Critical Information Infrastructure Protection in Norway

A paper for the Critical Infrastructure Protection (CIP) Workshop in September 2003 in Frankfurt

Kjell Olav Nystuen & Janne Merete Hagen

The Norwegian Defence Research Establishment (FFI)
P O Box 25 Kjeller
N-2027 KJELLER
NORWAY
kon@ffi.no
jmh@ffi.no

Abstract: This paper outlines the position of a new project with focus on the vulnerability of critical information infrastructures in Norway. The Critical Infrastructure Protection Studies at FFI have uncovered vulnerabilities in telecommunications, electric power supply and transport. Society's dependency on information and communication technology and information infrastructure is also underlined. To some extent, vulnerability within the sectored information infrastructures has also been studied. Knowledge gained from these studies has been in much demand and it has proven very useful for the authorities. The Norwegian government has issued made several White Papers based on this work. Due to the successful research as well as to weaknesses in existing regimes for critical information infrastructure protection, FFI plans to continue such research, with greater emphasis on high-level threats.

1 Introduction

The past ten years have seen an increasing focus on the vulnerability of modern society, with particular emphasis on its dependency on a several key infrastructures. So far the sector functions *telecommunications, electrical power supply* and *transportation* have been subject to in-depth vulnerability analysis at FFI.

One important result of the studies of these three sector functions has been to identify their increasingly high dependence on internal services from information and communication systems. Even minor failures in these systems may lead to extensive disruptions in the end-user services delivered from each individual sector function. Moreover, these information and communication systems have often proven inherently vulnerable because of the way the technology is applied in the systems. Systems dependence on external systems and functions increases this vulnerability [MTI00] [MTI00E].

Against this backdrop it was decided to initiate a research project on the vulnerability of Critical Information Infrastructures (CII). The present paper sketches out some of the background and initial positions for this study, as well as some of the main challenges. In addition we present a brief overview of the results from previous CIP-research activity.

2 Critical Infrastructure Protection in Norway

2.1 Critical infrastructures in Norway

The first FFI study on vulnerability in Norwegian society identified four sector functions as particularly critical: *electrical power supply, telecommunications, transport,* and *information & management* [HOF97]. An important aspect uncovered in the analysis was the degree of integration among and interdependencies between the various sector functions. Serious disturbances in one function would result in spreading effects for the other functions [HOF97].

The next sector study analysed vulnerability in the national public telecommunications infrastructure, as well as the societal consequences of severe outages in that infrastructure. It became clear that the entire society, including the Norwegian Defence Forces and the Civil Emergency Planning organisations, were highly dependent on public telecommunication systems, and that this dependency would increase in the future with more extended use of electronic services. Moreover, commercial and technological developments would result in an even more vulnerable telecommunications system, unless the authorities started implementation of counter-measures. Several measures were identified, briefly categorised as follows:

- protection of critical parts of the infrastructure against physical and electronic threats
- enhanced network flexibility and redundancy
- protection of internal information infrastructures for network management and service production
- increased efficiency of services and resources in crisis management

Four strategies of protection for the telecommunication system were then analysed. As these varied in scope, cost and effectiveness, each strategy emerged with a different "level of protection" and costs [HF99] [HN99]. On the basis of this analysis, the Norwegian government established a new government body responsible for the protection of the national telecommunication infrastructure in a new competitive market [SDWP01].

In the study of the Norwegian electrical power supply sector, it became clear that also that sector was crucial for modern society, although with more redundancy in infrastructure than was the case in telecommunication. Even a short interruption of

electrical power supply would affect other sectors, and stop the production of goods and services [H01]. The operation and management of Norwegian power supply, with its distributed production sites and transmission grid, were also decisive for the vulnerability of the infrastructure. The increasing dependency on a robust internal information infrastructure was an important factor in this vulnerability. Shortage of personnel, and a steady focus on effectiveness and internationalisation, were other factors that could increase vulnerability in the future [FHH01]. The strong focus on effective transmission of electricity, new flexible AC/DC transmission systems (FACTS), and thereby more use of information and communication technology, would further affect vulnerability in the future [F02]. Measures recommended included security measures for internal information infrastructures, training of personnel in emergency and security matters, and an improvement of the capacity to re-establish and repair the infrastructure [FHH01].
A recently finished transport study has analysed vulnerability in Norway's national road, rail, air, and sea transport infrastructures, primarily in the context of sabotage and terror threats. As a whole, the transport system was found to be less vulnerable than the telecommunication and electrical power supply system, due to greater redundancy. But, even if the transport sector today can be accused of being conservative with respect to the use of modern information and communication technology (ICT), this is likely to change in the future, and dependency on the information infrastructures will increase [HRL03].

2.2 Information infrastructures

FFI's research on the vulnerability of society was a contributing factor for the Norwegian government's decision to appoint a Vulnerability Commission in 1999. Here the focus was on the vulnerability of modern society to all types of possible threats, spanning from natural disasters to man-made attacks and sabotage [NOU, 2000:4]. In parallel, the Ministry of Trade and Industry (NHD) established a project to identify the vulnerability of society due to its dependence on information and communication technology [MD03]. On the basis of experiences in connection with Y2K and the results from the FFI studies, the NHD project contributed to the work of the Commission.

The conclusions from the Commission were documented in a White Paper that recommended a range of different measures to reduce the vulnerability of Norwegian society, as well as the suggestion to reorganise the Civil Emergency Preparedness organisation. The White Paper also outlined a national strategy for information infrastructure security [JDWP00]. A Green Paper, 'National Strategy for Information Security', was later presented for comments. The strategy suggests, among various measures, further research on the vulnerability of society, with a focus on critical information infrastructures [NHGP03].

3 Critical Information Infrastructures and Security

3.1 Dependency on technologies and systems

The production of most goods and services depends, in some way or other, on services from information infrastructures, which in turn consist of systems and structures based on information and communication technology (ICT). The national economy and modern society have thus become completely dependent on services from these information infrastructures, which have become an integral part of the systems with which we surround ourselves and which help safeguard our welfare. This also means that any major malfunctions in critical information infrastructures could interrupt critical public and private goods and services in a way that few of us can as yet foresee. Even minor failures in information infrastructures may lead to extensive disruptions in such important areas of modern society as telecommunications, electrical power supply, transportation, oil and gas supply, finance and banking, and emergency services [MTI00].

In this context, reliable access to telecommunications is crucial to most sectors. Telecommunications services are a basic part of any distributed information system, and are in turn highly dependent on its internal information infrastructures in order to function. A stable power supply is necessary for electronic information processing and exchange; moreover, power supply is dependent on its own internal information infrastructure in order to function.

The relationship between information infrastructures in general, and telecommunications and power supply infrastructures in particular, also illustrates the trend towards increased interdependencies across corporate and public sector boundaries. All players are in reality dependent on each other's information infrastructures. Telecommunications and power supply constitutes an important foundation of nearly all types of information infrastructures.

The telecommunication sector study revealed the consequences of serious malfunctions in these information infrastructures, through war- and crisis-games. In short, these games showed that crisis management very soon became incapable of action because of lack of updated information [OMS00].

3.2 Vulnerability of Critical Information Infrastructures

In parallel with the development towards increased utilisation and dependency on information infrastructures, there is a rapid technological development. The result is a flow of new and more advanced services. At the same time, the systems and infrastructures where information technology is applied are growing increasingly complex and exposed to more rapid changes than before.

As part of the previous sector studies, we at the FFI have also carried out some case-studies of the vulnerability of internal information infrastructures within the selected sectors. These studies involved government-operated infrastructures as well as ones under private operation. Information infrastructures were found to be critical for the execution of maintenance and control, as well as service development and production. The experience and knowledge gained from these case-studies, in combination with other broader studies, constitutes in many ways the foundation for the decision to establish the new research project on the vulnerability of Critical Information Infrastructures. Some of these experiences are categorised and briefly described below.

Policy and procedures

There seems to be a lack of clear and holistic policies on systems security and vulnerability, even for systems vital to society. Typically, information infrastructures have grown from separate systems with relatively low criticality, to large interconnected systems where process control and business applications are interlinked. Also the need for extended cooperation with partners and customers requires connection to the information in these systems. Internet or specifically dedicated dial-up connections are often used as platforms for this type of interconnection. In the midst of this development there has also been frequent changes in company structures lately, in addition to the out-sourcing of functions. Expansion and adaptation of networks has been carried out continuously according to current needs, apparently without any clear holistic policy or procedure.

Even now, when many government-operated functions have been de-monopolised and taken over by private companies, the government has not issued any clear policies or requirements. At the same time, the complexity of systems has increased dramatically. The result has been an absence of focus on high-capability threats that have a low probability of occurring – and this is very negative from a national security perspective.

Resources and Capabilities

There is an apparent lack of adequate skilled and trained personnel for holistic systems security, even in large operations. Many have received basic training in establishing and configuring single components, like firewalls and virus protection solutions, but have no understanding of the holistic system aspect, which is much more complex and difficult. One obvious reason has been the lack of national training possibilities in this field until recently. Very few persons have more than superficial knowledge of other threats against their systems than the daily and mostly probable ones.

Basic measures like firewalls and virus detection software are normally installed, but the use of, for example, more complex functions for Computer Incident Response seems limited so far. Important infrastructure in this respect is a highly automated Intrusion Detection Capability.

Risk and vulnerability studies, if implemented at all, often appear to be too simple, and the aspect of high-capability threats seems to have been completely excluded as irrelevant. One cause of this is lack of capability and resources.

Information about the robustness of public communication infrastructures and services offered from these infrastructures must also be classified as lacking. This is a factor vital for establishing robust information infrastructures, as well as for making risk analysis. There also seems to be a relatively low focus on contingency planning, in the event that these services should fail.

Systems Security Architectures

Often there appears to be no holistic system security architecture in place. Such architecture is particularly important for sectors with heterogeneous information infrastructures, implemented over a long period of time. Within some sectors, there is for instance a high utilisation of proprietary communication protocols, many of which were developed at a time when computer security was a low-risk issue. In some systems, this factor may be more significant for system security than good configuration of a firewall on an IP connection.

Proper application of system security architecture helps to make use of a broad range of mechanisms in a holistic way, and is a condition for building and maintaining robust systems. This architecture also helps to give the operator a consistent overview of the system. Our studies have shown that it takes time and resources to get even simple details about systems. Systems are often tied closely with other systems, on the basis of a relatively high level of trust. The unquestioned assumption seems to be that one's counterpart has a well-designed system.

In general

In general, the technological solutions applied as part of information infrastructure often offer a built-in robustness and security solutions. In addition to this basic robustness, various types of information security products are available for end-users and service providers alike. These include anti-virus programmes, firewalls, intrusion detection systems (IDS), public key infrastructure (PKI) and authentication solutions based on cryptographic methods.

Nevertheless, the systems and networks of which these technologies and products are a part are still frequently vulnerable, especially as to threats and challenges from internal and external actors with a high capability of attack. Extensive implementation, maintenance and use of a well-integrated set of security mechanisms – all these cost time and money, from both the management and the user perspective. In a competitive market, the single business user will choose to secure his systems according to own interpretation of the risk involved. He will implement security solutions to meet the challenges that seem more or less likely. However, he will not, unless explicitly persuaded to do so, implement solution to meet challenges that seem very unlikely or barely possible.

Weak policies, the lack of basic resources and capabilities, as well as proper architectures, make the infrastructure services less robust against high-level capability threats. The lack of governmental involvement is another negative factor in this development. However, it may still be possible to keep one's operations fairly robust against day-to-day challenges.

4 New threats to modern society, and the focus on measures

4.1 Threats through the information infrastructures

While an attacker previously had to use physical means, the range of possible measures is considerably broader today. Of these, the so-called *logical means* are the most distinctive. Using such tools and with the help of computers with special software, the functions of other computers can be attacked. An attacker can, through a communication network, breach into computer systems that control critical infrastructures, such as telecommunications and energy supply, and disrupt or obstruct their functions. The consequences for society may be extremely serious. Easy access to such tools also makes it simpler for criminal individuals and organisations to inflict damage on their targets, either for profit or simply in order to show off to a particular environment.

Where computer systems are linked to the Internet, as is becoming increasingly common even in major production systems, such attacks could in principle be carried out from anywhere in the world. ICT has thus become a weapons platforms for those seeking to inflict damage on a nation, a company or an individual.

The expert – the person (or persons) responsible for the installation or day-to-day operation of the system – is an important factor in any information infrastructure. If an attacker manages to persuade an expert to carry out illegal operations, the attacker will have greater chance of success. The combination of such *social* and logical means may prove very effective for an attacker.

The increasing inherent complexity of information and communication infrastructures also constitutes a threat in itself. Today's systems and networks have become so complicated that it is often impossible to have a full overview of their structures. They cover large geographical areas – sometimes the entire world – and may embrace many spheres of activity. Simple random technical errors or the external influences of nature or individuals may initiate unpredicted chain reactions. Malfunctions as a result of even simple technical errors or defective human operations may rapidly become extensive. This can prove even more serious if a calculating enemy carries out the initiating event. On the other hand, this very complexity may also make it difficult for an attacker to be sure of reaching his goal. In any case, the uncertainty caused by this complexity constitutes a serious problem, because being able to have an overview of the system is a clear prerequisite to achieving a secure system.

4.2 Significance of high-capability threats to society

It is difficult to assess what threats we are facing today and will face in the future. In the papers we read of new breaches of information systems security in banks, hospitals and other individual companies. We also see frequent reports that malfunctions in telecommunications networks have led to malfunctions in critical functions in society – air traffic, emergency services, etc. In recent years, major accidents and natural disasters have also caused malfunctions in information infrastructures, primarily as a result of physical damage.

Most incidents of this type are the result of a single or few occurrences of actions with a low degree of simultaneity. Even with a human being behind the actions, the capability is so low that sheer luck is the reason for success, a success that is often limited. One example is the 14-year-old boy who was able to control the sluice gates of a North American power-supply plant from his bedroom [HN00]. This was a case of pure luck coinciding with unacceptable vulnerability in a control system. The attacker had probably no capability to use his action to cause anything more than occasional harm, and he probably did not have a motive either. Threats spanning from casual script-kiddies to individual criminals may result in disruption of services important for society, but usually with limited consequences. For actors of this type, the motive for damaging society must be considered as fairly low, even if the capability of some of them might be high and increasing. At any rate, it is certain that we in the future will have to expect threats from such actors.

It is more uncertain which players will have the combination of a significant *motive* and the necessary *capability* of means to constitute a serious threat to society. What does seem certain is that the capability for such attacks already exists. The more or less infamous exercise Eligible Receiver, carried out by the US intelligence service in 1997, can be used as an illustration of this [H98]. About 35 specialists who had access to the Internet and were pretending to be foreign enemies, managed to carry out, in a short space of time, computer attacks that, it was claimed, could have damaged both civilian and military targets in the USA. Among other things, they claimed they were capable of causing an electrical power blackout in large parts of the country and disruption in some of the national telecommunication services.

It is clear that both national intelligence services and military organisations are establishing and developing a capability on operations in information infrastructures. Computer Network Attack (CNA) is the most frequently used term for this capability in warfighters' organisations [SD00]. In a US Defence Science Board (DSB) report of 2000 it is indicated that approximately 20 nations at that time were developing such a military capability [DSB00]. Other sources have estimated this figure to be much higher.

So far, there is no proof that terrorist organisations or nations have been behind massive, structured information attacks, although it appears that such attacks were used during the Kosovo conflict in 1999, and during the Palestinian al-Aqsa Intifada that erupted in September 2000. Terrorists have also discovered the potential in using Internet and ICT to organising terror actions. Experts do not agree, but some have claimed that the cyber threat from radical Islamic terrorists is becoming even more relevant due to their rapidly growing computer knowledge [L03].

4.3 Today's focus on measures

Predicting future threats to information infrastructures in society is extremely difficult. When deciding which protective measures to take, what is believed to be *possible* must be assessed against with what is felt to be *probable*. For instance, no extensive war in Western Europe seems likely in the near future, but new players may arrive on the scene more quickly than we expect, and these may have a considerable capability, particularly with respect to modern forms of attack. It is important that the level of protection more or less matches the consequences any possible threat may have, both for individual companies and society as a whole. This in turn probably necessitates differentiating the level of protection according to how critical the consequences for society can be expected to be. This seems at first to be a simple matter, but is in reality an extremely complicated challenge, not least because of system interdependencies.

This differentiation is illustrated in Figure 1, where information infrastructures essential to private and governmental production of goods and services are ranked in four levels. At the top level are systems and infrastructures of high importance to national security, mainly in military organisations and the national government. Production of services from critical infrastructures like telecommunication and electric power supply are at the second level. At level three we find large companies and industries that produce goods of high importance for society. At the bottom level we find the majority of small and medium enterprises, as well as households. Some large companies are also to be found in this group.

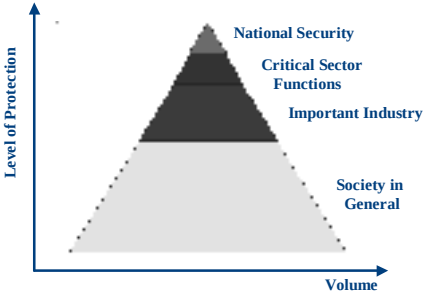

Figure 1: Level of protection versus volume of information infrastructures

For national security at the top level, the requirement to information security has traditionally been founded primarily on a very strict rule-based security regime. For the bottom part, the competition and the market forces will stimulate to an optimal security level based on customer willingness to pay for security, where this willingness of course will vary with the circumstances and the risk of loss. One challenge is thus to build a security regime that can span from top to bottom.

However, the greatest challenge is to be found in-between – in the information infrastructures supporting such critical sector functions as telecommunications and power supply, as well as important industry production. Today there are very few and modest requirements to information infrastructure security in this area, even if many claim that major disruptions may also be inflicted on national security in the context of the requirements of modern society. In the course of the past ten to fifteen years, these sector functions have been affected by dramatic changes in organisational structures as well as ownership. What used to be government-run operations are today normally privately owned and operated. The old security regime from the Cold War is generally no longer in place, without having been replaced by any new regime. This constitutes a serious challenge for modern society; in particular if it is faced with high-capability threats from nations or organisations.

5 Aim and analytical challenges of the ICT vulnerability project

The purpose of the planned project "Vulnerability in critical information infrastructures (ICT) of society" is to give recommendations on strategies with measures to reduce vulnerability in critical information systems. The project will examine the vulnerability of information infrastructures ranging from peacetime situations to security policy crises and war, focusing on high-capability man-made threats. Thus the project will represent a supplement to ongoing and planned research on information security conducted by civilian research institutes in Norway. The project will seek both national and international cooperation and information exchange, with an emphasis on methodology and exchange of data and main findings.

The project intends to employ the multi-methodological approach developed in previous research [H97] [HA97] [NH98]. This approach includes scenario analysis, causal mapping, crisis and war games, probabilistic cost estimation and multi-criteria decision analysis. We anticipate, however, a need to further develop this methodological "tool box". Perhaps system dynamics and network analysis can provide a good supplement to the existing and used methods. Consideration will also be given to using other techniques of soft operation analysis.

Thus far, we have decided to study in detail Norway's banking/finance sector and the health sector, both of which are heavily dependent on robust information infrastructures for information exchange and processing. Other interesting sectors for more in-depth study are oil and gas, and the forces of law and order. The final results will be generalised by extracting findings from all sector studies, including earlier research on vulnerability in society.

The vulnerability analysis will focus on vulnerability as a function of internal properties, application and the human factor, as well as interdependencies with other sectors. The consequences of system failure will be analysed on the system level, the organisational level and finally the level of society.

With the FFI studies on vulnerability in society we can claim to have succeeded in analysing complex socio-technological systems. However, we now face even greater analytical challenges, due to the huge complexity and the concomitant need to limit the analysis.

Literature

[F02] Fridheim Håvard, 2002: Survivability of the Modern Society – Deregulation of Services vs Critical Infrastructure Vulnerability, Paper presented at 1st European Survivability Workshop, 26–28 February, Köln-Wahn, Germany.

[FHH01] Fridheim Håvard, Hagen Janne, Henriksen Stein, 2001: A Vulnerable Electric Power Supply – Final Report from BAS3, FFI/RAPPORT-2001/023821, Forsvarets forskningsinstitutt, Kjeller, Norway (in Norwegian, with abstract in English).

[H97] Hagen Janne Merete, 1997: Economic Analysis of Civil Emergency Efforts – a Methodological Approach, FFI/RAPPORT-1997/03574, Forsvarets forskningsinstitutt, Kjeller, Norway.

[HA97] Hagen Janne, Arnestad Petter, 1997: Method for Economic Analysis of Civil Emergency Measures, FFI/RAPPORT-97/02025, Forsvarets forskningsinstitutt, Kjeller, Norway (in Norwegian, with abstract in English).

[HF99] Hagen Janne, Fridheim Håvard, 1999: Cost-Effectiveness Analysis of Measures to Reduce Vulnerabilities in the Public Telecommunication Sector, Paper presented at 16 ISMOR, 1–3 September 1999, The Royal Military College of Science, UK.

[H01] Henriksen Stein, 2001: Impacts due to Power Blackouts – What happens when loss of electricity occurs? FFI/RAPPORT-2001/01867, Forsvarets forskningsinstitutt, Kjeller, Norway (in Norwegian, with abstract in English).

[HN99] Hagen Janne, Nystuen Kjell Olav, 1999: Protection of Society with focus on Public Telecommunication, FFI/RAPPORT-99/00240, Forsvarets forskningsinstitutt, Kjeller, Norway (in Norwegian, with abstract in English).

[HRL03] Hagen Janne, Rodal Gry Hege, Lia Brynjar, Torp Jan Erik, Gulichsen Steinar, 2003: Protection of Society with focus on Transportation. FFI/RAPPORT-2003/00929, Forsvarets forskningsinstitutt, Kjeller, Norway (in Norwegian, with abstract in English).

[HOF97] Hæsken Ole Martin, Olsen Tor Gunnar, Fridheim Håvard, 1997: Protection of Society (BAS) – Final report. FFI/RAPPORT-1997/01459, Forsvarets forskningsinstitutt, Kjeller, Norway (in Norwegian, with abstract in English).

[HN00] Hagen Janne, Nystuen Kjell Olav, 1997: Protection of Critical Infrastructure – Meetings with private and governmental institutions in USA and Canada, February 2000. FFI/REISERAPPORT-1997/01096, Forsvarets forskningsinstitutt, Kjeller, Norway (in Norwegian, with abstract in English).

[H98] Hamre John J, 1998: Speech to the Council on Foreign Relations – June 5, 1998, Defense Link – http://www.defenselink.mil/news/Jun1998/t06181998_t0605cfr.html.

[SD00] Space Daily, 2000: US Space Command takes charge of Computer Network Attack – October 2, 2000, http://www.spacedaily.com/news/milspace-00n.html.

[L03] Lia Brynjar, 2003: Terror against Transport: A (re-) assessment of terrorist threats against transport related targets after September 11th, FFI/RAPPORT-2003/00731, Forsvarets forskningsinstitutt, Kjeller, Norway (in Norwegian, with abstract in English) (Exempt from public disclosure).

[MD03] The Ministry of Defence, 2003: National Strategy for Information Security. Challenges, Priorities and Measures, 2 February 2003, Draft version (in Norwegian).

[DSB00] Defense Science Board – Summer Study, 2000: Protecting the Homeland – Defensive Information Operations – 2000 Summer Study – Volume II.

[MTI00] Ministry of Trade and Industry, 2000: Society's Vulnerability due to its ICT-dependence, Report, October 2000 (in Norwegian).

[MTI00E] Ministry of Trade and Industry, 2000: Society's Vulnerability due to its ICT-dependence – Abridged version of the main report, October 2000.

[NH98] Nystuen Kjell Olav, Hagen Janne, 1998: Method for analysing measures to reduces the vulnerability in telecommunication. FFI/RAPPORT-98/06261, Forsvarets forskningsinstitutt, Kjeller, Norway (in Norwegian, with abstract in English).

[NOU00] NOU, 2000:4 (July 2000): A Vulnerable Society – Challenges for Security and Emergency Preparedness in the Society. Report from Government Commission, Submitted to the Ministry of Justice and Police (in Norwegian).

[JDWP00] White Paper no 17 (1999–2000): Vulnerability of Society – The road to a less vulnerable society, Ministry of Justice and Police (in Norwegian).

[SDWP01] White Paper no 47 (2000–2001): Telecommunication Security and Emergency Preparedness in a Competitive Market (in Norwegian).

[NHGP03] National Strategy for Information Security – Challenges, Priorities and Measures (Draft), Ministry of Trade and Industry, February 2003 (in Norwegian).

[OMS00] Hagen, Janne, 2000: The Vulnerability of the Norwegian Society – Threats and Consequences. In: *The Military in a New Era*, Oslo Militære Samfunds 175 års jubileumsbok, pp 203–204 (in Norwegian).