CIIP Country Surveys

Norway

Norway

Concept of CIIP and Description of System

A central premise underlying the Norwegian CIIP policy concept is that nowadays, the production of most goods and services depends in some way or other on information and communication technology (ICT) systems. This dependency may be as a part of the production process itself or as a part of the logistics to make the goods or services available to consumers. ICT forms an important part of the production of goods and services in a number of critical sectors of society. In Norway, the critical sectors are the following:[1]

- Banking and finance,
- (Tele-) Communications,
- Defense,
- Energy and utilities,
- Oil and gas supply,
- Police,
- Public health,
- Rescue services,
- Social security,
- Transport.

The main challenges for society concerning information infrastructure are seen in the areas of rapid technological development, deregulation, globalization, interdependencies, and the lack of expertise and outsourcing of manpower and systems.[2]

1 Ministry of Trade and Industry. *Society's Vulnerability due to its ICT-Dependence – Abridged Version of the Main Report*, (Oslo, October 2000), 9-10.

2 http://www.ntia.doc.gov/osmhome/cip/workshop/norway.ppt.

CIIP Initiatives and Policy

CIIP Initiatives

Since the end of the 1990s, CIIP has been seen as a safety issue in Norway. In fact, CIIP was put on the political agenda by the government commission on "A Vulnerable Society". The Ministry of Trade and Industry on the other hand perceives CIIP as an economic issue.[3]

Commission "A Vulnerable Society"

The governmental commission "A Vulnerable Society" was established by Royal decree on 3 September 1999. It was active from 1999 until 2000. The findings gave important input to the national planning process.[4] The duty of the commission was to study vulnerabilities in society with a broad perspective. The mandate was to assess the strengths and weaknesses of current emergency planning, to assess priorities and tasks, and to facilitate increased awareness, knowledge, and debate about vulnerabilities.[5]

The government commission identified several areas that should be focused on. One of these areas was CI.[6] In its green paper, NOU (2000: 24) – "A Vulnerable Society", the commission placed great emphasis on the significance of ICT for the vulnerability of society in general. The commission, in what was probably its most controversial proposal, recommended that the field of safety, security, and emergency planning should be concentrated in one single ministry.[7] Furthermore, a strategy based on the following pillars was proposed:[8]

- Partnership between public and private sectors,
- Promotion of information exchange,
- Establishment of early warning capacity,
- Harmonization and adjustments of laws and regulations,
- Public responsibility for CIP vital to ICT systems.

3 Interview with a representative of the Danish Directorate for Civil Defense and Emergency Planning (DSB), March 2002.
4 Interview with a representative of the Danish Directorate for Civil Defense and Emergency Planning (DSB), March 2002.
5 http://www.isn.ethz.ch/crn/extended/workshop_zh/ppt/Henriksen/sld001.htm.
6 http://www.ocb.se/dokument/filer/5b_gjengsto_henriksen_abstract.pdf.
7 http://www.ocb.se/dokument/filer/5b_gjengsto_henriksen_abstract.pdf.
8 http://www.ocb.se/dokument/filer/5b_gjengsto_henriksen_abstract.pdf.

ICT-Vulnerability Project [9]

The ICT vulnerability project consisted of an interdepartmental group commissioned by the Ministry for Trade and Industry. The project collaborated with the government commission on the "Vulnerable Society". Together, they coordinated their findings on ICT vulnerabilities.[10] In the ICT vulnerability project, each sector authority evaluated the risks linked to specific functions in that sector.[11]

eNorway Plan

The government produced the eNorway (eNorge) plan that describes the needs, responsibilities, and required action for the development of an information society.[12] With the eNorway plan, the government ensures that the country has equally ambitious objectives as those formulated by the EU in the eEurope Plan.[13]

"*Safety and Security of Society*"

On 5 April 2002, the Ministry of Justice and the Police presented report no. 17 on the "Safety and Security of Society" to the Norwegian Storting (Parliament). The report is a comprehensive statement on the government's proposals regarding the reduction of vulnerabilities in modern society and measures to increase safety and security in the future. It states that when assessing the vulnerability of society, it is important to "consider the consequences of lapses in CI, such as a lapse in the distribution of power or a lapse in telecommunication".[14] The recommendations will form the basis for the government's process of initiating measures.

9 Ministry of Trade and Industry, Society's vulnerability, 10.

10 Dependability Development Support Initiative (DDSI). *European Dependability Policy Environments*, *Country Report Norway.* (version April 2002).

11 A common feature of these evaluations is that each individual sector operation is dependent on its own ICT user systems as well as on the public telecommunications services. Therefore, robust access to telecommunications seems to be very important to most sectors. The telecommunications services are dependent on ICT systems in order to function.

12 Dependability Development Support Initiative, Country Report Norway (version April 2002).

13 http://odin.dep.no.

14 Report No. 17 to the Storting (2000-2001). *Statement on Safety and Security of Society (Summary)*, (April 2002).

CIIP Policy

Over the past few years, and as a result of technological developments, there has been an increased focus on CIIP. Moreover, US policy has been an important trigger in putting CIIP on the political agenda in Norway as a political, security, and economic issue.[15]

Policy Statements

In 1998, the State Secretary Committee for ICT (Statssekretærutvalget for IT – SSIT) formed a subcommittee with a mandate to report on the status of ICT vulnerability efforts being carried out in Norway. Furthermore, the importance of CIIP is also stressed by the Defense Review 2000 and the Defense Policy Commission 2000.[16] In the aftermath of 11 September 2001, the government considered it necessary to increase national safety and security, particularly within the civil defense, in the Police Security Service, and in emergency planning within the health sector.[17]

Definition of CIIP Goals

Norway's CIIP policy is based on the following goals:[18] CII must reach a level of robustness that does not degrade important society functions during a "normal" peacetime situation. And in crisis or war, the infrastructure has to be sufficiently robust to maintain functions that are critical for society. Due to the wide range of threats against the society and the challenges to many CII sectors, the government has initiated several relevant measures concerning CIIP.[19]

Law and Legislative Action

Penal Code, Paragraph 151b

The penal code states that whosoever causes comprehensive disturbances to the public administration or other parts of society by disrupting the collection of information, or by destroying or damaging power sup-

15 Interview with a representative of the Directorate for Civil Defense and Emergency Planning (DSB), March 2002.
16 Interview with a representative of the Directorate for Civil Defense and Emergency Planning (DSB), March 2002.
17 Report No. 17 to the Storting (2000-2001).
18 http://www.ocb.se/dokument/filer/5b_gjengsto_henriksen_abstract.pdf.
19 Report No. 17 to the Storting (2000-2001).

ply plants, broadcasting facilities, telecommunications services, or other kinds of communication, will be punished by incarceration for a maximum of 10 years. Unlawful negligence as mentioned in the first instance will be punished by incarceration for a maximum of 1 year. Accessories will be punished in the same manner. This section became law on 12 June 1987.[20]

In Norway, the laws generally tend to place the blame firmly with the operator in cases of accidents such as rail crashes or fires. However, during the last years, systemic errors and bad leadership have become apparent as the underlying causes of many accidents.[21]

Organizational Analysis

Public Agencies

The Ministries of Defense, Justice and Police, Communications, and Trade and Industry are involved to varying degrees in inter-ministerial cooperation.[22]

Directorate for Civil Defense and Emergency Planning (DSB)[23]

The Directorate for Civil Defense and Emergency Planning (direktoratet for sivilt beredskap, DSB) was established in 1970. The directorate works under the authority of the Ministry of Justice and the Police. The main task is to be a center of resources and expertise for emergency contingency planning. The DSB is a point of contact between central authorities and regional commissioners in peacetime disasters.

To ensure adequate preparedness measures in the community, the DSP devotes considerable efforts to ensure that all Norwegian municipalities carry out risk and vulnerability analyses. The DSB works to ensure that activities involving preparedness responsibilities lead to the implementation of internal control systems to ensure the quality of emergency planning at local government level. The DSB also supervises the planning in the ministries and offices of the regional commissioners.

20 Interview with a representative of the Directorate for Civil Defense and Emergency Planning (DSB), March 2002.
21 http://www.ocb.se/dokument/filer/5b_gjengsto_henriksen_abstract.pdf.
22 Interview with a representative of the Directorate for Civil Defense and Emergency Planning (DSB), March 2002.
23 http://www.dsb.no/presentation/index.asp.

OKOKRIM

The National Authority for Investigation and Prosecution of Economic and Environmental Crime is responsible for issues concerning cybercrime.[24] OKOKRIM has a unit called "IKT-teamet", which focuses on ICT-related crimes.

Changes in the Organizational CIIP Structure

Currently, several changes are taking place within the Norwegian organizational CIIP structure. For instance, part of the Chief Headquarters of Defense (CHO) will be established as an agency under the Ministry of Defense with double reporting lines: one to the Ministry of Defense on military issues and one to the Ministry of Justice on civilian issues. Furthermore, a Unit on Telecom Infrastructure Security has been established at the Post and Telecommunications Authority. In the future, the Ministry of Justice will have a greater coordinating role regarding security in civilian society, which will require several steps towards reorganization in civilian agencies.[25] The government also plans to establish a Directorate of National Protection, which will include CIIP tasks.

Cooperation between Public and Private Sectors

The most important public-private initiatives in Norway are the SIS (Ministry of Trade and Industry Initiative) and the VDI (Intelligence services initiative) projects. Both projects, the VDI (which is already operational) and the SIS (which is to be started in 2002), have clear public-private partnership participation profiles and roles.

Center for Information Security (SIS)

The Norwegian government decided some years ago to establish a Center for Information Security. In 2001, a pilot study was commissioned to investigate options for the establishment of this center.[26]

The main tasks of the SIS will include the exchange of information, competence, and knowledge about threats and countermeasures, and a

24 http://www.okokrim.no.

25 Interview with a representative of the Norwegian Ministry of Trade and Industry, June 2002.

26 Dependability Development Support Initiative (DDSI). *Public-Private Co-operation: Business Governmental Actions Towards Achieving a Dependable Information Infrastructure in Europe.* Issues and background paper for the DDSI workshop on Public-Private Co-operation (Stockholm, 6–7 June, 2002), 10.

holistic threat image generation.[27] The future clients of the SIS will be government agencies, security services, politicians, and private enterprises as a basis for assessing national security status. The SIS will not be operating as a government agency and will not be involved in privacy issues.

VDI (Intelligence Services Initiative)[28]

At the beginning of the new millennium, several agencies and business actors began cooperating with the Norwegian intelligence and security services to prevent computer crimes. The whole project is intended to enable intelligence and security professionals to chart the extent of the threat to vulnerable information infrastructure. One of these measures is the "Warning System for Digital Infrastructure" (VDI). The implementation of the VDI was clearly a cabinet reaction to the commission "A Vulnerable Society" and the Ministry of Trade and Industry report in summer/autumn 2000. The VDI will alert clients to breaches and attempted breaches of computer networks. Each member is free to report the incident to the police. Due to the success of the project, the government wants to prolong it. The success of the VDI is, to a great extent, attributed to its control structures, which alleviate possible concerns about business privacy and other issues.

Early Warning

UNINETT CERT

UNINETT CERT is the Norwegian computer emergency response team and the academic network for research and development. It was formed in 1995. The constituency is made up of the Norwegian state universities, colleges and R&D institutions.[29] The main motivations were to contribute to a better Internet security for UNINETT member institutions, and the perceived need of a focal point for security issues regarding UNINETT member institutions.[30] The basic duty of UNINETT CERT is to provide assistance on handling and investigating incidents involving one or more

27 http://www.isn.ethz.ch/crn/extended/workshop_zh/ppt/Henriksen/sld001.htm.
28 http://www.isn.ethz.ch/crn/extended/workshop_zh/ppt/Henriksen/sld001.htm.
29 Dependability Development Support Initiative, Country report Norway (version April 2002).
30 http://cert.uninett.no/policy.html.

members of the constituency. Examples of incidents are spamming, suspicious port-scanning, denials of service, etc.[31]

Research and Development

The government commission "A Vulnerable Society" suggested that one ministry should have the main responsibility for research in the field of safety and security, that the Norwegian Research Council should initiate and coordinate research, and that safety and security must be integrated in ICT education.[32] The main research since 1994 has been in the area of the protection of the society, based on the works of BAS (Beskyttelse av samfunnet; Protection of the Society).[33]

Since 1994, BAS has been an ongoing research activity. It is a joint project of the Directorate for Civil Defense and Emergency Planning (DSB) and the Norwegian Defense Research Establishment (FFI). The overall purpose is to make central decision-makers more aware and give them insights into the vulnerabilities of Norwegian society, and to point out cost-effective measures to reduce these vulnerabilities. The first BAS project focused on general trends toward increased vulnerabilities.[34] All the following research activities are based on these basic findings. The second BAS project (BAS2) performed an analysis of public telecommunication services in the period 1997-1999. The results of the project formed the basis for the Norwegian government's new strategy concerning security and emergency preparedness in the telecommunications sector.[35] The third BAS project (BAS3) focused its research on vulnerabilities in the electric power supply.[36] The findings recommended measures to reduce the increasing vulnerabilities in the Norwegian electric power supply. BAS4 is a still ongoing project seeking to map vulnerabilities and the impact of failures in the transportation sector. Furthermore, in recent years, the research papers published by the Defense Research Institute have provided a significant basis for the promotion of safety and security in society.[37]

31 http://cert.uninett.no/policy.html.
32 http://www.ocb.se/dokument/filer/5b_gjengsto_henriksen_abstract.pdf.
33 http://www.ntia.doc.gov/osmhome/cip/workshop/norway.ppt.
34 Four sectors were identified as particularly critical: telecommunications, electric power supply, transportation, and management/information.
35 This strategy was proposed in May 2001.
36 The Norwegian electric power market was deregulated in 1991.
37 Report No. 17 to the Storting (2000–2001).