CRN REPORT

Focal Report 4

Critical Infrastructure Protection

Protection Goals

Zurich, February 2010

Crisis and Risk Network (CRN)
Center for Security Studies (CSS), ETH Zürich

Commissioned by the Federal Office for Civil Protection (FOCP)

CRN
Supported by ISN

ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Purpose: As part of a larger mandate, the Swiss Federal Office for Civil Protection (FOCP) has tasked the Center for Security Studies (CSS) at ETH Zurich with compiling 'focal reports' (Fokusberichte) on critical infrastructure protection and on risk analysis to promote discussion and provide information about new trends and insights.

Authors: Elgin Brunner, Myriam Dunn Cavelty, Jennifer Giroux, Manuel Suter

Contact:
Center for Security Studies
ETH Zürich
Haldeneggsteig 4, IFW
CH-8092 Zürich
Switzerland
Tel.: +41-44-632 40 25

crn@sipo.gess.ethz.ch
www.crn.ethz.ch

Contracting entity: Federal Office for Civil Protection (FOCP)
Project lead FOCP: Stefan Brem, Head Risk Analysis and Research Coordination
Contractor: Center for Security Studies (CSS), ETH Zurich
Project supervision ETH-CSS: Myriam Dunn, Head New Risks Research Unit, Andreas Wenger, Director CSS

TABLE OF CONTENTS

1 INTRODUCTION

1.1 Focal Reports: The Task

In support of Switzerland's critical infrastructure protection (CIP) efforts and CIP strategy development, the Swiss Federal Office for Civil Protection (FOCP) has tasked the Center for Security Studies (CSS) at ETH Zurich with producing focal reports (*Fokusberichte)* on critical infrastructure protection.

These focal reports are compiled using the following method: First, a 'scan' of the environment is performed with the aim of searching actively for information that helps to expand and deepen the knowledge and understanding of the issue under scrutiny. This is a continuous process based on the following sources:

- *Internet Monitoring*: New publications and documents with a) a general CIP focus and b) a focus on scenarios with specific importance for the FOCP are identified and collected.
- *Science Monitoring*: Relevant journals are identified and regularly evaluated (with the same two focal points as specified above).
- *Government Monitoring*: The focus is predominantly on policy developments in the United States, Canada, Sweden, Norway, Germany, the Netherlands, and the United Kingdom as well as other states in the European vicinity that are relevant to Switzerland.

Second, the material collected is filtered, analyzed, and summarized in the focal reports.[1]

1 Previous focal reports can be downloaded from the website of the Crisis and Risk Network CRN (*http://www.crn.ethz.ch*).

1.2 Protection Goals in Critical Infrastructure Protection

For this focal report, we were tasked with analyzing *protection goals* in the area of CIP – a topic that is largely absent from the scientific-academic as well as the more practically oriented CIP literature. In this report, we use the 'Schutzziel Modell' (Protection Goals Model), published by the Swiss National Platform for Natural Hazards (PLANAT) in 2009, as a starting point for our theoretical-conceptual analysis. It introduces a model for developing unified protection goals in the natural hazards domain.[2] As we consider this document to be of generic value for the discussion, we will briefly summarize its content.

The PLANAT document emphasizes that the main prerequisites for a protection goal model are the determination of a) the objects/assets to be protected, b) the identification of areas of responsibility with regard to their protection, c) the clarification of what conditions the protection goals need to meet, and d) what general principles these conditions adhere to:[3]

a) Objects to be protected: The PLANAT document designates human life and welfare as the paramount asset to be protected, followed by protection of animals and substantial material assets (which contains infrastructures as a sub-category).

b) *Responsibilities*: Individuals can assume that state institutions (or other official bodies) limit certain risks due to legal requirements or generally accepted social practices. Institutions, on the other hand, can expect potentially affected parties to take their own precautions when it is their own re-

2 Nationale Plattform Naturgefahren PLANAT (2009), Schutzziel-Modell. *http://www.planat.ch/ressources/planat_product_de_1261.pdf*.

3 PLANAT, pp. 1-11.

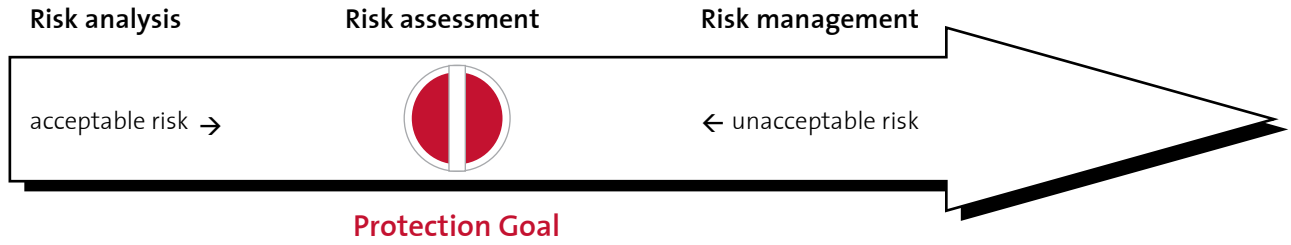

Figure 1: Role of protection goals in the risk analysis process

sponsibility. A central prerequisite for this 'division of labor' is full transparency and communication about who is responsible when and for what.

c) *Requirements*: According to PLANAT, protection goals have to meet certain conditions, for example: practical, scientific-technical, ethical, legal, economic, social, and environmental requirements.

d) *Principles*: Protection goals are tied to decisions with potentially substantial political/social consequences, for example about human lives. They must therefore be inferred in a transparent and comprehensible way. In addition, they must have a high degree of democratic legitimacy. PLANAT also lists the two guiding principles of due diligence and sustainability.

The last point is closely related to the function that the PLANAT document attributes to protection goals – stating that, in theory, protection goals provide guidance for when specific measures need to be taken because they help to differentiate acceptable risks from unacceptable risks. In this respect, they are a threshold value in the risk analysis and risk management process. Figure 1 illustrates this use of protection goals in the risk management cycle[4]:

Understood this way, protection goals are numerical boundary values related to indicators (such as number of [acceptable] human deaths or monetary damage) and identifiable objects in need of protection from specific threats/hazards. The PLANAT document also delineates the probability values (the probability that severe damage will result).[5]

In short, the PLANAT protection goal model aims to develop measurable, numeric protection goals that help to specify acceptable and unacceptable risks in the risk management process. While such measures might exist for specific installations (such as dams or power plants), it is futile to adopt a similar model to CIP as a whole. The reason is that most CIs are interdependent and embedded in a highly complex environment, which makes the quantification of risks extremely difficult to achieve, if not outright impossible. However, the model (and specifically the various concepts behind it) can be used as a loose framework for the comparison and analysis of protection goals in CIP practices.[6]

4 PLANAT, p. 1.

5 PLANAT, p. 13.

6 The usability of the PLANAT model is described in more detail in an additional document: "Grenzen und Möglichkeiten der Übertragbarkeit des Schutzziel-Modells (PLANAT, Mai 2009) auf den Bereich Schutz kritischer Infrastrukturen: Kurzabhandlung des Center for Security Studies (CSS) zuhanden des Bundesamts für Bevölkerungsschutz (BABS)".

1.3 Structure and Content of Focal Report

Guided by the basic assumptions described in the PLANAT protection goal model, this report will explore the manner in which protection goals are defined in CIP. In doing so, we will identify and analyze the protection goals in various countries and address the following questions based on the empirical analysis:

- What protection goals do states define in the practice of CIP?
- What purpose do they serve?
- What aspects do they cover?
- Who defines them?

In conclusion, we will discuss what seems to be missing from the CIP discussion: how applicable and useful are protection goals for CIP and what aspects they should cover.

The report has three parts:

- The first part examines how protection goals are handled in eight countries: Australia; Canada; Germany; Netherlands; Norway; Sweden; the United Kingdom; and the United States.
- The second part strives to evaluate these practices with regards to the above questions and compare them to the PLANAT model.
- The third part is the annex, containing a) excerpts sketching the protection goals in the policy documents analyzed and b) an annotated bibliography.

2 CRITICAL INFRASTRUCTURE PROTECTION GOALS IN COMPARISON

This chapter identifies and compares the protection goals in critical infrastructure protection (we abbreviate them by using CIPG) delineated in official documents released by Australia, Canada, Germany, the Netherlands, Norway, Sweden, the United Kingdom (UK), and the United States (US). The analysis revealed that there is no universal understanding or use of the term 'protection goal' or a related concept. In order to overcome this difficulty, we developed our own working definition of protection goals (loosely based on the definition given by the PLANAT document) that is drawn from a first reading of the policy documents as well as our previous expertise. Within the literature we looked for statements that identified one or all of the below:

- an object to be protected;
- the type of threat to which these objects are subject;
- the means by which these objects are to be protected.

In this regard, we used the following loose definition of 'protection goal' in CIP to identify the relevant content:

➡ *A protection goal is a statement about a desired (or required) state of protection and operation of a system (or parts of a system) against one or a variety threats.*

The analysis showed that there are CIPG *constructs* on three hierarchically distinguishable levels. Not surprisingly, CIPGs become more concrete the further down one moves:

- First, protection goals are described on a strategic level – linked to national security strategy documents.
- Second, protection goals are described in CIP strategies or similar documents.
- Third, sector-specific CIP documents strive to further define and specify protection goals.

In the following, we address the CIPGs on these three levels. We therefore use a very broad understanding of protection goals. Table 1 summarizes the availability of documents on these three levels for the countries that we scrutinized. Please refer to Annex A for the relevant text excerpts.

	'Protection Goals' in National Security Strategy	CIP Strategy (with Protection Goals)	Sector-Specific Protection Goals
Australia		X	(x) IT
Canada	x	X	
Germany		X	(x) IT
Netherlands	x	X	
Norway		X	(x) IT
Sweden			(x) IT
United Kingdom	x	X	
United States	x	X	x all sectors

Table 1: Availability of documents on three levels of Protection Goals

2.1 Level 1: National Security Strategies

Today, CIP is considered part of national security in most countries. Canada, the Netherlands, the United Kingdom (UK), and the United States (US) have national security strategies that contain CIPG on a strategic level. As is to be expected, these 'goals' are generally vague, all-embracing, and fairly abstract.

At the highest strategic level, the US references the protection of critical infrastructures in its *National Strategy for Homeland Security*. The document calls for the 'Protection of the American people, our critical infrastructures, and key resources'[7] and outlines three specific goals for critical infrastructures protection: deter the terrorist threat; mitigate the vulnerabilities; and minimize the consequences. Furthermore, this document singles out the *National Infrastructure Protection Plan* (NIPP) – developed pursuant to the *Homeland Security Presidential Directive-7* – as the main guidance for the efforts to protect critical infrastructures. The NIPP is designated within this national strategy as the tool to 'ensure that our government, economy, and public services continue to function in the event of a man-made or natural disaster.'[8] As elaborated in section 2.3 below, this task is carried out through sector-specific plans developed within identified critical infrastructures and key resources.

Turning to the Netherlands where the national security strategy states that its goal is to protect the 'vital interests of the Netherlands in order to prevent societal disruption'.[9] In this case, CIP is seen as the operational tool to ensure this. *The Dutch National Security Strategy* depicts CIP as risk management and positions it on a par with crisis management; the two concepts together cover the operational aspects of security, while national security covers the strategic aspects. Moreover, it specifies that 'with critical infrastructures the emphasis is primarily on prevention (measures for better security of the critical sectors), while with crisis management the emphasis is on preparation (preparation for incidents), response (if an incident has occurred) and after-care.'[10]

While the Dutch strategy locates critical infrastructure protection in to the context of both national security and crisis management, Canada and the United Kingdom view critical infrastructure vulnerability and its protection as a main challenge of emergency management. The UK, for example, defines it as the 'single overarching national security objective' to protect 'the United Kingdom and its interests, enabling its people to go about their daily lives freely and with confidence, in a more secure, stable, just and prosperous world'.[11] Furthermore, the British national security strategy identifies critical infrastructures among the key assets to be protected, stating the goal as 'to improve the protection of critical infrastructures, hazardous sites and materials, and crowded places'.[12]

These examples reveal the interrelationship between national security and CIP. In the former, national security is often described as being in some way related to ensuring the continuity of life, while in the latter CIP is the way to ensure this on an operational level. In other words, because critical infrastructures are

7 Homeland Security Council (2007), National Strategy for Homeland Security, p. 1.

8 Homeland Security Council (2007), op. cit., p. 26.

9 Ministry of the Interior and Kingdom Relation (2007), National Security Strategy and Work Programme 2007-2008, p. 16.

10 Ministry of the Interior and Kingdom Relation (2007), op.cit., p.13.

11 Cabinet Office (2008), The National Security Strategy of the United Kingdom. Security in an interdependent world, p. 5.

12 Cabinet Office (2008), op. cit., p. 26.

regarded as the 'fabric of society', the protection of society is equated with the protection of CI. This has several implications for protection goals: a) Because CIP is – among other things – a national security issue, there is a level of secrecy when it comes to concrete aspects such as protection goals; b) as noted in the PLANAT document, protection goals are directly linked to human life. The stakes are thus very high. If the security of entire nations depends on CIP measures, then protection goals in CIP are – or should have to be – top-level strategic-political decisions. This is an important aspect that will be addressed in some more detail below.

2.2 Level 2: CIP Strategies

Similar to national security strategies, CIPGs formulated in CIP strategy papers (usually at the national/federal level) tend to be very general. For instance, rather than providing specific mandates or (measurable values) they offer guiding principles or mission statements. With that said, on the second level, more information can be found about the objects to be protected, the measures, and the threats.

There are many similarities between CIP strategy documents and one common element is the importance of the concepts of resilience and of public-private partnerships, in different combinations. For example, the overarching goal of the United States' *National Infrastructure Protection Plan* (NIPP), one of the more elaborate strategies, is to "build a safer, more secure, and more resilient America by preventing, deterring, neutralizing, or mitigating the effects of deliberate efforts by terrorists to destroy, incapacitate, or exploit elements of our Nation's CIKR [Critical Infrastructures and Key Resources] and to strengthen national preparedness, timely response, and rapid recovery of CIKR in the event of an attack, natural disaster, or other emergency."[13] Similarly, in Canada, the document *Working Towards a National Strategy and Action Plan for Critical Infrastructure: Strategy* (2008) highlights the importance of enhancing resilience as a 'quasi' critical infrastructure protection goal 'that can be achieved through the appropriate combination of security measures to address human induced intentional threats; business continuity practices to deal with disruptions and ensure the continuation of essential services; and emergency planning to ensure adequate response procedures are in place to deal with unforeseen disruptions to critical infrastructure.'[14] Furthermore, this document reveals that partnerships, risk management, and information-sharing are viewed as key components of CIP. In Australian official documents, the stated CIPGs are: 'to identify critical infrastructure, analyze vulnerability, and interdependence, and protect Australia from and prepare for, all hazards.'[15]

Some of the strategies delegate the definition of CIPGs to specific bodies. In Australia, for instance, the Trusted Information Sharing Network for Critical Infrastructure Protection (TISN) – a collaborative platform – brings public and private owners and operators of critical infrastructure together to build relationships, exchange information, and articulate protection goals and methods for analysis. In the United Kingdom, the Centre for the Protection of

13 Department of Homeland Security (2009), National Infrastructure Protection Plan. Partnering to enhance protection and resiliency, p. 1.

14 Her Majesty the Queen in Right of Canada (2009), National Strategy and Action Plan for Critical Infrastructure, Available at: http://www.publicsafety.gc.ca/prg/em/ci/_fl/ntnl-eng.pdf

15 Elgin M. Brunner and Manuel Suter (2008), International CIIP Handbook 2008/2009. An Inventory of 25 National and 7 International Critical Information Infrastructure Protection Policies, Center for Security Studies, ETH Zurich, p. 49.

National Critical Infrastructure (CPNI) operates in a comparable way.

Among the countries studied, Germany is an interesting and exceptional case**.** In the document *Schutz Kritischer Infrastrukturen – Risiko- und Krisenmanagement. Leitfaden für Unternehmen und Behörden* (2007), protection goals play an important role. The document differentiates between strategic and operational protection goals.[16] On the one hand, strategic protection goals are defined not in terms of what they are but by what they should achieve. Further, they are seen to be influenced by ethical, operative, technical, financial, social, and environmental aspects and must describe the nominal condition. This resonates with the PLANAT model and its statement that protection goals must live up to a variety of requirements.[17] So to allow for evaluation, the goals, as formulated by the German strategy paper, are supposed to be specific, measureable, implementable, realistic, and time-phased.[18] Operational protection goals, on the other hand, are meant to help with the implementation of protection measures. The same document also delivers examples of protection goals, including: the best possible protection of personnel and other attendees; maintaining the functionality of an infrastructure in extreme situations; compliance with legal requirements; avoidance of high economic costs; avoidance of a potential image loss.[19] These details are by far the most elaborate that we were able to identify in the field of CIP – further research into how these ideas are being implemented could be very beneficial for the Swiss CIP strategy process.

2.3 Level 3: Sector-Specific Protection Goals

More tailored protection goals – very often tied specifically to definition and implementation of protection measures – can be found in sector-specific CIP plans. The United States (US) is the only country pursuing a comprehensive sector-specific protection approach – articulated in the 2006 (and updated version of 2009) *National Infrastructure Protection Plan* (NIPP), which provided the first road map for protection of the 18 critical infrastructure/key resources (CIKR).[20] Using a risk management framework, public and private agencies are required 'to prioritize protection activities within and across the sectors in an integrated, coordinated fashion.' In addition, sector-specific federal agencies[21] became responsible for coordinating CIP efforts with relevant public and private stakeholders and developing sector-specific plans. Thus far, nine plans have been made available in the following areas: agriculture and food, banking and finance, communication, defense industrial base, energy, information technology, national monuments and icons, transportation systems, and water. In all of the sectors discussed, the respective plans list specific implementation measures used to achieve the goals.[22]

16 Bundesministerium des Innern (2007), Schutz Kritischer Infrastrukturen – Risiko- und Krisenmanagement. Leitfaden für Unternehmen und Behörden, p. 14. Available at: *http://www.bbk.bund.de/cln_027/nn_398734/SharedDocs/Publikationen/Publikationen_20Kritis/Leitfaden__Schutz-Kritis.html*

17 PLANAT, pp. 9f.

18 Bundesministerium des Innern (2008), p. 15.

19 Bundesministerium des Innern (2008), op.cit., p. 16.

20 Homeland Security Presidential Directive 7: Critical Infrastructure Identification, Prioritization, and Protection. Available at: *http://www.dhs.gov/xabout/laws/gc_1214597989952.shtm.*

21 For a complete list of the sector-specific agencies, see the National Infrastructure Protection Plan, p. 19. Available at: *http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf.*

22 Other plans can be retrieved at *http://www.dhs.gov/files/programs/gc_1179866197607.shtm*.

All sector plans share a common framework (see Figure 2);[23] however, they also allow for flexibility and encourage customization. The water sector, for example, has developed the following main goals:[24] 1) sustain protection of public health and the environment; recognize and reduce risks in the water sector; 2) maintain a resilient infrastructure; 3) increase communication, outreach, and public confidence.[25] At first glance, these goals again appear to be rather general. However, more information can be found in the implementation efforts. For instance, to achieve goal 1, the 'Water Security Initiative' and 'Water Laboratory Alliance' were designed to detect water contamination, the former serving as a warning system.[26] In goal 2, measures include performing risk assessment to carrying out a consequence analysis project that aims to help improve security.[27]

In the United Kingdom (UK), which has 9 identified sectors, there are sector-specific plans, but they are not publicly available, according to a CPNI expert. Each sector is allocated the task of identifying critical assets to protect as well as the mandate to formulate tailored plans to protect those assets, with the overarching goal to reduce vulnerability in the sector. In the Netherlands, there is no indication that sector-specific plans exist, however, each sector defines and implements its own protection policies, which seems to indicate that bottom-up efforts to develop protection goals are encouraged. Similarly, Germany does not define specific protection goals outside of calling for prevention, reaction, and sustainability of its critical infrastructure (and outside of the very general framework provided in its document *Schutz Kritischer Infrastrukturen)*. Despite this, it has, like some countries, identified an extensive list of CI sectors and subsectors that should be protected. Though Germany does not define the protection goals of specific sectors in great detail, the extent to which it has outlined the varying sectors, sub-sectors, and the critical IT-dependent systems within each sector points to some underlying effort to create more customized protection goals.

NIPP SSP framework

- identify priority CIKR and functions within the sector
- assess sector risks
- assess and prioritize assets, systems, and networks
- develop detailed, sector-specific risk-mitigation programs
- provide protocols for the transition between steady-state —CIKR protection and incident response in an all-hazards environment
- use metrics to measure and communicate program effectiveness and risk management progress
- address R&D requirements and activities
- identify the process used to promote cooperation and information-sharing within the sector.

Figure 2

The IT sector is the one sector for which we find sector-specific protection goal efforts in countries other than the US. For instance, Germany emphasizes the importance of the information infrastructure, as illustrated in the 2005 *Nationaler Plan zum Schutz der Informationsinfrastruktur* (NPSI) and the subsequent 2007 report *Umsetzungsplan KRITIS*. For the

23 http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf.

24 http://www.dhs.gov/xlibrary/assets/nipp-ssp-water.pdf.

25 Ibid., pp. 65ff.

26 Ibid., p. 65.

27 Ibid., p. 66.

IT sector, the CIP Implementation Plan in Germany (UP KRITIS)[28] contains protection goals. Aside from prevention, reaction, and sustainability, the protection goals in this sector are identified as ensuring the availability, integrity, and confidentiality of information and information technology. The same goals are defined in Norwegian and Swedish documents. For instance, the *Information Security in Sweden – Situational Assessment 2009* defines information security 'as the ability to maintain the desired level of confidentiality, integrity and availability when handling information.'[29] Comparably, in Norway, the National Guidelines to Strengthen Information Security 2007–2010 identified the same three protection goals in the area of information security.[30] As one would expect, these goals are congruent with the core concepts of information security, a field established long before CIP became a policy issue of high saliency.

28 *http://www.bmi.bund.de/cln_144/SharedDocs/Downloads/DE/Broschueren/DE/2007/Kritis.html* (in German)

29 Information Security in Sweden: Situational Assessment 2008, p. 13

30 The Norwegian Government, 2007. National Guidelines to Strengthen Information Security 2007–2010, Available at: *https://www.nsm.stat.no/Documents/KIS/Publikasjoner/National%20Guidelines%200n%20Information%20Security%202007-2010.pdf*.

3 EVALUATION AND IMPLICATIONS

In the following, we begin by analyzing in the form in which protection goals appear in publicly available documents, specifically identifying three types of protection goals (3.1). We further address the purpose that the protection goals serve and the aspects they cover (3.2). Linked to these conceptual analyses is the more practical aspect of who defines the CIPGs on which levels (3.3). In a final chapter (3.4), we briefly compare protection goals in CIP practices with the PLANAT-ideal type and in doing so take into consideration the applicability and usefulness of protection goals in CIP and the aspects they should cover.

3.1 Three Types of Protection Statements on three Levels of Strategy: Principles – Policies – Goals

The analysis of CIP documents covered in this report has shown that 'protection goals' vary with regard to their specificity and purpose. As we highlighted in the previous section, on the level of national security strategies and policy papers CIPG tend to use rather general terms such as 'prevention', 'mitigation of vulnerabilities', or 'protection of vital interests'. We believe it would be useful to label these kind of statements '*protection principles*' rather than protection goals, because they provide the general framework for CIP. For the purpose of this analysis *protection principles* are on level one.

On the second level, slightly more specific protection goals are found in CIP strategies. These goals, formulated for all CIs, can be described as '*protection policies*', as they generally define what must be protected from which threats and the method to do so. Comparably, these are more precise and specific than the protection principles but still follow a systemic-abstract logic as they refer to the totality of all CIs rather than to one sector or to one infrastructure. On this aggregated level, protection goals include examples like: 'identifying critical infrastructures and key resources', 'enhancing resiliency', or 'analyzing interdependencies and vulnerabilities'.

The third level is the sector-specific dimension where goals are defined. On this level, the CIPGs are more concrete. Examples include goals that aim to ensure 'the availability, integrity and confidentiality of information and information technology' or 'sustain protection of public health and the environment'. They may be referred to as (sector-specific) '*protection goals*'.

3.2 Purposes and Characteristics of CIPGs

Characteristics and purposes differ for each of the three identified levels. Protection principles, for instance, are formulated in national security strategies or policy papers and can provide guidance to the administrative bodies in charge of CIP by describing potential threats and risks as well as highlighting the necessity to tackle them. In addition, the national security strategies and policy papers provide the framework for the risk analysis and management processes. While they differ from the concept of protection goals as presented in the PLANAT model, protection principles are very important in a complex field such as CIP as they ensure a necessary level of coherence between different levels of government and help in developing measures to ensure security.

In order to analyze and manage the risks in CIP, protection principles need to be translated into less abstract concepts. This translation process happens on the second level, the level of protection policies. Protection policies specify what protection principles

such as 'prevention' or 'resilience' mean for CIP and identify means for identifying, assessing, and managing the risks to CI. Such protection policies state, for example, that prevention shall be improved by public-private collaboration or that the resilience of CI (understood as the entirety of CIs, not as individual infrastructures) shall be strengthened by information-sharing between the owners and operators of CIs. These policies are necessarily broad as it is not possible to determine criteria for all sectors of CIs: the differences are too big. But, at the same time, the interdependencies between the different CIs make a coherent approach indispensable. One sector cannot be secure if another sector on which it depends is not. The development of shared frameworks for risk analysis and management is a crucial step in CIP, as it allows the formulation of sector-specific protection goals without risking a loss of coherence within CIP as a whole.

That leads us to the third level of CIPGs on a sector-specific level where the goals need to be sufficiently specific to enable implementation (cf. the concept of operational protection goals in the German approach). On this level, there needs to be clarity with regards to the overall aim and purpose of protection efforts, including what risks to focus on. Therefore, these goals come closest to fitting the definition of

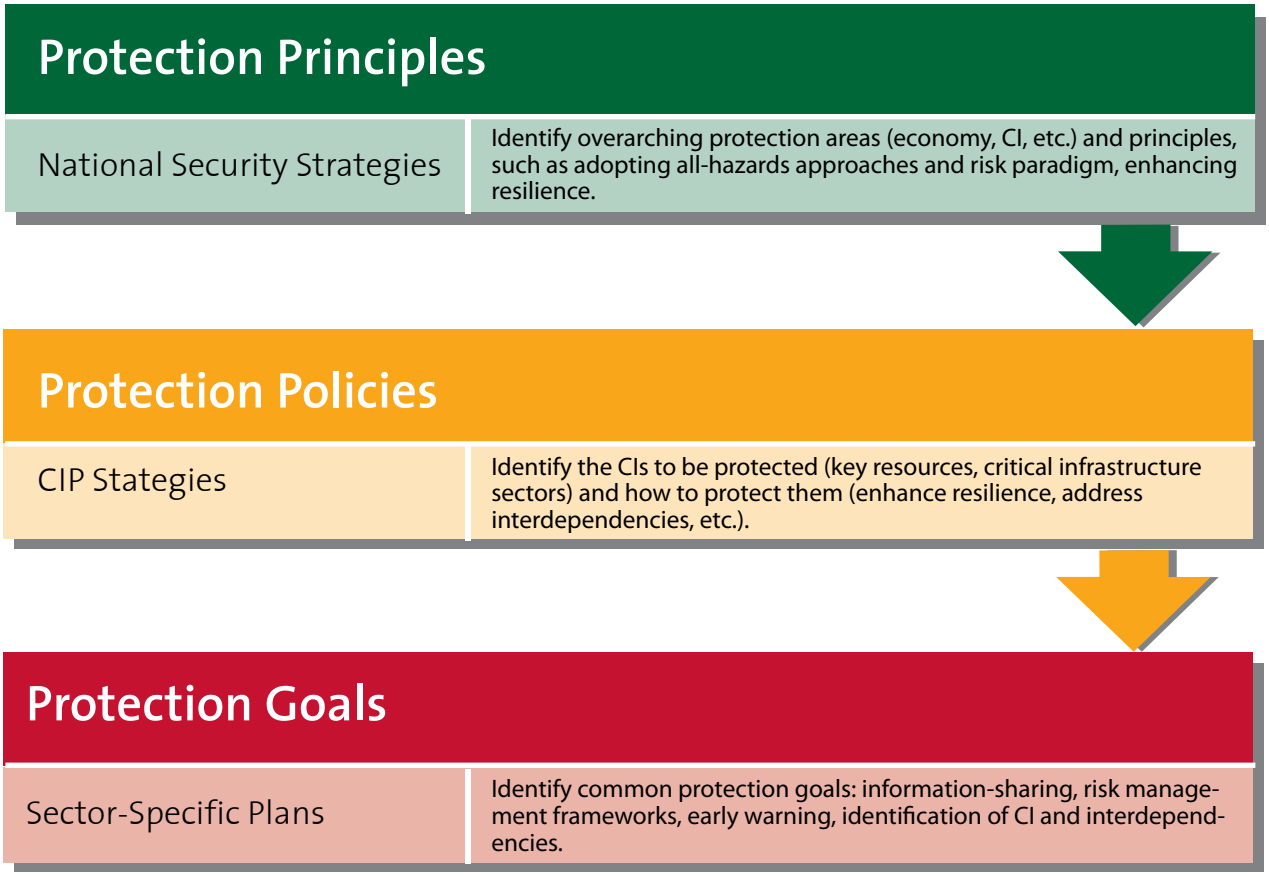

Figure 3

a protection goal as a threshold between acceptable and unacceptable risks, as specified in the PLANAT document. However, such a purpose demands a precise and quantitative (=numerical) definition of damage levels. Such metrics are lacking in the (public) CIP discussion. It is likely that they exist in some cases (for example, in the case of clearly identifiable assets such as nuclear reactors), but are not publicly available. It is also likely that in most cases such numerical values do not exist. In large and highly complex sectors such as the IT sector, such thresholds only make little sense. In addition, the processes of negotiation between public and private actors may hamper the formulation of clear-cut protection goals.

This hierarchy between the three levels and types of protection statements is illustrated in Figure 3.

3.3 Two Integrated Processes for Defining Protection Goals

From the above, it becomes clear that public and private actors play specific roles in the formulation of principles, policies, or goals. We can distinguish between two processes that lead to the definition of CIPGs. One the one hand, protection principles are formulated in political processes and formulated in national security strategies. On the other hand, sector-specific protection goals are formulated in collaboration with the owners and operators of CI. The function of protection policies is to connect these top-down and bottom-up processes (which cannot be regarded as being independent since they influence each other) and incorporate them into one coherent approach to CIP. More specifically, on all three levels CIPGs are usually the result of both political decisions and consultations with the private sector. However, public and private sectors have different responsibilities when it comes to protection goals. It is the role of the public actors to ensure that protection goals developed on the third level are in line with the protection principles and policies defined on the first and second levels. The private actors are responsible for ensuring that the protection goals are realizable and meaningful for the specific demands of their sector.

3.3.1 The Definition of Principles and Policies in Political Processes

Political decision-makers set general goals (=principles) for CIP and thereby guide the development of more specific protection goals. They also decide what needs to be protected from which threats and by which means.[31] The question of 'what needs to be protected' is a key question in CIP that is closely related to the definition of protection goals. The criticality of infrastructures depends on factors such as the importance for other infrastructures, for the national economy, or for society at large. However, these factors are difficult to quantify satisfactorily, so that the identification of CIs remains an inherently political decision. In consequence, the CI sectors and subsectors are often listed in strategy papers or government directives.[32]

Another political decision that affects the definition of protection goals is the question of which threats the CIs need to be protected from. The potential threat spectrum ranges from terrorist attacks to human error to technical failures and also includes natural hazards/disasters. To avoid turf battles among agencies, it is therefore crucial to address the dis-

31 Cf. Caudle (2009).

32 Such as, e.g: Department of Homeland Security (2003), Homeland Security Presidential Directive 7: Critical Infrastructure Identification, Prioritization and Protection.

cussion on sources of threats at the political level. In response to that need, many strategies and policy papers emphasize the importance of the 'all-hazards approach' in CIP.[33] This means that all relevant agencies need to be involved and that the concrete protection goals need to be formulated in a threat-neutral way.

Finally, there are also some decisions to be taken on the political level concerning the means by which a goal should be protected. This question is all the more important since many CIs are owned and operated by the private sector. Protection can only be achieved if all stakeholders act in concert. This means that specific protection goals should be defined in collaboration with the private sector. Such an empowerment of non-state actors is not a routine process and needs to be anchored in political decisions. Hence, many strategies explicitly highlight the need for collaboration with the private sector.[34] The principle of public-private collaboration is thus another important political decision that shapes the formulation of concrete protection goals for CIP.

3.3.2 The Definition of Protection Goals in Consultative Processes with Practitioners

As indicated above, decisions on the political level determine the room of maneuver for the definition of protection goals for CIP. However, these goals are not only influenced by top-down political decisions, but also by bottom-up consultations with the owners and operators of CIs.

The private sector influences the definition of protection goals in three different ways: First, the owners and operators of CI are represented in advisory boards for CIP and contribute directly to the development of national CIP policies. The best known historic example is the Advisory Committee to the President's Commission for Critical Infrastructure Protection (PCCIP), which was composed of 15 industry leaders and informed the work of the PCCIP.[35] Today, similar advisory bodies exist in many countries. Examples include the Strategic Board for CIP (SOVI)[36] in the Netherlands; the National Infrastructure Advisory Council (NIAC)[37] in the United States; or the Critical Infrastructure Advisory Council (CIAC)[38] in Australia. These advisory bodies are key actors in the development of CIP policies and thus have an important influence on the definition of general protection goals.

Secondly, private actors closely collaborate with sector-specific agencies to develop and implement protection goals for their individual sectors. While

33 Trusted Information Sharing Network for Critical Infrastructure Protection (2004), Critical Infrastructure Protection National Strategy, p. 9. Available at: http://www.tisn.gov.au/www/tisn/rwpattach.nsf/VAP/(427A90835BD17F8C477D6585272A27DB)~Critical_Infrastructure_Protection_National_Strategy.pdf/$file/Critical_Infrastructure_Protection_National_Strategy.pdf; Public Safety Canada (2009), Working Towards a National Strategy and Action Plan for Critical Infrastructure, p. 6. Available at: http://www.publicsafety.gc.ca/prg/em/ci/_fl/nat-strat-critical-infrastructure-eng.pdf.

34 The important role of public-private partnerships in CIP is not only articulated in the documents reviewed in this report, but also evident in the establishment of state-sponsored partnership platforms such as Australia's Trusted Information Sharing Network (TISN), the United Kingdom's Centre for the Protection of National Infrastructure (CPNI), and the United States Critical Infrastructure Partnership Advisory Council (CIPAC), Sector Coordinating Councils (SCC), and Government Coordinating Councils (GCC).

35 Kathi Ann Brown (2006), Critical Path. A Brief History of Critical Infrastructure Protection in the United States, George Mason University, pp.82ff.

36 https://www.navi-online.nl/content/24/SOVI+werkgroep (in Dutch).

37 http://www.dhs.gov/files/committees/editorial_0353.shtm.

38 http://www.tisn.gov.au/www/tisn/tisn.nsf/Page/Aboutthe-TISN_CriticalInfrastructureAdvisoryCouncil_CriticalInfrastructureAdvisoryCouncil.

such collaborations are well-established across most sectors and in most countries, they often remain informal and only rarely publish reports identifying sector-specific protection goals. The Sector-Specific Plans in the United States,[39] which are mandated by the National Infrastructure Protection Plan (NIPP) and publicly available, are an exception. These plans list the sector-specific goals and identify the partners that contributed to the development of these goals. Another example of a jointly developed sector-specific plan that includes protection goals is the CIP Implementation Plan in Germany (UP KRITIS)[40] for the IT sector.

The third way in which private actors influence the definition of protection goals consists of lobbying activity where industry groups try to shape CIP policies according to their interests. By talking to politicians or issuing white papers and press releases, lobbyists can advocate for the importance of their own sector and/or to push for government initiatives. For example, in its Information Security Policy Agenda 2007, the Information Technology Association of America (which is a leading industry group for United States IT and electronics businesses) writes that it is the organization's goal to 'ensure that cyber security is an integral part of critical infrastructure protection.'[41] Another example is the strong public support of the Australian Bankers' Association for the development of the Trusted Information Sharing Framework.[42]

3.4 Conclusion

The three-level model in combination with the description of the combined top-down/bottom-up process outlined above provides a useful framework for the definition and use of protection goals in critical infrastructure protection, as it ensures coherence between the CIPGs in different sectors and a sufficient level of specification of CIPGs within the individual sectors. Figure 4 outlines an ideal CIP framework for this process of defining CIPGs and identifies two areas of decision-making – the political level, where national security policy and CIP is first articulated, and the sector-specific level, where the public and private sectors come together to create more tailored protection objectives.

Beginning at the political level, protection goals are first identified at the highest strategic levels and articulated in a national security framework/strategy. In this phase, overarching protection principles and goals, such as the protection of critical infrastructure, are addressed. The next step is the creation of CIP strategies where specific sectors and sub-sectors are highlighted and protection principles (such as promoting information-sharing, utilizing a risk framework, creating public-private partnerships, etc.) are applied and further refined. This step leads to a process of policy transfer, with CIPGs developed at the political level and applied at the sector-specific level where public agencies and CI operators in the private sector interact and exchange. The sector-specific level is where protection goals become customized based on the particular needs of an identified CI sector – resulting in the construction of sector-specific plans. At this stage, the role of the private sector is to manage CI, liaise with the public sector, and articulate goals and measures to achieve protection. Within the public sector, specialized agencies work to commu-

39 http://www.dhs.gov/files/programs/gc_1179866197607.shtm.

40 http://www.bmi.bund.de/cln_144/SharedDocs/Downloads/DE/Broschueren/DE/2007/Kritis.html (in German).

41 http://www.itaa.org/upload/infosec/docs/ITAA%20Info-Sec%20Public%20Policy%20Agenda%202007_FINAL.pdf.

42 http://www.bankers.asn.au/Critical-Infrastructure-Protection-Cybercrime-Submission-Lodged/default.aspx.

nicate federal mandates to CI operators and create platforms for information-sharing and partnerships.

While the CIP framework described herein points to a traditional top-down process – with the top level setting the agenda – there are bottom-up forces that inform the political level, creating feedback loops. At both levels, a broader informing environment provides insights and influence to those identifying goals and means of protection, for example. This informing environment includes public officials and local/regional state agencies as well as those operating in the private sector and in academia/think-tanks. Overall, this framework exemplifies a dynamic, interactive process where each sphere of influence has a key role to play in defining and refining protection goals.

If protection goals are to be defined for the Swiss CIP strategy, they should be oriented towards what we called 'protection policies', which help to translate protection principles into less abstract concepts. It is the role of the FOCP, as the coordinating body, to ensure that future protection goals developed in sectors and sub-sectors and the protection principles and policies are in line with each other. The working definition of protection goals (to be found in the document "Grundstrategie des Bundesrates zum Schutz Kritischer Infrastrukturen: Basis für die nationale Strategie zum Schutz Kritischer Infrastrukturen", May 2009 [and approved by the Federal Council in June 2009] www.infraprotection.ch) adopts a very similar understanding.[43] The downside of vague protection goals is that it becomes more difficult to 'measure' the success of protection measures. It is, however, not impossible: The quality of information exchange in public-private partnerships or the level of resilience are examples of how success in critical infrastructure protection can be measured.

43 "The protection goals describe the level of security to be attained and financed and determine the respective protective measures. The protection goals themselves are not absolute and depend on the security policy situation. General protection goals may be inferred from the status report, while specific protection goals must be agreed for each infrastructure sector (e.g., minimum level of power supply in the energy sector). They depend on the nature of the infrastructure and its criticality" (p. 2). However, because protection goals are necessarily vague in CIP, it does not make sense to change them in the case of 'exceptional situations' (e.g., war) (as stated in the same document). The goal of CIP is to ensure that the necessary level of services is upheld regardless of the type and level of threats in the environment – and at all times.

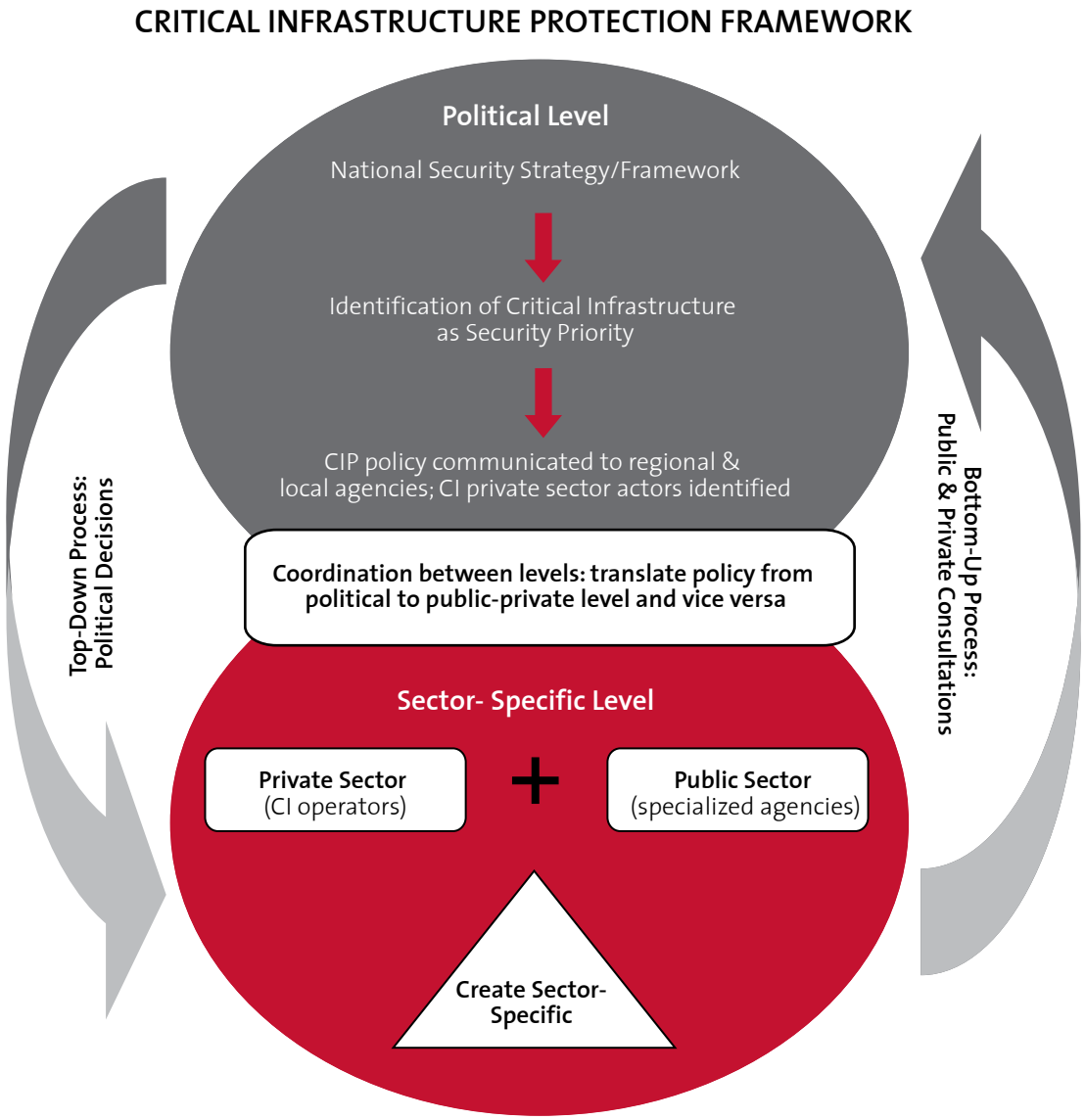

Figure 4: CIP Framework

4 ANNEX

4.1 Protection Goals (Texts)

	'Protection Goals' in National Security Strategy	Official CIP Strategy (with Protection Goals)	Sector-Specific Protection Goals
Australia		'CIP is centered on the need to minimize risks to public health, safety and confidence, ensure economic security, maintain Australia's international competitiveness and ensure the continuity of government services'.[44]	Australia maintains sector-specific goals in the area of CIIP. Overall goals include: awareness-raising, promoting e-security skills, advancing research and development, and coordinating the government policies related to e-security. More specifically, agencies have been mandated to address sophisticated and targeted attacks that are difficult to detect and fight by conventional measures. The E-Security national policy statement, updated in 2007, identified reducing e-Security risks to state information and communication systems as a key goal.[45] In particular, the document identified the protection roles of various departments, including those of the Defense Signals Directorate (DSD);[46] the Department of Finance and Administration's Government Information Management Office;[47] the Attorney-General's Department (AGD); the Australian Federal Police (AFP); the Department of Communications, Information Technology and the Arts (DCITA); and the Australian Communications and Media Authority.
Canada	1. Protecting Canada and Canadians at home and abroad; 2. ensuring Canada is not a base for threats to its allies; and 3. Contributing to international security.[48]	'The ultimate outcome of the CIP strategy will be that CI is sufficiently resilient, thereby assuring the continued availability of essential services to Canadians.'[49]	

44 Trusted Information Sharing Network for Critical Infrastructure Protection (2004), Critical Infrastructure Protection National Strategy version 2.1, p. 5.
45 http://www.dbcde.gov.au/__data/assets/pdf_file/0011/71201/ESNA_Public_Policy_Statement.pdf.
46 Ibid., p. 3.
47 Ibid.
48 Her Majesty the Queen in Right of Canada (2004), Securing an Open Society: Canada's National Security Policy, p. vii.
49 Public Safety and Emergency Preparedness Canada (2004), Government of Canada Position Paper on a National Strategy for Critical Infrastructure Protection, p. 6.

Germany		Wichtigstes inhaltliches Ziel der Nationalen Strategie ist es, das Schutzniveau für die Kritischen Infrastrukturen in Deutschland durch geeignete und mit allen Akteuren abgestimmte Maßnahmen gegenüber den vorhandenen und zu erwartenden Risiken so anzupassen, dass Risiken im Vorfeld erkannt werden, gravierende Störungen und Ausfälle vermieden bzw. auf ein Mindestmaß beschränkt werden (Prävention); Folgen von Störungen und Ausfällen durch Notfallmanagement, Redundanzen und Selbsthilfekapazitäten so gering wie möglich gehalten werden (Reaktion) und laufend fortgeschriebene Gefährdungsanalysen sowie Analysen von Störfällen zur Verbesserung der Schutzstandards genutzt werden (Nachhaltigkeit).[50]	Germany emphasizes the importance of CIIP as illustrated in the 2005 *Nationaler Plan zum Schutz der Informationsinfrastruktur* (NPSI) and the subsequent 2007 report *Umsetzungsplan KRITIS*. The protection goals are defined the most clearly in this document's glossary: IT-Sicherheit - Zustand, in dem Verfügbarkeit, Integrität und Vertraulichkeit von Informationen und Informationstechnik geschützt sind. In particular, these documents also highlight the fact that, in addition to protecting the critical information infrastructure, the IT dimension of this CI sector should also be factored in. This includes the continued safety of control centers, process control technology, supply chain management, traffic management, traffic safety, and navigation.
Netherlands	The goal of the strategy for national security is to protect the vital interests of the Netherlands in order to prevent societal disruption. [51]	With regard to the protection of critical infrastructures in the Netherlands, the professional and political ambition level aims to ensure that the government and business sector take responsibility and work together to: 1. do everything possible to prevent the large-scale failure or disruption of critical infrastructures (prevention); 2. ensure that the country is properly prepared for the consequences should such a failure or disruption occur (preparation); 3. take effective measures to minimize the loss that occurs as a result of failure or disruption (repression). [52]	

50 Bundesministerium des Innern (2009), Nationale Strategie zum Schutz Kritischer Infrastrukturen (KRITIS-Strategie), pp. 12f. Available at: http://www.bmi.bund.de/SharedDocs/Pressemitteilungen/DE/2009/mitMarginalspalte/06/kritis.html?nn=106228.

51 Ministry of the Interior and Kingdom Relations (2007), National Security Strategy and Work Programme 2007-2008, p. 16.

52 Ministry of the Interior and Kingdom Relations (2004), Critical Infrastructure Protection in the Netherlands. The Dutch Approach to CIP, p. 11.

Norway		'Critical infrastructures are those constructions and systems that are essential in order to uphold society's critical functions, which in time safeguard society's basic needs and the feeling of safety and security in the general public.'[53]	The National Guidelines to Strengthen Information Security 2007–2010 identified three protection goals in the area of information security:[54] Resilient and secure critical infrastructures and support systems for critical societal functions; a good security culture guiding the development and use of information systems and sharing of electronic information; high competence and a focus on research about information security. The government obliges all owners of CII to adopt protective measures and build more redundancy into information systems.[55]
Sweden			The report Information Security in Sweden –*Situational Assessment 2009* defines protection goals in the area of information security "as the ability to maintain the desired level of confidentiality, integrity and availability when handling information."[56] This includes protecting not only information systems, but also information management systems that are critical to society.[57] The 2008 Action Plan for Information Security defined this relationship as "societal information security".[58] Protection goals in Sweden's IT sector are thus tailored towards not only securing the physical information infrastructure, but also providing non-physical information security where issues such as mass disruption caused by hacking, fraud, and dissemination of malicious code are of concern. Protection goals are particularly targeted for internet security, medical care and healthcare, and e-government.

53 Ministry of Justice and the Police (2006), Protection of critical infrastructures and critical societal functions in Norway. Report NOU 2006:6, submitted to the Ministry of Justice and the Police by the government appointed commission for the protection of critical infrastructure on 5th April 2006, p. 4.

54 The Norwegian Government, 2007. National Guidelines to Strengthen Information Security 2007-2010. Available at: https://www.nsm.stat.no/Documents/KIS/Publikasjoner/National%20Guidelines%200n%20Information%20Security%202007-2010.pdf.

55 Ibid., p. 11.

56 Ibid., p. 13.

57 Ibid., pp. 14f. An information infrastructure system is considered critical to the functioning of society if it meets the following criteria: 1). A shutdown or severe disruption in its function, singlehandedly or in combination with other similar events, can rapidly lead to a serious emergency in society; 2). its societal function is important or essential for responding to an existing serious emergency and minimizing the damage.

58 Ibid., p. 15.

United Kingdom	It is the country's 'single overarching national security objective [...to] protect [...] the United Kingdom and its interests, enabling its people to go about their daily lives freely and with confidence, in a more secure, stable, just and prosperous world'[59]	Reduce vulnerability of the national infrastructure to terrorism and other threats, keeping the United Kingdom's essential services safer.[60]	
United States	'Protect[ion of] the American people, our critical infrastructures, and key resources'.[61]	'build a safer, more secure, and more resilient America by preventing, deterring, neutralizing, or mitigating the effects of deliberate efforts by terrorists to destroy, incapacitate, or exploit elements of our Nation's CIKR and to strengthen national preparedness, timely response, and rapid recovery of CIKR in the event of an attack, natural disaster, or other emergency.'[62]	The United States has created sector-specific plans for all identified critical sectors, some of which are publically available. Many share common characteristics and overarching goals. For example, the main goals in the water sector[63] include: (1) sustain protection of public health and the environment; (2) recognize and reduce risks; (3) maintain a resilient infrastructure; and (4) increase communication, outreach, and public confidence. Correspondingly, the goals in the energy sector are identified as: reliable information-sharing, effective risk management programs, coordinated response capabilities, and trusted relationships between public and private security partners at all levels of industry and government. For the IT sector, operators are to enhance prevention and protection through three guiding areas utilizing:[64] a risk management approach; situational awareness; and response, recovery, and reconstitution.

59 Cabinet Office (2008), The National Security Strategy of the United Kingdom: Security in an interdependent world, p. 5.
60 http://www.cpni.gov.uk/default.aspx.
61 Homeland Security Council (2007), National Strategy for Homeland Security, p. 1.
62 Department of Homeland Security (2009), National Infrastructure Protection Plan. Partnering to enhance protection and resiliency, p. 1.
63 http://www.dhs.gov/xlibrary/assets/nipp-ssp-water.pdf
64 Department of Homeland Security (2007), Information Technology Critical Infrastructure and Key Resources Sector Specific Plan as Input to the National Infrastructure Protection Plan, p.2. http://www.dhs.gov/xlibrary/assets/nipp-ssp-information-tech.pdf

4.2 Annotated Bibliography

4.2.1 Policy documents/reports

Australia. 2004. Critical Infrastructure Protection National Strategy. Trusted Information Sharing Network for Critical Infrastructure Protection. Available at: *www.tisn.gov.au/www/tisn/rwpattach.nsf/VAP/.../toKMVCM4.pdf*

This strategy is intended to provide an overarching statement of principles for critical infrastructure protection in Australia, and outline the major tasks and assign responsibilities necessary for their application. This strategy is for use not only by government, but also by the owners and operators of infrastructure, their representative bodies, professional associations, regulators and standards setting institutions. The strategy provides guidance for the medium term, with a three to five year outlook. It will require detailed implementation plans by governments and industry sectors, and will require the development of interfaces with many other areas of public policy.

Australia. 2008. Attorney General's Portfolio Security Environment Update 2007–08. Attorney General Office. Available at: *http://www.ag.gov.au/www/agd/rwpattach.nsf/VAP/(878CAEAF8D7CA41B4CD31727CCC28450)~Security+Environment+Update+2007-2008+(Budget+2007).pdf/$file/Security+Environment+Update+2007-2008+(Budget+2007).pdf*

This document refers to the Australian national security framework where CI is noted as an asset to protect. Protecting the state from the threat of terrorism is the focus. In response, strong cooperation between the Commonwealth, State, Territory and local governments is identified as a way to counter this threat. The update also notes that businesses and the broader Australian community also have an important role to play.

Australia. 2009. Defending Australia in the Asia Pacific Century: Force 2030. Department of Defense, White Paper. Available at: *http://www.defence.gov.au/whitepaper/docs/defence_white_paper_2009.pdf*

This new Defence White Paper explains how the Government plans to strengthen the foundations of Australia's defence. It sets out the Government's plans for Defence for the next few years, and how it will achieve those plans. Most importantly, it provides an indication of the level of resources that the Government is planning to invest in Defence over coming years and what the Government, on behalf of the Australian people, expects in return from Defence.

Canada. 2009. Working towards a National Strategy and Action Plan for Critical Infrastructure. Public Safety Canada. Available at: *http://www.publicsafety.gc.ca/prg/em/cip/strat-part1-eng.aspx*

This document lays out a proposed national strategy and action plan for critical infrastructure with the goal of enhancing the resiliency of Canada's critical infrastructure and protecting it from disruptions. The action plan identifies three key themes: creating trusted partnerships across all levels of government and the private sector, committing to an all-hazards risk management approach, and improving information sharing and protection.

Jenkins Jr., W.O. 2009. Preliminary Observations on FEMA's Community Preparedness Programs Related to the National Preparedness System. United States Government Accountability Office, Testimony before the Subcommittee on Emergency Communications, Preparedness, and Response, Committee on Homeland Security, House of Representatives. 1 October. Available at: *http://www.upmc-biosecurity.org/sebin/u/t/fema_emerg_mgmnt_prelim_obsrv_fema.pdf*

This testimony provides preliminary observations on (1) challenges FEMA faces in measuring the perfor-

mance of Citizen Corps, its partner programs, and the Ready Campaign and (2) actions FEMA has taken to develop a strategy to encompass how Citizen Corps, its partner programs, and the Ready Campaign operate within the context of the NPS. This testimony is based on work conducted from February 2008 to October 2009. GAO analyzed documents, such as FEMA's strategic plan, and compared reported performance data with observations from 12 site visits, selected primarily based on the frequency of natural disasters. The results are not projectable, but provide local insights.

Sweden. 2009. Information Security in Sweden –Situational assessment 2009.Available at: *http://www.msbmyndigheten.se/upload/Publikationer/0119_09_Information_security_in_Sweden.pdf*
The situational assessment constitutes support for players in society who are involved in managing information-security issues. The assessment is primarily based on developments during 2008 and the beginning of 2009. The report notes the increasing dependence on IT and the development of multiple threats and vulnerabilities; stressing the threat posed by cybercrime. It further proposes various measures (such as skills enhancement, promoting international collaboration, and establishment of basic information security) to enhance information security.

United Kingdom. 2009. The National Security Strategy of the United Kingdom: Update 2009 – Security for the Next Generation. UK Cabinet Office. Available at: *http://www.cabinetoffice.gov.uk/media/216734/nss2009v2.pdf*
'Security for the Next Generation' is the first annual update of the National Security Strategy and sets out an updated assessment of the national security threats facing the UK and includes proposals for combating threats to cyber security. The previous report, UK National Security Strategy – Security in an Interdependent World, was published in 2008. It also notes how the UK is addressing changing security threats in long-established environments and tackling challenges in new and evolving domains such as cyberspace.

United States. 2007. Critical Infrastructure Protection: Sector-Specific Plans' Coverage of Key Cyber Security Elements Varies. United States Government Accountability Office, Report to Congressional Requesters. Available at: *http://www.gao.gov/new.items/d08113.pdf*
This report is based on a study performed to evaluate sector-specific plans in the area of cyber security. The findings revealed that the plans varied in how comprehensively they addressed the cyber security aspects and argued that without comprehensive plans, stakeholders within the infrastructure sectors may not adequately identify, prioritize, and protect their critical assets, systems, networks, and functions; be prepared to respond to a significant attack; or identify the cyber risks they face. It concluded by recommending that DHS work with the sector representatives to ensure that the areas not sufficiently addressed are covered.

4.2.2 Academic literature

Caudle, S.L. 2009. National Security Strategies: Security from What, for Whom, and by What Means. . Journal of Homeland Security and Emergency Management, 6(1), Article 22. Available at: *http://www.bepress.com/jhsem/vol6/iss1/22/*
This article argues that fundamental changes are taking place in how countries view, approach, and implement strategies to protect their 'national security.' In the past, strategies underlying national

security narrowly focused on threats that could be addressed by military and/or diplomatic means. Now, however, 'national security' is viewed in a much broader context, with the focus on preserving that which makes a country unique, and that includes the intangibles of its culture as well as what physically lies within its borders. The result is that countries are revising existing national security strategies (including those covering homeland security or domestic security) or crafting entirely new ones to address this much broader view of that which is to be protected. Drawing on recent literature and documents addressing diverse national security strategies, this article discusses the following areas: (1) the definition of national security, (2) the purpose of a national security strategy, (3) how a national security strategy is evaluated, and (4) implications for The National Security Strategy of the United States and The National Strategy for Homeland Security as a new Administration governs.

Rose, A.Z. 2009. A Framework for Analyzing the Total Economic Impacts of Terrorist Attacks and Natural Disasters. Journal of Homeland Security and Emergency Management, 6 (1), Article 9. Available at: *http://www.bepress.com/jhsem/vol6/iss1/9/*

Policies to mitigate natural hazards and terrorism are facing increasing scrutiny, such as the benefit-cost test. The benefits are the losses that can be avoided by the mitigation actions. For sound policy-making, it is therefore necessary that the various types of losses and major factors affecting them be identified and that metrics be established for their measurement in accordance with economic principles. This paper presents a comprehensive framework for the analysis and measurement of ordinary economic impacts and two categories of impacts that have recently gained the attention of analysts and policy makers, but for which operational definitions are lacking. The first is resilience, which refers to how the economy manages to keep functioning and how quickly it recovers. The second major extension of loss estimation pertains to behavioral and systems linkages. These refer to considerations unique to disasters that cause indirect impacts to be orders of magnitude greater than ordinary indirect effects in cases where risks are amplified, systems are overwhelmed, and resilience is eroded. The framework combines a checklist of types of impacts, consistent definitions, metrics, and strategies for estimation. The framework is serving as a template for loss estimation and benefit-cost analysis by several offices of the U.S. Department of Homeland Security.

CSS
ETH Zurich

The **Center for Security Studies (CSS) at ETH Zurich** specializes in research, teaching, and information services in the fields of international relations and security policy. The CSS also acts as a consultant to various political bodies and the general public. The Center is engaged in research projects with a number of Swiss and international partners, focusing on new risks, European and transatlantic security, strategy and doctrine, state failure and state building, and Swiss foreign and security policy.

The **Crisis and Risk Network (CRN)** is an Internet and workshop initiative for international dialog on national-level security risks and vulnerabilities, critical infrastructure protection (CIP) and emergency preparedness.

As a complementary service to the International Relations and Security Network (ISN), the CRN is coordinated and developed by the Center for Security Studies at the Swiss Federal Institute of Technology (ETH) Zurich, Switzerland. (www.crn.ethz.ch)