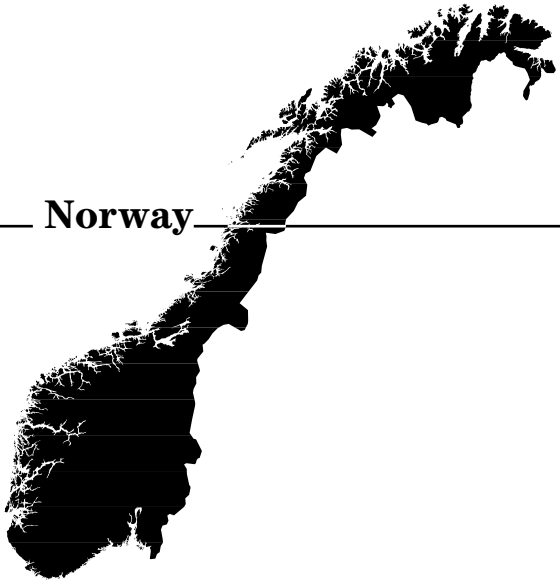
CIIP Country Surveys



Norway

The Country Survey of Norway 2004 was written with the help of Stein Henriksen, Roger Steen, and Kjetil Sørli, Directorate for Civil Protection and Emergency Planning (DSB) as well as Cort Archer Dreyer, Ministry of Trade and Industry.

Norway

Critical Sectors

A central premise underlying the Norwegian CIIP policy concept is that the production of most goods and services depends in some way or other on information and communication technology (ICT) systems. This dependency may occur as part of the production process itself, or as part of the logistics of making 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: [318]

- Banking and Finance,
- Central Government Administration,
- (Tele-)Communications,
- Defense,
- Energy and Utilities,
- Oil and Gas Supply,
- Police,
- Public Health,
- Rescue Services,
- Social Security,
- Transport,
- Water Supply and Drainage.

The main challenges for society concerning information infrastructure are seen in the areas of rapid technological development, deregulation, globalization, interdependencies, the lack of expertise, and outsourcing of manpower and systems. [319]

Norway's CIIP policy is based on the following goals: [320] 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 society and the challenges to many

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

319 Ministry of Trade and Industry. *Information and Infrastructure Protection – a Norwegian View* (no date). http://www.ntia.doc.gov/osmhome/cip/workshop/norway.ppt.

320 http://www.ocb.se/dokument/filer/5b_gjengsto_henriksen_abstract.pdf.

CII sectors, the government has initiated several relevant measures such as the security part of eNorway, the *ITSEC* (IT Security) national strategy, the Intelligence Services Initiative, and the *Center for Information Security* (SIS).[321]

Initiatives and Policy

Over the past few years, and as a result of technological developments, there has been an increased focus on CIIP. Since the end of the 1990s, CIIP has been regarded as a security 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.[322] Moreover, US policy has been an important trigger in putting CIIP on the political agenda in Norway as a political, security, and economic issue.[323]

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*.[324] In the aftermath of 11 September 2001, the government considered it necessary to increase national safety and security, particularly within civil defense, in the Police Security Service, and in emergency planning within the health sector.[325]

321 Report no. 17 to the Storting (2000–2001).
322 Information provided by a Norwegian expert of the Directorate for Civil Protection and Emergency Planning (DSB), March 2002.
323 Information provided by a Norwegian expert of the Directorate for Civil Protection and Emergency Planning (DSB), March 2002.
324 Information provided by a Norwegian expert of the Directorate for Civil Protection and Emergency Planning (DSB), March 2002.
325 Report no. 17 to the Storting (2000–2001).

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.[326] The commission's task 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.[327]

The government commission identified several focus areas. One of these was CI.[328] 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.[329] Furthermore, a strategy based on the following pillars was proposed:[330]

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

ICT-Vulnerability Project

The *ICT Vulnerability Project*[331] was commissioned by the *Ministry of Trade and Industry* in 1999 and consisted of an interdepartmental group. The project collaborated with the government commission on the '*Vulnerable Society*', and the two groups coordinated their findings on ICT vulnerabili-

326 Information provided by a Norwegian expert of the Directorate for Civil Protection and Emergency Planning (DSB), March 2002.

327 http://www.isn.ethz.ch/crn/extended/workshop_zh/ppt/Henriksen/sld001.htm.

328 Jan Hovden. *Public policy and administration in a vulnerable society.* Norwegian University of Science and Technology and the Norwegian Academy of Science and Letters, Center for Advanced Study (June 2001). http://www.delft2001.tudelft.nl/paper%20files/paper1074.doc.

329 Ibid.

330 Ibid.

331 Ministry of Trade and Industry, *Society's vulnerability*, p. 10.

ties.[332] In the ICT Vulnerability Project, each sector authority evaluated the risks linked to specific functions in that sector.[333] This project resulted in the *National Strategy for ICT Security.*

National Strategy for ICT Security

The *Ministry of Trade and Industry* published a national strategy for securing ICT systems in Norway in June 2003,[334] which proposed several initiatives for improving security based on the *OECD Guidelines for the Security of Information Systems and Networks* (→ for more details see Part III). The strategy involves all aspects of ICT security, ranging from security for individuals, businesses, and the daily activities of the government to the security of IT-dependent critical infrastructure.

The Norwegian national authorities started implementing the suggested measures in the autumn of 2003. The establishment of the *Center for Information Security* (*SIS*, see below), is one of them already carried out. Other initiatives include the establishment of a coordination committee for ICT security and campaigns to raise awareness of challenges and problems related to the use of ICT systems.[335]

eNorway 2005 Action Plan

The government presented in May 2002 the *eNorway (eNorge) 2005 Action Plan*, which describes the needs, responsibilities, and action required for the development of an information society.[336] With *eNorge*, the government ensures that the country has equally ambitious objectives as those formulated by the EU in the *eEurope Plan*.[337] eNorway is an evolving plan and deals predominantly with the furtherance of e-Government and e-Business.

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

333 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.

334 http://www.odin.dep.no/archive/nhdvedlegg/01/06/Nasjo006.pdf.

335 http://www.norsis.no/detailse.php?type=news&id=176.

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

337 http://www.odin.dep.no/archive/nhdvedlegg/01/06/Nasjo006.pdf.

"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 of 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."[338] The recommendations laid the basis for new government measures, including most importantly the formation of the new *Directorate for Civil Protection and Emergency Planning* (DSB).[339]

Organizational Overview

Public Agencies

In Norway, the ministry or authority that has the responsibility for an area during peace or non-crisis times also has the responsibility during times of crisis and war. This system also applies to CIIP. The coordinating authority on the civilian side is the *Ministry of Justice and Police*. The overall authority for ICT security is the *Ministry of Trade and Industry*, while the *Ministry of Defense* is responsible on the military side. The *Ministry of Transport and Communications* has responsibility for the communication sector in Norway, including all related security issues. Directorates and authorities that are responsible for handling the different sides of CIIP on behalf of the ministries are subject to the respective ministries.[340]

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.[341]

338 Report no. 17 to the Storting (2000–2001). *Statement on Safety and Security of Society (Summary)* (April 2002).

339 http://www.dsb.no.

340 Information provided by a Norwegian expert from the Directorate for Civil Protection and Emergency Planning (DSB), 2003.

341 Information provided by a Norwegian expert from the Norwegian Ministry of Trade and Industry, June 2002.

Directorate for Civil Protection and Emergency Planning (DSB)

The *Directorate for Civil Protection and Emergency Planning* (DSB)[342] was established on 1 September 2003, replacing the former *Directorate for Civil Defense and Emergency Planning* and the *Directorate for Fire and Electrical Safety.*

The new DSB is subordinate to the *Ministry of Justice and Police*, and its 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 during disasters in peacetime.

To ensure adequate preparedness measures in the community, the DSB 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.

In the context of CIIP, the DSB coordinates and carries out research on vulnerabilities and the protection of critical assets in co-operation with other actors.

National Authority for Investigation and Prosecution of Economic and Environmental Crime (OKROKRIM)

The *National Authority for Investigation and Prosecution of Economic and Environmental Crime* (OKOKRIM) is responsible for issues concerning cyber-crime.[343] OKOKRIM has a unit called IKT-*teamet* that focuses on ICT-related crimes.

The Directorate of National Protection

The *Directorate for National Protection* (Nasjonal sikkerhetsmyndighet)[344] was established in January 2003. Its main CIIP task is to produce secure solutions and technology, together with enforcing laws and regulations on handling classified information and securing critical objects. It also handles certification systems (SERTIT) according to Common Criteria standards.[345]

342 http://www.dsb.no.
343 http://www.okokrim.no.
344 http://www.nsm.stat.no.
345 Information provided by a Norwegian expert from the Directorate for Civil Protection and Emergency Planning (DSB), 2003.

Public Private Partnerships

The most important public private initiatives in Norway are the *Center for Information Security* (SIS) and the *Warning System for Digital Infrastructure* (VDI) project.

Center for Information Security (SIS)

The Norwegian government decided some years ago to establish a *Center for Information Security* (SIS). In 2001, a pilot study was commissioned to investigate options for the establishment of this center.[346]

SIS is now responsible for coordinating activities related to information and communication technology security in Norway. This includes the exchange of information, competence, and knowledge about threats and countermeasures, and a holistic threat image generation.[347] The clients of the SIS are government agencies, security services, politicians, and private enterprises, offering a broad basis for assessing the status of national security. SIS is closely linked to UNINETT CERT (see below).

Warning System for Digital Infrastructure (VDI)

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 *Warning System for Digital Infrastructure* (VDI) [348] is an initiative by the intelligence services intended to enable intelligence and security professionals to chart the extent of the threat to vulnerable information infrastructure through the use of Intrusion Detection Systems (Sniffers). The project was a cabinet reaction to the commission on '*A Vulnerable Society*' and the *Ministry of Trade and Industry* report in summer/autumn of 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

346 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), p. 10.

347 Henriksen, Stein. "National Approaches to CIP: Norway". *ETH-ÖCB-CRN Workshop on Critical Infrastructure Protection in Europe: Lessons Learned and Steps Ahead*. (Zurich, 8–10 November 2001). http://www.isn.ethz.ch/crn/extended/workshop_zh/ppt/Henriksen/sld001.htm.

348 Ibid.

privacy and other issues. VDI co-ordination has now moved to the *National Security Agency*.

Early Warning Approaches

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.[349] The team was created to contribute to better Internet security for UNINETT member institutions, and to serve as a focal point for security issues regarding UNINETT member institutions.[350] The basic duty of UNINETT CERT is to provide assistance on handling and investigating incidents involving one or more members of the constituency. Examples of incidents are spamming, suspicious port-scanning, and denials of service.[351]

349 Dependability Development Support Initiative, country report Norway (version April 2002).
350 http://cert.uninett.no/policy.html.
351 http://cert.uninett.no/policy.html.

Center for Security Studies, ETH Zurich
Volume 2, Zürich 2004.

The International CIIP Handbook 2004: An Inventory and Analysis of Protection Policies in Fourteen Countries

Myriam Dunn and Isabelle Wigert

edited by
Andreas Wenger and Jan Metzger