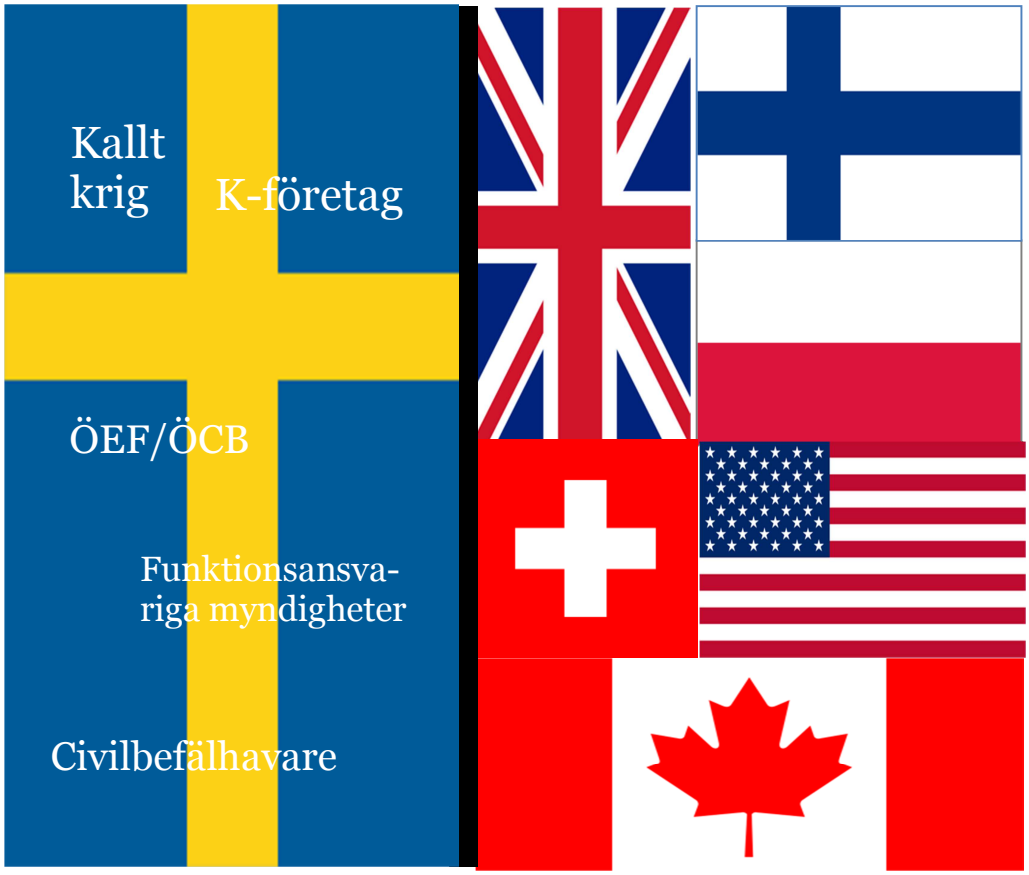
Myndigheten för samhällsskydd och beredskap

SKYDD AV SAMHÄLLSVIKTIG VERKSAMHET

En historisk respektive internationell kartläggning av arbetet med skydd av samhällsviktig verksamhet



MSB:s kontaktpersoner:
Anna Rinne, 010-240 54 15
Omar Harrami, 010-240 53 59

Publikationsnummer MSB841 – Mars 2015
ISBN 978-91-7383-563-3

Förord

Detta är en övergripande kartläggning av hur skyddet av samhällsviktiga verksamheter har organiserats, samordnats och styrts i Sverige sedan 1970-talet respektive hur skyddet av samhällsviktiga verksamheter idag organiseras, samordnas och styrs i sex andra länder: Schweiz, Finland, Polen, Storbritannien, Kanada och USA.

Kartläggningen syftar till att ge arbetsgruppen för MSB:s delprojekt Sektorsvisa planer samt representanter från myndigheter och näringsliv som deltog i en workshopserie i november 2014 om sektorsvisa planer en ökad kunskap om olika sätt att organisera, samordna och inrikta skyddet av samhällsviktiga verksamheter. Målet med kartläggningen har också varit att i möjligaste mån bidra till en ökad kunskap om för- och nackdelar med olika sätt att arbeta med samhällsviktiga verksamheter samt ökad förståelse för tänkbara orsaker till de olika sätten att organisera och samordna arbetet. Kartläggningen, som endast är övergripande, har genomförts av FOI, genom Per Larsson och Lotta Ryghammar.

Innehållsförteckning

Inledning **9**
Kartläggningens redovisning 9

DEL I

1 Inledning **11**
1.1 Bakgrund och förutsättningar 11
1.2 Ekonomiskt försvar 11
1.3 Ledningsstruktur 12
2 1970-talet **14**
2.1 Program 15
2.1.1 Exemplet programmet Livsmedel 16
3 1980-talet **18**
3.1 Funktioner 18
3.1.1 Överstyrelsen för civil beredskap (ÖCB) 19
3.1.2 Exemplet funktionen Industriell beredskap 19
3.1.3 Exemplet funktionen livsmedelsförsörjning med mera 21
4 1990-talet **22**
5 2000-talet **26**
6 En historisk överblick – några iakttagelser **31**
6.1 Utvecklingsbehov 31
6.2 Drivkrafter 31
6.3 Privat-offentlig samverkan 33
6.4 Sektorsansvaret 34
6.5 Slutord 34
7 Underlag **35**

Del II

1 Inledning **37**
1.1 Bakgrund och förutsättningar 37
1.2 Slutsatser 37
1.2.1 Generella iakttagelser 37
1.2.2 Sveriges arbete med skydd av samhällsviktiga verksamheter i förhållande till de kartlagda länderna 45
2 Schweiz **48**
2.1 Definition, mål och sektorsindelning 48
2.2 Doktrin och styrmedel 50
2.3 Organisering och ledning 51

2.3.1 Nationell nivå ... 51
2.3.2 Kantonerna ... 56
2.3.3 Ägare och operatörer ... 56
2.3.4 Federal Office for National Economis Supply (FONES) ... 56
3 Finland ... 58
3.1 Doktrin och styrmedel ... 58
3.2 Organisation och ledning ... 60
3.2.1 Statsrådet och ministerier ... 62
3.2.2 Försörjningsberedskapsorganisationen ... 63
3.2.3 Försörjningsberedskapscentralen ... 63
3.2.4 Försörjningsberedskapsrådet ... 64
3.2.5 Näringslivets sektorer och pooler inom försörjningsberedskapen ... 64
3.2.6 Regional och lokal nivån ... 65
3.2.7 Lokal nivå – Kommunerna ... 65
4 Polen ... 67
4.1 Definition, mål och sektorsindelning ... 67
4.2 Organisering och styrning ... 68
4.3 Doktrin och styrmedel ... 69
5 Storbritannien ... 76
5.1 Definition och sektorsindelning ... 76
5.2 Organisering och ledning ... 77
5.2.1 Departement ... 77
5.2.2 CCS och CPINI ... 78
5.2.3 CCS ... 79
5.3 Den lokala nivån ... 79
5.4 Utvecklingen av arbete med robusthet i kritisk infrastruktur på sektorsövergripande nationell nivå ... 80
5.5 Doktrin och styrmedel ... 81
5.5.1 Kontinuitetsplanering för företag och organisationer ... 86
6 Kanada ... 89
6.1 Definitioner, organisering och ledning ... 89
6.2 Doktrin och styrmedel ... 93
6.2.1 National Strategy for Critical Infrastructure” från 2009 och tillhörande ”Action Plan for Critical Infrastructure 2014-2017” ... 95
6.2.2 ”Risk Management Guide for Critical Infrastructure Sectors” ... 97
6.2.3 USA:s Regional Resilience Assessment Programme (RRAP) ... 97
6.3 Kanadensiskt samarbete med USA rörande kritisk infrastruktur 97
7 USA ... 100
7.1 Definitioner och sektorer ... 100
7.2 Organisation och ledning ... 101
7.2.1 Presidenten ... 101
7.2.2 Department of Homeland Security ... 101
7.2.3 Sektorspecifika departement och federala myndigheter ... 106

7.2.4 Regeringar och styrande organ på delstatsnivå, lokal nivå, stam- och territorium nivå samt regionala samverkansorgan (privat-offentlig samverkan) 106
7.2.5 Rådgivande organ på federal nivå 107
7.2.6 Ägare och operatörer av kritisk infrastrutkur 107
7.2.7 ”Partnerskap” för att skydda och stärka den kritiska infrastrukturen i USA 107
7.3 Doktrin och styrmedel 109

Bilaga 1: Program 114

Bilaga 2: Funktioner 115

Bilaga 3: Samverkansområden 116

Sammanfattning

I denna rapport redovisas en övergripande kartläggning av hur skyddet av samhällsviktiga verksamheter har organiserats, samordnats och styrts i Sverige sedan 1970-talet respektive hur skyddet av samhällsviktiga verksamheter idag organiseras, samordnas och styrs i sex andra länder: Schweiz, Finland, Polen, Storbritannien, Kanada och USA. De båda delarna redovisas separat.

Historisk kartläggning

Erfarenheterna från första världskriget visade att hela samhällsekonomin måste mobiliseras för att krigsberedskapens krav skulle kunna mötas. Ett strukturerat arbete påbörjades för att säkerställa strategiska resurser. Under det kalla kriget var skyddet av kritisk infrastruktur en central del av Sveriges civilförsvar. En del av skyddet var också att hålla Sverige oberoende antingen genom en egen produktion av centrala produkter eller genom beredskapslagring. Mot det kalla krigets slut avvecklades de flesta beredskapslager successivt.

Under årens gång har arbetet med samhällsviktig verksamhet bedrivits inom så kallade program och funktioner. Under 1990-talet fokuserades i allt högre grad infrastrukturfrågorna på nya sårbarheter till följd av samhällsutvecklingen. Utifrån en struktur med ett sektors- och områdesperspektiv inrättades 2002 dagens krisberedskapssystem. Eftersom det nya systemet skulle bygga på ett samverkansansvar organiserades samhällssektorerna i samverkansområden som skulle utgöra delar av landets infrastruktur. MSB ska idag i samverkan med de myndigheter som ingår i samverkansområdena utveckla formerna för arbetet med skydd av samhällsviktig verksamhet.

Exposén visar bland annat på en successiv utveckling från ett individperspektiv till ett samhällsperspektiv. Vidare ändras fokus på för totalförsvaret viktiga varor och tjänster i allt högre grad till flöden i samhällsviktig verksamhet.

Med anledning av den historiska överblicken görs några iakttagelser kring utvecklingen av arbetet med samhällsviktig verksamhet ur ett krisberedskapsperspektiv. Det handlar om grundläggande förutsättningar såsom drivkrafter och ett system som har att förhålla sig till ansvar, internationalisering och avreglering. Problemställningarna är sedan årtionden i många fall likartade. Det kan finnas skäl att beakta de absoluta grunderna för arbetet med krisberedskap och skydd av samhällsviktig verksamhet i strävan mot en verklig utveckling.

Internationell kartläggning

Den internationella kartläggningen visar på att Schweiz och Finland har kvar en ansats för skydd av samhällsviktiga verksamheter som i hög grad har fokus på totalförsvarets krav och förutsättningar höjd beredskap och krig (kritisk infrastruktur, kritisk produktion och kritiska resurser). Denna ansats övergavs

av Sverige vid nedmonteringen av det civila försvaret efter det kalla kriget. Här särskiljer sig således Sverige från dessa båda länder.

Vad som vidare särskiljer Sverige från samtliga kartlagda länder är att Sverige inte har samma tydliga ansvarsfördelning bland departement och myndigheter i arbetet med skydd av samhällsviktiga verksamheter. Frågor rörande skydd av samhällsviktiga verksamheter verkar också generellt sett ha en lägre politisk vikt i Sverige än i flera av de kartlagda länderna. I t.ex. USA finns det tydliga drivkrafter att skydda samhällsviktiga verksamheter mot terrorattentat.

I de kartlagda länderna tenderar departement och myndigheter att lägga större fokus på ett ömsesidigt givande ”partnerskap” mellan det offentliga och privata i arbetet med skydd av samhällsviktiga verksamheter än vad som är fallet i Sverige. I övrigt arbetar Sverige och övriga kartlagda länder med ungefär samma ”verktygslåda” med ett antal ”standardverktyg” när det gäller skydd av samhällsviktiga verksamheter. Dessa verktyg utgörs t.ex. av nationella program, risk- och sårbarhetsanalyser, kontinuitetsplanering, ”all-hazard”-ansats, särskilda samverkansstrukturer för privat-offentlig samverkan m.m.

Inledning

Myndigheten för samhällsskydd och beredskap (MSB) fick år 2010 ett regeringsuppdrag att ta fram en nationell strategi för skydd av samhällsviktiga verksamheter. År 2013 fick MSB i uppdrag att, med utgångspunkt i strategin, ta fram en handlingsplan för skydd av samhällsviktiga verksamheter enligt följande: ”Myndigheten för samhällsskydd och beredskap ska ta fram en handlingsplan för skydd av samhällsviktiga verksamheter, utifrån den strategi som myndigheten redovisade den 1 mars 2011. Handlingsplanen ska baseras på strategins principer och prioriterade aktiviteter samt tas fram i samverkan med andra myndigheter, kommuner, Landsting, Länsstyrelser och näringslivet”.

Handlingsplanen färdigställdes under hösten 2013, i den beskrivs ett antal aktiviteter för implementering av ett systematisk säkerhetsarbete. Dessa ska skapa förutsättningar och ge stöd till aktörerna att nå målet 2020: att ett systematiskt säkerhetsarbete är en integrerad del i all samhällsviktig verksamhet på lokal, regional och nationell nivå. För att uppnå målet krävs samverkan och ansvarstagande från samhällets aktörer.

En av de aktuella aktiviteterna är delprojektet Sektorsvisa planer. Inom ramen för detta delprojekt har FOI haft i uppdrag att som underlag till en workshop-serie med offentliga och privata aktörer göra en historisk svensk respektive internationell kartläggning av arbetet med skydd av samhällsviktiga verksamheter. Kartläggningen har varit av övergripande karaktär och är därför på intet sätt uttömmande, utan är främst tänkt att fungera som en allmän idébank. Underlaget till workshopserien har syftat till öka kunskapen om olika sätt att organisera, samordna och inrikta skyddet av samhällsviktiga verksamheter över tid och rum och därigenom ge uppslag och idéer för hur det framtid arbetet med sektorsvisa planer kan fortskrida.

Kartläggningens redovisning

Nedan redovisas kartläggningen i två från varandra fristående delar. I den första delen presenteras en historisk kartläggning av hur skyddet av samhällsviktiga verksamheter har organiserats, samordnats och styrts i Sverige sedan 1970-talet, med tillbakablickar till första världskriget. I den andra delen presenteras hur skyddet av samhällsviktiga verksamheter idag organiseras, samordnas och styrs i sex olika länder: Schweiz, Finland, Polen, Storbritannien, Kanada och USA.

Del 1.

En övergripande kartläggning av hur skyddet av samhällsviktiga verksamheter har organiserats, samordnats och styrts i Sverige sedan 1970-talet

1 Inledning

1.1 Bakgrund och förutsättningar

För att fördjupa och bredda kunskapen om hur skyddet av samhällsviktig verksamhet organiserats, samordnats och styrts i ett historiskt perspektiv har olika strukturer för skydd av samhällsviktig verksamhet i Sverige kartlagts sedan 1970-talet. Kartläggningen avser att ge en övergripande bild av de nationella och idémässiga grunderna som utgör sammanhanget i vilket arbetet med skydd av samhällsviktig verksamhet utvecklats. I det följande beskrivs *strukturer för skydd av samhällsviktig verksamhet – då och nu*.

1.2 Ekonomiskt försvar

Uttrycket ekonomiskt försvar förekom redan i totalförsvarsdiskussionerna under mellankrigstiden. Erfarenheterna från första världskriget visade att hela samhällsekonomin måste mobiliseras för att krigsberedskapens krav skulle kunna mötas. För Sveriges del medförde kriget livsmedelsbrist och fördelningsproblem som inte kunde klaras av en ohanterlig och illa förberedd krisbyråkrati.

Bild 1. En strukturerad försörjningsberedskap tog sin början i en annan tid.

För att ta till vara dessa erfarenheter och undvika en upprepning av misstagen inrättas en ny myndighet. Som central myndighet för försörjningsfrågor inrättades år 1928 Rikskommissionen för ekonomisk försvarsberedskap (RKE). Det ekonomiska försvaret syftade till att säkerställa tillgång på och produktionskapacitet av strategiska resurser. RKE arbetade den första tiden huvudsakligen med att bygga upp beredskapslager av viktiga varor med tanke på en avspärrningssituation liknande den rådande under första världskriget. Andra världskriget utvecklades till ett resurs- och produktionskrig och under kalla kriget kom även skyddad produktion att bli en viktig aspekt av det ekonomiska försvaret. Det ekonomiska försvaret utgjorde en intressant gränsgångare mellan civilt och militärt försvar. År 1962 ersattes RKE med Överstyrelsen för ekonomisk försvarsberedskap (ÖEF), senare kallad Överstyrelsen för ekonomiskt försvar.

I det totalförsvar som skapades var det ekonomiska försvaret en av grundpelarna. Totalförsvarets civila delar omfattade det ekonomska försvaret, det civila försvaret, det psykologiska försvaret och det som gick under bedömningen övrigt totalförsvar. I övrigt totalförsvar ingick bland annat hälso- och sjukvården, polisväsendet och telekommunikationerna. Det ekonomiska försvaret, det vill säga de åtgärder som krävdes för att förbereda och underlätta samhällets anpassning till skilda krissituationer, hade en annan karaktär än övrig verksamhet i den meningen att det här var näringslivet och inte myndigheterna som utgjorde den viktigaste resursen för försörjningsberedskapen. Det ekonomiska försvaret omfattade i princip hela näringslivet.

Uppfattningen var att i kriser och krig, då landets fred och frihet var hotad, måste stora uppoffringar göras och den fredstida standarden avsevärt sänkas. I sådana kriser kunde samhället inte fungera som i fredstid utan betydande omställningar var ofrånkomliga för att i största möjliga utsträckning öka värnkraften och mildra medborgarna prövningar och lidanden,

1.3 Ledningsstruktur

Inom totalförsvaret utövades fram till och med år 2000 områdesansvaret på fem ledningsnivåer av särskilt utsedda lednings- och samordningsorgan. Den högsta ledningen utgjordes av riksdagen och regeringen. Ansvarsfördelningen inom totalförsvarets övriga fyra ledningsnivåer under delar av 1980-talet samt under 1990 talet framgår av tabell 1.

Ledningsnivå	Civilt försvar	Militärt försvar
Central	ÖCB[1] och andra FAM[2]	ÖB och HKV[3]
Högre regional	CB och andra civila ledningsorgan	MB
Lägre regional	Länsstyrelser och andra civila ledningsorgan	Fobef
Lokal	Kommuner och andra civila ledningsorgan	Lokal militär chef

Tabell 1: Totalförsvarsmyndigheter under delar av 1980-talet samt under 1990-talet.

Civilbefälhavaren (CB)[4] var i fred ett rent beredskapsorgan. I krig samordnade CB verksamheten inom civilområdet i samverkan med militärbefälhavare (MB).

[1] Överstyrelsen för civil beredskap, se vidare kapitel 3 om 1980-talet.

[2] Funktionsansvariga myndigheter, se vidare kapitel 3 om 1980-talet.

[3] Högkvarteret.

[4] Civilbefälhavarinrättningen tillkom 1952 och upphörde den 31 december 2000.

Beroendet mellan totalförsvarets civila och militära del var ömsesidig. I fred skulle CB i samverkan med MB utarbeta en grundsyn som underlag för planeringen av totalförsvarets verksamhet inom civilområdet, upprätta planer för civilområdet, tillsammans med MB leda regionala ledningsövningar inom civilområdet, verka för att personal hos civila myndigheter inom civilområdet utbildades, organisera och öva det egna kansliet samt leda och samordna signalskyddstjänsten inom området. CB meddelade länsstyrelserna de föreskrifter som behövdes för planläggningen inom totalförsvaret. CB meddelade också andra myndigheter föreskrifter om inriktningen av de beredskapsförberedelser som berörde civilområdet.

Samverkan inom totalförsvarets militära och civila delar skedde även genom att operativa grundsyner, det vill säga gemensamma inriktningar, utarbetades på lägre regional nivå av länsstyrelser och försvarsområdesbefälhavare (fobef).

Centrala myndigheter med ett särskilt ansvar, kunde också utse särskilda samverkansgrupper eller kontaktpersoner som i kris skulle tjänstgöra hos de områdesansvariga lednings- och samordningsorganen.

2 1970-talet

Under 1970-talet angav målen för totalförsvaret att folkförsörjningen i vidaste bemärkelse skulle tryggas genom det ekonomiska försvaret. Även med tillägget ”i vidare bemärkelse” ledde det tanken bort från de komplicerade beroendeförhållanden mellan olika varor och tjänster som måste beaktas för att försörjningssystemen hjälpligt skulle fungera och individens försörjning tryggas. I 1977 års försvarsbeslut fastställdes som ett allmänt mål för det ekonomiska försvaret till att ”trygga försörjningen för det svenska samhället”. Formuleringen innefattade både individerna, näringslivet och samhällsapparaten i övrigt. Det uttrycktes vidare att olika försörjningsområden måste ha en standard och uthållighet som fordrades för en tryggad försörjning och för en trovärdig försörjningsberedskap gentemot omvärlden.

Under andra världskriget baserades den svenska industrin i väsentlig omfattning på inhemska råvaror och produkterna avsattes till största delen inom landet. 30 år senare hade bilden förändrats starkt genom utvecklingen mot specialisering och internationalisering samt beroende av import med följden att försörjningen blev alltmer sårbar för olika störningar. Fredskriser aktualiserade ökad beredskapslagring av olja enligt program med skyldighet för oljebolag och storkonsumenter att medverka. Till textil-, konfektions-, sko- och garveriindustrierna utgick statligt stöd för att kunna upprätthålla en ur beredskapssynpunkt nödvändig produktionskapacitet.

I det ekonomiska försvarets planläggningsarbete deltog företag och olika sammanslutningar. Till skillnad mot militärt och civilt försvar bestod det ekonomiska försvaret inte av olika enheter utan utgjorde snarare ett samlingsbegrepp för hur näringslivet skulle anpassa sig till ändrade förhållanden. De behov som fanns av varor och tjänster inom respektive område utgjorde underlag för planläggningen. Det militära försvaret, civilförsvaret, sjukvården, kommunikationsverken och andra totalförsvarsmyndigheter skulle var och en för sin del klara ut vilka behov som kunde förutses. För övriga behov, det vill säga för planläggningen inom områden som inte kunde hänföras till någon annan myndighets fredstida verksamhet, till exempel befolkningen, bränsle- och drivmedelsförsörjningen, huvuddelen av industriproduktionen samt det mesta av beredskapslagringen svarade ÖEF, i fråga om livsmedel och fodermedel svarade Statens jordbruksnämnd. Tillgångarna var näringslivets lager och produktionsresurser samt statliga och kommunala lager.

Ansvaret för beredskapen var fördelad på ett stort antal myndigheter. Därför krävdes samordning, en uppgift som åvilade ÖEF. Flera centrala myndigheter hade en rådgivande delegation, ett beredskapsråd, vid sin sida för behandling av frågor med särskild betydelse. Det gällde Socialstyrelsen, Statens jordsbruksnämnd, Transportnämnden och ÖEF.

För den samlade försörjningsberedskapen var uppsatt ett försörjningsmål. För de kompletterande åtgärderna uppställdes särskilda mål, till exempel lagringsmål, vilka skulle uppfyllas genom det ekonomiska försvarets verksamhet i

fred. Ansvaret för att beredskapsåtgärder vidtogs åvilade såväl myndigheter som näringsliv och organisationer. En grundläggande princip inom totalförsvaret var att den myndighet som i fred svarade för viss för totalförsvaret viktig verksamhet hade motsvaranden ansvar i krig och därmed också ansvar för erforderliga beredskapsförberedelser. Beredskapsverksamheten på regional nivå var knutet till de centrala myndigheternas läns- och distriktorganisationer. Därutöver utfördeds regionala beredskapsförberedelser av landets civilbefälhavare och länsstyrelser. På lokal nivå ankom det främst på kommunerna att vidta beredskapsåtgärder.

Det kan konstateras att beredskapsverksamheten inom det ekonomiska försvaret i ökande omfattning inriktades mot att förstärka landets försörjningsberedskap mot fredskriser. Försvarsutskottet hade i olika sammanhang från och med 1974 uttalat att fredstidsproblematiken måste ägnas en ökad uppmärksamhet i det ekonomiska försvarets planering.

Bild 2. Oljekrisen 1973/74 visade på leverans- och beroendeförhållanden samt behov av åtgärder från statsmakterna att möta en fredskris.

Ambitionsnivån för uthållighet vid fredskriser borde enligt utskottet vara att så långt möjligt upprätthålla normal fredsstandard samt att undvika störningar i viktiga samhällsfunktioner.

2.1 Program

Från och med budgetåret 1975/76 redovisades ÖEF:s verksamhet i programtermer. Det innebar att verksamheten i fortsättningen delades upp på ett antal program enligt följande indelning.

1. Livsmedel
2. Beklädnad med mera
3. Bränsle, drivmedel
4. Sjukvård
5. Kemiska produkter med mera
6. Metaller med mera
7. Övrigt

Se vidare om programindelningen i bilaga 1.

Inom programmet *Livsmedel* föll huvuddelen av beredskapsförberedelserna för livsmedelsförsörjningen inom Statens jordbruksnämnds ansvarsområde. Nämnden svarade för alla behovsberäkningar. Till programmet *Övrigt* hänfördes dels verksamhet inom ÖEF:s utredningsbyrå och varubyrå som var gemensamma för flera program eller inte hänförligt till något program. Vid programredovisningen delades verksamheten in i sex verksamhetsområden enligt följande.

1. Övergripande planläggning
2. Företagsplanläggning
3. Beredskapslagring
4. Samordning
5. Information och utbildning
6. Administration

Verksamhetsområdena underindelades i sin tur utifrån olika krav och behov.

2.1.1 Exemplet programmet Livsmedel

Enligt instruktionen för statens jordbruksnämnd (JN) åvilade det nämnden att svara för sådana uppgifter i fråga om den ekonomiska försvarsberedskapen som avsåg livsmedel, fodermedel, utsäde och fettråvaror. Inköp och lagerhållning av sådana varor i beredskapssyfte ankom på JN endast i den omfattning regeringen bestämde. Någon mer preciserad målsättning för försvarsberedskapen (uthållighet och näringsstandard) inom nämndens område hade inte fastställts av statsmakterna år 1977. JN hade i sin planering utgått från att livsmedelsberedskapen borde vara så uppbyggd att den kunde möta en treårig handelspolitisk avspärrning utan krigshandlingar i vårt land. Därutöver skulle finnas viss beredskap för krigsfall.

Bild 3. Ett särskilt prioriterat område var naturligtvis livsmedelsförsörjningen. När det gäller de viktigaste baslivsmedlen var Sverige i stort sett självförsörjande. Landet var däremot importberoende av bland annat gödselmedel. Utan konstgödsel skulle avkastningen av vår åkermark minska betydligt.

Bland de beredskapsåtgärder som JN vidtagit under perioden märktes upprättande av lagringsplaner, påbörjad översyn av ransoneringssystemet, planering för ersättningsproduktion, statlig beredskapslagring, planläggning för omställning till krisorganisation samt information och utbildning.

På livsmedelsområdet räknade man med att vi skulle få lika mycket kalorier som i fredstid – 2900 kcal per person och dag – men med en näringssammansättning så att inte några bristsjukdomar skulle uppkomma. Vi skulle få äta en på annat sätt sammansatt kost, den så kallade kriskosten.

I en krigssituation angavs problemen främst uppkomma inom livsmedelsindustrin med hänsyn till dess ökande koncentration och utsatta lokalisering. Inom varudistributionen väntades utvecklingen gå mot ett minskat antal butiker och ett sjunkande antal centrallager med ökad sårbarhet som följd. Jordbruket var vidare i hög grad importberoende av drivmedel, maskindelar, handelsgödsel och bekämpningsmedel.

Styrinformation för programplanen utgjordes av genomförda perspektivstudier, 1974 års försvarsberednings betänkande (SOU 1976:5) samt chefens för handelsdepartementet programplaneanvisningar som angav programmets omfattning och ekonomiska förutsättningar. Utifrån ett antal mål för beredskapsverksamheten föreslog JN förslag till beredskapsåtgärder.

3 1980-talet

För att planeringen och beredskapsåtgärderna skulle få en enhetlig inriktning var samordning nödvändig. Verksamheten inom den civila delen av försvaret indelades i funktioner motsvarande samhällssektorerna med en funktionsansvarig myndighet (FAM) för varje funktion.

Redan 1978 års försvarskommitté konstaterade att samordningsfunktionen på den centrala nivån var splittrad och att ingen central myndighet kunde överblicka de civila delarna av totalförsvaret. Allmänna utgångspunkter för myndigheterna planering var dels den fortgående utvecklingen inom berört område, dels de oftast mycket allmänt formulerade riktlinjer för beredskapen som lämnades av regeringen och riksdagen. Det fanns emellertid ingen myndighet utöver ÖEF som hade till uppgift att vidare utveckla och konkretisera dessa. De kunde därför ges olika innebörd av ansvariga beredskapsmyndigheter. På flera områden saknades dessutom konkreta utgångspunkter för planeringen. För att planeringen och beredskapsåtgärderna skulle få en enhetlig inriktning var samordning nödvändig. Med syfte att effektivisera verksamheten fattade riksdagen våren 1985 vissa beslut om ledningen av den civila delen av totalförsvaret.

Ett system för ledning och samordning att tillämpas inom det civila försvaret trädde i kraft den 1 juli 1986. Ett syfte med detta system var att möjliggöra den kraftsamling av resurser som krävs för att landet skall kunna möta ett väpnat angrepp. Ett annat syfte var att tillhandahålla effektiva former för samverkan mellan militärt och civilt försvar. Dimensionerande för det system för ledning och samordning som infördes år 1986 var den säkerhetspolitiska hotbild som var aktuell vid denna tidpunkt. Den mest krävande situation som systemet skulle kunna hantera var ett väpnat angrepp mot Sverige som syftar till en ockupation av landet som helhet eller en del av detta.

3.1 Funktioner

1986 års reform av ledningssystemet inom det civila försvaret innebar bland annat att verksamheten med utgångspunkt i funktionsbegreppet delades upp i funktioner motsvarande samhällssektorerna med en funktionsansvarig myndighet (FAM) för varje funktion (se bilaga 2). En funktion måste kunna upprätthållas i större eller mindre omfattning också under kriser och krig samt omfattade all samhällsverksamhet som inom det aktuella sakområdet hade särskild betydelse för totalförsvaret. Den omfattade inte endast statlig och kommunal verksamhet. I många funktioner hade organisationer och företag viktiga eller dominerande uppgifter vid genomförande av verksamheten. Kriteriet för när en verksamhet inom det civila försvaret skulle anses vara en funktion var att verksamheten krävde någon form av central statlig styrning och att flera myndigheters verksamhet måste samordnas. En funktion bestod därför normalt av flera myndigheter och andra organ som bedrev verksamhet på flera

samhällsnivåer. Den ansvariga myndigheten hade inte något ledningsansvar för funktionens verksamhet utan en samordnande och inriktande roll för beredskapsförberedelserna. All verksamhet inom det civila försvaret bedrevs emellertid inte i funktioner. Bland annat utfördes viss verksamhet av så kallade fristående beredskapsmyndigheter. Behovet av styrning uppstod till följd av att verksamheten var komplicerad och hade starka kopplingar till annan verksamhet inom totalförsvaret och det övergripande syftet torde ha varit att underlätta överblicken över och samordningen av en verksamhet som består av ett mycket stort antal aktörer. Grundläggande för det nya lednings- och samordningsansvaret inom det civila försvaret var två skilda typer av ansvar – områdesansvar och funktionsansvar.

3.1.1 Överstyrelsen för civil beredskap (ÖCB)

Överstyrelsen för ekonomiskt försvar ombildades den 1 juli 1986 till Överstyrelsen för civil beredskap (ÖCB) som var central förvaltningsmyndighet för frågor om ledning och samordning av verksamheten inom totalförsvarets civila del. ÖCB ledde och samordnade programplaneringen inom de civila delarna av totalförsvaret och föreslog i detta sammanhang vilka beredskapsåtgärder som borde vidtas inom den ekonomiska planeringsramen samt hur denna borde fördelas på skilda funktioner. ÖCB ansvarade också för funktionerna Civil ledning och samordning, industriell beredskap samt kyrklig beredskap.

3.1.2 Exemplet funktionen Industriell beredskap

Inom funktionen Industriell beredskap fanns tre delfunktioner; Beklädnad med mera, Kemiska produkter med mera samt Metall- och verkstadsprodukter. För att fullgöra uppgifter inom delfunktionerna fanns motsvarande tre byråer. Inom byråerna utarbetades försörjningsanalyser. Byråerna skulle följa utvecklingen inom näringslivet och i samhällets i övrigt med avseende på försörjningsberedskapen inom sina respektive delfunktioner. Det åvilade även byråerna att initiera att nödvändiga beredskapsåtgärder vidtogs.

Med utgångspunkt i det aktuella försörjningsläget och i krisbehoven identifierades och analyserades eventuella brister i försörjningsberedskapen, beredskapsläget för varan/tjänsten fastställdes. Mot bakgrund av beredskapsläget arbetades olika beredskapsåtgärder fram. Syftet med dessa var att de skulle reducera eller helt upphäva bristerna i försörjningsberedskapen.

I förordningen (1982:517) om beredskapslån och beredskapsgaranti reglerades under vilka förutsättningar lån och garanti fick lämnas till den som upprätthöll eller stärkte försörjningsberedskapen. Följande åtgärder angavs som grund: Upprätthålla viss produktionskapacitet eller produktion, utveckla inhemska ersättningsprodukter, förbereda viss alternativ produktion, beredskapslagra vissa varor samt vidta annan åtgärd som regeringen har godkänt.

Bild 4. Varor och tjänster som var oundgängliga för individens överlevnad och samhällets funktion skulle alltid finnas tillgängliga. Det innebar att försörjningsförmågan skulle säkerställas bland annat vad gällde beklädnad. Men i kriser och krig måste man vara beredd att göra stora uppoffringar. På beklädnadsområdet skulle vi ha en tilldelning av kläder och skor som i rimlig grad täckte kraven på värme, skydd, hygien och andra väsentliga funktioner. I kristid förväntades man ta fram den gamla symaskinen och börja lappa och laga.

Grunden för funktionens verksamhet var de resurser som näringslivet förfogade över i fred. Beredskapsförberedelserna inom funktionen genomfördes i nära samverkan med näringslivet och syftade till att komplettera de resurser som näringslivet hade. Målet var att underlätta den anpassning av produktionen som måste ske i en kris- eller krigssituation. Försörjningsviktiga företag planlades i fred som K-företag. K-företagsplanläggningen innebar att företagets möjligheter att upprätthålla produktionen på en viss nivå under en kris underlättades, bland annat genom att nyckelpersoner inte togs ut i militärtjänst. K-företagen skulle fortsätta sin verksamhet, i vissa fall med ändrad inriktning till med hänsyn till totalförsvarets behov. Övriga företag skulle fortsätta sin verksamhet i den omfattning förhållandena så medgav vid beredskapshöjning.

Även SAF hade en roll vid beredskapshöjning. Den innebar att föreningens regionkontor bland annat skulle biträda företagen inom regionen i förekommande arbetsgivarfrågor samt samarbeta med länsstyrelser (CB kansli). I samarbete med ÖCB gav SAF 1986 ut skriften *Att vara K-företag – ett åtagande och en förmån*.

K-företagsplanläggningen genomfördes centralt av ÖCB för företag som hade betydelse på riksnivå och av länsstyrelserna för övriga försörjningsviktiga företag. ÖCB:s beredskapsåtgärder omfattade också beredskapsavtal med enskilda företag. En åtgärd kunde vara att företaget i en krissituation förbands sig att upprätthålla en viss produktionskapacitet.

Regeringen kunde vid beredskapshöjning bestämma att en ny myndighet – Försörjningskommissionen – skulle inrättas som dels skulle överta vissa delar

av ÖCB:s uppgifter och dels verka för att försörjningen till prioriterade samhällsverksamheter kunde tryggas.

3.1.3 Exemplet funktionen livsmedelsförsörjning med mera

Till funktionen hörde verksamhet som avsåg produktion, förädling och distribution av livsmedel inklusive dricksvatten, ransonerings- och regleringsåtgärder samt livsmedelshygien och civil veterinärverksamhet. En mindre varierad kost och en lägre energitillförsel måste under en period accepteras. Funktionen omfattade samtliga led i produktionen. Beredskapen byggde på näringslivet och dess förmåga till anpassning vid höjd beredskap. Inom jordbruket fanns redan i fred en särskild beredskapsorganisation som skulle underlätta att vid höjd beredskap fördela och utnyttja tillgängliga produktionsmedel – personal, fordon och drivmedel – på bästa sätt.

I egenskap av funktionsansvarig myndighet samordnade jordbruksverket planeringen inom funktionen. Beredskapsförberedelserna genomfördes i samverkan med övriga myndigheter på central, regional och lokal nivå inom funktionen. Verket hade också ett samarbete med jordbrukets branschorganisationer, de större livsmedelföretagen samt handelns organisationer. Livsmedelsverket ansvarade för försörjningen med dricksvatten samt för frågor om livsmedelshygien och livsmedelskontroll. Verket var också chefsmyndighet för besiktningsveterinärsorganisationen.

Statens Naturvårdsverk och Fiskeriverket hade begränsade uppgifter inom funktionen.

På högre regional nivå hade civilbefälhavarna i krig samordnande uppgifter avseende livsmedelsförsörjningen inom civilområdet. De skulle enligt sin instruktion bland annat ägna sig åt utnyttjande av beredskapslager. På lägre regional nivå svarade länsstyrelserna i fred för en stor del av planläggningen inom funktionen. I krig skulle de bland annat verka för att länets livsmedelstillgångar fördelades på bästa sätt samt vissa uppgifter kring ransoneringar. På lokal nivå svarade kommunerna för vattenförsörjningen och annan kommunalteknisk försörjning sam vissa uppgifter kring livsmedelskontroll.

Även för att kunna upprätthålla en tillräcklig livsmedelsproduktion var ett villkor att de berörda företagens nyckelpersonal och fordon undantogs från inkallelser till Försvarsmakten och civilförsvaret.

4 1990-talet

En helhetssyn på beredskapsåtgärderna tillsammans med det vidgade säkerhetsbegreppet innebar en väsentlig förändring av det civila försvarets inriktning och ett nytt arbetssätt. Det blev nu nödvändigt att i planeringen konsekvent analysera effekten av beredskapsåtgärder inte bara för krig utan också med avseende på fredstida störningar.

Inför riksdagens beslut våren 1992 om totalförsvarets inriktning för den kommande femårsperioden framhöll försvarsutskottet att det kunde finnas skäl att i särskild ordning överväga hur samhällets beredskap mot olika fredstida hot skulle kunna stärkas. Med anledning av uttalandet tillsattes Hot-och riskutredningen enligt regerings direktiv med uppdrag att analysera påfrestningar och risker i det fredstida samhället samt vissa frågor inom totalförsvarets civila del. Syftet var inte att riskanalysera Sverige utan att öka medvetenheten hos myndigheter och andra om att de skulle göra bedömningar av risker och hot så att de kunde vidta åtgärder som skyddar människor, egendom och miljö. Utredningen redovisade 1995 i slutbetänkandet Ett säkrare samhälle en bredare hotbild än de säkerhetspolitiska risker som länge varit styrande för diskussionerna. I betänkandet beskrivdes en samhällsutveckling med ökade beroenden mellan verksamheter, system och länder samt segregering och andra sociala förändringar.

Bild 5. Urbaniseringen medförde nya typer av hot och risker.

”Tillväxten av de tätbefolkade områdena har en gång för alla brutit sönder många för tidigare generationer viktiga sammanhang… Förändringar i samhället gör att många människor utsätter sig själv och andra för större risker än tidigare… De ökande internationella kontakterna är ett annat drag i utvecklingen. Vi kan inte avskärma oss från de risker som växer fram och de påfrestningar som förekommer i andra länder.”

Utredningen lyfte ett brett spektrum av risker vid sidan av de rent militära – till exempel massflykt, terrorism, sabotage, internationell kriminalitet, miljökatastrofer och kärnkraftsolyckor. Ett antal scenarion utgjorde hörnstenar i utredningens arbete, bland annat massflykt, översvämningar och omfattande avbrott i försörjningssystem. Mot bakgrund av dessa föreslog utredningen ett antal åtgärder på olika områden för att förebygga och hantera allvarliga störningar i viktiga samhällsfunktioner.

Bild 6. Andra hot än de rent militära började beaktas i allt högre grad.

ÖCB bedrev den så kallade BIS-verksamheten[5] i samverkan med olika myndigheter och organ. Under senare år hade nya metoder för riskanalyser utvecklats inom områdena kommunalteknisk försörjning, datasystem och försörjning i k-företag. Arbetsmetoderna var flera, till exempel rådgivning, utbildnings- och konferensverksamhet, etablering av nätverk, utarbetande av exempelsamlingar och initiativ till utvecklings- och forskningsinsatser. Tyngdpunkten låg på utbildning och information med målsättningen att nå ett stort antal beslutsfattare inom olika samhällssektorer. Utredningen konstaterade att BIS-verksamheten hade många positiva effekter på samhällets förmåga att uthärda påfrestningar även i fred. Huvudsyftet var dock att höja förmågan att motstå krig. BIS-insatserna riktades därför mest mot de delar av samhällsverksamheten som hade särskild betydelse för totalförsvaret.

Som en åtgärd föreslog därför utredningen bland annat säkerhetskrav i samhällsplaneringen, uttrycket skulle fungera som ett samlande begrepp för fredsriskhänsyn och krigsberedskapshänsyn. Åtgärder skulle integreras i hela hotskalan fred – krig enligt en helhetssyn på ansvar och befogenheter för civila organ inom området.

Riskfrågorna behandlades inom en rad verksamheter i samhället, till exempel fysisk planering, trafiksäkerhetsarbete, räddningstjänst och arbetarskydd. Statsmakterna hade i en del fall fastställt mål för verksamheten som mer eller mindre utförligt angav även säkerhetskrav. Synen på dessa frågor – och arbetsmetoderna – varierade dock mellan sektorerna. Myndigheterna anlade sällan ett tvärsektoriellt eller övergripande perspektiv. Det var vanligare att

[5] Beredskapshänsyn i samhällsplaneringen

varje myndighet utvecklade ett synsätt som var anpassat till den egna verksamhetens behov och förutsättningar. Bristen på enhetlighet i hanteringen av frågorna om säkerhetskrav i samhällsplaneringen ansågs kunna leda till att kraven inom en del sektorer gick för långt och blev för kostsamma och tvärtom. Utredningen ansåg också att kunskaper om risker och metoder för riskbedömning ännu var outvecklade och att myndigheterna inte samarbetade tillräckligt effektivt för att identifiera risker och förebygga dem.

Som en anpassning till den säkerhetspolitiska och samhälleliga utvecklingen med nya hot och risker av icke-militär natur som trädde fram anlades så i totalförsvarsbeslutet 1996 en helhetssyn på det militära och civila försvarets uppgifter. Totalförsvaret skulle utformas med utgångspunkt i ett vidgat säkerhetsbegrepp som rymde också icke-militära hot och risker. Det nya säkerhetstänkandet innebar att man i planeringen också skulle analysera effekterna av sådana fredstida störningar som innebar svåra påfrestningar på samhället. Totalförsvaret skulle inte bara värna vårt lands frihet och oberoende och skydda befolkningen i krig och kris, utan dess resurser skulle även bidra till vår förmåga att möta svåra påfrestningar i fred. Totalförsvarets resurser skulle således utnyttjas i en bredare hotskala än tidigare.

Regeringen redogjorde också för de delar i samhällsutvecklingen som hade särskilt stor betydelse för det civila försvarets förmåga. Det gällde främst områdena elförsörjning, telekommunikationer och informationsteknologi. På dessa områden var den tekniska utvecklingen snabb med både positiva och negativa konsekvenser från sårbarhetssynpunkt. Bilden komplicerades av stora förändringar när det gäller avreglering och internationalisering inom dessa sektorer.

Bild 7. På vissa samhällsområden skedde en snabb teknisk utveckling samtidigt med en ökad avreglering och internationalisering inom dessa sektorer.

Enligt regeringens inriktning skulle det civila försvaret kunna anpassas till förändringar i det säkerhetspolitiska läget. Samhällets inneboende förmåga att klara fredstida påfrestningar utgjorde själva grundförutsättningen för det civila försvarets möjligheter att klara uppgifterna i krig. Särskilt betydelsefull var kapaciteten inom räddningstjänst, hälso- och sjukvård samt stabiliteten och flexibiliteten hos viktiga infrastruktursystem. Med denna fredstida förmåga som bas vidtogs särskilda kompletterande beredskapsåtgärder. För att ha en

handlingsberedskap inför en anpassningsperiod var det bland annat viktigt att det för varje funktion utarbetades planer för anpassning. I fråga om andra slag av kompletterande åtgärder var det emellertid inte möjligt att avvakta till ett anpassningsskede och inte heller till en långsiktig anpassning. Det var här främst fråga om sådana åtgärder som vidtogs i samband med fredstida investeringar i infrastrukturen och som syftade till att skapa en extra stabilitet inför krigstida störningar. Regeringen ville betona att det här var fråga om åtgärder som också hade stor betydelse för samhällets förmåga att klara svåra påfrestningar på samhället i fred.

Enligt regeringens inriktning skulle också en helhetssyn på beredskapsåtgärderna tillämpas vilket tillsammans med det vidgade säkerhetsbegreppet innebar en väsentlig förändring av det civila försvarets inriktning och ett nytt arbetssätt. Det blev nu nödvändigt att i planeringen konsekvent analysera effekten av beredskapsåtgärder inte bara för krig utan också med avseende på fredstida störningar. Även om det var krigets krav som huvudsakligen skulle avgöra dimensionering och utformning av beredskapsåtgärderna var det enligt regeringen väsentligt att behoven vid fredstida störningar gavs stor vikt i avvägningarna.

Enligt regeringens inriktning skulle vidare de kompletterande beredskapsåtgärderna i större utsträckning än hittills avse de viktigaste infrastrukturområdena. Som nämnts vilade det civila försvarets förmåga till anpassning ytterst på att vårt samhälle trots ökande sårbarhet på samma gång var både stabilt och flexibelt. Regeringen föreslog därför särskilda satsningar för att förbättra beredskapen på de viktigaste infrastrukturområdena. Liksom ÖCB framhöll i programplanen för det civila försvaret ansåg regeringen att om riskerna i samhället skulle kunna hållas på en godtagbar nivå måste alla verksamheter inom olika sektorer uppfylla rimliga säkerhetskrav. För att uppnå detta var det enligt ÖCB väsentligt att statliga myndigheter som arbetade med beredskapshänsyn och säkerhetsfrågor stödde och tog initiativ som på olika sätt höjde den allmänna kunskapsnivån inom risk- och säkerhetsområdet. Det var enligt regeringen också både av beredskaps- och samhällsekonomiska skäl av största vikt att olika aktörer i samhället i samband med investeringar hade sådan kunskap om det allmänna beredskapsbehovet att de beaktade möjligheterna att vidta beredskapsåtgärder.

Enligt regeringens inriktning skulle också den fredstida samordningen och ledningsförmågan förbättras. Utifrån den av regeringen redogjorda inriktningen för planeringen av det civila försvaret under försvarsbeslutsperioden konstaterades sammanfattningsvis att för att förverkliga denna inriktning borde, mot bakgrund av det bedömda beredskapsläget, vid resursfördelningen ledningssystem, kompetensutveckling hos personal, infrastruktur samt insats- och katastrofberedskap prioriteras högre än vad tidigare varit fallet. Mot samma bakgrund borde lägre prioritet ges åt försörjningsfunktionerna.

5 2000-talet

Till följd av den nya hotbilden avskaffades det gamla funktionssystemet och ersattes av ett nytt system med samverkansområden och samverkansansvariga myndigheter.

Regeringen tillsatte 1999 Sårbarhets- och säkerhetsutredningen. Utredningen skulle enligt sina direktiv pröva om nuvarande funktionsindelning inom det civila försvaret samt nuvarande myndighetsuppgifter och samordningssystem inom det civila försvaret och beredskapen mot svåra påfrestningar på samhället i fred behövde ändras. Den analys som utredningen redovisade av utvecklingstendenser och problembild inom krishanteringsområdet visade att relativt omfattande förändringar av befintliga system behövde genomföras. Mot denna bakgrund redovisade en ny grundstruktur för ledning och samordning av samhällets hantering av allvarliga kriser.

Utredningen föreslog i sitt betänkande utifrån en bedömning av utvecklingstendenser och nuvarande brister ett nytt system för hanteringen av allvarliga kriser i samhället. Utredningen föreslog också att en planeringsmyndighet skulle inrättas med uppgift att sköta vissa planeringsuppgifter, samordna forskning och utvecklingsinsatser inom krishanteringsområdet.

Utredningen lade vidare fast vissa grundläggande krav som borde ställas på det nya systemet. Det borde bland annat också bygga på ett samverkansansvar.

Bild 8. Ett nytt planeringssystem skulle bygga på ett uttalat samverkansansvar.

Med samverkansansvar avsågs att en central statlig myndighet skulle åläggas att samverka med andra organ i syfte att tillgodose de krav på samordning som finns inom vissa sakområden som har betydelse för hanteringen av mycket allvarliga kriser i samhället. Samverkansansvaret skulle göra det möjligt för de

områdesansvariga organen att koncentrera sig på övergripande och tvärsektoriella frågor, till exempel prioriteringen av olika krishanteringsinsatser inom det aktuella geografiska området. Om samverkansansvaret fungerade som avsett skulle de områdesansvariga organen inte behöva engagera sig i den fackmässiga samordningen av krishanteringsinsatserna inom ett sakområde eller en sektor. Utredningen ansåg att inriktningen av en myndighets samverkansansvar borde läggas fast i myndighetens instruktion. Kompletterande anvisningar kunde vid behov ges i myndighetens regleringsbrev. Samverkansansvaret borde omfatta såväl verksamheten under ett förberedelse- och planeringsskede som verksamheten i en akut krissituation. Tyngdpunkten torde dock komma att ligga på förberedelse- och planeringsskedet.

Utredningen lyfte också sektorsbegreppet och att begrepp som sektorsmyndighet och sektorsansvar användes relativt ofta inom statsförvaltningen. Det fanns dock ingen allmänt accepterad definition av dessa begrepp. Med sektorsmyndighet, menade utredningen, torde närmast avses en statlig myndighet som har någon typ av tillsyns- eller planeringsansvar för ett samhällsområde som i sin tur har ett visst syfte eller inriktning och som omfattar såväl statlig som icke-statlig verksamhet. I denna mening kunde Socialstyrelsen och Skolverket sägas vara sektorsmyndigheter. Däremot var Rikspolisstyrelsen med denna definition av begreppet inte någon sektorsmyndighet. Detta var dock endast en av flera möjliga tolkningar av begreppet, ansåg utredningen. Ytterst berodde dessa terminologiska oklarheter på att det inom statsförvaltningen inte fanns någon heltäckande sektorsindelning. Det som kom närmast detta begrepp torde ha varit den statliga budgetens politik- och utgiftsområden och det civila försvarets funktionsindelning. Båda dessa indelningar hade dock tillkommit i ett avgränsat och speciellt syfte och var inte avsedda att tillhandahålla en grund för en generellt användbar sektorsindelning av den statliga verksamheten.

Utredningens förslag utifrån säkerhetspolitiska och samhälleliga utvecklingstendenser behandlades av regeringen i två propositioner 2002. För att nå en helhetssyn i hanteringen av kris- och krigssituationer skulle några grundläggande principer införas att gälla för organisation och ledning. Dessa var ansvarsprincipen, likhetsprincipen och närhetsprincipen.

Enligt den av regeringen föreslagna strukturen vid fredstida krishantering och för civilt försvar skulle alla statliga myndigheter i syfte att stärka krishanteringsförmågan analysera om det finns sådan sårbarhet eller sådana risker inom myndighetens ansvarsområde som mycket allvarligt kunde nedsätta förmågan hos verksamheten inom området. Samtliga statliga myndigheter borde vara skyldiga att i sin verksamhet beakta totalförsvarets krav. De borde även planera för att under höjd beredskap kunna fortsätta verksamheten så långt det är möjligt. Regeringen ansåg i detta sammanhang också att det fanns skäl att peka ut ett antal statliga myndigheter som skulle åläggas ett särskilt ansvar för att vidta de förberedelser som behövdes för att möta svåra påfrestningar på samhället i fred och inför höjd beredskap. Regeringen konstaterade att det fanns ett behov av fackmässig samordning, en typ av samordning som saknade en entydig geografisk dimension och i stället gällde själva verksamheten oavsett på vilken plats eller nivå som denna bedrivdes. Regeringen lyfte behovet av samordning som genererades av starka ömsesidiga beroendeförhållanden, som till exempel

inom den tekniska infrastrukturen, eller från ett behov av att utgå från vissa gemensamma förutsättningar vid genomförandet, till exempel vid utbildning och övningar om krishantering. Regeringen ansåg att sådana beroendeförhållanden fanns på olika nivåer i samhället. Inte minst gällde detta mellan centrala statliga myndigheter. Ett exempel på hur samordning inom ett aktuellt sakområde skulle kunna ske var att berörda tilldelades ett samverkansansvar enligt utredningens förslag.

Regeringen pekade på att principerna för samhällets krishantering och de förändrade kraven på civilt försvar hade gjort att den nuvarande funktionsindelningen hade förlorat sin betydelse. Även utskottet ansåg att det efter riksdagens beslut år 1985 införda systemet med funktioner för planeringen inom det civila försvaret, och funktionsansvariga myndigheter, var alltför starkt kopplat till planering och förberedelser för höjd beredskap och de hot som gällde då systemet infördes. För att bryta den statiska och kalla kriget orienterade planeringen bedömde regeringen att den existerande funktionsindelningen inom civilt försvar skulle avskaffas och ersättas av en struktur med samverkansområden och myndigheter med ett särskilt samverkansansvar som var mer flexibel i och med att den omfattade både beredskapen för svåra påfrestningar på samhället i fred och höjd beredskap. Regeringen konstaterade att det mellan många verksamheter fanns ett starkt inbördes samband som har betydelse vid såväl planeringen för, som hanteringen av, svåra påfrestningar och höjd beredskap. Samverkansområdena skulle därmed bidra till en ökad samordning och en förbättrad krishanteringsförmåga. Ingen myndighet skulle pekas ut som ansvarig för den övergripande planeringen inom respektive område. De utpekade myndigheterna borde ha ett gemensamt ansvar för att säkerställa planeringen inom området. En ny myndighet, Krisberedskapsmyndigheten, skulle komma att ha det övergripande ansvaret för samordning av samverkansområdena. Vissa myndigheter skulle dock även i fortsättningen ha ett ansvar som var kopplat till totalförsvaret. Ett exempel på ett sådant ansvar var det så kallade bevakningsansvar som utredningen föreslog.

Regeringen betonade i detta sammanhang om samverkan också att verksamheten i den offentliga sektorn inte var tillräcklig för att säkerställa ett säkert och robust samhälle. Problem måste lösas underifrån och i en nära samverkan mellan det offentliga och det privata. Regeringen bedömde därför att det inom för samhället viktiga områden måste skapas en strukturerad samverkan mellan offentlig sektor och näringsliv. Om så inte skedde skulle vår förmåga att förebygga och hantera kriser aldrig att bli så bra som var nödvändigt. Regeringen avsåg därför att initiera skapandet av olika samverkansfora mellan näringslivet och det offentliga inom de föreslagna samverkansområdena. Ett exempel på den samverkan som borde åstadkommas var det nyligen initierade samverkansforumet inom elområdet.

Vad gällde inriktningen för det civila försvaret bedömde regeringen att för att stärka samhällets förmåga att möta de nya säkerhetspolitiska hoten måste det civila försvarets ominriktning fortsätta. Det civila försvarets resurser skulle i första hand inriktas mot att möta hot som kunde uppstå ur nuvarande omvärldsläge. Hoten kunde vara biologiska, kemiska eller nukleära, det kunde vara informationsoperationer riktade mot Sverige och svenska intressen eller

hot riktade mot den tekniska infrastrukturen. Genom ominriktningen skulle det svenska samhället bli bättre rustat för att även kunna motstå terroristattacker. Först i andra hand skulle det civila försvarets resurser inriktas mot att efter en anpassning kunna möta ett mer omfattande angrepp som berör Sverige. Samhällets planering av åtgärder inom beredskapen mot svåra påfrestningar på samhället i fred skulle ske samordnat med planeringen för det civila försvaret inom ramen för de samverkansområden som skulle utgöra delar av landets infrastruktur.

Utifrån en struktur med ett sektors- och områdesperspektiv inrättades och utvecklades det nya planeringssystemet mot ett nationellt krisberedskapssystem med fokus på större fredstida kriser. Samtidigt påbörjades en utveckling mot en integrering av krisberedskapsfrågor med frågor längs övriga hotskalan som rör robusthet, säkerhet och trygghet i samhället. Det handlade alltmer om att säkerställa en samlad förmåga; om att förebygga, avvärja och hantera samhällsstörningar, såväl stora som små, dygnet runt. På den nationella nivån manifesterades denna utveckling organisatoriskt i att MSB inrättades 2009, samtidigt som KBM, SRV och Styrelsen för psykologiskt försvar lades ned. MSB fick ett brett ansvar längs hela hotskalan

Enligt Förordning (2006:942) om krisberedskap och höjd beredskap anges att för att främja en helhetssyn i planeringen för krisberedskap och höjd beredskap ska planeringen för de myndigheter som anges i bilaga till förordningen bedrivas inom samverkansområden (se bilaga 3). Samverkansområdena anges i bilagan. I bilaga till förordningen finns således en desförteckning över samverkansområden och myndigheter som har ett särskilt ansvar inom områdena. Myndigheterna har ett särskilt ansvar för att planera och vidta förberedelser för att skapa förmåga att hantera en kris och för att förebygga sårbarheter och motstå hot och risker.

MSB ska, i samverkan med de myndigheter som ingår i samverkansområdena, utveckla formerna för arbetet i områdena. MSB presenterade 2011 en nationell strategi för skydd av samhällsviktig verksamhet - *Ett fungerande samhälle i en föränderlig värld*. Under 2014 har MSB vidare tagit fram *Vägledning för samhällsviktig verksamhet* om att identifiera samhällsviktig verksamhet och kritiska beroenden samt bedöma acceptabel avbrottstid. MSB har också utifrån uppdrag i regleringsbrev för 2013 under 2014 tagit fram *Handlingsplan för skydd av samhällsviktig verksamhet* och påbörjat ett arbete i enlighet med denna. [6]

MSB genomför också ett arbete som bygger på gemensamma riktlinjer för EU:s medlemsländer. Den nationella risk- och förmågebedömningen ska bidra till det gemensamma arbetet med att utveckla individens och samhällets förmåga att förebygga och hantera olyckor och kriser.

---

[6] Tidigare avsåg begreppet *Skydd av samhällsviktig verksamhet* skydd av till exempel vissa anläggningar genom bevakningsresurser såsom hemvärnet och beredskapspolisen.

Förändrade förutsättningar för samhällets krishantering innebär att nya arbetssätt och nya metoder för att skapa beredskap och robusthet i samhället har utvecklats. De beredskapsåtgärder som behöver vidtas idag är i många fall mycket olika de beredskapsåtgärder som genomfördes under slutet av 1980-talet. Idag genomförs mycket mer ”mjuka” beredskapsåtgärder som till exempel omvärldsanalys, kompetensuppbyggnad, utbildning och övning, olika former av utrednings- och utvecklingsarbete, forskning, nätverksbyggande och samverkan etc.

6 En historisk överblick – några iakttagelser

Med anledning av den historiska överblicken görs några iakttagelser kring utvecklingen av arbetet med samhällsviktig verksamhet ur ett krisberedskapsperspektiv och i ett större sammanhang. Det handlar om ramen inom vilken utvecklingen med skyddet av samhällsviktig verksamhet ska ta sin form.

6.1 Utvecklingsbehov

1970 års försvarsutredning avlämnade i januari 1972 betänkandet (SOU 1972:4) Säkerhets- och försvarspolitiken. Utredningen beskrev utvecklingstendenserna inom näringslivet med strukturförändringar inom jordbruk och industri samt det ökande importberoendet. I krig var det enligt utredningen framför allt sårbarheten hos näringslivet och olika samhällsfunktioner som var av intresse. För landets förmåga till försvar var det av utslagsgivande betydelse att de förnödenheter och tjänster som behövdes för krigsmaktens och civilförsvarets mobilisering kunde tillhandahållas. Dessutom måste det övriga krigssamhällets nödvändiga behov av förnödenheter och tjänster tillgodoses. Samhällsstrukturen var också av betydelse för befolkningens förmåga att bära de påfrestningar som krig innebär liksom att motstå utifrån kommande propaganda.

En historisk överblick visar på att identifierade problemområden och utvecklingsbehov ofta kvarstår såsom de uttrycks i olika sammanhang. Frågor kring samordning, kunskap, sårbarheter, beroenden, tvärsektoriella perspektiv, privata aktörer, internationalisering, IT-utveckling, reservkraftaggregat etc. – stort och smått – väckts i många sammanhang. Under åren betonas också själva betydelsen av att beakta beredskapsfrågor i samhällsplaneringen samt den stora roll folkförankringen och metoderna för denna spelar.

Några viktiga frågor att ställa inför det fortsatta arbetet kan vara: Varför kvarstår problemen och behoven? Vilka framsteg har gjorts i förhållande till samhällsutvecklingen? Hur utvecklas förutsättningarna i samhället och av statsmakterna i förhållande till dessa återkommande problem? Är statsmakternas inriktning och ambition för krisberedskapen realistisk och tydlig? Finns det en enhetlig bild av vad en tillräckligt god krisberedskap innebär?

6.2 Drivkrafter

Som nämnts ovan uttrycker 1970 års försvarsutredning att samhällsstrukturen också är av betydelse för befolkningens förmåga att bära de påfrestningar som krig innebär. Det finns många exempel på tidigare tilltal och förhållningssätt.

”Grunden för att befolkningen i ett krig eller eljest i ett krisläge skall vilja och kunna uthärda de påfrestningar som den utsätts för är enligt utredningen att den känner solidaritet i stort med det svenska samhället. Det är uppenbart att det överväldigande flertalet medborgare i Sverige känner en sådan solidaritet, grundad på att landet och dess samhällsskick för dem representerar väsentliga värden. Denna solidaritet innebär att man på väsentliga punkter känner gemenskap samtidigt som man på andra, mindre väsentliga punkter kan ha olika uppfattningar. … Folkrörelserna och partiorganisationerna skänker stabilitet och långsiktighet åt samhällsarbetet. Detta system fungerar väl.”[7]

Statsministern slår under andra halvan av 1970-talet fast att:

”Det svenska samhället präglas av en djup och grundläggande värdegemenskap. Den inre stabilitet, som vårt samhälle skapar, förblir en väsentlig förutsättning för att statsmakterna ska kunna föra en fast politik både i fred och krig. Vårt totalförsvar är ett uttryck för vår vilja att slå vakt om nationens säkerhet och oberoende. Totalförsvaret är därför en hela folkets angelägenhet och bygger på att varje medborgare efter förmåga bidrar till landets försvar. Den allmänna värnplikten, civilförsvarsplikten, våra frivilliga försvarsorganisationer och folkrörelser har också stor betydelse för totalförsvarsidéns förankring i samhället.”[8]

Idag är uttrycket betydligt mer instrumentellt och det saknas i princip tilltal som dessa i liknande sammanhang, oavsett det faktum att världen då såg annorlunda ut. Det nuvarande krisberedskapssystemet är långt utvecklat och bygger vidare på ett delat ansvar där såväl ett vertikalt som ett horisontellt ansvar ska möjliggöra en god krisberedskap. Ansvarsprincipen stipulerar det offentliga organets eget ansvar och arbete på samma gång som det individuella ansvaret lyfts i allt högre grad. Samtidigt ska ”vi alla tillsammans” åstadkomma något. Arbetet med krisberedskap och samhällsviktig verksamhet ska också ta sin grund i ett mer globalt, internationellt, EU- och avreglerat perspektiv vilket i detta sammanhang torde vara av yttersta vikt att beakta.

Tanken på frivillig samverkan och frivilligt deltagande från individer och organisationer kan ställas mot en samverkan av mer tvingande karaktär såsom lagstiftning. Om man till stor del väljer frivilligvägen kan mjuka faktorer såsom drivkrafter, värdegemenskap och delaktighet utgöra en viktig grund för arbetet med krisberedskap.

Utöver frågorna om utvecklingsbehov kan några viktiga frågor att ställa i det fortsatta arbetet vara: Vilken gemensam grund vilar vårt arbete med krisberedskap på? Vilka faktorer behöver utvecklas och hur för att engagera oss alla som aktörer och individer? Vilket ”samhälleligt krisberedskapskontrakt” ska vi ha?

---

[7] Kungl. Majst:s proposition 1972:75 angående försvarets fortsatta inriktning

[8] Handelsdepartementets prop. 1976/77:74 om inriktningen av säkerhetspolitiken och totalförsvarets fortsatta utveckling

Bild 9. Vilken gemensam grund vilar vårt arbete med krisberedskap på?

6.3 Privat-offentlig samverkan

Regeringen har under åren återkommande betonat att verksamheten i den offentliga sektorn inte varit tillräcklig för att säkerställa ett säkert och robust samhälle. Problem måste lösas underifrån och i en nära samverkan mellan det offentliga och det privata. Vad gäller den generella samhällsutvecklingen fram till idag kan konstateras att samtidigt som beroendeförhållandena mellan olika samhällsverksamheter fortsatt har ökat så bedrivs alltmer av den samhällsviktiga verksamheten inte längre i offentlig utan privat regi och alltmer samhällsviktiga resurser finns i privat ägo. Detta faktum ställer ökande krav på en väl fungerande privat-offentlig samverkan för att möjliggöra inriktning och styrning av arbetet med samhällsviktig verksamhet. Privata aktörer har i allmänhet ingen laga skyldighet att upprätta risk- och sårbarhetsanalyser. Den aktuella utvecklingen kräver inte bara mer privat-offentlig samverkan. Av betydelse för arbetet är också att själva antalet aktörer i krisberedskapssystemet ökar och att samverkan och samordning många gånger blir mer tidskrävande och komplicerad. I ett historiskt perspektiv har delar av försörjningsberedskapen styrts och inriktats genom lagstiftning, till exempel genom förordning om skyldighet för näringsidkare att medverka vid lagring av försörjningsberedskap. Idag finns fortfarande lagar för höjd beredskap såsom förfogandelagen samt förordning om förberedelser för leverans av varor och tjänster.

Vad gäller privat-offentlig samverkan kan, förutom de redan nämnda iakttagelserna kring ansvarskänsla, drivkrafter, värdegemenskap, internationalisering samt frivillighet kontra tvingande åtgärder, i det fortsatta arbetet beaktas frågan om betydelsen av avreglerade/icke avreglerade samhällssektorer i det fortsatta arbetet.

6.4 Sektorsansvaret

Redan på 70-talet konstaterades att samordningsfunktionen på den centrala nivån var splittrad. Under de kommande åren infördes funktionsansvaret, avsaknaden av en heltäckande sektorsindelning inom statsförvaltningen lyftes och med ominriktningen av det civila försvaret ersattes funktionsindelningen av ett nytt system med samverkansområden och samverkansansvariga myndigheter med skyldighet att redovisa risk- och sårbarhetsanalyser. Arbetet med skydd av samhällsviktig verksamhet bör enligt regeringen idag ske utifrån dessa risk- och sårbarhetsanalyser och med utgångspunkt i dessa bör åtgärder genomföras för leveransförmåga och robusthet. En oklarhet i detta sammanhang gäller den redovisande myndighetens eget perspektiv på sitt eventuella sektorsansvar och på vilket sätt ett sådant ansvar i dagens förvaltning ännu tydliggjorts från statsmakternas sida.

Några viktiga frågor, vid sidan av de kring utvecklingsbehov, drivkrafter och privat - offentlig samverkan, att ställa inför det fortsatta arbetet kan därför vara: Behöver sektorsansvaret för analys och åtgärder utvecklas och tydliggöras och i så fall hur? Hur förhåller sig sektorerna till varandra och vilka myndigheter ingår i vilken/vilka? Vilka goda exempel finns? Vilken roll spelar Regeringskansliet? Hur kan MSB stödja utifrån sin roll?

6.5 Slutord

Iakttagelserna avser grundläggande förutsättningar såsom drivkrafter och ett system som har att förhålla sig till ansvar, internationalisering och avreglering. Problemställningarna är sedan årtionden i många fall likartade. Det kan finnas skäl att beakta de absoluta grunderna för arbetet med krisberedskap och skydd av samhällsviktig verksamhet i strävan mot en reell utveckling.

7 Underlag

Kartläggningen är gjord utifrån ett omfattande skriftligt material samt internetmaterial. Nedan listas ett urval av källor i kronologisk ordning.

- Propositioner, skrivelser, utskottsbetänkanden, utredningsbetänkanden 1970 –
- Totalförsvarets upplysningsnämnd (TUN), 1975, Sveriges säkerhet – en översikt över säkerhetspolitik och totalförsvar
- Pettersson Lennart, 1977, Det sårbara samhället, Folk och försvar
- Westemar Berthold, 1982, Ekonomiskt försvar i omvandling, Folk och försvar
- Sköldfors Walter, 1985, Försörjningsberedskap mot 90-talet, Folk och Försvar
- Riksrevisionsverket, 1990, ÖCB och den industriella beredskapen
- Totalförsvarets chefsnämnd (TCN), 1994, Samverkan inom totalförsvaret
- ÖCB, 1997, Civil beredskap
- ÖCB, Försvarsmakten, 1998, Handbok regional samverkan
- Bjuström Erik, Collin Charlotte, Lundmark Martin, 2000, Funktionernas förmågebedömning för Årsbok civilt försvar
- KBM, 2003, Översyn av beredskapsåtgärder
- Barck-Holst Svante, 2005, Nationellt säkerhetsarbete inom samhällsviktig infrastruktur
- Eriksson Pär, Barck-Holst Svante, 2005, Politik för skydd av kritisk infrastruktur i EU och Sverige – en jämförande analys, FOI
- Larsson Per, Lotta Ryghammar, 2013, Från civilt försvar till kontraktbaserad samhällssäkerhet, FOI fokus Samhällssäkerhet
- Larsson Per, Lotta Ryghammar, 2013, Vad hotar oss?, FOI fokus Samhällssäkerhet
- www.msb.se, 2014

Del 2

En övergripande kartläggning av hur skyddet av samhällsviktiga verksamheter idag organiseras, samordnas och styrs i ett urval länder

1 Inledning

1.1 Bakgrund och förutsättningar

För att fördjupa och bredda kunskapen om hur man kan arbeta med att skydda och stärka svenska samhällsviktiga verksamheter (funktioner) har ett mindre antal andra länder utifrån olika policydokument övergripande kartlagts med avseende på hur de nationellt organiserar, samordnar och styr sitt arbete på det aktuella området (exklusive deras bi- och multilaterala internationella samverkan). Med aktuellt område avses närmare bestämt vad som länderna vanligen benämner ”kritisk infrastruktur” (inklusive försörjningsberedskap i vissa fall). Begreppen samhällsviktig verksamhet och kritisk infrastruktur kommer därför att användas synonymt. Länderna som kartlagts är:

- Schweiz
- Finland
- Polen
- Storbritannien
- Kanada
- USA

Transparansen och den tillgängliga informationen om arbetet med skydd av kritisk infrastruktur varierar mellan länderna och har på olika sätt begränsat kartläggningen. Underlaget utgörs av officiella dokument upplagda på internet och myndigheters officiella hemsidor (Polen och Schweiz engelskspråkiga versioner av dokument och hemsidor). Olika aspekter av arbetet belyses med olika detaljrikedom av länderna och i vissa fall saknas information helt. Men informationen får ändå sägas vara tillräcklig för att man ska kunna få en övergripande bild av det nationella arbetet och dess idémässiga grunder.

1.2 Slutsatser

Inledningsvis presenteras här generella iakttagelser rörande arbetet med skydd av kritisk infrastruktur/samhällsviktig verksamhet hos de kartlagda länderna. Därefter presenteras några reflektioner om hur Sverige avviker från de kartlagda länderna i sitt arbete med skydd av samhällsviktig verksamhet eller förutsättningarna härvid.

1.2.1 Generella iakttagelser

- Flertalet av de kartlagda länderna har inrättat specifika nationella program, eller en strategisk samordning, för sektorsspecifikt och sektorsö-

vergripande arbete med att skydda och stärka sin kritiska infrastruktur (samhällsviktiga verksamheter). Dessa program har inrättats tämligen nyligen, de senaste 5-10 åren. Det gör att dessa fortfarande till delar befinner sig i en uppstartsfas, varför det oftast också är för tidigt att se effekterna av dessa program. Finland avviker genom att inte ha samma typ av nationellt program som övriga länder. Finlands arbete på området har gradvis vuxit fram inom ramen för totalförsvaret och behovet av att kunna möta krigets krav. Finlands arbete med skydd av kritisk infrastruktur, som alltså inte är lika explicit som andra länder, är mer att betrakta som en integrerad del av arbetet med totalförsvaret och dess målsättningar. Avslutningsvis, kartläggningen kan på intet sätt konstatera om de lösningar som länderna valt i praktiken är framgångsrika eller inte, vilket bör tas i beaktande vid den fortsatta läsningen.

- De nationella handlingsprogrammen (inklusive Finlands strategiska arbete) fokuserar på nivå- och sektorsamverkan och utgår från befintligt säkerhets- och skyddsarbete som finns inom alla sektorer och branscher och som både utgörs av lagar, förordningar, föreskrifter av tvingande karaktär och av frivilliga branschstandarder och andra former av frivilliga överenskommelser. Detta säkerhets- och skyddsarbete har ofta en lång historia och växt fram stegvis baserat på incidenter, olyckor, riskforskning etc. Det är därför viktigt att inse att ländernas arbete med skydd av kritisk infrastruktur inte påbörjats i samband med inrättandet av deras nationella handlingsprogram utan kontinuerligt pågått långt dessförinnan. De nationella handlingsprogrammen utgör bara en konsolidering och en strävan till bättre sektorsöverskridande samverkan av existerande skydds- och säkerhetsarbete.

- De kartlagda länderna har i det stora en gemensam syn på vad som innefattas i begreppet ”kritisk infrastruktur” (samhällsviktiga verksamheter). Indelningen av kritisk infrastruktur i fråga om antal sektorer och subsektorer (eller system som Polen använder som begrepp) samt typ av sektorer skiljer sig dock åt. Antalet sektorer varierar från 10-16 stycken. Schweiz identifierar 31 subsektorer. Schweiz graderar också utifrån en skala hur kritisk en sektor är för samhällets funktionalitet. Finland talar om kritisk infrastruktur (5 st, t.ex. transportlogistiska system) och kritisk produktion (5, st, t.ex. livsmedelsförsörjning) som två sammanlänkade samhällsviktiga komponenter eller funktioner

- Drivkraften bakom att inrätta de nationella handlingsprogramen har varit en förändrad hotbildsutveckling främst gällande terrorism och klimatförändringar som hot mot infrastrukturen; det i kombination om insikten om betydande brister i sektorsövergripande samordning. För USA är i synnerhet en framträdande drivkraft att skydda kritisk infrastruktur mot terrorattentat och att säkerställa produktion av försvars-

materiel, vilket bland annat återspeglas genom att en sektor för kritisk infrastruktur utgörs av en sektor för produktion av försvarsmaterial. (Defense Industrial Base). För Finland, men även i viss mån för Polen och Schweiz, så har drivkraften som nämnts snarare främst varit en kontinuerlig utveckling inom ramen för totaltförsvaret för att kunna möta krigets krav. Med andra ord att kunna skydda kritisk infrastruktur vid militära territoriella angrepp och avspärrning i samband med säkerhetspolitiska kriser samt att kunna återuppbygga skadad och totalförstörd infrastruktur efter kriget. Terrorism, klimatförändringar etc. och dess hot mot infrastrukturen tillkommer därtill som drivkrafter i det nationella arbetet med att skydda och stärka kritisk infrastruktur.

- Bland de kartlagda länderna är utvecklingen inom området skydd av kritisk infrastruktur i en övergångsfas bort från scenariobaserat tänkande om hur man bäst ska skydda kritisk infrastruktur (”Protection”) mot olika hot för att istället fokusera på stärka den inneboende robustheten i teknik och ledning för att hantera alla former av störningar (”Resilience”). Ledordet i de nationella handlingsprogrammen är oftast ”resilience”. Men den faktiska skillnaden mellan ”Protection” och ”Resilience” är oftast svår att greppa. I USA, som har ett uttalat fokus på terrorism, är ledorden ”Security and Resilience”.

- Det mycket stora ömsesidiga beroendet när det gäller amerikansk-kanadensisk kritisk infrastruktur har föranlett de båda länderna att inrätta en gemensam transnationell handlingsplan för skydd av kritisk infrastruktur ”Canada-United States Action Plan for Critical Infrastructure (2010)”. (I övrigt gäller att ländernas internationella samarbeten inte har studerats eller samarbetet inom EU).

- Skydd av kritisk infrastruktur och tillgång på kritiska resurser (som t.ex. vissa metaller) för produktionen av varor och tjänster ses av Finland och Schweiz, men även USA, som ömsesidigt sammankopplade behov. För Finland och Schweiz del handlar det om att beredskapslagra utvalda kritiska resurser och att ha mandat att kunna prioritera dessa till samhällsviktiga verksamheter.

- Ingen sektorsövergripande portallagstiftning för skydd av kritisk infrastruktur instiftas som ett led i inrättandet av ländernas nationella program för skydd av kritisk infrastruktur eller existerar på förhand. Däremot har t.ex. Polen genom förordningen ”541 Regulation of the Council of Ministers of 30 April 2010 on Critical Infrastructure Protection Plans” lagt fast hur berörda ministerier och myndigheter ska verkställa arbetet med det nationella programmet för skydd av kritisk

infrastruktur i samverkan med (privata) ägare och operatörer av kritisk infrastruktur (installationer, anläggningar etc.).

- I arbetet med att skydda den kritiska infrastrukturen har de studerade länderna (Polen delvis undantaget) primärt inte valt att gå lagstiftningsvägen utan istället valt den frivilliga ”partnerskapsvägen” för att få ägare och operatörer av kritisk infrastruktur eller olika samhällsnivåer (delstater, kommuner etc.) att samverka och vidta behövliga åtgärder. Arbetet inom de nationella handlingsprogrammen för skydd av kritisk infrastruktur sker således företrädesvis inom ramen för vad från brittiskt håll kallas en ” light-touch regulation environment”.

- Alla de kartlagda länderna har en mer eller mindre uttalad ansvarsprincip för arbetet med att skydda och stärka landets kritiska infrastruktur (samhällsviktig verksamhet). Det innebär att ansvaret för arbetet är fördelat mellan nationella regeringar, delstatsregeringar, kommuner (etc.) myndigheter och privata och offentliga ägare och operatörer av kritisk infrastruktur. Mycket av de privata aktörernas ansvar villar dock på frivillighetens grund. Men även samverkan mellan den nationella nivån och övriga nivåer i samhället, inte minst eftersom flera länder har federativa statsbildningar, måste ske på mer eller mindre frivilligt samförstånd. Länderna ser ett välutvecklat och fungerande, vad som ofta kallas, ”partnerskap” mellan nationella regeringar, delstatsregeringar och lokala politiska organ samt privata aktörer med ansvar för kritisk infrastruktur som helt avgörande för att kunna skydda och stärka landets kritiska infrastruktur. Med andra ord är ”partnerskap” (som alltså är något större än privat-offentlig samverkan) huvudpelaren i de berörda ländernas arbete med att skydda och stärka landets kritiska infrastruktur.

- Gemensamt för de kartlagda länderna är att de ser en snabb utveckling, och har att hantera en faktisk situation, där alltmer av den kritiska infrastrukturen på grund av avreglering, outsourcing etc. ägs eller drivs av privata aktörer. Merparten av den kritiska infrastrukturen är således idag inte längre i offentliga händer med ökade krav på privat-offentlig samverkan (partnerskap).

- Arbetet med ”partnerskap” mellan myndigheter och privata aktörer och olika samhällsnivåer återspeglas genom att länderna skapar mer eller mindre utvecklade strukturer för partnerskap inom i statsförvaltningen: genom särskilda organisatoriska enheter för partnerskap, samverkansforum, på olika nivåer i samhället och särskilda nätbaserade samverkansstruktur (webbportaler) för partnerskap. Partnerskapvägen återspeglas t.ex. i USA i myndighetsorganisering. I ”Office of Infra-

structure Protection” finns ”Sector Outreach and Programs Division” som specifikt arbetar med de nationella ansträngningarna att bygga, vidmakthålla och utveckla frivillig privat- offentlig samverkan med privata ägare eller operatörer av kritisk infrastruktur. I Schweiz fall utgör Federal Office for National Economic Supply (FONES) ett en väl utvecklad partnerskapsstruktur mellan det offentliga och privata.

- I sitt partnerskapsarbete för skydd av kritisk infrastruktur inom och mellan sektorer söker USA matcha redan existerande strukturer för privat-privat samverkan (branschorgan) med strukturer för samverkan mellan myndigheter. De sektorsöverskridande partnerskapsorganen som inrättats består av ett urval av representanter från de olika nämnda sektorsstrukturerna.

- Ett led i partnerskapstanken hos de kartlagda länderana är att nationella samordningsansvariga myndigheter tar fram handböcker, vägledningar, analysverktyg för att understödja övriga aktörer i deras arbete med att skydda och stärka den kritiska infrastrukturen.

- I flera av de kartlagda ländernas nationella handlingsprogram betonas mer eller mindre tydligt att offentliga aktörer aktivt måste arbeta för att skapa och tydliggöra ett mervärde för de privata aktörerna för att få till stånd ett effektivt ”partnerskap”. Mer passivt uppmanna till samverkan utan tydliggöra mervärden duger inte. Mervärde för de privata aktörerna förvänta skapas genom att erbjuda dessa t.ex. aktuell underrättelseinformation om hotbilder mot deras sektor eller enskilda anläggningar, verktyg för risk- och sårbarhetsanalyser eller kontinuitetsplaner, olika former av expertstöd, utbildningar m.m.

- Ett mervärde för öka de privata aktörernas villighet att delta i ett partnerskap för skydd av kritisk infrastruktur är personlig prestige. I USA har t.ex. presidenten ett särskilt rådgivande organ för frågor gällande skydd av kritisk infrastruktur bestående av representanter från näringsliv, forskningsvärlden, delstatsregeringar m.fl. som formellt är utnämnda av presidenten. Dessa representanter kan med andra ord kallas sig presidentrådgivare, med den personliga prestige det medför.

- En grundpelare i ett fungerande ”partnerskap” och ett effektivt skydd av kritisk infrastruktur är enligt flera av de studerade länderna säkerställandet av att det på ett säkert och snabbt sätt går att dela känslig information rörande hotbilder, skyddsåtgärder, best practice m.m. mellan och inom både offentliga och privata aktörer samt inom och mellan olika sektorer. Det innebär i praktiken att det behövs skapas strukturer

i form av fysiska mötesforum för informationsdelning och webbaserade informationsdelningsportaler inklusive protokoll för hur och vilken information som kan delas över nätet. Men det räcker inte bara att tillskapa dessa strukturer utan det krävs också att berörda aktörer får förtroende för strukturerna och är villiga att nyttja dessa på ett kontinuerligt och konsekvent sätt. En viktig uppgift för sektorsansvariga myndigheter är därför att bygga upp ett sådant förtroende inom ramen för partnerskapet.

- Polen betonar vikten av ömsesidigt ”partnerskap” med privata aktörer men har samtidigt väl utvecklade och tvingande strikta administrativa (”byråkratiska”) processer för hur det nationella arbetet med skydd av kritisk infrastruktur ska ske. Polen avviker bland annat från de andra kartlagda länderna genom att ha mycket strikta administrativa krav på ägare och operatörer av kritisk infrastruktur när det gäller att genomföra och inkomma med risk- och sårbarhetsanalyser samt förmågebedömningar avseende hantering av risker, hot och störningar. Ett flertal instanser (t.ex. räddningstjänst, polis och/eller länsveterinärer beroende på typ av anläggning) ska oberoende av varandra godkänna ägarna eller operatörernas inkomna underlag för ett slutligt godkännande. Polens arbete med skydd av kritisk infrastruktur ser till synes ut att återspegla ett kulturellt byråkratiskt arv från kommunisttiden i kombination med de förutsättningar som en ökad privatisering och avreglering av samhällsviktiga verksamheter ställer. I mycket framstår Polen som ett föregångsland väl värda att studera närmare när det gäller ha tydligt utvecklade nationella processer för arbetet med skydd av kritisk infrastruktur. Samtidigt är ett stort frågetecken hur dessa processer fungerar i praktiken och skulle kunna fungera i andra länder.

- Den vanliga formen av organisering och ansvarsfördelning på regerings- och departementsnivå för arbetet med skydd av kritisk infrastruktur i de kartlagda länderna är att det finns utpekade sektorsansvariga departement och ett departement med ansvar för sektorsövergripande samordning. På myndighetsnivå återfinns samma upplägg.

- I t.ex. Storbritannien har varje sektorsansvarigt departement skyldighet att årligen redovisa resilensplaner för sin sektor och den kritiska infrastruktur som ingår i den. Departementen har också skyldig att ta fram handlingsplaner för att åtgärda brister i skyddet av den kritiska infrastrukturen när så är påkallat.

- Flera av de kartlagda länderna, USA, UK och Schweiz, har ett eller ett flertal specifika centra, funktioner, enheter, rådgivande organ (etc.) som har säkerhet, skydd av eller stärkande av kritisk infrastruktur som

huvuduppgift och som är ansvarsmässigt kopplade till regeringskansli och departement eller till centrala myndigheter. Det kan möjligen, tillsammans med andra aspekter som bland annat nämnts ovan, ses som en indikation på vilken prioritet länderna ger dessa frågor.

- Flertalet kartlagda länder betonar, direkt eller indirekt, att dess nationella handlingsprogram för skydd av kritisk infrastruktur är en pusselbit i deras övergripande säkerhets- och krisberedskapsarbete och att denna bit måste samspela lagmässigt, policymässigt och praktiskt med övriga pusselbitar. Inte minst gäller det olycks- och krishantering, då arbetet med skydd av kritisk infrastruktur oftast har en tonvikt på det förebyggande arbetet.

- En bredare hotbild mot infrastruktur och ett ökat behov av sektoröverskridande samarbete har bland vissa av de kartlagda länderna tvingat fram behovet av integrering av politikområden och myndighetssfärer som tidigare arbetat självständigt med frågor rörande säkerhet eller skydd av kritisk infrastruktur utifrån olika perspektiv och målsättningar. Det gäller framförallt den polisiära underrättelse- och säkertjänsten i relation till mer öppna myndigheter. En subjektiv bedömning är att detta rikserar att skapa oklara ansvarsförhållanden och dubbelarbete framöver. I fallet med Storbritannien är det arbetsfördelningen mellan Centre for the Protection of National Infrastructure (som lyder under MI5) och ”The Civil Contingencies Secretariat” i Cabinet Office som ter sig något oklara för en utomstående betraktare.

- Cybersäkerhet kopplad till säkerhet och skydd av fysisk kritisk infrastruktur tenderar av allt att döma att utgöra en domänöverskridande och integreringsmässig utmaning för flera av de kartlagda länderna. I USA har detta bland annat genom särskilt presidentbeslut resulterat i att det t.ex. inrättats en särskild funktion, ”Office of Cyber and Infrastructure Analysis”, för komma tillrätta med detta.

- Av vad som kunnat utläsas av tillgängligt material ges inga storskaliga nya eller särskilda anslag för arbetet med skydd av kritisk infrastruktur som en direkt följd av inrättande av de nationella handlingsprogrammen i de studerade länderna. Huvudlinjen verkar vara att ansvariga departement eller ministerium får själv finna medel för det aktuella arbetet inom ramen för sina givna anslag i statsbudgeten.

- Samtliga kartlagda länder har ”all-hazard” (dvs. att alla former av hot och risker ska beaktas såsom naturolyckor, teknisk-industriella olyckor och antagonistiska attentat) som en grundläggande princip för sitt nat-

ionella arbete med att skydda och stärka sin kritiska infrastruktur, även om tonvikten på de olika hoten kan variera.

- Samtliga kartlagda länder har också som en grundläggande princip för sitt arbete med skydd av kritisk infrastruktur att arbetet ska bedrivas i krisberedskapens alla faser, dvs. före-under-efter.

- Flertalet kartlagda länder eftersträvar genom uppmuntran och stöd ett aktivt allmänt bruk av kontinuitetsplanering hos ägare och operatörer av kritisk infrastruktur. Sådan kontinuitetsplanering ska i sin tur vara baserad på en grundliga risk- och sårbarhetsanalys. Ett allmänt bruk och tillämpningen av risk- och sårbarhetsanalyser och kontinuitetsplaner hos privat och offentliga berörda aktörer ses sammanfattningsvis som grundpelare för de nationella programmen för skydd av kritisk infrastruktur.

- Flera av de kartlagda länderna eftersträvar bruket av internationella eller/och nationellt anpassade standarder (ISO-standarder) i arbetet med att skydda och stärka den kritiska infrastrukturen, t.ex. för ”risk management” eller ”business continuity management”. Kanada basera t.ex. sin handledning ”Risk Management Guide for Crictical Infrastructure Sectors” på internationell ISO-standard 31000 ”Risk Management – Principles and guidelines on implementation” och Storbritannien har sin nationella ”Business continuity management standard, BS25999” som bas för sin kontinuitetsplanering.

- De kartlagda länderna betonar vikten av utbildning och övningar som en viktig komponent i arbetet med att skydda och stärka den kritiska infrastrukturen.

- I Storbritannien samarbetar deras ”Centre for the Protection of National Infrastructure” (CPNI) inom den privata domänen med särskilda ”Trusted Partners”, vilka främst utgörs av olika säkerhets- eller teknikföretag som via upphandling jobbar med att skydda och serva anläggningar som utgör särskild säkerklassad infrastruktur. För att bli ”Trusted Partner” måste företagen leva upp till särskilda krav som CPIN ställt upp, dvs. bli säkerhetsklassade.

- De studerade länderna betonar vikten av att ha ett väl utvecklat samarbete med universitet och högskolor för att fördjupa kunskapen kring säkerhet och skydd av kritisk infrastruktur.

- Den enskilde individens mentala beredskap och praktiska förmåga att hantera störningar i kritisk infrastruktur anses som mycket betydelsefulla av vissa studerade länder, t.ex. Kanada och Finland, varför arbetet med just dessa frågor också utgör en särskild del av det nationella handlingsprogrammet/säkerhetsstrategin.

1.2.2 Sveriges arbete med skydd av samhällsviktiga verksamheter i förhållande till de kartlagda länderna

Avviker Sverige på något tydligt sätt från de här kartlagda länderna när det gäller att organisera, samordna och styra sitt nationella arbete med skydd av samhällsviktig verksamhet (kritisk infrastruktur inklusive kritisk produktion och kritiska resurser)? Ger kartläggningen av länderna några lärdomar för svensk del? Den översiktliga kartläggningen är endast baserad på olika former av policydokument. Utifrån dem går det inte att säga hur de olika ländernas konkreta arbete med skydd av kritisk infrastruktur verkligen fungerar. De olika länderna skiljer sig också i många fall från Sverige vad gäller konstitutionell- och förvaltningsmässig struktur, historiska erfarenheter m.m. Organisering, samordning och styrning som passar för ett land kan i värsta fall var helt olämpligt för svensk del. Man måste därför vara försiktig och eftertänksam om man från svensk sida tänker låna in idéer från andra länder.

Finland och Schweiz har kvar en ansats som övergavs av Sverige vid nedmonteringen av civilt försvars efter kalla kriget

Sverige skiljer sig påtagligt i jämförelse med Finland och Schweiz i den övergripande ansatsen när det gäller att skydda landets samhällsviktiga verksamheter/kritisk infrastruktur. Den ansats som Finland och Schweiz bygger, som tidigare framgått, ytterst på tankar om civilt försvar anpassat till krigets krav. Ländernas ansats inbegriper därför beredskapslagring av olika former av kritiska resurser för folkförsörjning och industriproduktion, möjligheter till betydande marknadsinterventioner och betydande möjligheter att prioritera resurser till samhällsviktiga verksamheter. Styrel är här ett undantag för svensk del. Finland och framförallt Schweiz arbete med skydd av samhällsviktiga verksamheter backas därför också upp av ett mycket starkare lagstöd än vad som är fallet för svensk del. För Schweiz handlar om det om stöd i landets konstitution när det gäller försörjningsberedskap. Fram till slutet av det kalla kriget hade Sverige en ansats rörande skydd av samhällsviktiga verksamheter som i det stora liknar den ansats som Finland och Schweiz nu har. Sverige ersatte denna ansats efter kalla kriget med en ansats för hantering av fredstida kriser. En ansats som idag tillsynes går mot inbyggd robusthet, resiliens. Vad återuppväckandet av Sveriges försvarsplanering och civilt försvar innebär för denna utveckling återstår att se.

Alla de kartlagda länderna arbetar med ungefär samma ”verktygslåda”

En jämförelse mellan Sveriges och de kartlagda ländernas ”verktyglåda” för arbetet med skydd av samhällsviktiga verksamheter/kritisk infrastruktur visar, utöver vad som nyss nämndes rörande den ansats Finland och Schweiz har, inte på några större avvikelser. Sverige har likt de kartlagda länderna, i varierande omfattning, en ”verktygslåda” som inbegriper: en ansvars- och närhetsprincip för arbetet med skydd av kritisk infrastruktur (även om den kan variera till sin karaktär), en nationell strategi och handlingsplan för skydd av kritisk infrastruktur, samverkansforum för privata och offentliga aktörer inom och mellan sektorer på olika samhällsnivåer, anmodad kontinuitetshantering för företag och myndigheter, föreskrivna eller frivilliga risk- och sårbarhetsanalyser, kartläggning av kritiska beroendeförhållanden inom och mellan sektor och anläggningar, internationella/nationella standarder inom området, framtagande och spridning av handledningar, verktyg och analysmetoder rörande kritisk infrastruktur från nationell nivå, övningar m.m. Några viktiga olikheter existerar dock.

Den första olikheten har att göra med att hos flera av de kartlagda länderna, främst USA och Storbritannien, finns det en tillsynes mycket större politisk tyngd och ett driv när det gäller frågor rörande skydd av kritisk infrastruktur. Frågorna är därför också mer profilerade rent organisatoriskt i departement och myndighetstrukturer med särskilda centra, sekretariat (etc.) för skydd av kritisk infrastruktur eller resiliens. Terrorism är inte sällan en stark drivkraft. I Sverige får nog frågan om skydd av samhällsviktiga verksamheter sägas sakna motsvarande politisk tyngd och vara relativt organisatoriskt profillös i det allmänna krisberedskapsarbetet.

Den andra olikheten har att göra med att vissa länder som Polen, Schweiz och Finland har lagstiftning som möjliggör att utifrån ansvarsprincipen kravställa mot privata ägare/operatörer när det gäller risk- och sårbarhetsanalyser, kontinuitetshantering och/eller att prioritera resurser till samhällsviktiga verksamheter. Sverige har ett mycket svagare lagstöd att luta sig mot.

Den tredje olikheten har att göra med regerings- och förvaltningsstrukturen med större inslag av centralstyrning på den nationella nivån hos de kartlagda länderna. För arbetet med skydd av kritisk infrastruktur finns tydligt utpekade departement och/eller myndigheter med ansvar för arbetet med skydd av kritisk infrastruktur inom eller flera sektorer samt ett sektorsövergripande ansvar. I Storbritannien har t.ex. ansvariga departement också ansvar att årligen ta fram en åtgärdsplan för sin sektor. I Sverige finns inga utpekade departement eller myndigheter med kopplat ansvar för genomförande av den nationella handlingsplanen för skydd av samhällsviktiga verksamheter.

Den fjärde olikheten har att göra med att t.ex. länder som USA, Kanada och Schweiz tillsynes bygger sitt arbete med skydd av kritisk infrastruktur mycket mer kring ett integrerat och livfullt ”partnerskap” mellan privata aktörer och offentliga aktörer på nationell, regional (delstats) och regional nivå än vad Sverige gör. Det återspeglas t.ex. organisatoriskt i olika organ som bara arbetar med ”outreach” (USA) till näringslivet och hur befattningshavare från närings-

livet jobbar deltid med offentliga försörjningsfrågor som en del av skyddet av kritisk infrastruktur (Schweiz). Flera av de kartlagda länderna betonar också vikten av att myndigheterna måste kunna erbjuda handfasta mervärden för att kunna engagera privata aktörer. Det kan t.ex. handla om att erbjuda aktuella hotbilder mot en sektor, analysverktyg för riskmangement m.m. USA försöker också höja statusen i partnerskapet genom att göra befattningshavare från näringslivet till ”presidentrådgivare” i frågor rörande skydd av kritisk infrastruktur. Sverige arbetar givetvis med privat-offentlig samverkan i olika former, men mer som ett tillägg till den offentliga samverkan och mer trevande än som verkar vara fallet i flera av de kartlagda länderna.

Den femte olikheten har att göra med att länder som USA och Kanada ser webbaserade informationsdelningsstrukturer, dvs. webbportaler, för säker och snabb informationsdelning (om t.ex. aktuella hot mot kritisk infrastruktur) mellan privata aktörer och myndigheter som en grundpelare i ett effektivt partnerskap. Sverige har veterligen inga ambitioner om att systematiskt utveckla sådana nationella webbportaler (exklusive EU:s varningssystem) för dess olika samhällssektorer.

2 Schweiz

2.1 Definition, mål och sektorsindelning

Schweiz definierar infrastruktur som omfattande ”människor, organisationer, processer, produkter, tjänster, informationsflöden, likväl som tekniska och strukturella installationer och konstruktioner som, enskilt eller som del av ett nätverk, möjliggör det för samhället, ekonomin och landet att fungera”.

Kritisk infrastruktur utgörs enligt Schweiziskt synsätt av infrastruktur som vid avbrott, bortfall eller ödeläggelse har en allvarlig inverkan på det allmänna hälsoläget, miljön, nationella säkerheten, sociala och ekonomiska välståndet samt på det politiska livet och samhällslivet i övrigt. Det uttalade målet med Schweiz arbete med skydd av nationell kritisk infrastruktur är att minska sannolikheten för inträffandet av och/eller omfattningen på skador, störningar eller ödeläggelse av kritisk infra-struktur på nationell nivån samt att minimera tiden som det tar att återgå till normal kapacitet.

Sectors	Sub-sectors
Energy	Natural gas supply
	Oil supply
	Power supply
Financial services	Banks
	Insurance companies
Information- & communication technologies (ICT)	Information technologies
	Media
	Telecommunication
Industry	Chemical and Pharmaceutical Industry
	Mechanical and Electrical Engineering Industries
Public administration	Foreign representations and headquarters of international organizations
	Cultural property
	Parliament, government, justice, administration
	Research institutes
Public health	Medical care and hospitals
	Laboratories
Public safety	Armed forces
	Civil defense
	Emergency organizations (police, fire service, emergency medical service and rescue services)
Transport	Air transport
	Water transport
	Postal services
	Rail transport
	Road transport
Water and Food	Food supply
	Drinking water supply
Waste disposal	Waste
	Wastewater

	Very high criticality
	High criticality
	Regular criticality

→ All sub-sectors are critical.
→ Criticality refers to the importance of the sub-sector in terms of interdependency, the population, and the economy (not its general importance or its mission-criticality).
→ Even sub-sectors whose criticality is regular may contain highly critical individual elements.
→ Weighting is based on an ordinary thereat level.

Figur 1. Schweiz sektorsindelning av kritisk infrastruktur.

Schweiz delar upp sin infrastruktur i tre nivåer:

- Sektor (t.ex. energi, hälso- och sjukvård)
- Subsektor (t.ex. elförsörjning, oljeförsörjning)
- Inviduella objekt/element (t.ex. ledningscentraler för elnät, kontrollsystem, dammar)

Schweiz identifiera 10 sektorer och 31 subsektorer som framgår av tabellen ovan. Utifrån en särskild framtagen metodologi prioriterar Schweiz hur kritisk en subsektor är utifrån dess effekter på andra subsektorer, på befolkningen och på ekonomin vid störningar i subsektorn. Graden av kritiskhet är indelad i 1)

mycket hög, 2) hög, och 3) normal. Resultatet av indelningen framgår i figuren ovan).

2.2 Doktrin och styrmedel

Schweiz baserar sitt arbete med skydd av kritisk infrastruktur på ett antal centrala förhållningssätt eller doktrinelement som vägleder det praktiska arbetet. Ett första, och kanske det mest grundläggande, doktrinelementet är att arbetet med skydd av kritisk infrastruktur baseras på och bygger vidare på redan existerande lagar och regelverk, professionella nationella och internationella bransch- och sektorsstandarder, skydds- och säkerhetsarbete, nätverk för samverkan etc. Det finns inte någon särskild och sektorsöverskridande lag för skydd av kritisk infrastruktur, inte heller är någon sådan tilltänkt. Däremot finns det specifikt för försörjningsberedskapen (se nedan). Ett andra doktrinelement är att eftersom merparten av den kritiska infrastrukturen är privatägd så utgörs grunden för inriktning och styrning i arbetet med skydd av kritisk infrastruktur av frivilliga överenskommelser genom privat-offentlig samverkan. Vägen är frivillighet inte lagstiftning. Ett tredje doktrinelement är att arbetet med skydd av kritisk infrastruktur ska omfatta alla faser i krisberedskapscykeln, dvs förebygga, hantera och återställa. Ett fjärde doktrinelement är att arbetet med skydd av kritisk infrastruktur ska baseras på en ”All-hazard” ansats, dvs. alla typer av hot och risker (naturolyckor, olyckor i tekniska system, terrorism m.m.) ska beaktas utan att någon av dessa prioriteras. Ett femte doktrinelement är att arbetet med skydd av kritisk infrastruktur ska inbegripa inbyggd riskhantering (”Integral risk management”). Inbyggd riskhantering, som är kopplat till de två senast nämnda doktrinelementen, består av två delar. Den första är en noggrann risk- och sårbarhetsanalys. På basis av den vidtas åtgärder inom följande områden:

- Förebyggande (Prevention): (t.ex. strukturell-tekniska åtgärder)
- Förberedande (Preparation): (t.ex. kontinuitetsplanering)
- Ingripande (Intervention): (.t.ex. alarmsystem, fysiskt skydd genom säkerhetspersonal)
- Reperation (Recondtion): (t.ex. tillfällig reperation av infrastruktur)
- Återuppbyggnad (Reconstruction): (återuppbyggnad av infrastruktur)

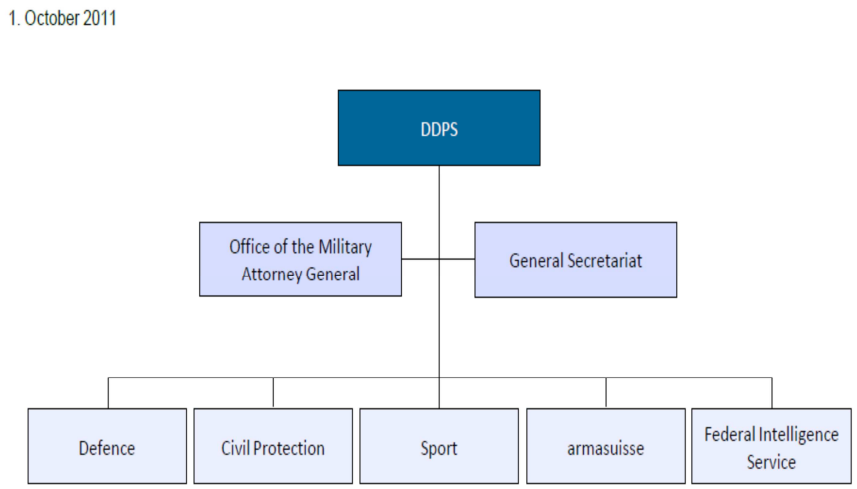
Ett sjätte doktrinelement är resiliens. Eftersom det är omöjligt att skydd all kritisk infrastruktur permanent eller att eliminera alla sårbarheter fullständigt så är enligt Schweiziskt synsätt resiliens av stor vikt i arbetet med skydd av kritisk infrastruktur. Målet med resilensen är att kunna återgå till ett normalläge så snart som möjligt efter en störning. Resiliens består av fem komponenter 1) robustheten i systemet (infrastrukturen) som sådan, 2) tillgången till backup-enheter (redundans), 3) möjligheten att mobilisera hjälpinsatser, 4) snabbheten i hjälpinsatserna samt 5) samhällets förmåga att hantera krissituationer. Ett sjunde doktrinelement är vidmakthållande av proportionalitet. De åtgärder som vidtas för att skydda kritisk infrastruktur måste vara i proportion till riskbedömningen och till skyddsmål som ska uppnå. Proportionalitet ska också vidmakthållas med avseende till kostnader, skydd och säkerhet likväl

som personlig frihet och integritet. Dessutom måste onödiga störningar av den fria konkurrensen på marknaden undvikas. Ett åttonde doktrinelement är subsidaritetsprincipen, eller vad som kan sägas motsvara ansvars- och närhetsprincipen i svensk krisberedskap. Med andra ord är det ägarna eller driftansvariga av infrastrukturen som har ett eget ansvar för att vidta behövliga skyddsåtgärder och hantera störningar i sina anläggningar etc. Ett nionde doktrinelement är riskkommunikation genom hemsidor, broschyrer etc. till allmänheten, företagare och andra relevanta aktörer i samhället om sårbarhet i kritisk infrastruktur och dess konsekvenser som dessa kan behöva hantera.

2.3 Organisering och ledning

2.3.1 Nationell nivå

Det yttersta nationella ansvaret för arbetet med skydd av nationell kritisk infrastruktur ligger hos den schweiziska federala regeringen och dess departement för ”Defence, Civil Protection and Sports” (DDPS). DDPS är uppdelat i fem olika sektorer, avdelningar, inklusive ”Civill Protection” (se figur nedan).



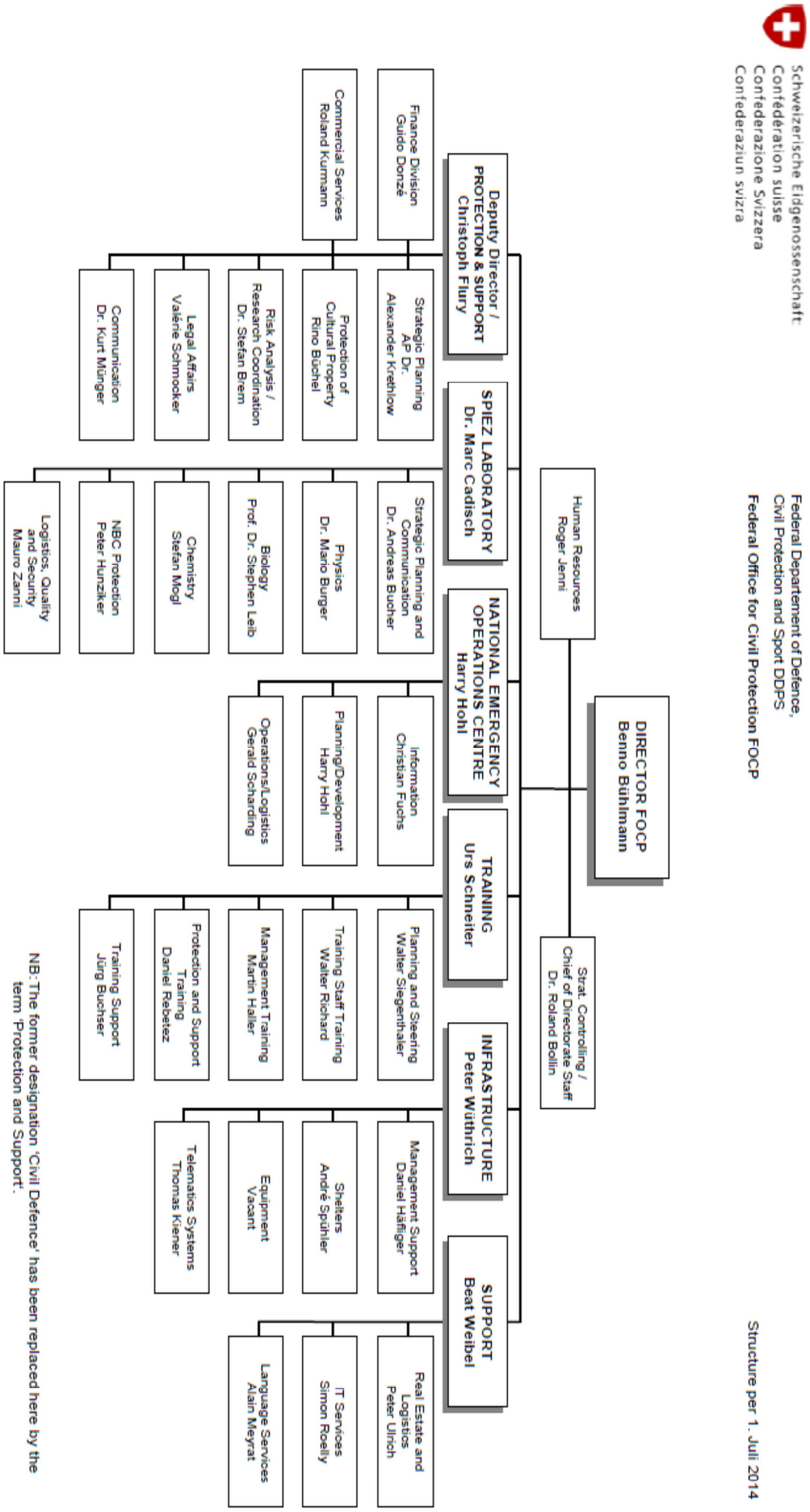
Figur 2. Organisationsskiss över Schweiz departement för ”Defence, Civil Protection and Sports” (DDPS).

Inom sektorn ”Civil Protection” återfinns organisatoriskt ”Federal Office for Civil Protection (FOCP)” som har det direkta nationell ansvaret för att samordna arbetet med att skydda nationell kritisk infrastruktur. FOCP, som bildades 2003, kan närmast sägas motsvara MSB i Sverige. FOCP har ca 300 medarbetare och arbetar övergripande med att stödja landets kantoner på regional niivå och kommuner på lokal nivå med ”Civil Protection”, dvs.

krisberedskap och civilt försvar. FOCP stödjer och samverkar också med näringslivet i frågor rörande krisberedskap. Inom FOCP är det avdelningen för ”Infrastructure” som ansvarar för arbetet rörande skydd av nationell kritisk infrastruktur (se figur nedan). När det gäller skydd av kritisk infrastruktur har FOCP följande roller och ansvar:

- Leder den särskilda arbetsgruppen för skydd av kritisk infrastruktur (se nedan)
- Koordinerar och säkerställer nationell enhetlighet i arbetet med skydd av kritisk infrastruktur
- Utvecklar, implementerar och följer upp arbetet med den nationella strategin för skydd av kritisk infrastruktur (se nedan)
- Ansvarar för information och kommunikation i frågor som rör skydd av kritisk infrastruktur
- Informerar och rådgör med regeringen (Federal Counil) i frågor rörande skydd av kritisk infrastruktur

Figur 3. Organisationsskiss för Schweiz "Federal Office for Civil Protection (FOCP"



Före bildande av FOCP pågick inom alla samhällssektor i Schweiz olika former av arbete med att skydda nationell kritisk infrastruktur, men det saknades ett sammanhållande sektorsöverskridande arbete. FOCP fick därför år 2005 ett regeringsuppdrag att koordinera det pågående arbete med skydd av kritisk infrastruktur inom olika sektorer och nivåer samt att etablera en arbetsgrupp för skydd av kritisk infrastruktur (”CIP Working Group”) som innefattade alla relevanta nationella myndigheter som arbetade med skydd av kritisk infrastruktur. Arbetsgruppen innefattar i dagsläget 30 olika representanter från alla de sju existerande sektordepartementen i Schweiziska regeringskansliet, Finansdepartementet och kantonerna. Följande organ är representerade i ”CIP Working Group”:

- Federal Chancellery FCh
- Division for Security Policy and Crisis Management DSEC
- Swiss Agency for Development and Cooperation SDC
- Federal Office for Public Health FOCP
- Federal Office of Meteorology and Climatology MeteoSwiss
- Federal Office of Police fedpol
- Federal Intelligence Service FIS
- Cyber Defence Project of the General Secretariat of the DDPS
- Security Policy sector SECPOL
- Federal Office for Civil Protection FOCP
- Armed Forces Joint Staff AFJS
- Armasuisse
- Information Security and Facilities Protection IOS
- Federal Finance Administration FFA
- Swiss Federal Office for Buildings and Logistics SFBL
- Swiss Federal Office of Information Technology, Systems and Telecommunication FOIIT
- Federal IT Steering Unit FITSU
- Federal Office for National Economic Supply FONES
- General Secretariat of the Federal Department of the Environment, Transport, Energy, Communications
- Federal Office of Transport FOT
- Federal Office of Civil Aviation FOCA

- Swiss Federal Office of Energy SFOE
- Federal Office for Communications OFCOM
- Federal Office for the Environment FOEN
- Federal Roads Office FEDRO
- Swiss Federal Electricity Commission ElCom
- Federal Nuclear Safety Inspectorate ENSI
- Canton of Basel-Town BS
- Canton of Geneva GE

De enskilda representanterna i ”CIP Working Group” har följande roll och uppdrag inom sina respektive departement:

- Tjäna som kontaktpunkt i departementet i frågor som gäller skydd av kritisk infrastruktur
- Stödjer det egna departementet i implementeringen av arbete rörande skydd av kritisk infrastruktur inom dess (sektor)ansvarsområde
- Ansvarar för att kontakt etableras med existerande plattformar och nätverk som finns med näringslivet inom departementets ansvarsområde, dvs. ansvarar för frågor rörande skydd av kritisk infrastruktur inom existerande samverkansstrukturer på nationell nivå för privat-offentlig samverkan, partnerskap.

”CIP Working Group” är den organisatoriska kärnan i arbetet med skydd av nationell kritisk infrastruktur. Arbetsgruppen inriktar, leder och utvärderar arbetet samt utgör en plattform för informationsutbyte och för att sprida best practice inom och mellan sektorer. Till CIP finns det knutit en särskild stödgrupp som tjänar som ett strategiskt rådgivningsorgan. Stödgruppen utgörs av representanter för näringslivet och ägare av infrastruktur, forskningsvärlden, den offentliga sektorn och ”…society at large” [?][9].

Inom ”CIP Working Group” har det tagits fram en grundläggande strategi som tjänar som ett handlingsprogram för Schweiz arbete med att skydda kritisk nationell infrastruktur. Schweiz samlade arbete med skydd av kritisk infrastruktur bygger i övrigt på existerande strukturer, organisationer och nätverk. De åtgärder som vidtas i varje sektor och subsektor implementeras så långt som möjligt inom ramen för existerande politiska processer och genom bruket av existerande politiska, legala och administrariva verktyg. Härigenom ligger också det offentliga ansvaret för arbetet med skydd av kritisk nationell infrastruktur hos olika sektorsansvariga departement och myndigheter på federal nivå.

[9] The Federal Council’s Basic Strategy for Critical Infrastructure Protection, 2009, kapitel 6.

2.3.2 Kantonerna

Kantonerna på regional nivå utgör en viktig part i att utveckla och implementera det nationella arbetet med att skydda kritisk infrastruktur. Kantonerna har också krishanteringsansvaret vid störningar i infrastruktur inom deras geografiska ansvarsområde. Mot denna bakgrund är också kantonerna (två stycken) representerade i ”CIP Working Group” och de olika arbetsprojekt som gruppen bedriver. Varje kanton (26 stycken totalt) har också utsedda kontaktpunkter för att underlätta informationsflödet och samarbetet med den nationella nivån i frågor rörande skydd av kritisk infrastruktur.

2.3.3 Ägare och operatörer

Privata och offentliga ägare eller operatörer av kritisk infrastruktur ses från nationell nivå som de centrala kontaktpunkterna och samarbetsparterna i arbetet med skydd av kritisk infrastruktur och dithörande kontinuitetsplanering för anläggningar, system etc. Samarbetet från nationell nivå med dessa ägare och operatörer säkerställas genom deras representation i den ovan nämnda rådgivande stödgruppen till ”CIP Working Group” och genom de existernande nätverk och kontaktforum för privat-offentlig samverkan som finns inom varje sektor och subsektor.

2.3.4 Federal Office for National Economis Supply (FONES)

En viktig komponent kopplad till ovan nämnda strukturer för skydd av kritisk infrastruktur är Schweiz beredskapsstruktur för nationell ekonomisk försörjning ”Federal Office for National Economic Supply (FONES)”. FONES uppgift är att säkerställa och prioritera tillgången på kritiska resurser vid kortare och medellånga störningar i samhället, t.ex. på grund av säkerhetspolitisk oro i omvärlden som stoppar import till landet. FONES har sitt mandat konstitutionellt fastlagt (artikel 102):

[1] *The Confederation shall ensure that the country is supplied with essential goods and services in the event of the threat of politico-military strife or war, or of severe shortages that the economy cannot by itself counteract. It shall take precautionary measures to address these matters.*
[2] *In exercising its powers under this Article, it may if necessary depart from the principle of economic freedom.*

FONES fullgöra sin uppgift genom att ha tillgång till lagstiftad beredskapslagring av bland annat livsmedel, läkemedel, olja, drivmedel och olika insatsvaror till industrin samt genom att ha befogenhet att prioritera resurser och tjänster till samhällsviktiga verksamheter. FONES samarbetar nära med näringslivet, Kantoner och kommuner. Inte minst får FONES stöd av experter ute i Kantonerna och kommunerna som förbereder och överser implementeringen av FONES beslut. FONES leds av en person på deltid som alltid hämtas från det privata näringslivet. Till sitt stöd har denne FONES egna personal och ca 300 personer på deltid ifrån näringslivet och statsförvaltningen.

Underlag

Swiss Federal Office for Civil Protection FOCP, hemsida:
http://www.bevoelkerungsschutz.admin.ch/internet/bs/en/home/das_babs.html

National Economic Supply Strategy: A brief summary. Federal Office for National Economic Supply, FONES, 2007:
www.bwl.admin.ch/.../00532/index.html

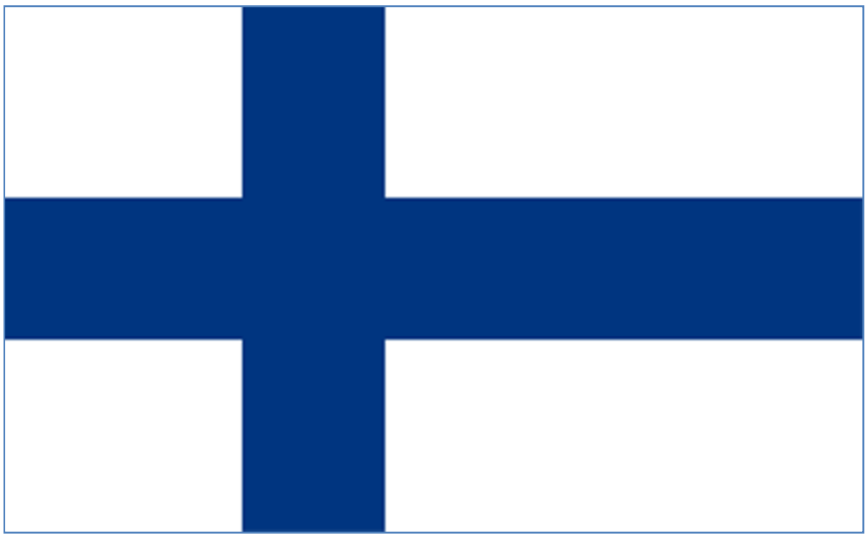
Federal Office for National Economic Supply, FONES, hemsida:
http://www.bwl.admin.ch/index.html?lang=en

The Federal Council's Basic Strategy for Critical Infrastructure Protection Basis for the national critical infrastructure protection strategy, 18 May 2009.
(http://www.bevoelkerungsschutz.admin.ch/internet/bs/en/home/themen/ski.parsysrelated1.82246.downloadList.42043.DownloadFile.tmp/grundstrategieski20090518e.pdf)

The Swiss Programme on Critical Infrastructure Protection.
(http://www.bevoelkerungsschutz.admin.ch/internet/bs/en/home/themen/ski.parsysrelated1.82246.downloadList.18074.DownloadFile.tmp/factsheete.pdf)

Critical Infrastructure Protection: Second Report to the Federal Council and Measures for the Period 2009-2011. Federal Office for Civil Protection FOCP, 2009.:
http://www.bevoelkerungsschutz.admin.ch/internet/bs/en/home/themen/ski/publikationen_ski.parsys.60516.downloadList.59025.DownloadFile.tmp/2berichtski20090605e.pdf

3 Finland



3.1 Doktrin och styrmedel

Finlands har en ansats som skiljer sig från övriga studerade länder när det gäller arbetet med skydd av kritisk infrastruktur. Finland har inget specifikt och tydligt urskiljbart nationellt program eller dylikt för skydd av kritisk infrastruktur, som finns eller är under utveckling i de andra kartlagda länderna. Medan många länder tämligen nyligen etablerat ett särskilt nationellt sektorsövergripande program för skydd av kritisk infrastruktur mot bakgrund av ett bedömt ökat terrorhot och/eller klimatförändringar så har Finlands arbete på området gradvis vuxit fram inom ramen för totalförsvaret och behovet av att kunna möta krigets krav. Finlands arbete med skydd av kritisk infrastruktur, som inte är lika explicit som andra länder, är mer att betrakta som en integrerad del av arbetet med totalförsvaret och dess målsättningar. Förutom på redan existerande lagar och regelverk, professionella nationella och internationella bransch- och sektorsstandarder, vardagligt skydds- och säkerhetsarbete, nätverk för samverkan m.m. så bygger arbetet med skydd av kritisk infrastruktur på landets så kallade försörjningsberedskap (se vidare nedan,) som kan sägas stå på tre ben. Det första benet är skydd av kritisk infrastruktur, dvs. tekniska system och strukturer. Med samhällets kritiska infrastruktur inbegrips:

- Överförings- och distributionsnät för energi
- Elektroniska data- och kommunikationssystem
- Transportlogistiska system
- Vattenförsörjning och annan kommunalteknik
- Byggande och underhåll av infrastruktur

Det andra benet är kritisk produktion av varor och tjänster som framställs med hjälp av den kritiska infrastrukturen. Med kritisk produktion inbegrips:

- Livsmedelsförsörjning
- Energiproduktion
- Hälso- och sjukvård
- Produktion som stöder försvaret
- Främjande av de allmänna verksamhetsförutsättningarna för exportindustrin

Det tredje benet är beredskapslagring (säkerhetsupplag, obligatoriska upplag och skyddsupplag) av produkter och material för den kritiska produktionen och folkförsörjningen. Till dessa tre ben kan också räknas olika internationella avtal som på olika sätt stödjer försörjningsberedskapen. Doktrinmässigt utgår arbetet med skyddet av den kritiska infrastrukturen främst från Finlands övergripande ”Säkerhetsstrategi för samhället” och dess ansvarsfördelning och målsättningar (se nedan). Utöver ovan nämnda baserar Finland sitt arbete med skydd av kritisk infrastruktur på ytterligare ett antal centrala förhållningssätt eller doktrinelement som vägleder det praktiska arbetet. De mer framträdande ska här nämnas.

Det först är att arbetet med försörjningsberedskapen och skyddet av den kritiska infrastrukturen anses behöva vila på ett utvecklat frivilligbaserat samarbete mellan myndigheter och näringslivet då merparten av den kritiska infrastrukturen ägs av privata företag och industrier. Härvid har det utvecklats olika strukturer för privat-offentlig samverkan, främst branschvisa ”sektorer” och ”pooler” (se nedan). Det andra doktrinelementet är att förutom viss lagstiftning kring beredskapslagring m.m. så ligger tonvikten på att allmänt stärka kontinuitetshanteringen hos både privata och offentliga ägare och driftansvariga för kritisk infrastruktur och kritisk produktion. Ansvariga myndigheter uppmuntrar och stödjer härvid ägare och driftansvariga med handledningar, metodverktyg m.m. Det tredje doktrinelementet är att kontinuitetshantering och planläggning ska grunda sig på grundliga risk- och sårbarhetsanalyser.

Det fjärde doktrinelementet är ansvarsprincipen. dvs. de myndigheter som ansvarar för en viss verksamhet under normala förhållanden har också ansvar för verksamheten vid allvarliga störningar och i krig. Det femte doktrinelementet är sektorsansvar som innebär att varje ministerium har ansvar för arbetet med skydd av kritisk infrastruktur inom ramen för sitt ansvarsområde, sektor, inklusive särskilt tilldelade strategiska uppgifter enligt landets säkerhetsstrategi. Det sjätte doktrinelementet är att arbetet med skydd av kritisk infrastruktur ska omfatta alla faser i krisberedskapscykeln, dvs. förebygga, hantera och återställa. Det sjunde doktrinelementet är att arbetet med skydd av kritisk infrastruktur ska baseras på en ”All-hazard” ansats, dvs. alla typer av hot och risker (naturolyckor, olyckor i tekniska system, terrorism m.m.) ska beaktas, även om kriget, ”undantagsförhållanden” får en framträdande plats i olika styrdokument på ett helt annat sätt än hos andra länder. De främsta (offent-

liga) sektorsövergripande styrdokumenten när det gäller Finlands arbete med skydd av kritisk infrastruktur ur ett krisberedskapsperspektiv utgörs av:

- Säkerhetsstrategin för samhället, Statsrådets principbeslut 16:12.2010
- Lagen om försörjningsberedskap (1390/1992)
- Statsrådets beslut om målen med försörjningsberedskapen, utfärdat i Helsingfors den 5 december 2013

Styrdokument och planer för arbetet med skydd av kritisk infrastruktur inom enskilda sektorer har i sammanhanget inte kunnat identifieras, utöver de allmänna målsättningar som framgår av målen med försörjningsberedskapen.

3.2 Organisation och ledning

Finlands sektorsövergripande arbete med skydd av kritisk infrastruktur kan sägas utgå främst från den finska säkerhetsstrategin och dess målsättning om att samhällets vitala funktioner ska tryggas i alla situationer. Med samhällets vitala funktioner avses tvärsektoriella ”funktionshelheter” som är nödvändiga för samhällhets och som alltid måste vara tryggade. Det finska samhällets vitala funktioner är:

- Ledning av staten
- Internationell verksamhet
- Finlands försvarsförmåga
- Den inre säkerheten
- Ekonomins och infrastrukturens funktionsförmåga
- Befolkningens utkomstskydd och handlingsförmåga
- Mental kristålighet

För varje vital funktion finns ett av Statsrådet (regeringen) fastlagt måltillstånd som fastställer de strategiska uppgifter som varje ministerium fått ansvar för inom ramen för sitt ansvarsområde.

STRATEGISK UPPGIFT	ANSVARS-MINISTERIUM
Den inre säkerheten	
Tryggande av rättsskyddssystemets verksamhetsförmåga	JM
Upprätthållande av den allmänna ordningen och säkerheten	IM
Upprätthållande av räddnings- och sjöräddningsverksamheten	IM
Hantering av översvämningsrisker och dammsäkerhet	JSM
Nödcentralsverksamhet	IM
Avvärjande av olje- och kemikalieolyckor till lands och till havs	MM
Upprätthållande av gränssäkerheten	IM
Hantering av invandring	IM
Hantering av massinvandring	IM
Ekonomins och infrastrukturens funktionsförmåga	
Anskaffning och fördelning av ekonomiska resurser	FM
Finansieringssystemet och penningförsörjningen	FM
Tryggande av försäkringsverksamheten	SHM
Tryggande av bränsleförsörjningen	ANM
Tryggande av kraftförsörjningen	ANM
Säkerställande av de elektroniska informations- och kommunikationssystemens funktioner	KM
Tryggande av statsförvaltningens IT-funktioner och datasäkerhet samt ett gemensamt tjänstesystem för statsförvaltningen	FM
Stöd för uppbyggande och underhåll av varnings- och larmsystem	KM
Tryggande av kontinuerliga transporter	KM
Tryggande av primärproduktionen inom livsmedelsförsörjningen	JSM
Tryggande av vattenförsörjningen	JSM
Tryggande av förädlingen och distributionen av livsmedel	ANM
Tryggande av den vitala industri- och serviceproduktionen	ANM
Tryggande av boende och byggande	MM
Tryggande av tillgången till arbetskraft	ANM
Upprätthållande av utbildnings- och forskningssystemet	UKM
Observation av förändringar i miljön, begränsning av och anpassning till dem	MM
Tryggande av avfallshanteringen	MM

Figur 4. Ansvarsfördelning för kritisk infrastruktur bland Finlands ministerier. (FM= finansministeriet, SHM= social- och hälsovårdsministeriet, ANM= arbets- och näringslivsministeriet, KM= kommunikationsministeriet, MM= miljöministeriet, JSM= Jord- och skogsbruksministeriet UKM= undervisnings- och kulturministeriet).

Varje ministerium har således ansvar för att måltillståndet uppnås och att beredskapen utvecklas gynnsamt inom sitt ansvarsområde. I figuren ovan redovisas de olika ministeriernas ansvarsområde inom funktionen ”ekonomins och infrastrukturens funktionsförmåga”.

Till den sektorsvisa ansvarsfördelningen så tillkommer att Finlands sektors- och nivåöverskridande arbete med skydd av kritisk infrastruktur till stor del, som antytts ovan, utgår från och binds samman genom landets så kallade ”försörjningsberedskap”. Syftet med denna försörjningsberedskap handlar om: ”… tryggande av befolkningens utkomst, landets näringsliv och sådan väsentlig produktion, ser-vice och infrastruktur som är nödvändig för landets försvar i situationer med allvarliga störningar och i undantagsförhållanden”.[10] Målen med försörjningsberedskapen indelas i tryggandet av samhällets kritiska infrastruktur och tryggande av kritisk produktion och service. Statsrådet, regeringen, fastställer målen med försörjningsberedskapen ca vart femte år, de nuvarande målen är från 2013. Kostnaderna för upprätthållande av försörjningsberedskapen täcks centralt från försörjningsberedskapsfonden, som står utanför statsbudgeten och förvaltas av ”Försörjningsberedskapscentralen” (se nedan). Medel till fonden kommer från en särskild försörjningsberedskapsavgift på energi. Intäkterna från avgiften är ca 50 miljoner euro årligen. Fonden har en balansomslutning på 1,2 miljarder euro. Från denna fond finansieras beredskapslager och vissa reservarrangemang som utförs i syfte att trygga den tekniska infrastrukturen.

3.2.1 Statsrådet och ministerier

Statsrådet, dvs. regeringen, lägger fast principbeslut om mål med säkerhetsstrategin för samhället och målen för försörjningsberedskapen. Det sker vanligen en gång under mandatperioden. De viktigaste ministerierna i det här sammanhanget att lyfta fram utgörs av Försvarsministeriet och Arbets- och näringsministeriet. *Försvarsministeriet* ansvarar för samordning av totalförsvaret som inkluderar skyddet av kritisk infrastruktur. I samordningen ingår att samordna den offentliga sektorn, dvs. statsrådets, statens myndigheters och kommunernas, samt den privata sektorns åtgärder och medborgarnas frivilliga verksamhet för att samhällets vitala funktioner ska kunna tryggas i alla situationer. *Säkerhets- och försvarskommittén* bistår försvarsministeriet i ärenden som gäller totalförsvaret och samordningen av det. Kommittén följer och samordnar också åtgärder som hänför sig till totalförsvaret och till tryggandet av samhällets vitala funktioner inom statsförvaltningens olika områden. *Arbets- och näringsministeriet* ansvarar för utvecklandet och samordning av ”försörjningsberedskapen” samt samarbetet mellan myndigheter och näringslivet i detta sammanhang. Till sitt stöd har man myndigheten ”Försörjningsberedskapscentralen” (se nedan). Varje ministerium ansvarar dock för försörjningsberedskapen inom sitt ansvarsområde som tidigare påpekats.

[10] Statsrådets beslut om målen med försörjningsberedskapen. Utfärdat i Helsingfors den 5 december 2013.

3.2.2 Försörjningsberedskapsorganisationen

Försörjningsberedskapen, inklusive skydd av kritisk infrastruktur, bygger på en försörjningsberedskapsorganisation i form av ett nätverk som utvecklar och upprätthåller försörjningsberedskapen i utifrån principen om partnersamarbete mellan den offentliga och den privata sektorn. I försörjningsberedskapsorganisationen arbetar flera hundra företag, myndigheter och organisationer från olika samhällsområden för att uppnå de gemensamma målen. Försörjningsberedskapsorganisationen består av Försörjningsberedskapscentralen, försörjningsberedskapsrådet och de branschvisa försörjningsberedskapssektorerna och poolerna inom näringslivet.

3.2.3 Försörjningsberedskapscentralen

”Försörjningsberedskapscentralen” (FBC) är en institution under arbets- och näringsministeriet och som har i uppgift att planera och operativt genomföra upprätthållandet och utvecklingen av landets beredskap, inklusive skydd av kritisk infrastruktur. Försörjningsberedskapscentralens mer specifika uppgifter är främst att:

- *Utveckla samarbetet mellan den offentliga förvaltningen och näringslivet i frågor som gäller försörjningsberedskapen*

Samarbetet mellan näringslivet och den offentliga förvaltningen ses som vara av avgörande betydelse när det gäller att trygga den finska försörjningsberedskapen. Försörjningsberedskapscentralen stöder detta samarbete bl.a. genom att utveckla redskap för kontinuitetshantering i företagen och ge företagen utbildning i användningen av dessa redskap, samt genom att genomföra gemensamma övningar för företagen och myndigheten och stöda och styra de branschvisa sektorerna och poolernas verksamhet. Försörjningsberedskapscentralen erbjuder företagen stöd i sitt arbete med kontinuitetshantering genom olika verktyg. Hit hör bland annat webbportalen HUOVI och projektet SOPIVA.

- *Säkerställa funktionen hos tekniska system, dvs. kritisk infrastruktur, som är livsviktiga med tanke på försörjningsberedskapen*

Försörjningsberedskapscentralens uppgift är att i samarbete med andra myndigheterna och näringslivet säkerställa att de mest kritiska systemen för samhället fungerar i alla situationer. Därför planerar och finansierar Försörjningsberedskapscentralen bl.a. olika säkerhets- och reservarrangemang för datasystem, datakommunikation, finansbranschen och masskommunikation.

- *Trygga kritisk varu- och tjänsteproduktion samt sådan produktion som stöder det militära försvaret*

Försörjningsberedskapscentralen stöder med tekniska och finansieringsmässiga arrangemang förutsättningarna för varu- och tjänsteproduktion som behövs vid undantagsförhållanden samt produktion som stöder det militära landsförsvaret. Inom detta område samarbetar Försörjningsberedskapscentralen med Försvarsmakten.

- *Sköta den obligatoriska upplagringen och skyddsupplagringen*

Syftet med ”obligatoriska upplag” är att trygga landets försörjningsberedskap vid allvarliga störningar i tillgången på importerade bränslen eller läkemedel. Målet med ”skyddsupplag” är att trygga befolkningens försörjning och företagens produktionsverksamhet vid störningar i tillgången på nödvändiga råvaror och material. Försörjningsberedskapscentralens uppgift är att sörja för de praktiska åtgärderna i anslutning till upprätthållandet av dessa upplag.

- *Upprätthållandet av material i statliga säkerhetsupplag*

Staten lagrar material i beredskapslager, så kallade ”säkerhetsupplag” för att trygga befolkningens försörjning och näringslivets verksamhet vid svåra kriser. Genom säkerhetsupplagen tryggas produktion som stöder energiförsörjningen, livsmedelshushållningen, hälso- och sjukvården samt landsförsvaret. Försörjningsberedskapscentralens uppgift är att upprätthålla de material som ska lagras

Försörjningsberedskapscentralen har ca ett fyrtio antal anställd och är uppdelade på, verkställande direktör, administrationsavdelning, infrastrukturavdelning, bastproduktionsavdelning, energiförsörjningsavdelning samt försörjningsberedskapssekretariatet. Med andra ord en mycket liten organisation personellt sett.

3.2.4 Försörjningsberedskapsrådet

Försörjningsberedskapsrådet, som är tillsatt av regeringen, upprätthåller och utvecklar kontakter med centrala nätverk inom myndighetsfären och inom näringslivet, bevakar försörjningsberedskapens tillstånd och kommer med förslag till eventuella åtgärder.

3.2.5 Näringslivets sektorer och pooler inom försörjningsberedskapen

Näringslivet med dess olika industrier och företag utgör basen för försörjningsberedskapen. Företagen deltar i försörjningsberedskapsorganisationen via ”sektorer” och ”pooler”. Ett stort antal branschspecifika samarbetsorganisationer, så kallade ”sektorer”, existerar idag för olika prioritetsområden inom försörjningsberedskapen. Olika myndigheter och organisationer och de främsta företagen i branschen deltar i samarbetet inom en sektor. Sektorernas övergripande uppgift är att styra, samordna och följa upp beredskapsåtgärderna inom respektive bransch och att fastställa målen för de så kallade poolerna inom sektorn. Poolerna svarar för den operativa beredskapen i egenskap av organ som fungerar under näringslivets ledning. Deras uppgift är att tillsammans med företagen i branschen följa upp, utreda, planera och förbereda åtgärder i syfte att utveckla försörjningsberedskapen i branschen och att definiera de företag i branschen som är kritiska för försörjningsberedskapen.

3.2.6 Regional och lokal nivån

Regional nivån – Regionförvaltningen
På den regionala nivån ligger på myndighetsnivå ansvaret för skyddet av kritisk infrastruktur på regionförvaltningen. ”Statens regionförvaltning” (RFV) förnyades i början av år 2010, varvid det tidigare förvaltningssystemet som grundade sig på länsindelningen ersattes med regionförvaltningsverk (RFV) samt närings-, trafik- och miljöcentraler (NTM). Regionförvaltningsverken har till uppgift att samordna aktörernas beredskap i sin region, ordna utbildning och beredskapsövningar och stöda kommunernas beredskapsplanering. Under verkens ledning har det grundats regionala beredskapskommissioner, i vilka de instanser som svarar för säkerheten i regionen – till exempel räddningstjänsten, polisen och frivilligorganisationerna – samordnar sitt beredskapsarbete. Närings-, trafik- och miljöcentralerna svarar för den beredskap och krisledning som anknyter till deras uppgifter. Eftersom regionförvaltningssystemet ännu är ganska nytt, utvecklas dess beredskapsuppgifter fortsättningsvis. Det heter i den finska säkerhetsstrategin för samhället att ”…RFV:s och NTM-centralernas beredskapsuppgifter kräver ännu precisering och utveckling.” För Ålands del har landskapsregeringen ansvar för krisberedskapen inom sitt ansvarsområde.

3.2.7 Lokal nivå – Kommunerna

Kommunens verksamhet i krissituationer baserar sig på en lagstadgad beredskapsplanering. De sektorer som svarar för kommunens tjänster, t.ex. undervisningsväsendet, tekniska väsendet och socialväsendet, utarbetar var och en sina egna planer för händelse av kriser. Planerna sammanställs till en gemensam beredskaps- eller räddningsplan för kommunen. Vid behov deltar kommunerna också i räddningsverksamheten tillsammans med de regionala räddningstjänsterna. När det sker en olycka sörjer kommunen för att olycksoffren får psykosocialt stöd. Beredskapsarbetet leds av kommundirektören tillsammans med kommunstyrelsen. Kommunen får stöd för sin beredskapsplanering av de regionala räddningsverken och statens regionförvaltning. Försörjningsberedskapscentralen ger också stöd i form av stödhandledningar som t.ex. ”Anvisning till kommunerna om beredskap och kontinuitetsplanering inom försörjning av dagligvaror”. Ofta deltar också frivilligorganisationerna i kommunernas beredskapsplanering och de kompletterar myndigheternas verksamhet i en krissituation. Sammantaget liknar arbetet med krisberedskap, inklusive arbetet med skydd av kritisk infrastruktur, i Finland i mycket det som sker i Sverige med risk- och sårbarhetsanalyser och krisberedskapsplaner.

Underlag

Säkerhetsstrategi för samhället. Statsrådets principbeslut 16.12.2010:
www.yhteiskunnanturvallisuus.fi/sv/.../23-sakerhetsstrategi-for-samhallet

Samhällets säkerhet, hemsida: http://yhteiskunnanturvallisuus.fi/index.php

Försvarsministeriet, hemsida: http://www.defmin.fi/svenska

Arbets- och näringsministeriet, hemsida:
https://www.tem.fi/index.phtml?109339_m=108856&l=sv&s=5236

Försörjningsberedskapscentralen, hemsida:
http://www.se.nesa.fi/forsorjningsberedskap/

Finlex (rättsdatabas): http://www.finlex.fi/sv/laki/ajantasa/2008/20080539

Statsrådets beslut om målen med försörjningsberedskapen (2013), hemsida:
http://www.tem.fi/files/38232/Statsradets_beslut_om_malen_med_forsorjningsberedskapen_051213.pdf

Anvisning till kommunerna om beredskap och kontinuitetsplanering inom försörjningen av dagligvaror. Försörjningsberedskapscentralen, 2013:
www.huoltovarmuus.fi/static/pdf/613.pdf

4 Polen

4.1 Definition, mål och sektorsindelning

Med kritisk infrastruktur avser Polen system eller ömsesidigt sammanbundna objekt därinom, inklusive byggnader, anläggningar, installationer och tjänster med central betydelse för statsens säkerhet och dess medborgare samt är av betydelse för funktionaliteten för administrativa myndigheter, institutioner och företag. Med skydd av kritisk infrastruktur avser Polen alla åtgärder som vidtas för att säkerställa funktionalitet, kontinuitet och integritet av kritisk infrastruktur i avsikt att förebygga hot, risker, sårbarheter och begränsningar samt att neutralisera deras effekter. Vidare avses förmågan till snabb återställande av infrastruktur i fall av störningar, attentat och andra händelser som avbryter dess normala funktionalitet. Polen delar upp sin kritiska infrastruktur i följande sektorer eller områden/system (Polen använder inte begreppet sektor):

- Energi-, bränsle- och energiförsörjningssystem
- Kommunikationssystem
- Tele-informationsnätverkssystem (Tele-information network systems)
- Finansiella system
- Livsmedelsförsörjningssystem
- Dricksvattenförsörjningssystem
- Hälso- och sjukvårdssystem
- Transportsystem
- Räddningstjänstsystem (Rescue systems)
- System för upprätthållande av administrativa tjänster

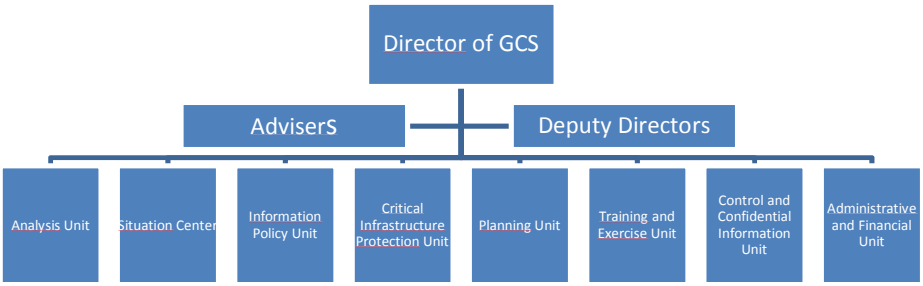
- System för produktion, förvaring och bruk av kemiska och radioaktiva substanser, inklusive pipelines för farliga ämnen

Enligt Polens nationella program för skydd av kritisk infrastruktur är målet med det aktuella arbetet att skapa förhållanden som stärker säkerheten för den kritiska infrastrukturen, särskilt med avseende på att:

- Förhindra störningar i kritisk infrastruktur
- Vidta förberedelser för kriser som negativt kan påverka kritisk infrastruktur
- Kunna hantera händelser som leder till störningar eller ödeläggelse av kritisk infrastruktur
- Återbygga ödelagd kritisk infrastruktur

4.2 Organisering och styrning

Det yttersta ansvaret på nationell nivå för Polens arbete med skydd av kritisk infrastruktur villar på ”Ministerådet” (dvs. regeringen) och dess departement. Ministerrådet antar Polens nationella program för skydd av kritisk infrastruktur (National Critical Infrastructure Protection Program) som lägger fast landets arbete och ansvarsfördelning inom det aktuella området. Men det är dock det departementsövergripande organet ”Government Centre for Security” (RCB) som är det centrala organet på området på den nationella nivån. RCB motsvarar grovt MSB och SBKH i Sverige. RCB har varit verksamt som nationellt krisberedskapsorgan med ansvar för kritisk infrastruktur sedan 2008.



Figur 5. Organisationsskiss för Polens Government Centre for Security (RCB)

RCB är ett stabsorgan åt premiärministern och regeringen och koordinerar krisberedskapsarbetet inom polska regeringskansliet. RCB inriktar, styr, koordinerar, stödjer och samverkar med myndigheter på lägre nivåer och med näringslivet när det gäller krisberedskap i stort, inklusive skydd av kritisk infrastruktur. RCB sammanställer nationella risk och förmågebedömningar med underlag från lägre nivåer samt svara för utveckling och verkställighet av det nationella program för skydd av kritisk infrastruktur De nivåer under den nationella nivån och RCB som har särskilt ansvar för arbetet med skydd av kritisk infrastruktur utgörs av: 1) Provinsnivå, 2) Distriktnivå och 3) Kommunnivå. De olika politiska organen på dessa nivåer har det aktuella ansvaret härvid.

4.3 Doktrin och styrmedel

Centrala doktrinelement i Polens arbete med skydd av kritisk infrastruktur är framförallt en ansvarsprincip till delar likt den svenska , en ”all-hazard”-ansats, arbete i hela krisberedskapscykeln (före-under-efter), bruk av risk- och sårbarhetsanalyser, bruk av kontinutietshantering och fokus på resiliens. Polen särskiljer sig genom att ha mycket kraftfulla styrmedel i form av olika lagar och förordningar som riktar sig både mot myndigheter och ägare och operatörer av kritisk infrastruktur. Dessa ska beskrivas ingående nedan.

Polens arbete med krisberedskap och skydd av kritisk infrastruktur är tydligt reglerat genom ”Act of 26 April 2007 on Crisis Management”. Ansvariga organ på nämnda nivåer ska enligt lagen upprätta en krisberedskapsplan som ska uppdateras vartannat år. Planen ska bland annat inbegripa en beskrivning av hot och risker, sannolikheten för att dessa ska inträffa, inklusive de hot och risker som är riktad mot kritisk infrastruktur. Till planen ska det finnas bilagor av operativ karaktär som specificerar hur olika krishanteringesuppgifter ska verkställas, inklusive de som är relaterade till skydd av kritisk infrastruktur. I bilagorna ska det också finnas en lista över den kritiska infrastruktur (anläggningar etc.), som finns inom det aktuella geografiska ansvarsområdet, och som inbegrips i krisberedskapsplanen.

När det gäller civilt försvar har varje nivå ansvar för att: ”…working out the solutions in the event of destruction or disruption of critical infrastructur” (artikel 4)[11]. För nivåerna under den nationella nivån fastslåss det i lagen att respektive ansvarigt organ på sin nivå har ansvar för …”organization and performance of the critical infrastructure protection tasks[12]” som är att härleda från det nationella programmet. För provinsnvån anges det också att den har ansvar för att insamla och bearbeta information om kritisk infrastruktur inom sitt geografiska ansvarsområde. När det gäller terrorhot mot kritisk infrastruktur fastslår lagen att alla ansvariga myndigheter samt ägare och operatörer av kritisk infrastruktur har ansvar för att informera RCB om dessa hot: ”…including the threats to the funktioning of energy, water and sewer as well as heating, telecommunication systems and networks of key importance to

[11] ACT of 26 April 2007 on Crisis Management, artikel 4.

[12] ACT of 26 April 2007 on Crisis Management, se t.ex. artikel 14.

the national security." (artikel 12a)[13]. RCB har befogenhet att utfärda särskilda rekommendationer till berörda myndigheter i samband med hot mot och vid attentat mot kritisk infrastruktur.

Krisberedskaplagen fastslår att ett nationellt handlingsprogram för skydd av kritisk infrastruktur (National Critical Infrastruckture Protection Programme) ska upprättas och revideras vartannat år. Programmet ska utabetas av RCB i nära samarbete med ansvariga ministrar och myndighetschefer ifråga om kritisk infrastruktursystem (se ovan). Syftet och målet med programmet är som tidigare nämnts att:

- Förhindra störningar i kritisk infrastruktur
- Vidta förberedelser för kriser som negativt kan påverka kritisk infrastruktur
- Kunna hantera händelser som leder till störningar eller ödeläggelse av kritisk infrastruktur
- Återbygga ödelagd kritisk infrastruktur

Enligt lagen ska programmet specificera:

- Nationella prioriteringar, mål, krav och standarder för att säkerställa att den kritiska infrastrukturen fungerar smidigt.
- Fastställa vilka ministrar och myndighetschefer som har ansvar för ett specifikt kritiskt infrastruktursystem.
- Lägga fast detaljerade kriterier som möjliggör identifiering av objekt, installationer, anläggningar och tjänster som ingår i kritisk infrastruktursystem, härvid beakta dess betydelse för statens funktionalitet och ta tillvara medborgarnas behov.

Det är RCB i samarbete med berörda ministrar och myndighetschefer, som utifrån ett antal specifika kriterier [inte tillgängliga för denna kartläggning då de är hemliga], ska sammanställa en nationell lista på objekt, installationer, anläggningar och tjänster som ska räknas som kritisk infrastruktur uppdelat på olika system (sektorer) (se ovan). I denna lista ingår också sådan infrastruktur som ska räknas som europeisk kritisk infrastruktur i förhållande till samarbetet inom EU, inklusive kritisk infrastruktur i andra medlemsstater som har betydelse för polskt vidkommande [arbetet med europeisk kritisk infrastruktur behandlas inte i denna kartläggning].

Listan över nationell kritisk infrastruktur ska vara hemligstämplad. RCB ska efter sammanställan av listan över kritisk infrastruktur informera ägare och operatörer samt ministrar och myndighetschefer som berörs av listan. Ägare och operatörer av kritisk infrastruktur ska senast 30 dagar efter att ha blivit informerade utse en kontaktperson för arbetet med skydd av kritisk infrastruktur. Enligt krisberedskapslagen är ägare och operatörer skyldiga att "...protect them, particulary through the preparation and implementation, according to the anticpated threat, of critical infrastructure protection plans

[13] ACT of 26 April 2007 on Crisis Management, artikel 12a.

and holding their own reserve systems ensuring security and maintaining the functioning of the infrastructure until it is fully recovered." (artikel 6)[14].

Förordningen "*541 Regulation of the Council of Ministers of 30 April 2010 on Critical Infrastructure Protection Plans*" lägger fast hur berörda ministerier och myndigheter ska verkställa arbetet med det nationella programmet för skydd av kritisk infrastruktur i samverkan med (privata) ägare och operatörer av kritisk infrastruktur (instatllationer, anläggningar etc.). De kriterier som ska ligga till grund för urval av kritisk infrastruktur ska som framkommit ovan tas fram och uppdateras av RCB för att sen förmedlas till berörda ministrar och myndighetschefer ("Ministers and Head of central Officies"). Senast sex veckor efter berörda ministrar och myndighetschefer mottagit dessa kriterier ska dessa till RCB inkomma med förslag om vilken infrastruktur inom deras ansvarsområde (sektor) som bör föras upp på en lista över kritisk infrastruktur. RCB ska i sin tur senast sex veckor efter att mottagit förslagen sammanställa en lista över samtlig nationell kritisk infrastruktur innefattande:

- Namn och plats för den kritiska infrastrukturen
- Inom vilken minister och myndighets ansvarsområden den kritiska infrastrukturen faller
- Uppgifter om den driftansvariga för den kritiska infrastrukturen och dess ansvarige chef

Berörda ministrar och myndighetschefer ska senast sex månader efter att de mottagit listan på nämnda kriterier sammanställa och delge RCB information innefattande:

- Deras ansvarsområde inklusive resurser, subsystem, funktion och ömesidigt beroende mellan kritisk infrastruktur inom deras ansvarsområde
- Bedömningar av vilka förutsättningar som måste föreligga för att den kritiska infrastrukturen ska fungera
- Risk- och sårbarhetsanalyser för infrastrukturen inom deras ansvarsområde, inklusive indentifierade hot och sårbarheter och konsekvenserna av störningar i infrastrukturen
- Bedömningar och förslag på prioriteringar vid återuppbyggnad av skadad infrastruktur
- Möjliga sätt att förhindra störningar inom verksamhetsområdet tillföljd av störningar i kritisk infrastruktur
- Förslag till forskning och utvecklingsprogram med syfte att stärka skyddet av den kritiska infrastrukturen

Utifrån inkommit underlag från ministrar och myndighetschefer ansvarar RCB för att utveckla ett utkast till ett nationellt program för skydd av kritisk infrastruktur, som sen ska gå ut på remiss till berörda parter. En månad efter avslutad remiss ska RCB förelägga utkast till ett program, inklusive redogörelser för vilka avvikande uppfattningar som framkommit rörande programmet.

---

[14] ACT of 26 April 2007 on Crisis Management, artikel 6.

Samverkan mellan berörda ministerier och myndigheter för verkställighet av programmet ska ske genom konferenser, seminarier, diskussionsforum, övningar och träning samt informationsutbyte rörande:

- Identifiering av åtgärdsområden för stärkande av skyddet av kritisk infrastruktur
- Hot mot kritisk infrastruktur
- Förväntade eller observerade ökning av efterfrågan av tjänster eller produkter som tillgodoses av kritisk infrastruktur
- Förväntade avbrott eller störningar i tjänster och produkter som tillgodoses av kritisk infrastruktur
- Stöd som operatörer av kritisk infrastruktur behöver när de vidtar åtgärder för att avhjälpa problem i form av störningar och ödelägges av kritisk infrastruktur
- Skydd av kritisk infrastruktur, inklusive det inre organisatoriska arbetet med skydd och krisberedskap
- Utarbetande och uppdatering av programmet för skydd av kritisk infrastruktur

Programmet för skydd av kritisk infrastruktur ska uppdateras vid behov på eget initiativ av RCB eller på välgrundad begäran av deltagare i programmet. Sex veckor efter regeringens godkännande av ett uppdaterat program ska RCB sammanställa en ny sammanfattande lista (abstrct) av kritisk infrastruktur och förmedla denna till berörda ministerier, myndigheter och provinsregeringar. Ansvariga för driften av berörd infrastruktur (anläggningar, installationer etc.) ska också skriftligen informeras att deras infrastruktur är upptagen på den nya listan.

Utan att det sker en uppdatering av hela programmet kan en uppdatering ske av listan över identifierad kritisk infrastruktur. En sådan uppdatering kan ske på eget iniativ av RCB eller på begäran av enskilt ministerium eller myndighet med utpekat ansvar för ett system av kritisk infrastruktur (sektor), provinsregering eller ansvarig för drift av kritisk infrastruktur. Senast trettio dagar efter en uppdatering av listan ska RCB ha tagit fram en sammanfattande lista (abstract) över befintlig nationell kritiska infrastruktur.

Förordningen “542 Regulation of the Council Ministers of 30 April 2010 on National Critical Infrastructure Protection Programme” fastslår hur planer för skydd av kritisk infrastrukur ska upprättas, struktureras och uppdateras av ägare och operatörer av kritisk infrastruktur och hur de ska fullgöra sina skyldigheter enligt nämnda planer. Planen ska upprättas både elektronisk form och i pappersform och vara upprättad senast nio månader efter att de fått besked av RCB av den aktuella infrastrukturen finns upptagen på listan över identifierad kritisk infrastruktur. Planen ska uppdateras efter behov eller minst vartannat år.

Planen ska omfatta tre delar. Den första delen ska innehålla information om bland annat namnet på infrastrukturen, utdrag ur ett antal företags- och

skatteregister, personuppgifter om ansvarig chef m.m. Den andra delen ska innehålla information om själva den kritiska infrastrukturen:

- Beskrivning av och grundläggande teknisk parameterar rörande objektet
- En karta med inritade anläggningar, installationer etc.
- Verksamhetsmässig sammanlänkning med andra anläggningar, installationer m.m.

Den tredje delen ska innehålla information om ytteligare olika egenskaper om den kritiska infrastrukturen:

- Hot riktade mot infrastrukturen och sannolikheten för att de ska realiseras samt scenario för händelseutvecklingen härvid
- Ömsesidigt beroende mellan infrastrukturen och annan kritisk infrastruktur och hur störningar kan spridas mellan dessa
- Tillgång till egna resurser för att hantera skydda den kritiska infrastrukturen
- Förmågor och resurser som kan ställas till myndigheternas förfogande för att skydda den kritiska infrastrukturen

Den fjärde delen ska innehålla information om resiliens:

- Säkerställande av drift av kritisk infrastruktur vid olyckor och kriser
- Återuppbyggande av ödelagd kritisk infrastruktur

Den femte delen ska innehålla information om samverkan med myndigheter:

- Krishanteringscentra
- Förvaltningsmyndigheter

Planen ska för godkännande underställas ansvarigt ministerium eller central myndighet samt följande officiella geografiskt berörda befattningshavare/myndighetsfunktioner:

- Provinsregeringen/länsstyrelsen/landsthövdingen (Voivode)
- Regionala byggnadsinspektören (Provinsial Inspector of Building Control)
- Länsveterinären (Provinsal Vetrinarian)
- Länspolischefen (Provincial Commandant of the Police)
- Chefen för regional statlig räddningstjänst (Provincial Commandant of the State Fire Service)
- Regionala hälsoskyddsinspektören (State Provincial Sanitary Inspector)
- Chefen för Sjöfartsverket (Director of Maritime Office)

Berörda befattningshavare/myndighetsfunktioner ska godkänna eller förkasta planen senast fjortondagar efter den underställts dem. För berörda ministerier och centrala myndigheter är tiden satt till fyrtiofem dagar. Förkastande av hela eller delar ska understödjas av skriftliga förklaringar om vad som mer exakt inte får godkänt. Förkastande av en plan kan ske ifall den:

- Presenterar lösningar som inte säkerställer skyddet av den kritiska infrastrukturen
- Brister i överensstämmelse med det nationella programmet för skydd av kritisk infrastruktur
- Planen inte lever upp till bestämmelser rörande formalia och beskrivning av infrastrukturen (anläggning etc.) , hotbild, resurser m.m. (se ovan)

Ägaren eller operatören till infrastrukturen ska senast fjorton dagar efter alla berörda myndigheter enligt ovan givit sitt godkännande inkomma med planen till RCB. Om planen inte blir godkänd av alla behöriga instanser så skall planen inkomma till RCB med de anmärkningar som framförts. RCB har då att ta ställning till om planen ska godkännas trots anmärkningarna. RCB ska fatta beslut om inkomna planer senast nittio dagar efter att de inkommit. Om ägaren eller operatören till kritisk infrastruktur under annan lagstiftning tagit fram en plan som motsvarar de krav som ställs i den här aktuella planen så kan RCB efter bedömning godkänna den som en motsvarande giltig plan.

Underlag

RCB, Government Centre for Security, hemsida: http://rcb.gov.pl/eng/

National Critical Infrastructure Protection Programme, (http://rcb.gov.pl/eng/?page_id=249)

ACT of 26 April 2007 on Crisis Management: http://rcb.gov.pl/eng/wp-content/uploads/2011/03/ACT-on-Crisis-Management-final-version-31-12-2010.pdf

541, Regulation of the Council of Ministers of 30 April 2010 on National Critical Infrastructure Protection Programme. (http://rcb.gov.pl/eng/wp-content/uploads/2011/03/REGULATION-on-NATIONAL-CRITICAL-INFRASTRUCTURE-PROTECTION-PROGRAMME-AB.pdf)

542, Regulation of the Council of Ministers of 30 April 2010 on Critical Infrastructure Protection Plans. (http://rcb.gov.pl/eng/wp-content/uploads/2011/03/REGULATION-ON-CIP-PLANS.pdf)

471, REGULATION of the Prime Minister of 11 April 2011 on the organisation and operating mode of the Government Centre for Security. (http://rcb.gov.pl/wp-content/uploads/Regulation-on-the-organisation-and-operating-mode-of-the-Government-Centre-for-Security-pdf.pdf)

Power Point presentation: *Polish Critical Infrastructure Protection System*. Thomas Szewczyk & Maciej Pyznar, RCB.

Jacek DWORZECKI. *CRISIS MANAGEMENT SYSTEM IN POLAND,* i The Science For Population Protection 2/2012 (http://www.population-protection.eu/prilohy/casopis/eng/11/52.pdf)

5 Storbritannien

5.1 Definition och sektorsindelning

Nationell infrastruktur omfattar enligt officiellt brittiskt synsätt nätverk, system, anläggningar, platser och affärsverksamhet som är nödvändiga för landets funktionalitet och för leverans av nödvändiga varor och tjänster som vardagslivet i landet är beroende av. Storbritannien delar in den nationella kritiska infrastrukturen i elva sektorer och fjorton subsektorer (se tabell).

Sektor	**Subsektor**	**”Sector Resilience Lead (Sektorsanvar)**
Communications	-Broadcast -Postal -Telecoms	-Department for Culture, Media and Sport -Department for Business, Innovation and Skills -Department for Business, Innovation and Skills
Emergency Services	-Ambulance -Coastguard - Fire & Rescue -Police	-Department of Health -Department of Transport -Department for Communities and Local Government -Home Office
Energy	-Electricity	-Department of Energy and Climat Change

	-Gas - Oil	-Department of Energy and Climat Change -Department of Energy and Climat Change
Finance		HM Treasury
Food		Department for Environment, Food and Rural Affairs
Government		Cabinet Office
Hazardous Sites		Department for Business, Innovation and Skills
Health		Department of Health
Nuclear		Department of Energy and Climat Change
Transport	-Aviation -Ports -Rail -Raod	-Department for Transportation -Department for Transportation -Department for Transportation -Department for Transportation
Water		Department for Environment, Food and Rural Affairs

Tabell 1. Ansvarsfördelning för kritisk infrastruktur/resiliens i brittiska Cabinet Office.

5.2 Organisering och ledning

5.2.1 Departement

Regeringen har det yttersta ansvaret på nationell nivå för arbetet med skydd av kritisk infrastruktur. I regeringen finns således en särskild ”Permanent Secretary for Intelligence, Security and Resilience”. ”Cabinet Office” (Regeringskansliet) har ansvaret för sektorsövergripande frågor vad rör arbetet med skydd av nationell kritisk infrastruktur/resiliens. 18 stycken fackdepartement samt Cabinet Office, ”Home Office” och ”HM Treasury” har ett utpekat sektorsansvar för arbetet med skydd av kritisk infrastruktur. I detta ansvar ingår att i samverkan med ägare och operatörer identifiera åtgärdsbehov, följa upp åtgärder, ansvara för eventuell lagreglering och statlig finansiering. Departementen och övriga nämnda har inte minst ansvar för att årligen redovisa resiliensplaner för sina sektorer och den kritiska infrastruktur som ingår i sektorn, att göra ansvariga ministrar uppmärksamma på identifierade sårbarheter i förhållande

till de risker och hot som identifieras i Storbritanniens nationella risk- och sårbarhetsanalys (”Nationell Risk Assesment”). Departementen har också ansvar för att ta fram handlingsplaner för hur man ska förbättra robustheten i sektorns infrastruktur när så behövs. De individuella sektorsplanerna är hemligstämplade, men årligen gör Cabinet Office en mer generell och övergripande sammanställning av sektorsplanerna som är offentligt tillgänglig. De första sektorsplanerna togs fram (se nedan) 2010. Fokus för sektorsplanerna har varierat lite de få år som arbetet med sektorsvisa planer pågått:

- 2010 fokuserade sektorsplanerna på hur robusta kritisk nationell infrastruktur var när det gällde att hantera översvämningar.
- 2011 vidgades fokus till att även inkludera andra naturolyckor och något mindre kritisk nationell infrastruktur.
- 2012 var fokus på robustheten i sektorns mest kritiska infrastruktur när det gällde alla typer av risker och hot (”hazards and threats”). Här vidgas fokus även till antagonistiska hot.
- 2013 var fokus detsamma som under 2012. Nytt för 2013 var att även planer togs fram för sektorena ”Nuclear” och ”Hazardous sites”, vilket inte gjorts 2012 [oklart varför!]

Departmentet ”Department Communities & Local Government” har ett särskilt ansvar för arbetet på den lokala nivån med resiliens och infrastruktur. Regering och departement samverkar med berörda självstyrande organ i Wales, Skottland och Nordirland. Departementen understöds av berörda underlydande myndigheter.

5.2.2 CCS och CPINI

”Civil Contingencies Secretariat” (CCS) respektive ”Centre for the Protection of National Infrastructure” (CPNI) kan sägas vara de två mest centrala organen i Storbritannien på nationell nivå när det gäller ansvar för arbetet med skydd av nationell kritisk infrastruktur, utöver de sektorsansvariga fackdepartementen som nyss nämnts. CCS är en enhet inom ”National Security Secretariat” (NSS) i Cabinet Office. CCS med huvudansvar för risker och hot av icke-antagonistisk karaktär och ett mer (men något oklart) allmänt ansvar för arbetet med skydd av kritisk infrastruktur som även innefattar antagonistiska hot (dvs. primärt terrorism). CPNI, som lyder under säkerhetsunderrättelstjänsten MI5, har det främsta ansvaret när det gäller säkerhet och skydd för kritisk infrastruktur mot antagonistiska hot.

Insynen i CPNI:s arbete är begränsat genom att centrat inte lyder under ”Freedom of Information Act”, dvs. CPINI:s arbete med att skydda kritiskt infrastruktur mot terrordåd är till största del hemligt. Fokus kommer nedan därför att ligga på CCS och krisberedskapsspåret i beskrivningen nedan. Internationellt samarbete i de aktuella frågorna behandlas heller inte nedan. Genom uppdelning av huvudansvar mellan CCS och CPNI har arbetet med skydd av kritisk infrastruktur härigenom två olika huvudfåror (krisberedskap och terrorismbekämpning) som förts samman och som skapar en hel del oklarheter för en ut-

omstående betraktar när det gäller ansvarsfördelningen och samverkan mellan dessa organ.

Centre for the Protection of National Infrastructure (CPNI
CPNI bildades 2007 genom en sammanslagning av ”National Infrastructure Security Co-ordination Centre” (NISCC) och ”National Security Advice Centre” (NSAC). NISCC:s främsta uppgift var att ge råd till ägare och operatörer av kritisk infrastruktur och NSCA:s främsta uppgift, som en enhet inom MI5, var att ge råd till regeringen och ansvariga departement i Cabinet Office. CPNI lyder under “Director General of the Security Service”, (MI5). CPNI:s huvuduppgift är att ge råd (“protective security advice”) till företag, myndigheter och organisationer med ansvar för kritisk infrastruktur för att minska sårbarheten för och verkningarna av terrorhot och andra antagonistiska hot. CPNI ger råd inom främst områdena cybersäkerhet, skalskydd och personlig säkerhet.

CPNI samverkar med ett stort antal aktörer. Inom den offentliga sfären är det departement med sektorsansvar för kritisk infrastruktur, ”Civil Contincencies Secretariat” (CCS), “Office of Cyber Security & Information Assurance” (OCSIA), “Cyber Security Operations Centre” (CSOC), “The Communications-Electronics Security Group” (CESG), “National Counter Terrorism Security Office” (NaCTSO) och “Counter Terrorism Security Advicers” (CTSAs). Inom den privata sfären samarbetar man med ett stort antal företag och branschorgan.

CPNI arbetar med särskilda ”Trusted Partners” som måste möta särskilda krav som CPNI har ställt upp. Det rör sig här främst om olika säkerhetsföretag eller teknikföretag som har att skydda eller serva anläggningar (etc.) som utgör kritisk infrastruktur. CPNI arbetar också med flera olika branschorgan för att utveckla olika formar av professionella standarder. Ett exempel i sammanhanget är upprättandet av ”Register of Security Enigineers and Specialists” (RSES) som stöds av CPNI men som administreras av ”The Institution of Civil Engineers”.

5.2.3 CCS

”The Civil Contingencies Secretariat” (CCS) bildades 2001 och är placerat i Cabinet Office för att stödja regeringen och Cabinet Office och för att ansvara för krisberedskapsfrågor ur ett resiliensperspektiv, med avseende på att förutsäga, bedöma, förhindra, förbereda, hantera och återställa. CCS ansvar för ”The National Risk Assesment ” (nationell RSA) och ”The National Risk Register”. CCS leder ett sektorsöverskridande handlingsprogram för att förbättra samhällets förmåga att hantera kriser, leder arbete med kontinuetsplanering samt Storbritanniens resiliensprogram för kritisk infrastruktur (The Critical Infrastructure Resilience Programme, se nedan).

5.3 Den lokala nivån

På lokal nivå har kommuner (motsvarande) ett mer allmänt ansvar för samhällelig resiliens, som inkluderar lokal kritisk infrastruktur, enligt ”The Civil Con-

tingencies Act 2004". Britiska regeringen och nationella myndigheter uppmuntrar och stödjer i sammanhanget lokalsamhällen (kommuner, byar och andra lokala frivilligorganisationer) att aktivt arbete med att stärka sin robusthet mot olika former av störningar, inte minst då sådan som kan drabba kritisk infrastruktur. Ett särskilt program för resiliens på lokalsamhällesnivå introducerades 2008. Härvid har ett antal metodmässiga resurser och verktyg utvecklats och som är tillgängliga via internet. Inte minst arbetar man från nationell nivå med att sprida "best practice" mellan lokalsamhällena genom att sammanställa dessa nationellt och göra dem tillgängliga via nätet. Särkskilda mallar och riktlinjer har tagit fram för hur lokalsamhällen på ett enhetligt sätt ska inrapportera fall (case) av hur de arbetar med lokal robusthet.

5.4 Utvecklingen av arbete med robusthet i kritisk infrastruktur på sektorsövergripande nationell nivå

Beskrivningen som följer är fokuserad på "The Civil Contingencies Secretariat" (CCS) krisberedskapsorienterade arbete och inte på antiterrorarbetet, som det flaggats för ovan. Mot bakgrund av de svåra översvämningar som Storbritannien drabbades av 2007 tillsattes en utredning. Utredningen konstaterade brister i regeringens arbete med att förhindra störningar i kritisk infrastruktur orsakade av hot och risker i naturmiljön (Natural hazards), dvs. av icke-antagonistisk karaktär. En av utredningens slutsatser var:

...that the Government should establish a systematic, coordinated, cross-sector campaign to reduce the disruption caused by natural events to critical infrastructure and essential services.[15]

Som ett svar på utredningen utarbetade regeringen ett strategiskt ramverk för arbetet med att öka robustheten i kritiska infrastruktur ("Strategic Framwork and Policy Statement on Improving the Resilicence of Critical Infrastructure to Disruption from Natursal Hazards"). Ramverket som offentliggjordes våren 2010 fastställde en färdplan framåt för arbetet, den idé- och policymässiga grund som arbetet ska villa på, en sammanställning av de första sektorsvisa planer för resiliens för översvämningar som tagits fram samt temporära riktlinjer för icke-avreglerade samhällssektorer ("Economic Regulated Sectors"). De sektorsvisa planerna var resultatet av det arbete som föregått mellan utredningen 2007 och offentliggörandet av det strategiska ramverket. Det strategiska ramverket lades fast 2011, efter en remissrunda, som ett nationellt program för infrastrukturresiliens *("The Infrastructure Resilience Programme").*

Syftet med programmet är att främja offentliga och privata (ägare och driftansvariga för anläggningar, myndigheter, blåljusmyndigheter m.fl.) aktörers enskilda och gemensamma arbete med att stärka robustheten i landets infrastruk-

[15] Strategic Framework and Policy Statement on Improving the Resilience of Critical Infrastructure to Disruption from Natural Hazards, (March 2010), sidan 5.

tur, leverans- och distributionssystem i förhållande till de hot och risker som redovisas i Storbritanniens nationella risk- och sårbarhetsanalys (”National Risk Assesment”). Infrastruktur resiliensprogrammet leds som framgått tidigare av” Civil Contingencies Secretariat” i regeringskansliet (Cabinet Office). Hösten 2011 publiceras som en del av programmets arbete en handbok (”Keeping the Country Running: Natural Hazards and Infrastructure. A guide to improving the resilience of critical infrastructure and essential services”) för hur olika aktörer med ansvar för kritisk infrastruktur bör arbeta med att öka robustheten i kritisk infrastruktur på olika nivåer i samhället och inom olika sektorer. Handboken togs fram i ett samarbete med departement och myndigheter, infrastruktur ägare och operatörer samt branschorgan.

Handboken förklarar grundläggande principer och utgångspunkter, förmedlar råd och ”best practices” om hur man identifierar och bedömer risker och hot från naturmiljön, belyser existerande standarder för resiliens, belyser kontinuitetsplanering och ledning för främjande av resiliens i företag, ger riktlinjer arbetet med resiliens inom icke-avreglerade sektor, belyser informationsdelning mellan aktörer, belyser ömsesidiga beroendeförhållanden inom och mellan aktörer och sektorer m.m.

5.5 Doktrin och styrmedel

Centrala doktrinkomponenter i Storbritanniens arbete med skydd av kritisk infrastruktur är resiliens (robusthet) och kontinuitetsplanering baserad på risk- och sårbarhetsanalyser på organisation och systemnivå. Arbetet med robusthet och kontinuitetsplanering ska ske ur ett ”All hazard” och ett före-under-efter-perspektiv. Storbritannien har härvid övergivet det tidigare mer traditionella synsätt att arbeta med att ”skydda” och ”hantera”. En ytterligare central doktrinkomponent är att ägare eller operatörer av kritisk infrastruktur har ansvaret för att identifiera hot och risker mot deras anläggningar (etc.)och säkerställa att deras anläggningar (etc.) är robusta i förhållande till dessa hot och risker samt att finansiera arbetet härvid. Regeringen och myndigheter understödjer med råd, etablerar strukturer för samverkan mellan berörda aktörer för utbyte av information, best practice m.m. Med andra ord gäller en ansvarsprincip likt den som finns i Sverige. De sektorsansvariga departementen eventuella finansiella stöd för resiliensarbetet i sektorn sker inom budgetram. Den kritiska infrastrukturen ägs i Storbritannien till 80% av privata företag, varför utveckling av privat-offentlig samverkan är helt central i Storbritanniens arbete med robust kritisk infrastruktur.

En ytterligare central doktrinkomponent är att arbetet med robusthet i kritisk infrastruktur bygger på redan existerande professionella nationella och internationella standarder, föreskrifter, lagar, branschöverenskommelser m.m. som finns på plats inom en sektor eller sakområde. Någon enskild lag som styr arbetet med robusthet i kritisk infrastruktur existerar inte och avses heller inte införas. Man talar i sammanhanget om en ”light-touch regulation environment”[16]

[16] PowerPoint presentation: Critical National Infrastructure: A UK Civil Contingencies Resilience, Dr Nigel P Brown.

för det övergripande arbetet med robusthet i kritisk infrastruktur. En ytterligare central doktrinkomponent är att sträva efter att integrerar existerande strategier, handlingsprogram etc. som finns för olika politikområde och som på ett eller annat sätt berör robusthet i kritisk infrastruktur. Här handlar det främst om arbetet med skydd mot ”Natural Hazards”(se nedan), programmet för att skydda kritisk infrastruktur mot terrorism, som utgör en del av Storbritanniens kontraterrorism strategy (CONTEST) samt landets klimatanpassnings strategi.

De strategiska komponenterna i Storbritanniens arbete med en robust infrastruktur (enligt handbok för ”Natural Hazards and Infrastructure, se nedan) utgörs av a) motståndskraft (Resistance), b) pålitlighet (Reliability), c) redudans (Redundancy) samt d) hantering och återställande (Response & Recovery) enligt figuren nedan. Varje sektor eller organisationsstrategi för att skapa robusthet/resiliens bör enligt det brittiska synsättet utgöras av en kombination av dessa olika komponenter. Kombinationen varierar dock från fall till fall.

Figure 2: The components of infrastructure resilience: In building resilience, the contribution made by each of these four components needs to be considered

Figur 7. Komponenterna för infrastruktur resiliens enligt officiell brittiskt synsätt

Ansatsen för arbetet med att stärka robustheten bör vidare i varje enskilt fall följa en resilienscykel enligt figuren nedan. Stegen i denna cykel är att identifiera hoten och riskerna, bedöma konsekvenser och sannolikheten för hoten och riskerna, vidta robuststärkande, utvärdera effekterna av vidtagna åtgärder. I centrum för detta arbete står hela tiden ett utbyte av information och ”best practice” med andra aktörer i området och inom sektorn.

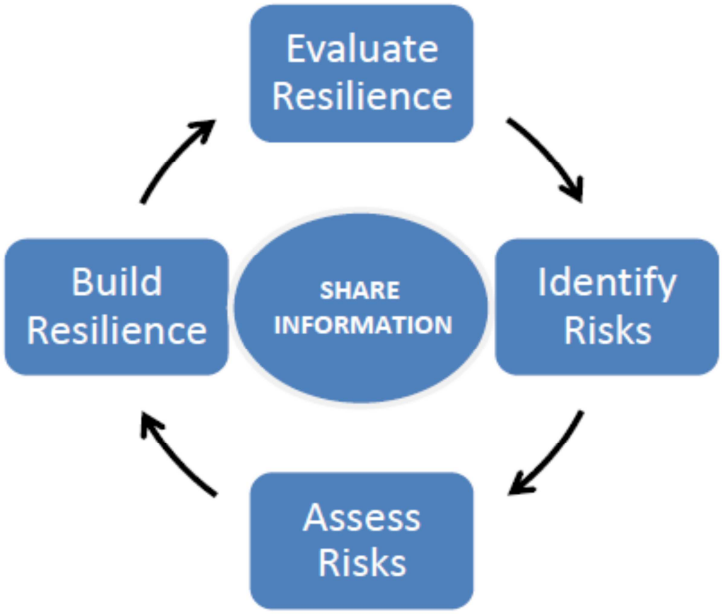


Figure 3: Resilience Cycle for Infrastructure Owners

Figur 8. Resilienscykel för infrastruktur ägare enligt officiellt brittiskt synsätt.

Arbetet med nyss nämnda resilienscykel är kopplat till olika checklistor, enligt exemplet nedan:

Resilience Checklist for Infrastructure Owners and Operators

Identify Risks
Understand your criticality
STEP 1: Determine the elements of infrastructure critical to the provision of essential services provided by your organisation.
STEP 2: For your critical infrastructure, identify linkages with other elements of critical infrastructure within your supply chain.
Understand Hazards
STEP 3: Using the scenarios in the Natural Hazards Guidance (Guide 1), identify which hazards are of greatest concern to your critical infrastructure and supply chains.
Self Assessment Questions
1) Have you worked with external agencies to assess the natural hazards risks to your organisation"s critical infrastructure? For example:
a) Met Office;
b) Local Authorities;
c) Environment Agency;
d) British Geological Survey
e) Ordnance Survey
2) Does the location of your critical infrastructure make it more vulnerable to disruption from natural hazards?
3) Have you identified your key / critical suppliers / customers? Do some of those deliver an essential service for your community?

Assess Risk Understand your vulnerability
STEP 4: Understand what level of resilience you have to those hazards through design and service standards.
STEP 5: Using the findings from your investigations into (3) and (4) determine your level of residual risks.
Self Assessment Questions
4) What standards (design, protection, network design, service, performance, recovery time) offer resilience to your critical infrastructure? Where are the gaps?
5) Could there be a surge in demand for your services as a consequence of disruption from natural hazards? Will you be able to manage this?
6) Have you worked with key / critical supply chain partners to understand their vulnerability to disruption by natural hazards? How could their disruption affect the delivery of your essential services?
7) Have you worked with emergency responders, and others that your organisation would rely on during a period of disruption to improve your understanding of:
a) Their vulnerability to disruption from natural hazards;
b) The assistance that your organisation could expect to receive from them during a period of disruption from natural hazards?

Build Resilience

STEP 6: What is the risk appetite within your organisation? How is resilience of critical infrastructure considered and weighted by the corporate Board in decision making? Does this need to change?
STEP 7: Based on the conclusions of (6) and the principles set out in Section A of this Guide, decide what level of resilience is required and what resilience strategy will be adopted to provide the required level of resilience. Consider if the design of your infrastructure needs to evolve to provide greater resilience to future climates.
STEP 8: Embed organisational resilience at the core of your strategic decision making processes.
STEP 9: Engage with emergency responders for the area over which your organisation supplies essential services.

Self Assessment Questions

8) For disruption as a result of natural hazards, are you willing to:
a) Accept the risk, do nothing (tolerate); or
b) Mitigate the risk through emergency and business continuity plans (treat); or
c) Outsource your product / service to another supplier or purchase insurance (transfer); or
d) Cease the activity, move to another location or invest in greater resilience (terminate)?

9) Is the Board aware of the risk of disruption from natural hazards?
10) Has your organisation"s risk appetite to disruption from natural hazards been agreed at Board level?
11) Is the Organisational Resilience Strategy championed at Board level?
12) Has the Board committed resources to improving the resilience of your critical infrastructure to disruption from natural hazards?
13) Has the Board overseen the production of contingency plans to manage disruption from natural hazards?
14) Do you have plans in place to manage (a combination of)?
a) Loss of primary transport routes;
b) Reduced staff availability;
c) Impaired site access;
d) Loss of power supplies; and lack of availability of alternative power supply;
e) Loss of water supplies; and lack of availability of alternative water supplies;
f) Closure of local businesses;
g) Increased demand for health; emergency services, your products / services and those within your supply chain;
h) Supply chain disruption
15) Have these plans been shared with emergency responders and supply chain partners (up and down stream)?
16) Does the Board seek assurances on the resilience of critical infrastructure to disruption from natural hazards at least annually?
17) Do you have a resilience based education and awareness programme in place within your organisation? If not, do you have board / senior management level support to put in place a resilience based education and awareness programme?
18) Have key staff been trained to implement emergency and business continuity plans?
19) Is there evidence that resilience, and particularly the risk from natural hazards, has been factored into the organisation"s strategic decision making including medium to longer term investment plans?
20) Have your business continuity plans been tested against the British Standard, BS25999?

21) Does your organisation aim to achieve BS25999 alignment / certification?
22) Are your critical suppliers aligned or certified to BS25999? Do you make this a requirement?

Evaluate Resilience
STEP 10: Challenge, test and exercise your organisational resilience strategy. Report to your Board, Regulator or Lead Government Department residual vulnerability of any CNI within your remit.

Self Assessment Questions
23) Have you reviewed your Organisational Resilience Strategy?
24) Have you identified and tested any assumptions that underpin the delivery of your strategy?
25) Do you have an exercise programme in place that addresses the risk from natural hazards? Has it been approved by the Board? Do Board members take part in exercises?
26) Have you exercised more than one type of disruption at any one time ie loss of primary transport routes, coupled with loss of power and water supplies?
27) Are plans tested at least annually? Have findings been recorded and lessons learned?
28) Were supply chain partners and emergency responders included in these tests / exercises?
29) Were findings shared with the Board, supply chain partners, emergency responders, regulators and / or government?
30) Have you taken part in your supply chains‟ and / or emergency responder‟s tests / exercises?

Figur 9. Resilienschecklista för ägare av kritisk infrastruktur enligt officiellt brittiskt synsätt.

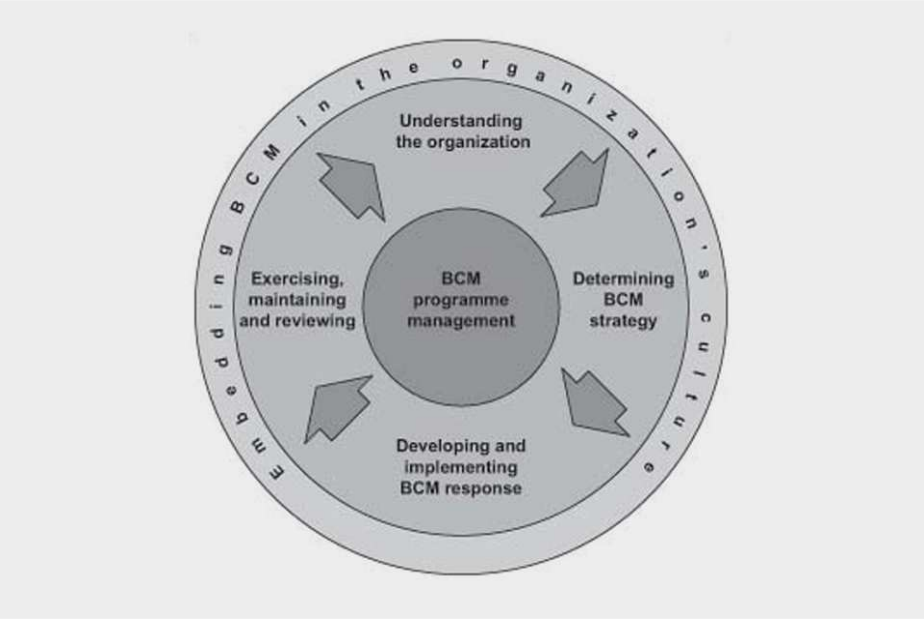
5.5.1 Kontinuitetsplanering för företag och organisationer

Kontinuitetsplanering utgör som nämnts ovan en central komponent i Storbritanniens arbete med att göra sin kritiska infrastruktur mer robust. En särskild ”Corporate Resilience Strategy har härvid utvecklats och leds av ”Civil Contingency Secretariat”. Den brittiska regeringen strävar efter att säkerställa att företag och organisationer brukar ”Business Continuity Management” (BMC).

BMC är en process för att hantera risker som kan störa företagets eller organisationens vardagliga produktion av tjänster och produkter, som säkerställer tillgången på kritiska funktioner i företaget eller organisation vid störningar och en snabb återgång till en normal produktion av tjänster och varor. Regeringen uppmanar företagen och organisationen att standardisera sin verksamhet enligt den brittiska standarden för BMC (The business continuity mananagment standard, BS25999). Standarden är en allomfattande ansats för BMC som baseras på ”best practice” och täcker hela BMC livscykeln (se figur x nedan).

En överväldigande majoritet av de 4,8 miljoner företagen i den privata sektorn i Storbritannien är små eller medelstor. Dessa utgör oftast en viktig länk i försörjningskedjan för stora företag och myndigheter med ansvar för nationell kritisk infrastruktur. Samtidigt har det visat sig att dessa små och medelstora företag i betydligt mindre grad har BCM. Den ovan nämnda standarden har många gånger visat sig var mindre lämplig för småföretag.

Storbritannien stadfäste år 2004 en särskild lag ”The Civil Contingencies Act 2004”. Lagen kan sägas lägga fast det brittiska krisberedskapssystemet i form av ett ramverk för beredskap och hantering av kriser från lokal till nationell nivå. I denna lag regleras bruket av BCM genom att den förpliktar blåljusorganisationer (emergency services) och lokala myndigheter (lokal authorities) definierade som ”Category 1 responders” att göra riskbedömningar, planera och öva för olyckor och kriser samt att vidta ”business continuency management” (BCM) för deras verksamhet. Dessa ”Category 1 responders” är också skyldiga att förmedla BCM-råd till lokala näringsidkare.



Figur 10. The business continuity mananagment standard, BS25999

Underlag

PowerPoint presentation*: Critical National Infrastructure: A UK Civil Contingencies Resilience Perspective*. Dr Nigel P Brown, 2014.

PowerPoint presentation: *Uk Critical National Infrastructure*. Alex Carmichael, BSIA.

Keeping the Country Running: Natural Hazards and Infrastructure. A Guide to improving the resilience of critical infrastructure and essential services. Cabinet Office, 2011:
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/61342/natural-hazards-infrastructure.pdf

Guidance, Resilience in society: infrastructure, communities and businesses, hemsida: https://www.gov.uk/resilience-in-society-infrastructure-communities-and-businesses.

A Summary of the 2013 Sector Resilience Plans, November 2013, Cabinet Office, 2013. (https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/271370/SRP_Public_Summary_2013.pdf) .

Collection, Sector resilience plans. Sector resilience plans set out the resilience of the UK's critical infrastructure to hazards, risks and other threats. Cabinet Office 2014. (https://www.gov.uk/government/collections/sector-resilience-plans#documents).

Strategic Framework and Policy Statement on Improving the Resilience of Critical Infrastructure to Disruption from Natural Hazards, Cabinet Office, 2010. (https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/62504/strategic-framework.pdf)

CPNI, Centre for Protection of National Infrastructure, hemsida: http://www.cpni.gov.uk/Templates/CPNI/pages/Default.aspx

6 Kanada

6.1 Definitioner, organisering och ledning

Med kritisk infrastruktur avses i Kanada processer, system, anläggningar, teknologier, nätverk, tillgångar och tjänster nödvändiga för hälsa, säkerhet eller ekonomiskt välstånd för befolkningen samt för ett väl fungerande styre av landet. Kritisk infrastruktur, menar man vidare, kan vara fristående eller sammankopplad och ömsesidigt beroende inom och mellan provinser, territorium och landets nationsgränser. Störningar och avbrott i den kritiska infrastrukturen kan resultera i katastrofala förluster av människoliv, svåra ekonomiska följdverkningar och betydande skada hos befolkningens förtroende till myndigheter och samhällets funktioner.

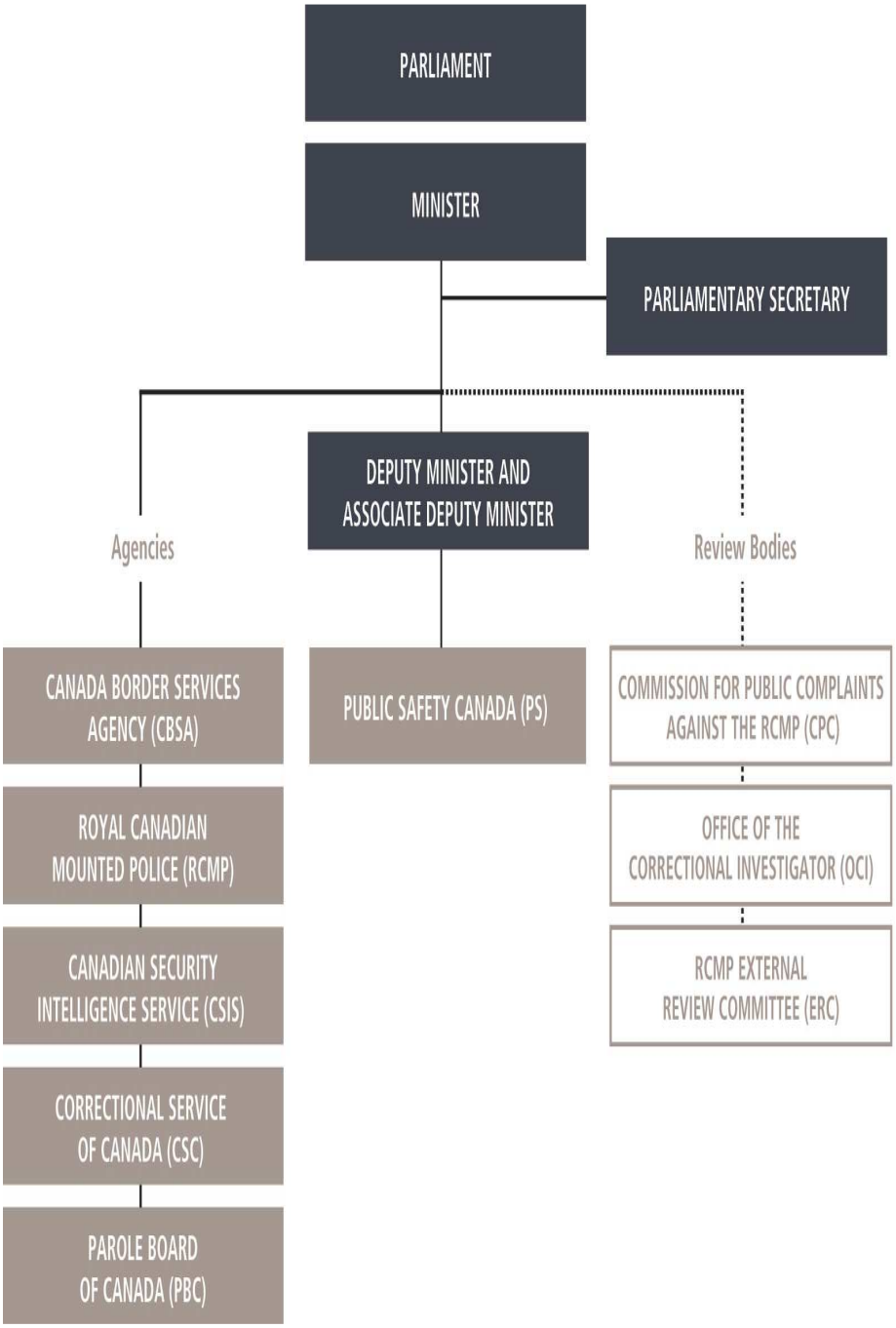
Ansvaret för arbetet med skydd av kritisk infrastruktur i federationen Kanada är delat på den federala regeringen, provinserna, territorierna och de enskilda ägarna/operatörerna av infrastruktur. Det huvudsakliga ansvaret läggs på ägarna/operatörerna av infrastrukturen, såväl offentliga som privata. Ansvarsfördelningen i stort redovisas i figuren nedan. Fokus framöver rörande organisering och ledning ligger emellertid på den nationella nivån, då närmare information om de lägre nivåerna inte kunnat erhållas.

	Roles	Responsibilities
Federal government	Lead federal activities	• Advance a collaborative federal, provincial and territorial approach to strengthening the resiliency of critical infrastructure • Collaborate with provincial and territorial governments to achieve the objectives of the Strategy • Collaborate with national associations • Collaborate with critical infrastructure owners and operators within federal mandate in consultation with provinces and territories
Provincial/ territorial governments	Lead provincial/ territorial activities	• Advance a collaborative federal, provincial and territorial approach to strengthening the resiliency of critical infrastructure • Collaborate with federal, provincial and territorial governments to achieve the objectives of the Strategy • Coordinate activities with their stakeholders, including municipalities or local governments where it applies, associations and critical infrastructure owners and operators
Critical infrastructure owners/ operators	Collaboratively manage risks related to their critical infrastructure	• Manage risks to their own critical infrastructure • Participate in critical infrastructure identification, assessment, prevention, mitigation, preparedness, response and recovery activities

Figur 11. Ansvarsfördelning för kritisk infrastruktur på olika samhällsnivåer i Kanada

På nationell nivå ligger ansvaret för arbetet med skydd av nationell kritisk infrastruktur hos den federala regeringen och dess olika sektorsansvariga departement och myndigheter. Departementet för ”Public Safety Canada” har dock ett särskilt samordningsansvar inom regeringen och ut mot samhället när det gäller arbetet med skydd av kritisk infrastruktur.

Departementet Public Safety Canada inrättades 2003 för att säkerställa samordning mellan federala departement och myndigheter med ansvar för säkerhet och samhällsberedskap. Departementet samverkar med och samordnar arbetet mellan fem olika myndigheter och granskningsorgan, vilka framgår av figuren nedan. Departementet ansvara för Kanadas nationella strategi och handlingsplan för skydd av kritisk infrastruktur och utvecklingen av dess styrinstrument.



Figur 12. Organisationsskiss för Kanadas "Departement Public Safety Canada".

Kanada delar upp sin infrastruktur i tio olika sektorer. I figuren nedan framgår vilka dessa sektorer är och ansvarigt departement på nationell nivå.

Sectors	Sector-specific federal department/agency
Energy and utilities	Natural Resources Canada
Information and communication technology	Industry Canada
Finance	Finance Canada
Health	Public Health Agency of Canada
Food	Agriculture and Agri-Food Canada
Water	Environment Canada
Transportation	Transport Canada
Safety	Public Safety Canada
Government	Public Safety Canada
Manufacturing	Industry Canada Department of National Defence

Figur 13. Ansvarsfördelningen för kritisk infrastruktur inom Kanadas federala regering.

På den nationella nivån är sektorsspecifika nätverk för arbetet med att skydda och stärka kritisk infrastruktur under uppbyggnad. Dessa sektorsnätverk är tänkt att omfatta representanter från federala departement och myndigheter, provinser och territorier, branschorgan och nyckelaktörer i fråga om ägare/operatörer av kritisk infrastruktur. Deltagandet i sektorsnätverken baseras helt på frivillighet. För att främja det sektorsövergripande arbetet med att skydda och stärka kritisk infrastruktur har det inrättats ett särskilt sektorsövergripande forum: ”*National Cross-Sector Forum*”.

Figur 14. Sektor- och sektorsövergripande samverkansforum för kritisk infrastruktur i Kanada.

”The National Cross-Sector Forum” omfattar representanter från de tio nyss nämnda sektorsnätverken som återspeglar dess sammansättning i fråga om offentliga och privata aktörer och nivåer i samhället (se figur ovan). Det årliga huvudmötet för forumet leds av expeditionschefen (högsta opolitiska tjänstemannen) (Deputy Minister) för departementet ”Public Safety Canada” och en representant för antingen ett territorium eller provins.

Under den nationella nivån och det nämnda sektorsövergripande forumet finns också ett särskilt permanent forum: ”FPT CI Working Group”. Det är en särskild arbetsgrupp för samarbete rörande skydd och stärkande av kritisk infrastruktur mellan den federala nivån, provinsregeringarna och de territoriella regeringarna. Arbetsgruppens möte leds av en tjänsteman från departementet ”Public Safety Canada” samt en representant för provinserna och territorierna.

6.2 Doktrin och styrmedel

Det centrala doktrindokumentet i Kanadas arbete med att skydda och stärka sin kritiska infrastruktur är dess ”National Strategy for Critical Infrastructure”

från 2009 och tillhörande ”Action Plan for Critical Infrastructure 2014-2017”, ”Risk Management Guide for Critical Infrastructure Sectors” samt USA:s Regional Resilience Assessment Programme (RRAP)”. I dessa dokument läggs det fast, explicit eller implicit, ett antal doktrinelement som vägleder det praktiska arbetet. Ett först, och kanske det mest grundläggande, doktrinelementet är att arbetet med skydd av kritisk infrastruktur baseras på och bygger vidare på redan existerande lagar och regelverk, professionella nationella och internationella bransch- och sektorsstandarder, skydds- och säkerhetsarbete, nätverk för samverkan etc.

Det finns inte i Kanada någon sektorsöverskridande och allmän lag för skydd av kritisk infrastruktur, inte heller är någon sådan planerad. Ett andra doktrinelement är att varje aktör, från den enskilde ägaren eller operatören av en kritisk infrastruktur till federala regeringen, har ett ansvar för att inom ramen för sin verksamhet agera för att skydda och stärka den kritiska infrastrukturen. Med andra ord råder en motsvarighet till den svenska ansvarsprincipen.

Ett tredje doktrinelement är privat-offentligt samverkan, benämnt ”partnerskap”. Eftersom merparten av den kritiska infrastrukturen i Kanada är privatägd så måste grunden för inriktning och styrning i arbetet med skydd av kritisk infrastruktur baseras på frivilliga överenskommelser mellan privata företag och offentliga aktörer. Kanada talar i sammanhanget tydligt om att bygga partnerskap baserat på frivillighet mellan det offentliga och privata, men också mellan den federala nivån, provinserna och territorierna då det saknas tvingande nationell lagstiftning på området. Verktyg är här t.ex. de ovan beskrivna sektorsnätverken och sektors- och nivåövergripande forum och arbetesgrupper. I det privat-offentliga partnerskapet ingår också att gemensamt stärka befolkningens beredskap för att kunna hantera störningar i infrastruktur.

Ett fjärde doktrinelement är att arbetet med skydd av kritisk infrastruktur ska omfatta alla faser i krisberedskapscykeln, dvs förebygga, hantera och återställa. Ett femte doktrinelement är att arbetet med skydd av kritisk infrastruktur ska baseras på en ”All-hazard” ansats, dvs. alla typer av hot och risker (”accidental, intentional and natural hazards”) ska hanteras inom ramen för en helomfattande riskhanteringsprocess. Ett viktigt inslag i denna ansats är systematiska risk- och sårbarhetsanalyser, att kartlägga ömsesidiga beroendeförhållanden och att öva systematiskt för att kartlägga olika typer av risker och hot. Ett sjätte doktrinelement är resiliens.

Arbetet med att kritisk infrastruktur ska fokusera på att stärka dess robusthet genom en lämplig kombination av säkerhets- och skyddsåtgärder för motverka antagonistiska hot och olyckor orsakade av människor, kontinuitetshantering för att hantera störningar och säkerställande av produktion av varor eller tjänster samt krisberedskap för kunna hantera naturolyckor och plötsliga och storskaliga störningar och kriser. Ett sjunde är att främja och understödja informationsdelning och säkerställa informationssäkerhet mellan berörda privata och offentliga aktörer i frågor rörande kritisk infrastruktur, före, under och efter en kris. Det handlar här om ökat utbyte av risk- och sårbarhetsanalyser, incidentrapporter, best practices, vunna erfarenheter, förmågebedömningar, förbätt-

rade tekniska informationsöverföringskanaler, förbättrat skydd mot att obehöriga får tillträde till delad information etc. Den legala basen här utgörs av Kanadas ”Emergency Management Act” från 2007 som lägger fast undantag från ”Acces to Information Act” när det gäller känslig information från kritisk infraststruktur. Ett särskilt protokoll för säkert informationsutbyte är under utveckling. Härvid finns särskilda föreskrifter för privata aktörer hur de ska ”märka” känslig information så att den kan skyddas i kommunikation med myndigheterna: ”Identifying And Marking Critical Infrastructure /Emergency Management (Ci/Em) Information Shared In Confidence With The Government Of Canada: Guide For Private Sector Entities”. En teknisk plattform för informationsutbyte om kritisk infrastruktur mellan myndigheter och/eller privata aktörer har etablerats i form av en särskild internetbaserad portal: ”Canadian Critical Infrastructure Gateway”. Portalen administreras av departementet Public Safety Canada.

6.2.1 National Strategy for Critical Infrastructure” från 2009 och tillhörande ”Action Plan for Critical Infrastructure 2014-2017”

Strategic Objective	Action Item	Year	Status
Build Partnerships	Establish sector networks	1	Completed
	Establish National Cross Sector Forum	1	Completed
	Renew FPT CI Working Group	1	Completed
Share and Protect Information	Establish an information sharing framework	2	Completed
	Develop statement of requirements for the information sharing portal	1	Completed
	Establish the Public Layer of the information sharing portal	2	Completed
	Develop and test secure, web-based user authentication	2	Completed
	Implement the Secure Layer of the information sharing portal	2	Completed
	Enhance information dissemination	Ongoing	Ongoing
	Populate Public and Secure Layers of the information sharing portal	Ongoing	Ongoing
Implement an All-Hazards Risk Management Approach	Develop risk assessments of CI in Canada	2 and ongoing	Ongoing
	Develop and share sector-specific work plans	3 and ongoing	In progress
	Conduct national exercises	Ongoing	Ongoing

Figur 15. Hittills verkställda åtgärder för de tre strategiska målen i Kanadas nationella strategi för kritisk infrastruktur sedan 2009/2010.

Den nationella strategin uttrycks i ett kortfattat dokument. I dokumentet fastslås ett antal doktrinelement som lyfts fram ovan, som t.ex. ansvarsprincipen och en ”all-hazard” ansats. Strategin vilar på tre ben, strategiska mål. Det första

strategiska målet är att vidmakthålla och utveckla partnerskap mellan offentliga och privata aktörer som har ansvar för kritisk infrastruktur inom och mellan olika nivåer och sektorer. Det andra strategiska målet är att främja informationsdelning mellan berörda infrastrukturaktörer samt att informationsdelningen kan ske på ett säkert sätt. Det tredje strategiska målet är att implementera en ”all-hazard” riskhanteringsansats för kritisk infrastruktur

Strategic Objective	Action Item	Year to Achieve
Sustain and Enhance Partnerships	Develop a call to action for critical infrastructure resilience	1 and ongoing
	Provide guidance to ensure appropriate representation on sector networks	1
	Address cross-sector issues through multi-sector meetings	Ongoing
	Strengthen public communications and awareness	2 and ongoing
Share and Protect Information	Expand stakeholder membership and participation on the *Canadian Critical Infrastructure Gateway* and leverage the CI Gateway's capabilities to improve information sharing and collaboration on specific projects	1 and ongoing
	Sponsor security clearances among private sector stakeholders in order to enable increased sharing of sensitive information	1 and ongoing
	Expand information sharing and investigate rationalization of existing information sharing arrangements	2
	Provide impact assessments during unfolding events of national significance	2 and ongoing
Implement an All-Hazards Risk Management Approach	Implement the Regional Resilience Assessment Program (RRAP) across Canada	1 and ongoing
	Provide an overall description of key risks for critical infrastructure, including dependencies and emerging trends	1 and ongoing
	Assess impacts of potential high impact / low frequency events on critical infrastructure sectors to increase awareness and understanding of risks to critical infrastructure	1 and ongoing
	Promote the adoption of existing standards and determine whether additional standards are needed to improve critical infrastructure resilience	1 and ongoing
	Conduct exercises to strengthen readiness and response efforts	1 and ongoing
	Develop targeted risk assessment products in response to emerging critical infrastructure issues	2 and ongoing
	Finalize national application of an interdependencies model	2
	Measure progress toward resilience to demonstrate results and monitor progress	2 and ongoing

Figur 16. Handlingsplan för åren 2014-2017 för de tre strategiska målen i Kanadas nationella strategi för kritisk infrastruktur.

En konkret färdplanen för implementeringen av strategin läggs fast i ”Action plan for Critical infrastruture 2014-2017”. I den färdplanen redovisas också vad som hittills uppnåtts sedan 2009/2010 (se figurer ovan).

6.2.2 ”Risk Management Guide for Critical Infrastructure Sectors”

”Risk Management Guide for Critical Infrastructure Sectors” är en handledning för hur ansvariga offentliga och privata aktörer praktiskt på sektor/subsektornivå kan samarbeta för att stärka skyddet av och robustheten i sektorns kritiska infrastruktur. Handledningen är en anpassad version av standarden ISO 31000 .

6.2.3 USA:s Regional Resilience Assessment Programme (RRAP)

”The Regional Resiliency Assessment Program” (RRAP) är ett amerikanskt handlingsprogram för att identifiera och analysera robusthet och ömsesidiga beroendeförhållande hos kritisk infrastruktur inom en sektor på regional nivå utifrån en ”all-hazard” ansats. RRAP-processen inbegriper bedömningar av enskild kritisk infrastruktur och en regional analys av omgivande infrastruktur. RRAP utvärderar kritisk infrastruktur på regional (inklusive nationsöverskridande) nivå för att kartlägga sårbarheter, hot och potentiella konsekvenser av dess från ett ”all-hazard” perspektiv. RRAP syftar till att identifiera ömsesidiga beroenden, kaskadeffekter, resiliensegenskaper och brister i robusthet rörande kritisk infrastruktur. Vid tillämpningen av RRAP kommer departementet Public Safety Canada att samverka med provinser, territorier och privata ägare/operatörer av kritisk infrastruktur.

6.3 Kanadensiskt samarbete med USA rörande kritisk infrastruktur

Mot bakgrund av att det finns ett omfattande ömsesidigt beroende när det gäller kritisk infrastruktur längs gränsen mellan Kanada och USA har regeringarna i de båda länderna enats om att koordinera sina nationella ansträngningar när det gäller att stärka robustheten i nämnda strukturer. Inriktningen på dessa ansträngningar läggs fast i handlingsplanen “Canada-United States Action Plan for Critical Infrastructure 2010” från 2010. Det uttalade syftet med planen, som mer har karaktären av en avsiktförklaring om samarbete, är att stärka säkerheten, beredskapen och robustheten i Kanada och USA genom att etablera en nationsöverskridande heltäckande all-hazard-ansats för robusthet i kritisk infrastruktur. I planen läggs ett antal handlingspunkter fast:

1. Söka vägledning från den arbetsgrupp för kritisk infrastruktur som redan finns etablerad inom ramen för Canada-U.S Agreement on Emergency Management Cooperation (2008) och dess Emergency Management Consultative Group (EMCG).
2. Skapa strukturer och möjligheter för Kanadas etablerade sektorsnätverk och dess amerikanska motsvarighet (U.S. Sector and Government Coordinating Councils) att förbättra sektorspecifik nationgränsöverskridande samarbete
3. Etablera en virituell kanadensisk-amerikansk infrastruktur riskanalys ”cell” (Infrastructure Risk Analysis Cell) för att utveckla och dela riskhanterings verktyg och information (förmågebedömningar, best practice m.m.)

4. Kanada och USA ska samarbeta för att utveckla kompatibla strukturer och protokoll för att skydd och dela känslig information om kritisk infrastruktur
5. Kanada och USA ska samarbeta för att identifiera vilka behov som finns hos berörda offentlig och privat aktörer ifråga om information och beslutsfattande för att kunna utveckla analysverktyg för deras behov att skydda och stärka den kritiska infrastrukturen
6. Kanada och USA ska samarbeta för att säkerställa effektiv informationsdelning under och efter en allvarlig störning i kritisk infrastruktur
7. Kanada och USA ska samarbeta för att bedöma risker och utveckla planer för att åtgärda prioriterade områden. Sekondära åtgärder ska identifieras genom en grundlig genomgång av de båda ländernas fastställda prioriterade risker och genom att fastställa område av ömsesidigt intresse

I handlingsplanen fastställd färdplan:

Milestone	Target
Seek direction from the Canada-United States working group on critical infrastructure	2010-11
Develop compatible mechanisms and protocols to protect and share sensitive critical infrastructure information	2011-12
Identify public and private sector information requirements to support the development of valuable analytic products tailored to their respective and unique decision-making, protection and resiliency requirements	2011-12
Collaborate to ensure effective information sharing during and following an incident affecting critical infrastructure	2011-12
Establish a Canada-U.S. virtual infrastructure cell to develop and share risk management tools and information	2011-12
Assess risks and develop plans to address priority areas, and measure the effectiveness of the plans in reducing risks to the United States and Canada	2012-13
Provide mechanisms and opportunities for the U.S. Sector and Government Coordinating Councils and the Canadian sector networks to work together to improve sector-specific cross-border collaboration	Ongoing

Figur 17. Färdplan för den kanadensisk-amerikanska handlingsplanen för skydd av kritisk infrastruktur

Underlag

Public Safety Canada: Critical Infrastructure, hemsida:
(http://www.publicsafety.gc.ca/cnt/ntnl-scrt/crtcl-nfrstrctr/index-eng.aspx)

National Strategy for Critical Infrastructure, Public Canada 2009.

(http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/srtg-crtcl-nfrstrctr/srtg-crtcl-nfrstrctr-eng.pdf)

Action Plan for Critical Infrastructure 2014-2017, Public Canada 2014. (http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/pln-crtcl-nfrstrctr-2014-17/pln-crtcl-nfrstrctr-2014-17-eng.pdf)

Canada-United States Action Plan for Critical Infrastructure 2010. Public Safety Canada/US Homeland Security: http://www.dhs.gov/xlibrary/assets/ip_canada_us_action_plan.pdf

Risk Management Guide for Critical Infrastructure Sectors, version 1. Public Safety Canada: http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/rsk-mngmnt-gd/index-eng.aspx

Canadian Critical Infrastructure Information Gateway: https://cigateway.ps.gc.ca/_layouts/pscbranding/trms-eng.pdf

7 USA

7.1 Definitioner och sektorer

Med kritisk infrastruktur avser man från amerikansk sida system och tillgångar, fysiska eller virituella, som är så viktiga för USA så att utslagning eller förstörelse av dessa får en försvagande effekt på säkerhet, nationell ekonomisk säkerhet, folkhälsan eller skyddet av befolkningen, eller någon form av kombination av dessa. USA delar in sin kritiska infrastruktur i 16 sektorer:

- Chemical
- Commercial Facilities
- Communications
- Critical Manufacturing
- Dams
- Defense Industrial Base
- Emergency Services
- Energy
- Financial Services
- Food and Agriculture
- Government Facilities
- Healthcare and Public Health
- Information Technology
- Nuclear Reactors, Materials, and Waste
- Transportation Systems
- Water and Wastewater Systems

7.2 Organisation och ledning

Ansvaret för arbetet med att skydda och stärka kritisk infrastruktur är i USA ett delat ansvar mellan den federala nivån, delstatsnivån, lokala-, stam- eller territoriella nivån, regionala samverkansorgan samt ägare/operatörer av landets kritiska infrastruktur och så kallade kritiska resurser (CIKR).

7.2.1 Presidenten

Som stats- och regeringschef har presidenten det yttersta ansvaret för den federala nivåns arbete med skyddet av den kritiska infrastrukturen. Det närmaste stödet härvid är "Department of Homeland Security" (DHS) (se nedan) och "The National Infrastructure Advisory Council" (NIAC). NIAC:s uppgift är att, via DHS, ge presidenten råd när det gäller säkerheten för landets kritiska infrastruktur och dess informationssystem.

Rådet består av max 30 personer, utsedda av presidenten, som kommer från den privata sektorn, universitetsvärlden samt från delstatsregeringar och lokala styrelseorgan. Presidenten har utfärdat två centrala styrdokument när det gäller skydd och stärkande av USA:s kritiska infrastruktur. Det ena är "Presidential Policy Directive (PPD-21) – Critical Infrastructure Security and Resilience". Det andra är "Executive Order 13636, Improving Critical Infrastructure Cybersecurity".

7.2.2 Department of Homeland Security

Department of Homeland Security (DHS) tillkom i kölvattnet av terrorattackerna 2001 och vars främsta ansvar är att skydda USA och dess territorium från terrorattacker, av människan orsakade storskaliga olyckor och katastrofer samt naturkatastrofer. DHS har på federal nivå samordningsansvaret för skydd och stärkande av den kritiska infrastrukturen samt egenansvar för 8 sektorer, dvs. hälften av de befintliga sektorerna. Vilka dessa sektorer är och vilka andra departement som har ansvar för övriga 8 sektorer framgår i figuren nedan:

Table 1 – Sector and Cross-Sector Coordinating Structures

		Critical Infrastructure Partnership Advisory Council		
Critical Infrastructure Sector	Sector-Specific Agency	Sector Coordinating Councils (SCCs)	Government Coordinating Councils (GCCs)	Regional Consortia
Chemical	Department of Homeland Security	✓	✓	
Commercial Facilities ⓘ		✓	✓	
Communications ⓘ		✓	✓	
Critical Manufacturing		✓	✓	
Dams		✓	✓	
Emergency Services ⓘ		✓	✓	
Information Technology ⓘ		✓	✓	
Nuclear Reactors, Materials & Waste		✓	✓	
Food & Agriculture	Department of Agriculture, Department of Health and Human Services	✓	✓	
Defense Industrial Base ⓘ	Department of Defense	✓	✓	
Energy ⓘ	Department of Energy	✓	✓	
Healthcare & Public Health ⓘ	Department of Health and Human Services	✓	✓	
Financial Services ⓘ	Department of the Treasury	Uses separate coordinating entity	✓	
Water & Wastewater Systems ⓘ	Environmental Protection Agency	✓	✓	
Government Facilities	Department of Homeland Security, General Services Administration	Sector does not have an SCC	✓	
Transportation Systems ⓘ	Department of Homeland Security, Department of Transportation	Various SCCs are broken down by transportation mode or subsector.	✓	

Critical Infrastructure Cross-Sector Council

Federal Senior Leadership Council

State, Local, Tribal, and Territorial Government Coordinating Council

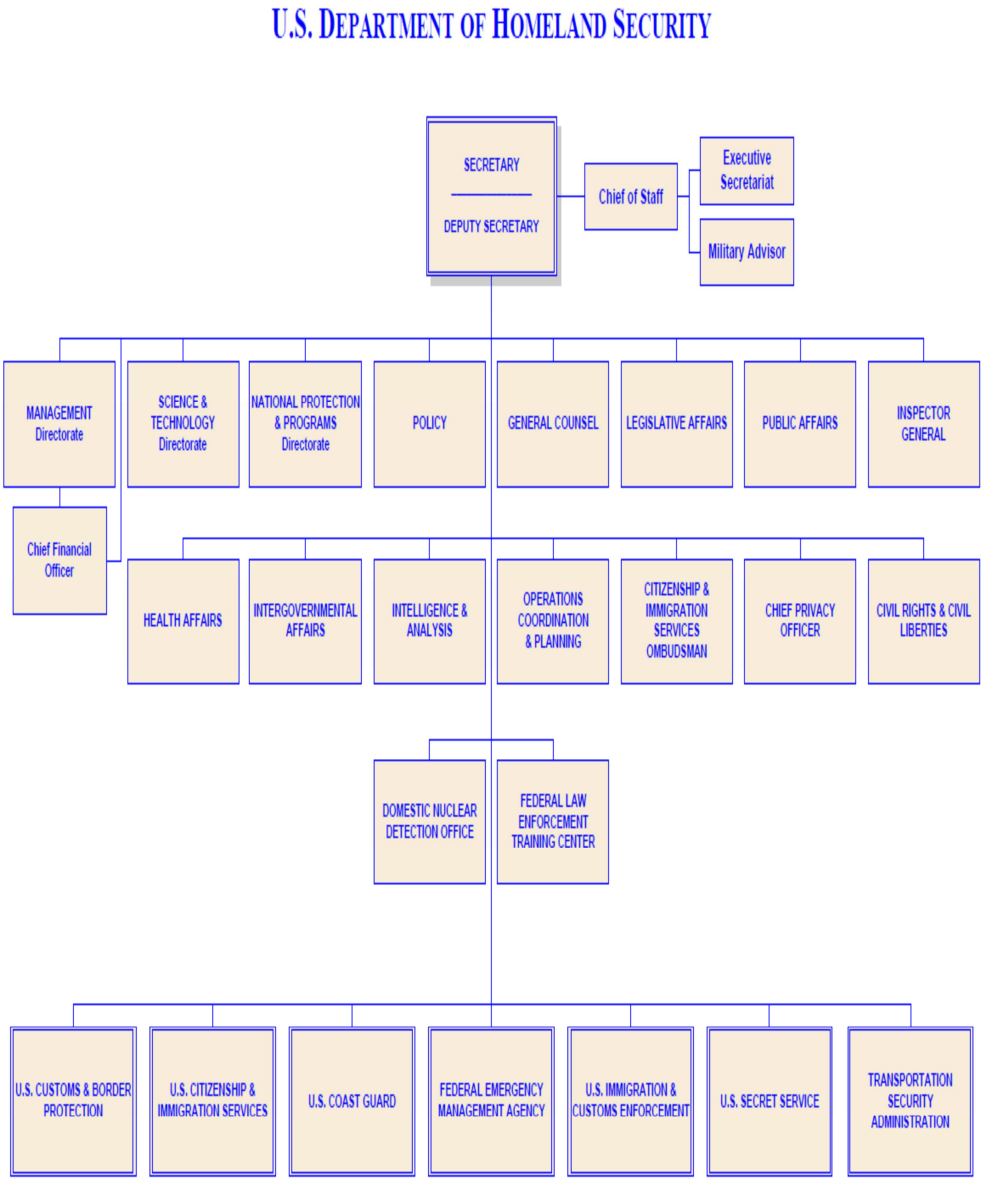
Regional Consortium Coordinating Council

ⓘ Indicates that a sector (or a subsector within the sector) has a designated information-sharing organization.

Figur 18. Sektors- och sektorsövegripande samverkanforum för skydd av kritisk infrastruktur i USA.

DHS är också förmedlare av expertis, anlysverktyg och andra relevanta resurser till olika samarbetspartner i samhället vad gäller skydd och stärkande av kritisk

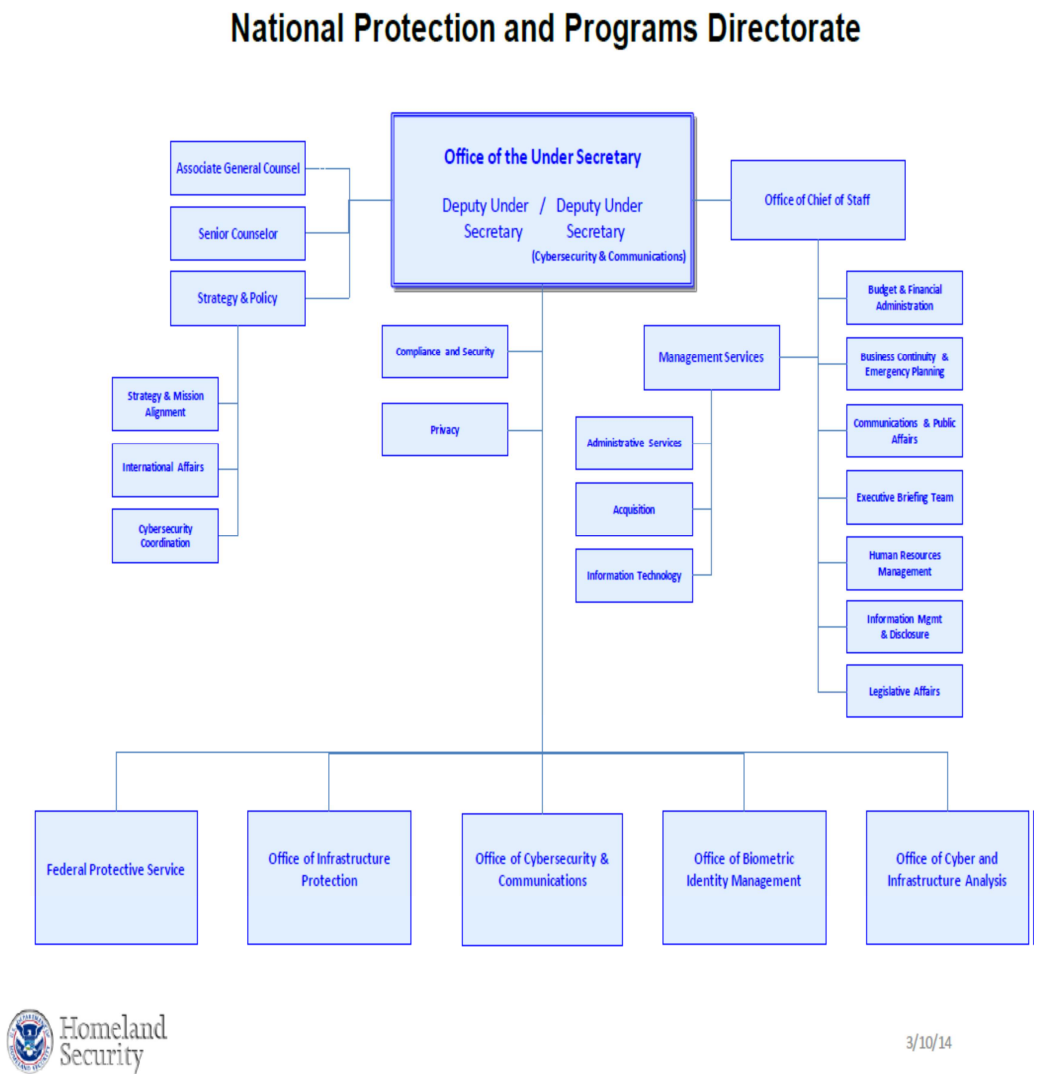
infrastruktur. Inom DHS organisation är det ”National Protection and Programs Directorate” (NPPD) som har ansvar för arbetet med skydd av kritisk infrastruktur (se figur).



Figur 19. Organisationsskiss för US. Departement of Homeland Security.

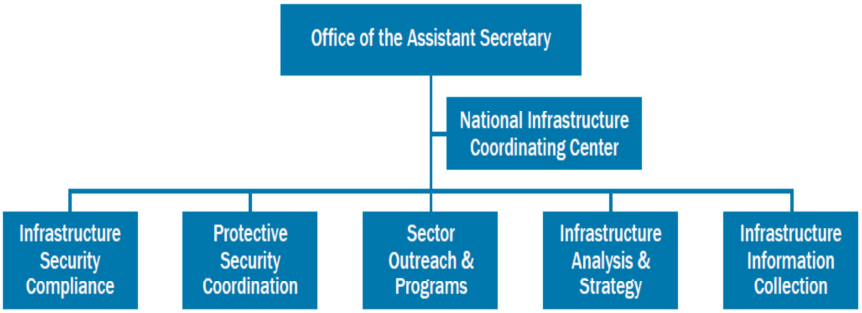
Inom NPPD är det i sin tur främst två olika funktioner som är av intresse i sammanhanget. Den första är ”Office of Infrastructure Protection” (IP). IP leder och koordinerar existerande nationella åtgärdsprogram på området kritisk

infrastruktur. IP genomför och stödjer också risk- och sårbarhetsanalyser och konsekvensbedömningar m.m. i samarbete med ägare/operatörer av kritisk infrastruktur och olika offentliga aktörer på olika nivåer i samhället. Vidare förmedlar IP information om existerande och gryende hot och risker till berörda parter samt erbjuder olika former av analysverktyg och övningsverksamhet till berörda parter i deras strävan att stärka sin förmåga att hantera hot och risker mot den kritiska infrastrukturen inom deras ansvarsområde.



Figur 20. Organisationsskiss för National Protection and Programs Directorate.

”Office of Infrastructure Protection” består av fem olika avdelningar och ett center (enligt figur nedan):



Figur 21. Organisationsskiss för USA:s "Office of Infrastructure Protection"

- "National Infrastructure Coordinating Centre" (NICC). NICC är ett operationellt informations- och koordineringsnav i ett nationellt närverk som samlar in och förmedlar information till berörda parter (myndigheter, operatörer mm.) om hot, incidenter etc. över hela USA i syfte att avvärja attacker, olyckor m.m. eller att mildra dess konsekvenser. NICC är med sin lägesbildsfunktion igång dygnet runt.

- "Infrastructure Security Compliance" (ISCD). ISCD leder det nationella arbetet med att säkra och skydda (secure) kemiska högrisk fabriker och anläggningar och att förhindra spridning av kemikalier som kan användas i terroristverksamhet. ISCD arbetar med regleringar, inspektioner och verkställighet av "Chemical Facility Anti-Terrorism Standards".

- "Protective Security Coordination" (PSCD). PSCD arbetar med strategisk koordinering och stöd till fältoperationer (t.ex. bombskydd) för att reducera sannolikheten för att landets kritiska infrastruktur ska drabbas av terroristattentat eller naturolyckor. PSCD arbetar härvid med:

    - Bedömningar
    - "Outreach" (etablering av privat-offentligt partnerskap)
    - Incident hantering
    - Särskilda event
    - Träning
    - Informationsspridning och koordinering
    -

- "Sector Outreach and Programs Division" (SOPD). SOPD arbetar med de nationella ansträningningarna att bygga, vidmakthålla och utveckla frivillig privat-offentlig samverkan med privata ägare/operatörer av kritisk infrastruktur. SOPD koordinerar samverkan över alla 16 sektorerna och har egenansvar för 6 sektorer. SOPD utvecklar och verkställer här olika program för att skydda och stärka infrastrukturen i samverkan med de privata aktörerna. SOPD bistår med expertis.

- ”Infrastructure Analysis and Strategy Division” (IASD). IASD förser DHS och dess samverkanspartner (myndigheter, operatörer m.m.) med strategiska, operativa och taktiska produkter samt tjänster via ett analytiskt ramverk som integrerar:

    - Kritisk infrastruktur och risk- och sårbarhetsanalyser som skrider över fysisk och cyber domäner
    - Strategiska, operativa och taktiska analyser
    - Utveckling av riskmetodologi, modellering och förmågeutveckling
    - Underrättelseanalys och operationer

- ”Infrastructure Information Collection Division” (IICD). IICD samlar in data och leder DHS ansträngningar att skydda och förse DHS samverkanspartners med standardiserad, relevant och kundfokuserad infrastrukturdata.

“Office of Cyber & Infrastructure Analysis” (OCIA) etablerades 2014 som svar främst på “Presidential Policy Directive 21” från 2013 (se nedan) som uppmanade DHS att bättre integrerar arbetet med att skydda fysisk kritisk infrastruktur respektive kritisk cyberinfrastruktur. OCIA arbetar således med förbättra förståelsen och kunskapen om hot och risker mot kritisk infrastruktur som sträcker sig över både den fysiska domänen och cyberdomänen. OCIA använder sig av olika typer av ”all-hazard” information från en mängd berörda parter för genomföra konsekvensmodellering, simulering och analyser.

7.2.3 Sektorspecifika departement och federala myndigheter

Vid sidan av ”Department of Homeland Security” med sitt särskilda huvud- och samordningsansvar för arbetet med att skydda och stärka USA:s kritiska är det flera departement som har ett särskilt utpekat sektorsansvar. Därtill har ett flertal andra departement och federala myndigheter olika former av tilldelat ansvar för att leda, verkställa, utveckla, samla in och/eller förmedla information rörande olika program och åtgärder rörande kritisk infrastruktur inom olika sektorer, inklusive att samverka med privata aktörer m.m. Deras ansvar läggs fast i ”Presidential Policy Directive (PPD-21) – Critical Infrastructure Security and Resilience”.

7.2.4 Regeringar och styrande organ på delstatsnivå, lokal nivå, stam- och territorium nivå samt regionala samverkansorgan (privat-offentlig samverkan)

Styrande organ under den federala nivån har ansvar för arbetet med skyddet av den kritiska infrastrukturen inom ramen för sin jurisdiktion och att samverka med den federala nivån när det gäller att identifiera kritisk infrastruktur, förmedla information om och att hantera incidenter (etc.), att verkställa federala program och åtgärder inom sin jurisdiktion samt att svara för regional och lo-

kal samverkan med privata aktörer som ansvarar för kritisk infrastruktur. Regionala samverkansorgan mellan privata och offentliga aktörer bidrar med att identifiera hot och risker, dela erfarenheter, verkställa program och åtgärder initierade av den federala nivån och delstatsnivån m.m.

7.2.5 Rådgivande organ på federal nivå

Till området skydd av kritisk infrastruktur finns det på federal nivå kopplat flera rådgivande organ som till presidenten, departement, myndigheter m.fl. tillhandhåller råd, rekommendationer och expertkunskap om kritisk infrastruktur. Dessa organ bidrar också till arbetet med att bygga partnerskap mellan den privata och offentliga sfären. Exempel på sådana rådgivande organ är:

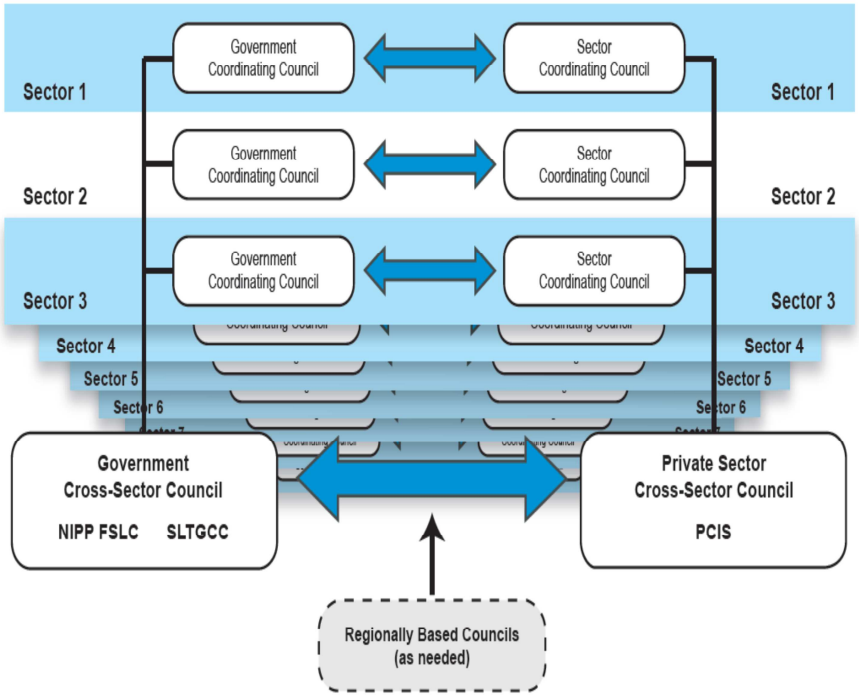
- "Homeland Security Advisory Council "(HSAC)
  Rådgivning till chefen för Department of Homeland Security rörande säkerhet och beredskap generellt inklusive kritisk infrastruktur.
- "Private Sector Senior Advisory Council". Rådgivningsorgan underordnat HSCA) bestående av chefer inom den private sektorn som förser HSCA med expertstöd, bland annat om kritisk infrastruktur.
- "National Infrastructure Advisory Council" (NIAC) Rådgivningsorgan åt presidenten via chefen för "Department of Homeland Security" (närmare beskrivit ovan).
- "Critical Infrastructure Partnership Advisory Council "(CIPAC). Syftet med CIPAC är utgöra ett forum för ägare/operatörer och myndigheter för att främja koordinering mellan offentliga infrastrukturprogram och infrastrukturprogram och åtgärder inom näringslivet.

7.2.6 Ägare och operatörer av kritisk infrastrutkur

Ägare och operatörer ansvarar för att för att egen del på olika sätt skydda och stärka den egna kritiska infrastrukturen (anläggningar, system etc.), göra risk- och sårbarhetsanalyser, hantera incidenter (etc.) samt att samverka med offentliga aktörer för att verkställa olika offentliga program och åtgärder kopplade till den egna kritiska infrastrukturen för att förbättra samhällets samlade skydd av kritisk infrastruktur. Samverkan med myndigheter och andra offentliga aktörer är oftast inte legalt tvingande utan baseras vanligen på frivillighet.

7.2.7 "Partnerskap" för att skydda och stärka den kritiska infrastrukturen i USA

Basen för USA:s arbete med att skydda och stärka landets infrastruktur utgörs, som framgått ovan, av olika legalt icke-tvingande "partnerskap" mellan olika regeringsnivåer i USA, dvs federal, delstatlig, stam och territorium och mellan respektive inom den privata och offentliga sfären. Syftet med dessa "partnerskap" är att säkerställa samverkan inom och mellan sektorer på olika nivåer samhället (se figuren nedan).



Figur 22. Figur för beskrivning av sektor- och sektorsöverskidande ”partnerskap” i USA (Sector Partnership Model)

Partnerskap för sektorsamverkan mellan ägare eller operatörer, branschorgan inom en sektor sker via ”Sector Coordinating Councils” (SCC) som kan se olika ut för varje sektor ifråga om sammansättning av aktörer, men som alla ska samverka med myndigheter på sektorsnivå. Myndighetsmotparten i sammanhanget är partnerskap för sektorssamverkan mellan myndigheter och regeringsorgan som sker via ”Government Coordinating Councils” (GCC) som alltså utgörs av olika offentliga berörda aktörer inom sektorn.

Partnerskap för sektorsöverskridande samverkan mellan privata aktörer sker via samverkansrådet ”Private Sector Cross-Sector Council”. Partnerskap för sektorsöverskridande samverkan mellan regeringsorgan/myndigheter sker via samverkansrådet ”Government Cross-Sector Council” som i sig består av dels ”National Infrastructure Protection Plan Federal Leadership Council” (FSLC) och dels ”State, Local, and Tribal Government Coordinating Council” (SLTGCC).

Andra samverkans- och koordineringsorgan är dels “Critical Infrastructure and Key Resources Cross-Sector Council” (CIKRCS) och dels “Regional Consortium Coordinating Council” (RCCC). CIKRCS syfte är att koordinera sektorsövergripande frågor som uppkommer bland “Sector Coordinating Councils” (SCC). CIKRCS utgörs av ledningen för de olika SCC inom varje sektor. RCCC är ett forum för representanter från olika regionala råd och nätverk för att främja interregional samverkan rörande skydd och stärkande av kritisk infrastruktur.

USA har också ett utvecklat partnerskap, samverkan, internationellt som dock inte ska belysas här (se dock avsnittet om Kanada för samarbete mellan USA och Kanada).

7.3 Doktrin och styrmedel

USA har ett antal central presidentdirektiv, handlingsplaner och program som utgör doktrin och styrmedel för det nationella att skydda och stärka landets kritiska infrastruktur. Gemensamt för dessa är de omfattar ett antal centrala doktrinelement. Några av dessa ska här nämnas. Ett av dessa doktrinelement är, som framgått ovan, ansvarsprincipen som betonar att ansvaret för att skydda och stärka den kritiska infrastrukturen delas mellan den federativa nivån, delstatsnivån m.fl. och privata ägare och operatörer av kritisk infrastruktur.
Ett annat doktrinelement är att denna ansvarsprincip måste bygga på ett aktivt integrerat partnerskap mellan alla inblandade parter. Ett tredje doktrinelement är en ”all-hazard” ansats i kombination med en riskmanagement-ansats i alla faser av krisberedskapscykeln. Ett fjärde doktrinelement är att arbetet med skydd av kritisk infrastruktur ska vila på två ben: att stärka säkerheten mot antagonistiska hot respektive att stärka den inneboende tekniska och organisatoriska robustheten hos den kritiska infrastrukturen. Härnäst ska de mest central direktiven, handlingsplanerna m.m. presenteras:

“President Policy directiv – Critical Infrastructure Security and Resilience” (PPD-21). Direktivet sätter ramarna för en nationell policy för säkerhet och resiliens och uppmanar till en uppdatering av det rådande nationella infrastrukturprogrammet från 2009 mot bakgrund av förändrad hotbild, teknikutveckling m.m. Direktivet fastlägger att ansvaret att arbetet med säkerhet och resiliens för kritisk infrastruktur är ett delat ansvar mellan den federala nivån, delstatsnivån, den lokala nivån, stam- och territoriumenheter samt offentliga och privata ägare eller operatörer av kritisk infrastruktur.

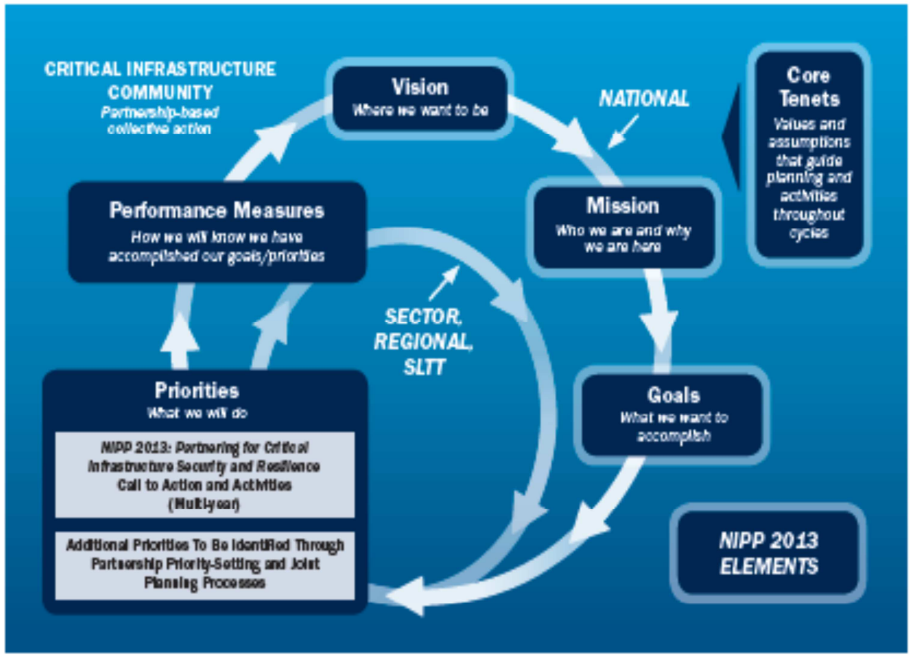
Direktivet fastlägger också ansvar, roller, sektorsindelning och samordning på den federala nivån för arbetet med kritisk infrastruktur. Bland annat ska två nya centra inrättas för bättre förmåga att integrera och analysera hot och risker kopplade till cyberinfrastruktur och fysisk infrastruktur samt en förbättrad förmåga till incidentövervakning. Direktivet ger besked om att utveckla och förbättra det rådande privat-offentliga samarbetet så att de privata aktörerna får mer ut av att samarbete med myndigheterna. Avslutningsvis ger direktivet bland annat också besked om att förbättra och underlätta informationsutbyte om kritisk infrastruktur på den federala nivån.

President direktiv *”National Preparedness” (PPD-8)* är ett inriktningsbeslut för att skapa en säker och robust nation med förmåga över hela samhället att förebygga, skydda, mildra, hantera och återhämta sig från allvarliga hot. Presidentens *”Climat Action Plan”* från 2013 lägger fast ett antal strategiska mål och anvisar federala myndigheter att bättre förbereda sig för klimatförändringar, inklusive stärka robustheten i kritisk infrastruktur.

"Executive Order 13636, Improving Critical Infrastructure Cybersecurity". Detta inriktningsbeslut uppmannar federala departement och myndigheter att bättre samverka med privata ägare och operatörer av kritisk infrastruktur för att förbättra informationsdelning och att i samarbete utveckla och verkställa en riskbaserad ansats vad gäller cybersäkerhet kopplat till deras fysiska anläggningar, system etc.

"National Infrastructure Protection Programme 2013 (NIPP 2013): Partnering for Critical Infrastructure Security and Resilience" är en uppdatering av versionen från 2009. NIPP 2013 lägger fast det övergripande strategiska arbetet med att förbättra säkerheten och robustheten för landets kritiska infrastruktur. Det handlar bland annat om visioner, uppdrag och mål för arbetet (se figur nedan)

Figure 1 – The National Plan's Approach to Building and Sustaining Unity of Effort



Vision

A Nation in which physical and cyber critical infrastructure remain secure and resilient, with vulnerabilities reduced, consequences minimized, threats identified and disrupted, and response and recovery hastened.

Mission

Strengthen the security and resilience of the Nation's critical infrastructure, by managing physical and cyber risks through the collaborative and integrated efforts of the critical infrastructure community.

Goals

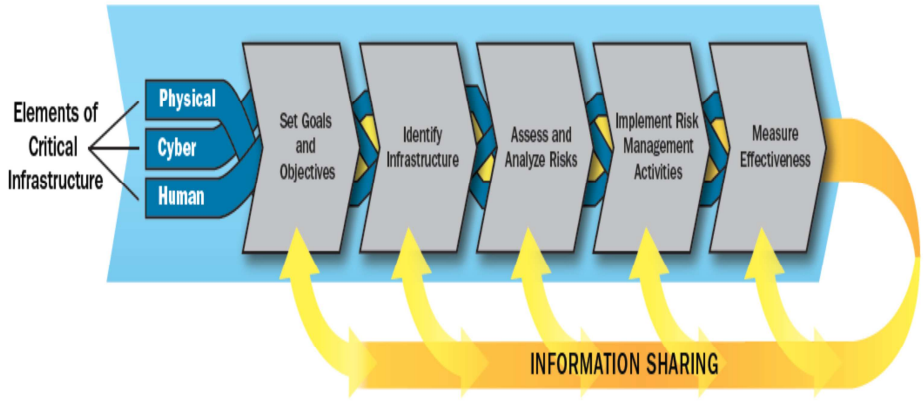
- Assess and analyze threats to, vulnerabilities of, and consequences to critical infrastructure to inform risk management activities;
- Secure critical infrastructure against human, physical, and cyber threats through sustainable efforts to reduce risk, while accounting for the costs and benefits of security investments;
- Enhance critical infrastructure resilience by minimizing the adverse consequences of incidents through advance planning and mitigation efforts, and employing effective responses to save lives and ensure the rapid recovery of essential services;
- Share actionable and relevant information across the critical infrastructure community to build awareness and enable risk-informed decision making; and
- Promote learning and adaptation during and after exercises and incidents.

Figur 23. USA:s modell över sitt strategiska upplägg för arbete med skydd av kritisk infrastruktur (NIPP 2013)

Som framgår av figuren ovan är visionen för USA:s del en nation i vilken kritisk infrastruktur, av både fysisk och cyber karaktär, uppvisar god säkerhet mot hot och är robust, sårbarheter och konsekvenser av hot och risker minskar, hot och risker identifieras och avvärjs samt att hanteringen och återställandet går skyndsamt. Uppgiften för berörda aktörer i samhället är att stärka säkerhet och robusthet i den kritiska infrastrukturen genom att via samarbete och integrerade ansträngningar hantera fysiska och cyberrelaterade hot och risker.

Mål är t.ex. att dela aktuell åtgärdsorienterad information mellan berörda aktörer i samhället för att möjliggöra välgrundat beslutsfattande när det gäller hot och risker rörande kritisk infrastruktur. Sammantaget, tämligen konventionella visioner, uppgifter och övergripande mål. I programmet slåss vidare fast förekomsten av en vidgad riskmiljö för kritisk infrastruktur och behovet därvid av en ”all-hazard”- och riskmanagment-ansats i arbetet. Riskmanagment-ansatsen illustreras i figuren nedan.

Figure 3 – Critical Infrastructure Risk Management Framework



Figur 24. USA:s ramverk för arbete med riskahantering (NIPP 2013)

Kärnvärderingar (Core Tenets) för arbetet som läggs fast för NIPP 2013 är t.ex. att risker ska identifieras och hanteras på ett koordinerat och allsidigt sätt mellan alla berörda aktörer i samhället för att möjliggöra ett effektiv utnyttjande av resurser för säkerhet och robust rörande kritisk infrastruktur. En mer allmän åtgärdsplan utan tidsmässiga hållpunkter presenteras i NIPP 2013 (se figur nedan)

Build upon Partnership Efforts:

1. Set National Focus through Jointly Developed Priorities
2. Determine Collective Actions through Joint Planning Efforts
3. Empower Local and Regional Partnerships to Build Capacity Nationally
4. Leverage Incentives to Advance Security and Resilience

Innovate in Managing Risk:

5. Enable Risk-Informed Decision Making through Enhanced Situational Awareness
6. Analyze Infrastructure Dependencies, Interdependencies, and Associated Cascading Effects
7. Identify, Assess, and Respond to Unanticipated Infrastructure Cascading Effects During and Following Incidents
8. Promote Infrastructure, Community, and Regional Recovery Following Incidents
9. Strengthen Coordinated Development and Delivery of Technical Assistance, Training, and Education
10. Improve Critical Infrastructure Security and Resilience by Advancing Research and Development Solutions

Focus on Outcomes:

11. Evaluate Progress toward the Achievement of Goals
12. Learn and Adapt During and After Exercises and Incidents

These actions will inform and guide efforts identified via the priority-setting and joint planning processes described below, as resources allow.

Figur 25. Åtgärdsplan enligt NIPP 2013.

Avslutningsvis, i NIPP 2013 fastläggs vilka aktörerna är i arbetet med att skydda och stärka USA:s kritiska infrastruktur och deras roller och ansvar.

Exempel på ytterligare program för kritisk infrastruktur är ”Regional Resiliency Assessment Program” (se avsnittet om Kanada), ”Protected Critical Infrastructure Information (PCII) Programme”Critical samt tidigare nämnda “United States-Canada Action Plan for Critical Infrastructure 2010”. Viktig att nämna i sammanhanget är också ”Infrastructure and Key Resources Support Annex”. Detta annex beskriver hur federala myndigheter, privata aktörer och frivilligorganisationer koordinerar och verkställer gemensamma fastlagda stödprocesser och administrativa uppgifter vid en kris. Procedurerna som beskrivs i annexet är generellt giltiga oavsett typ av kris.

Underlag

US. Department of Homeland Security, hemsida: www.dhs.gov

NIPP 2013: Partnering for Critical Infrastructure Security and Resilience. Homeland Security 2013.

Canada-United States Action Plan for Critical Infrastructure 2010. Public Safety Canada/US Homeland Security 2010.

Office of Infrastructure Protection Strategic Plan: 2012-2016. National Protection and Programs Directorate, Homeland Security 2012.

Presidential Policy Directive (PPD-21) – Critical Infrastructure Security and Resilience, 2013.
(http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil)

Critical Infrastructure Resilience: The Evolution of Policy and Programs and Issues for Congress. Congressional Research Service, John D. Moteff, 2012.

Power Point presentation: *National Infrastructure Protection Plan*. R. James Caverly, Homeland Security, 2010.

National Infrastructure Protection Plan Sector Partnership Model. Hemsida: http://www.dhs.gov/xlibrary/assets/NIPP_SectorPartnership.pdf

Bilaga 1: Program

Program och programmyndigheter

Program Delprogram	*Omfattning* Programmen omfattar frågor rörande försörjningen med:	*Programmyndighet*
1.	2.	3.
1. Livsmedel		Statens jordbruksnämnd
1.1 Livsmedel, fodermedel m. m.	Livsmedel, fodermedel, utsäde och fettråvaror	
1.2 Gödsel- och bekämpningsmedel	Handelsgödsel- och bekämpningsmedel	
2. Beklädnad	Beklädnads-, övriga textil- och lädervaror	Överstyrelsen för ekonomiskt försvar
3. Energi		
3.1 Bränslen och drivmedel m. m.	Bränslen och drivmedel utom gasbensin	Överstyrelsen för ekonomiskt försvar
3.2 Elkraft	Elektrisk energi	Statens vattenfallsverk
4. Övriga försörjningsviktiga varor		Överstyrelsen för ekonomiskt försvar
4.1 Kemiska produkter m. m.	Andra mineraler än metaller, trävaror, massa, papp och papper, grafiska produkter, gasbensin, gummi- och plastvaror samt övriga kemiska produkter dock ej läkemedel.	[1]
4.2 Metaller m. m.	Malmer, järn, stål och andra metaller samt verkstadsprodukter dock ej sjukvårdsmateriel	
5. Transporter	Transporter samt konsumtionsbegränsning av flytande drivmedel.	
5.1 Transportsamordning		Transportnämnden
5.2 Järnvägstransporter		Statens järnvägar[2]
5.3 Landsvägstransporter		Transportnämnden
5.4 Vägar		Statens vägverk
5.5 Flygtransporter		Luftfartsverket
5.6 Sjötransporter		Sjöfartsverket
6. Tjänster		
6.1 Arbetskraft	Civil arbetskraft	Arbetsmarknadsstyrelsen
6.2 Penningmedel och betalningsförmedling	Penningmedel och betalningsförmedling	Riksbanken
6.3 Postal kommunikation	Postala tjänster	Poststyrelsen
6.4 Ledning och samordning	ÖEF:s ej programanknutna verksamhet	Överstyrelsen för ekonomiskt försvar

Bilaga 2: Funktioner

Verksamheten inom totalförsvarets civila del var indelad i samhällsfunktioner med en funktionsansvarig myndighet (FAM). I beredskapsplaneringen vidtogs åtgärder för att motverka sårbarheten inom respektive samhällsområde. Planeringen genomfördes av de funktionsansvariga myndigheterna. En viktig uppgift för dem var att identifiera problemområden i detta avseende. Förutom de funktionsansvariga myndigheterna fanns i flera fall även andra myndigheter med uppgifter inom funktionen. Nedan framgår indelningen år 1990.

Samhällsfunktion	Ansvarig myndighet
Civil ledning och samordning	Överstyrelsen för civil beredskap
Domstolsväsende	Domstolsverket
Ordning och säkerhet med mera	Rikspolisstyrelsen
Kriminalvård	Kriminalvårdsstyrelsen
Utrikeshandel	Kommerskollegium
Befolkningsskydd och räddningstjänst	Statens räddningsverk
Psykologiskt försvar	Styrelsen för psykologiskt försvar
Socialförsäkringar med mera	Riksförsäkringsverket
Hälso- och sjukvård med mera	Socialstyrelsen
Postbefordran	Postverket
Betalningsväsende	Riksbanken
Telekommunikationer	Televerket
Transporter	Transportrådet
Försäkringar	Försäkringsinspektionen
Skatte- och uppbördsväsende	Riksskatteverket
Prisreglering	Statens pris- och konkurrensverk
Skolväsende	Skolöverstyrelsen
Livsmedelsförsörjning med mera	Statens jordbruksnämnd
Arbetskraft	Arbetsmarknadsstyrelsen
Flyktingverksamhet	Statens invandrarverk
Landskapsinformation	Lantmäteriverket
Energiförsörjning	Statens energiverk
Försörjning med industrivaror	Överstyrelsen för civil beredskap
Kyrklig beredskap	Överstyrelsen för civil beredskap

Bilaga 3: Samverkansområden

Samverkansområden (SO)	Myndigheter med särskilt ansvar inom SO
Teknisk infrastruktur	Affärsverket svenska kraftnät Elsäkerhetsverket Livsmedelsverket MSB Post- och telestyrelsen Statens energimyndighet
Transporter	Luftsfartsverket Sjöfartsverket Statens energimyndighet Trafikverket Transportstyrelsen
Farliga ämnen	Folkhälsomyndigheten Kustbevakningen Livsmedelsverket MSB Rikspolisstyrelsen Socialstyrelsen Statens jordbruksverk Statens veterinärmedicinska anstalt Strålsäkerhetsmyndigheten Säkerhetspolisen Tullverket
Ekonomisk säkerhet	Finansinspektionen Försökringskassan Pensionsmyndigheten Riksgälskontoret Skatteverket
Geografiskt områdesansvar	Länsstyrelserna MSB

Myndigheten för samhällsskydd och beredskap
651 81 Karlstad Tel 0771-240 240 www.msb.se
Publ.nr MSB841 – Mars 2015 ISBN 978-91-7383-563-3