/cgov/trade/cargo_security/csi/ports_in_csi.xml

Giermanski, James,
http://www.logasiamag.com/article-1190-smartcontainers-LogisticAsia.html

Holländska tullen, *Dutch Client System*, *www.douane.nl/zakelijk/aeo/en/*

New Zealand Customs Service, *Secure Exports Scheme*,
www.customs.govt.nz/exporters/Secure+Exports+Scheme.html, 2010-06-17

Secure Freight Initiativ,
www.cbp.gov/xp/cgov/border_security/secure_freight_initiative/

SFI,
www.cbp.gov/linkhandler/cgov/newsroom/fact_sheets/trade_security/sfi/sfi_scanning.ctt/
sfi_scanning.pdf, 2010-07-22

SFI Honduras Port,
www.cbp.gov/linkhandler/cgov/newsroom/fact_sheets/trade_security/sfi/sfi_honduras.ctt/sfi_honduras.pdf, 2010-07-22

Singapore Customs, *Secure Trade Partnership*,
http://www.mardep.gov.hk/en/publication/pdf/portstat_2_y_b5.pdf

Statistik från Transportbildguiden, antalet nyregistrerade bilar under början av 2009
www.transportbilsguiden.se

Tollkonsuly, *www.tollkonsult.no/uploads/DagensHandel.pdf*

Trade Act of 2002 – Advance Electronic Information,
www.cbp.gov/xp/cgov/trade/trade_outreach/advance_info/

U.S. Customs and Border Protection;

15.3 Muntliga källor

Transportsäkerhetsdagarna 2009, Per-Arne Nilsson, Polismyndigheten i Västra Götaland

Ekwall, Daniel, Transportindustriförbundets säkerhetskommitté, möte om securityfrågor 23 mars

Bilagor

Bilaga 1 – Kriminologiska teorier

Det första blocket påvisar ett antal (5 st) exempel på teorier vilka kan ge svaret på biologiska och psykologiska orsaker till varför ett brott begås.

Lombroso (1876) Den födde brottslingen, Varför blir människor brottslingar?
Brottsligt beteende orsakas (i senare versioner – i huvudsak) av medfödda egenskaper hos vissa individer. Dessa människor utgör ett slags tillbakagång (atavism) i den naturliga evolutionen av arten människa.

Kindberg (1930) Klinisk kriminologi, Varför blir människor brottslingar?
Brottsligt beteende är i huvudsak medfött, miljön kan dock ha en viss påverkan.

Bla Darnasio (1995) Skador på hjärnans frontal lob, Vad orsakar brottslighet och annat antisocialt beteende hos en människa?
Brottsligt beteende orsakas av att de delar av hjärnan, främst frontalloben, som styr socialt beteende är skadade eller felutvecklade.

Bla Linnoila (1983) Svagt eller instabilt serotonergt system, Vad orsakar ökade risker för brottsligt – i synnerhet våldsamt beteende hos individen?
Brottsligt beteende är relaterat till underskott av signalsubstansen serotonin i individens hjärna. Detta underskott orsakar att individen utvecklar sensationssökande personlighet som i sin tur kan uttrycka sig i våldsamt och annat antisocialt beteende. Det finns samband mellan låga serotoninnivåer och bland annat ADHD och psykopatiska personligheter.

Bla Trasler (1962) Kriminell personlighet, Vad ökar risken för grovt brottsligt beteende hos individen?
Risken för grovt brottsligt beteende är stor hos individer som på grund av medfödda eller förvärvade egenskaper är känsliga för händelser i livshistorien som hindrar en normal socialiseringsprocess.

Nedan följer ett antal (4 st) kontrollteorier vilka kan ge läsaren en inblick i varför vissa människor väljer att inte begå brott medan andra gör det.

Sykes och Matsza (1957, 1978) Neutraliseringstekniker, Vad möjliggör för människor att begå brott?
Brottsligt beteende blir möjligt genom att individer med hjälp av olika tekniker förmår att neutralisera de i samhället rådande normerna. Dessa neutraliseringar underlättas av att individen tillhör en grupp som ägnar sig åt brott. I synnerhet pojkar, som har ytliga relationer till andra medlemmar i gruppen, kan ”driva in” i ett brottsligt beteendemönster som de tror är vanligt hos andra av gruppens medlemmar.

Hirschi och Kornhauser (1978,1969) Sociala bandteorin, Vad gör att människor begår brott?
Människor begår inte brott om de har starka band med det etablerade samhället. Brottligt beteende blir möjligt när individens band med det etablerade samhället, definierade som anknytning, åtagande, delaktigt och övertygelse, är svaga.

Cornish och Clarke (1986), Clarke (1995) Tillfällesstrukturteorin, Vad påverkar brottsnivån i ett samhälle?
Brottsnivån påverkas i första hand av förändringar i tillfällesstrukturen. Människors beslut att begå brottsliga handlingar är rationella. Är tillfällesstrukturen gynnsam för vissa typer av brott ökar dessa.

Cohen och Felson (1979), Felson (1998) Rutinaktivitetsteorin, Vad påverkar brottsnivån i ett samhälle?
Variationer i brottsnivån orsakas av förändringar av befolkningens rutinaktiviteter (levnadssätt) som påverkar samspelet mellan motiverade förövare, sårbara objekt och avsaknaden av kapabla väktare.

Nedan följer 2 st integrerade teorier. Dessa är en produkt av att en kriminologisk ansats ej är användbar fullt ut, framför allt inte när det gäller med djupgående studier av specifik brottslighet, eller ett fördjupat forskningsområde exempelvis brottslingens karriär. Då man ställer två teorier mot varandra (integrerade teorier) lyckas man sällan få en entydig bekräftelse eller falsifiering. Vanligen blir utfallet av sådan testning att båda teorierna får ett visst stöd.

Thornberry (1996), Thornberrys interaktionistiska teori, Vad ökar sannolikheten för brottslighet hos individer?
Brottslighet orsakas av en process bestående av interaktioner mellan försvagade band till samhället (till att börja med föräldrar) och inlärning i brottsligt beteende (främst av jämnåriga klamrater).

Farrington (1996) Farringtons multifaktorella teori, Vad orsakar kriminellt beteende?
Kriminellt beteende orsakas av att följande psykologiska och sociala variabler interagerar med varandra under individens livscykel: impulsivitet och låg intelligens hos individen, dåligt fungerande uppfostran, antisocialt beteende hos föräldrar, social och ekonomisk fattigdom samt barnets tidigare antisociala beteende.

Nedan följer 2 st teorier vilka ligger till grund för samhällets reaktion på brott ses ur ett kriminologiskt perspektiv.

Beccaria (1764) klassisk teori, Varför skall samhället reagera på brott?
Syftet med samhällets reaktion på brott ska vara prevention. Reaktionen skall vara human. Genom att tillfoga pain som reaktion på den pleasure som orsakas av brottet kan man få både allmän- och individualpreventiva effekter.

Justitiedepartementet (1996) lokal brottsprevention, Hur kan brott förebyggas?
Brott kan förebyggas på en lokal nivå och utanför den traditionella straffrättspolitiska sfären. Detta kan göras genom social och situationell brottsprevention där utöver de lokala myndigheterna och företagen också frivilliga organisationer och vanliga medborgare kan engageras.

Bilaga 2 - Intervjufrågor

INTERVJUFRÅGOR

1. Vilket är det största säkerhetshotet idag i er verksamhet?

Rubrik	
Stöld (hot,våld,rån)	
Smuggling	
Trafficking*	
Terrorism	
Skadegörelse	

*Trafficking (människosmuggling)

2. Hur ofta händer något av rubriker nedan er?

Rubrik	**Aldrig**	**1-50ggr/år**	**Oftare**
Stöld			
Smuggling			
Trafficking			
Terrorism			
Skadegörelse			

3. Var i transportkedjan händer något av rubriker nedan er?

Rubrik	Terminal (er)	På väg/JVG	Rastpl. (er)	Omlastn. term. (er)	Annan plats geografiskt
Stöld					
Smuggling					
Trafficking					
Terrorism					
Skadegörelse					

4. Ser ni en trend till ökning i något av nedanstående ingrepp?

Rubrik	Ja	Nej
Stöld		
Smuggling		
Trafficking		
Terrorism		
Skadegörelse		

5. Hur tror ni trenden ser ut om 2 år?

Rubrik	Minskning	Ökning
Stöld		
Smuggling		
Trafficking		
Terrorism		
Skadegörelse		

6. Vad tänker ni göra för motåtgärder för rubrikerna nedan?

Rubrik	Åtgärd
Stöld	
Smuggling	
Trafficking	
Terrorism	
Skadegörelse	

7. Har ni uppskattat kostnader för dessa motåtgärder?

Rubrik	Åtgärd
Stöld	
Smuggling	
Trafficking	
Terrorism	
Skadegörelse	

8. Vilka rutiner har ni för rapportering av ingreppen internt?

Rubrik	Via telefon	Rapp-system	Via e-mail	Inget	På annat sätt
Stöld					
Smuggling					
Trafficking					
Terrorism					
Skadegörelse					

9. Vilka rutiner har ni för rapportering av ingreppen externt och vilka parter involveras i så fall?

Rubrik	Via telefon	Rapp-system	Via e-mail	Inget	På annat sätt	Involverade parter
Stöld						
Smuggling						
Trafficking						
Terrorism						
Skadegörelse						

10. För ni statistik över ingreppen?

Ja	**Nej**

11. Gör ni kostnadsanalyser av ingreppen?

Ja	Nej

12. Tror ni att det finns ett mörkertal för rapportering av ingrepp om ja, hur många procent tror ni att det handlar om?

Ja	Nej

13. Kan vi få ta del av er statistik till detta projekt?

Ja	Nej

14. Vilka kostnader har Ni för dessa områden respektive ingrepp enlig rubriker nedan?

Rubrik	Kr/år
Stöld	
Smuggling	
Trafficking	
Terrorism	
Skadegörelse	

15. Vad tror ni kan tänkas hända som ännu inte hänt (ge exempel, mellanlastning m.m.)?

Rubrik	Orsaker

16. Vad gör Ni för att höja säkerheten inom ert företag, terminal, uppställningsområde och under transporten?

Kategori	Rubrik	Ja	Nej
Säkerhetsledningssystem Rutiner/procedurer			
	Anställning		
	Utbildning		
	ID kort		
	Nyckel/kort hantering		
	Regel/rutin Uppföljning		
	Riskanalys transport		
	Informationssäkerhet		

Kategori	Rubrik	Ja	Nej
Fysiskt skydd fastighet/område			
	Lås		
	Larm		
	Perimeter skydd		
	Belysning		
	Cctv		
	Bevakning		
Fysiskt skydd lastbärare			
	Lås		
	Larm		
	Positionering		

17. Om Ni vidtagit åtgärder för att höja säkerheten inom ert företag, terminal, uppställningsområde och under transporten. Vilka kostnader har detta medfört?

Kategori	Rubrik	Kr/år
Säkerhetsledningssystem Rutiner/procedurer		
	Anställning	
	Utbildning	
	ID kort	
	Nyckel/kort hantering	
	Regel/rutin Uppföljning	
	Riskanalys transport	
	Informationssäkerhet	
Fysiskt skydd fastighet/område		
	Lås	
	Larm	
	Perimeter skydd	
	Belysning	
	Cctv	
	Bevakning	

Kategori	Rubrik	Kr/år
Fysiskt skydd lastbärare		
	Lås	
	Larm	
	Positionering	

18. Vilken sort av lastbärare hanterar Ni?

Rubrik	Ja	Nej
Containers		
Flak med kapell		
Skåpspåbyggnad		
Gardintrailer		
Öppna flak		
Annat:		

19. Vilken sort av lastbärare har Ni haft flest ingrepp i/mot?

Rubrik		
Sort:		

20. Har ni noterat någon skillnad i ingrepp mellan de olika latbärarna – plomberade/oplomberade och låsta/olåsta, som ni använder?

Rubrik	Plomberad	Oplomberad	Låsta	Olåsta
Containers				
Flak med kapell				
Skåpspåbyggnad				
Gardintrailer				
Öppna flak				
Annat:				

21. Om ni vidtagit åtgärder för att höja säkerhet på era terminaler och på era lastbärare, har ni då fått ut något mervärde av dessa åtgärder från nedan listade intressenter?

Rubrik	Ja	Nej
Försäkringsbolag Lägre premier, rabatter..		
Godsägare Ökade transporter, höjda fraktkostnader..		
För ert namn Goodwill, större andelar på marknaden..		
Annat:		

22. Ange vilka regelverk, konventioner, frivilliga överenskommelser, ledningssystem, kundkrav som gäller för transporter/terminaler inom ert företag?

Rubrik	Ja	Nej
TVL Trafikvägslagen		
JVTL Järnvägstrafiklagen		
TSVFS Trafiksäkerhetsverkets författningssamling		
SFS Svensk författningssamling		
AFS Arbetsmiljöverkets författningssamling		
VBL Vägarbetstidslagen		
ADR		
RID		
IMDG		
ISPS		
ISO 9001		
ISO 14001		
CIM Det internationella fördraget ang. godsbefordran på järnväg. Föredraget från 1970 ersattes 1980 av COTIF-konventionen.		

Rubrik	Ja	Nej
C-TPAT Customs-Trade Partnership Against Terrorism		
TAPA The Transported Asset Protection Association (TAPA)		
CMR Konventionen den 19 maj 1956 om fraktavtalet vid internationell godsbefordran på väg.		
CMR-lagen Lag den 24 januari1969 med anledning av Sveriges tillträde till konventionen den 19 maj 1956 om fraktavtalet vid internationell godsbefordran på väg (SFS 1969:12)		
Kundkrav		
Annat:		

23. Ser ni några motsägelser mellan de olika regelverken som påverkar er verksamhet?

Rubrik	**Ja**	**Nej**	**Hur?**
Motsägelser			

24. Hur bevakar ni kommande regelverk som kan påverka er verksamhet?

Rubrik	Ja	Nej	Hur?
Kommande regelverk			

25. Känner ni till följande EN förslaget för säkrare transporter och ISO/PAS 28000:2005 standarden?

Rubrik	Ja	Nej
EN/EU Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on enhancing supply chain security "Secure operator"		
ISO/PAS 28000:2005 specification for security management systems for the supply chain is a risk based management system.		

26. Vad tror ni inom branschen krävs för att höja säkerhetens minimikrav "security" (morot eller piska/skall krav för alla)?

Rubrik	Åtgärder
Höja säkerhetens minimikrav	

27. Transporterar/hanterar ni farligt gods?

Rubrik	Ja	Nej
Farligt gods		

28. Enligt vilket regelverk transporterar/hanterar ni farligt gods?

Rubrik	Ja	Nej
ADR		
RID		
IMDG		
Östersjöavtalet		

29. Känner Ni till de reviderade delarna i nedan angivna regelverk?

Rubrik	Ja	Nej
ADR (Kap. 1.10)		
RID (Kap. 1.10)		
IMDG (Kap. 1.4)		

MariTerm AB

Tel. +46 (0)42 33 31 00
Fax. +46 (0)42 33 31 02
P.O. Box 74
SE-263 21 Höganäs
SWEDEN

www.mariterm.se