FFI RAPPORT

ICT CRISIS MANAGEMENT - Actors and Roles

MØRKESTØL Kristin, BOGEN Lene

FFI/RAPPORT-2006/00235

ICT CRISIS MANAGEMENT - Actors and Roles

MØRKESTØL Kristin, BOGEN Lene

FFI/RAPPORT-2006/00235

FORSVARETS FORSKNINGSINSTITUTT
Norwegian Defence Research Establishment
P O Box 25, NO-2027 Kjeller, Norway

FORSVARETS FORSKNINGSINSTITUTT (FFI)
Norwegian Defence Research Establishment

P O BOX 25
N0-2027 KJELLER, NORWAY

UNCLASSIFIED

SECURITY CLASSIFICATION OF THIS PAGE
(when data entered)

REPORT DOCUMENTATION PAGE

1) PUBL/REPORT NUMBER	2) SECURITY CLASSIFICATION	3) NUMBER OF PAGES
FFI/RAPPORT-2006/00235	UNCLASSIFIED	25
1a) PROJECT REFERENCE	**2a) DECLASSIFICATION/DOWNGRADING SCHEDULE**	
FFI-I/1014	-	

4) TITLE

ICT CRISIS MANAGEMENT - Actors and Roles

5) NAMES OF AUTHOR(S) IN FULL (surname first)

MØRKESTØL Kristin, BOGEN Lene

6) DISTRIBUTION STATEMENT

Approved for public release. Distribution unlimited. (Offentlig tilgjengelig)

7) INDEXING TERMS

IN ENGLISH:	IN NORWEGIAN:
a) ICT	a) IKT
b) Critical Infrastructure	b) Kritisk infrastruktur
c) Crisis management	c) Krisehåndtering
d) Scenarios	d) Scenarier
e)	e)

THESAURUS REFERENCE:

8) ABSTRACT

This report is an extended abstract/short version of a similar report in Norwegian. It presents an analysis and overview of the different actors involved in ICT crisis management in Norway. It looks at the responsibilities, roles and the measures available, and also gives an introduction to ICT crisis management in Italy and France. The study is part of a comprehensive project, “Critical Information Infrastructure Protection”, and has been conducted to provide background information for future recommendations and the ranking of measures for reducing vulnerabilities.

Interviews and a workshop, based on several crisis scenarios, lead to the conclusion that an ICT crisis is often treated as any other crisis. It proves especially challenging to define an “owner” of an ICT crisis, due to the difficulty in allocating it in a specific sector. The operational crisis management is executed at the lowest possible level, as is also the findings from other countries.

9) DATE	AUTHORIZED BY	POSITION
	This page only	
2006-02-08	Jan Erik Torp	Director

ISBN 82-464-0992-1

UNCLASSIFIED

SECURITY CLASSIFICATION OF THIS PAGE
(when data entered)

CONTENTS

ICT CRISIS MANAGEMENT - Actors and Roles

1 INTRODUCTION

This report is an extended English abstract of the report "ICT crisis management: actors and roles"[1]. The report is the result of a ten-week summer project under the project "Critical Information Infrastructure Protection" (BAS5)[2], lead by the Norwegian Defence Research Establishment (FFI)[3]. This English report has been prepared in order to give access to the results from the summer project to a broader audience, in particular those persons who were contacted during the summer project.

The activities of the BAS5 project are within the field of information and communication technology (ICT) and infrastructure protection. It will contribute to the development of methods to analyse vulnerabilities in critical information systems. The report "ICT crisis management: actors and roles" analyses different actors and their roles when involved in an ICT *crisis*, and provides background information for the future ranking of critical infrastructures, a sub goal of the BAS5 project. The report presents an overview of the different actors involved in ICT crisis management in Norway. It particularly studies the responsibilities, roles and measures available. To compare Norway's approach to this challenge, the report also gives a description of ICT crisis management in Italy and France.

An ICT crisis can have several causes, for instance a technical error, an act of sabotage or a natural disaster. The goal of the analysis is to see how an ICT crisis can be managed in Norway, given different situations causing the crises. The analysis explores this with respect to three main areas:

- Responsibility, authority and tools available in a given ICT crisis
- Instruments available for the national authorities
- Do different forms of crisis require different management?

The method used for data collection is based on primary data such as interviews with relevant actors, as well as secondary data (existing literature), mainly assembled through Internet research. A workshop with Norwegian actors took place on the 23rd of August 2005, to discuss the results of the analytical findings and to rectify potential misunderstandings or possible sources of error in the work.

---

[1] Bogen L, Mørkestøl K (2005): Håndtering av IKT-kriser – Aktører og Roller, FFI/RAPPORT-2005/03536. The report is in Norwegian.
[2] BAS is the Norwegian acronym for "Beskyttelse av samfunnet", roughly translated to "Protection of the society". The number 5 indicates that this is the fifth BAS project.
[3] FFI is the acronym for Forsvarets forskningsinstitutt, aka. the Norwegian Defence Research Establishment.

Italy and France were chosen as foreign case studies. Italy's handling of the Tsunami catastrophe was generally perceived as a successful operation, and it was of interest for the project to look at Italy's approach to ICT crisis management in light of this. France holds an important position in several ICT-related international forums, such as the EU agency ENISA.

Chapter 2 of this report briefly describes the concept of an ICT crisis and the use of scenarios. It gives an introduction to the new crisis management structure in Norway, before discussing the different actors involved in Norwegian ICT crisis management at the various stages. In chapter 3, the handling of a potential ICT crisis in Italy and France are analysed. Finally, chapter 4 and 5 present a discussion and the concluding remarks.

2 CRISIS MANAGEMENT IN NORWAY

2.1 What is an ICT crisis?

An *ICT crisis* is not easily defined. For the purpose of this analysis we have used a definition where an ICT crisis implies "*a situation where ICT systems are put out of play and cannot be restored by normal manning and routines"*.

In order to discuss an ICT crisis in a larger perspective, focus has been set on the distinction between *safety* and *security* related challenges. A stronger cooperation between research communities in these fields is necessary in order to better deal with an ICT crisis.

2.2 Scenarios

In order to visualise ICT crisis management in Norway, three scenarios of possible ICT crises were developed and discussed with the actors involved. The outcome of the discussions is illustrated in three separate models in order to evidence which actors are involved at the different stages of the crisis.

The first scenario is an ICT crisis caused by an internal error in a telecommunication operator's supervisory control and data acquisition (SCADA) systems. The error might occur due to an accidental or deliberate (i.e. sabotage) failure, either technical or operational, and causes a failure of delivery of important communication services to a large area in Norway for at least two days.

The second scenario is based on high wind causing a critical power failure due to fallen power line poles, which subsequently causes disruptions in the

telecommunication systems. Without electrical power and ICT services available, agitation and unrest in the public occur due to the lack of basic services (available heating, food and information). This scenario differs from the first, as it strikes more sectors simultaneously.

The third ICT scenario looks at security threats, where several sectors are struck by a number of politically motivated and well-organised cyber attacks. Targets include the national railway and civil aviation control.

Three models were developed in order to illustrate the actors involved in the different scenarios. The model below (Figure 1) represents an example of how these models were employed.

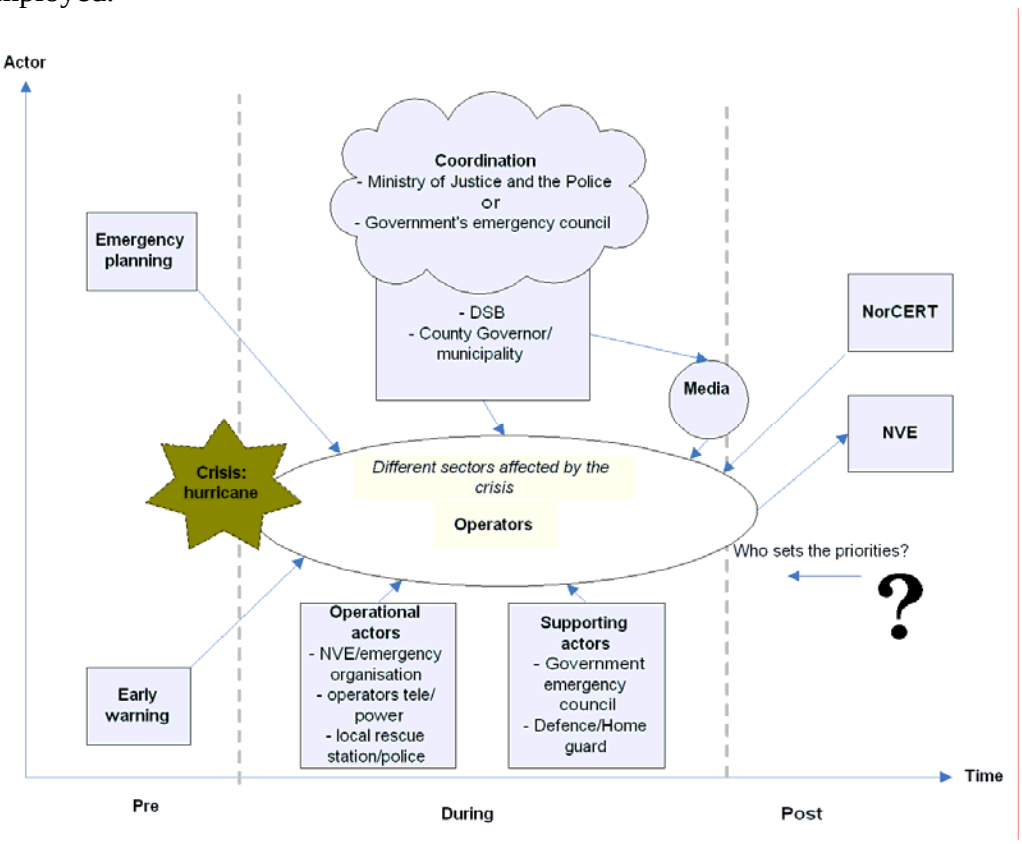

Figure 1: Example of involved actors in one scenario

The scenarios were used to give a better understanding of the actors involved in the management of an ICT crisis with varying degree of seriousness. At the early stages of the analysis, it was believed that there would be different patterns in the handling of the different scenarios, according to its level of seriousness. Instead, what we found was that there are several similarities in the scenarios and in their management, but that the management changes as the crisis escalates.

The scenarios all involve three similar stages. They have been divided into a pre-, during and a post-crisis stage. The actors that have been identified in the management

of the crisis are classified in equal categories: planning, early warning, system owners/operators, actors with supporting role, operational actors, ICT technical expertise and investigating actors[4]. If we look at the management of the crises in the pre-, during and post-critical phase, further similarities emerge between the scenarios.

2.3 Managing an ICT crisis in Norway

A guiding principle for Norwegian societal security is that every ministry in the government is responsible for the security in its own sector. The crisis organisation should be as similar as possible to the organisation used in normal operations, and the crisis should be managed at the lowest possible level. For instance, this means that a situation occurring in the telecommunications sector should be solved by the telecommunication operators or enterprises that are involved, but that the Ministry of Transport and Communications (SD) has a political responsibility for coordinating the situation should the crisis escalate.

In July 2005, the Norwegian parliament (Stortinget) established a new national structure for crisis management and coordination. The *Government's emergency council* (Regjeringens Kriseråd) will have the overall coordinating responsibility in case of a national crisis. It consists of permanent representatives from the Prime Minister's Office[5] (PMO), the Ministry of Foreign Affairs (Utenriksdepartementet, UD), Ministry of Justice and the Police (Justis- og Politidepartementet, JD), Ministry of Defence (Forsvarsdepartementet, FD) and Ministry of Health and Care (Helse- og Omsorgsdepartementet, HOD). The Ministry most affected by the crisis will be asked to take the leading position in the Council. A *crisis support unit* (available 24/7) can provide communication networks and other technical support.

2.3.1 Actors involved in ICT management prior to an ICT crisis

An important warning of an imminent cyber attack can be provided by suppliers' security solutions (Symantec, Microsoft etc.), or by the "Early Warning Unit for Digital Infrastructure" (VDI[6]), if the attack originates from cyber space. VDI has installed a tracking device at the enterprises that are member of the VDI cooperation, which supervises the cyber traffic towards the firm. The VDI only has a small number of members as of today, but may give general warnings to other enterprises if it detects massive attacks towards several of its members.

Updated emergency plans should be an integrated part of all enterprises, as well as at the ministerial levels. The quality of such plans is uncertain. For instance, the Norwegian Post and Telecommunications Authority (PT) requires obligatory

[4] Note that not all actors are present in all scenarios: for instance is the role of the investigating actors different in the scenario presented in this model, because it represents a natural disaster and not a targeted cyber attack.
[5] Prime Minister's Office: Statsministerens Kontor.
[6] VDI is the Norwegian acronym for "Varslingssystem for Digital Infrastruktur".

emergency planning in the telecommunication sector, but does not set a standard as to its content. This finding is relevant in all three scenarios.

2.3.2 Actors involved in ICT management during the ICT crisis

The findings show that during the crisis, it is mainly the task of the operator or enterprise subject to the attack (in this case: telecommunication operator, power plant, national railway etc.) to manage the situation and restore the systems attacked, although some technical advice and support can be provided by systems - and software suppliers as well as by the VDI. In the most severe crisis, one can expect that the operator may quickly be assisted by the Police. The enterprise reports progress to supervisory bodies.

The newly established national Computer Emergency Response Team (NorCERT[7]) is intended to have an advisory role in an ICT crisis. The media will be early involved in information handling, but will not participate directly in the resolving of the crisis.

If life and health is in danger, the police, the local government and the county governor (Fylkesmannen) may provide coordination and support in all three scenarios. The Armed Forces (Forsvaret) was mentioned during the interviews as a possible source of support, but this will probably only be the case when they are the only supplier of a specific service.

If the crisis escalates, higher levels of coordination will be necessary. The first scenario does not necessarily call for higher levels of coordination, unless the situation persists or life and health are in danger. In that case, a temporary local rescue station will be established, coordinated by the police with assistance from the county governor. Formal cooperation with neighbouring countries is organised through the Ministry of Justice and the Police and the Ministry of Foreign Affairs, but the different authorities have also established direct contact with their foreign counterparts, for instance in Sweden. Military equipment might be used, and army personnel (in particular the Home Guard) can be called in for assistance.

If the responsible sector can easily be designated, as in for instance scenario one, this will determine the main political coordinating unit in the crisis if it escalates to a high level. If this is not feasible, the Ministry of Justice and the Police (JD) will be given the coordinating role. The Directorate for Civil Protection and Emergency Planning (DSB) has the coordinating role between the JD and the county governor. The county governor is the connecting link between the municipalities in the affected county, but if several counties are struck, this coordination is transferred to the JD. If the crisis escalates in time and seriousness, the Government’s emergency council will be established, as is most probably the case in scenario three.

[7] The national CERT, NorCERT, is in this report discussed based on its current activity. There might be changes to the activities once its mandate is finally decided upon.

2.3.3 Actors involved in ICT management after the ICT crisis

The operator handles the restoring of the systems, with the support from system suppliers (and in the future, possibly by NorCERT). A general complicating issue for all three scenarios is how to resolve the issue of prioritisation between customers, when prioritised lists of sectors and enterprises (critical infrastructures) are not always available.

Investigation, in the case of a malicious attack, is the task of the Police cyber crime unit (Datakrimavdelingen at Kripos). In the third scenario, investigation is the task of the police security service (PST) and the reporting is made by the sector responsible in the crisis, to the nearest supervisory body.

Another challenge common for all three scenarios is time. When is the crisis grave enough for the ministries to react? No absolute criterion for this is established, but we found that each crisis depends on a continuous evaluation of the situation. The first crisis represents a sector crisis, while the others were cross-sectoral. The two latter will more quickly lead to the need for coordination on a governmental level. The Armed Forces will not enter into assistance in the crisis prior to national decision, underscoring and evidencing the need for governmental readiness and responsibility.

2.3.4 Different management in the three scenarios due to the nature of the crisis

Not all elements in an ICT crisis are managed the same way in the three scenarios.

Scenario two differs from the others due to its “natural” causes. Early warning will not be the task of the system suppliers, but will rather be performed by the Norwegian Meteorological Institute. The need for a public warning was not mentioned by any of the actors during the data collection, but this could be important, especially with regard to operators that handle critical infrastructures. Furthermore, in the second scenario there is need for cooperation between telecommunication operators and power suppliers at the local level. In this case, the Norwegian Water Resources and Energy Directorate (NVE) will work together with the county governor, and can decide to establish the power suppliers’ emergency preparedness organisation if needed. An additional challenge arises in this scenario due to the difficult restoration of ICT systems after a long period of power blackout.

The usefulness of emergency plans and early warning is important in all cases, but particularly noticeable in the third scenario, involving security threats. This scenario differs from the others due to its serious nature and because it implies a threat to national security. Prior to the crisis, the seriousness of the crisis is underlined by the fact that VDI warnings will be supplemented by threat assessments carried out by the PST. In a growing national security crisis, the political coordination becomes all the

more essential, yet problematic. Determining the responsible actor for coordination is the main challenge, i.e. determining who *"owns"* the crisis. Many of the actors interviewed believe that the crisis will be managed by the sector subject to the attack. In reality this will be difficult, as more than one sector is hit in this scenario. It is, however, highly probable that the Government's emergency council will be established, but it is less clear which ministry they will point to as the "owner" of the crisis. At the workshop organised in August 2005, the actors expected widespread cooperation between the military and the civilian authorities (JD and FD). The newly constituted Ministry of Modernisation (MOD[8]) was discussed as a potential owner, due to its general responsibilities for governmental ICT, but participants at the workshop claimed other actors would be more appropriate.

DSB as well as the county governor will have the same responsibilities as in the previous scenarios. Due to the serious character of this crisis, the participants at the workshop assumed that international resources could be called upon for assistance. Article 5 in the North Atlantic Treaty was mentioned as a possible measure (but perhaps not a very likely one), as Norway could invoke the support of the allies and possibly access capabilities in the NCIRC (NATO Computer Incident Response Capability). In Europe, the newly created Agency for European Network and Information Security (ENISA) could be of useful assistance, if it manages to pool resources and information from the different member states in the EU.

In order to set priorities and make the best use possible of the supporting systems available, a clear distribution of responsibilities is absolutely necessary. Who takes what priorities in which domain seems unclear for the time being.

3 ICT MANAGEMENT IN ITALY AND FRANCE

Knowledge about ICT management in other European states can be useful in order to enhance national capabilities in the field. The study mainly reflects information from official homepages, documents and reports collected on the Internet. In the case of Italy, several telephone interviews have also been conducted in order to increase the quality of the collected data.

Organisational differences in the European states are mirrored in the attempts to create a common forum in the EU, which will be further depicted below. Our description of the organisational structure for handling an ICT crisis in Italy and France follows the logic of the organisation in Norway, i.e. it is described by referring to the timeline and the actors involved at the different stages of the crisis: before the crisis occurs, during the ICT crisis, and after the critical phase is over.

[8] The Ministry of Modernisation is renamed the Ministry of Renewal and Administration (Fornyings- og administrasjonsdepartementet) 1.January 2006.

3.1 ICT management in Italy

Today, warning of cyber attacks and possible ICT crises in Italy comes from the different CERTs or from the operator's collection of warnings from system suppliers (Symantec, Microsoft etc). The main CERT in Italy as of today is the CERT-IT, a state authorised warning unit run by the students at the University of Milan, under supervision of Professor Danilo Bruschi.

Two initiatives are in the pipeline: the creation of a national CERT (GovCERT.IT) under minister without portfolio Lucio Stanca, and the broader Centre for national anticrime and the Protection of Critical Infrastructure (Cnaipic), reporting to the Ministry of the Interior. Both of these will have warning tasks, but the latter will not be limited to the ICT sector. Cnaipic will also supervise and handle cyber attacks directed towards other critical infrastructure. It is still unclear which of the two units will hold the position as the national warning unit.

During the crisis, the ministry responsible for coordination will be the Ministry of the Interior, unless life and health is in danger. If the crisis escalates, the coordination will be transferred to the Department for Civil Protection, administratively reporting to the Prime Minister's Office (PMO). The operational management of the crisis is the responsibility of the system operators, assisted by CERTs and systems suppliers. If the crisis' range is broad, the county and region will have coordinating responsibilities according to the principle of subsidiarity. The system of Civil Protection may be called upon in a national crisis to appoint the ministry responsible for the crisis, and can contribute with local staff and manning if need be. The Cnaipic centre has increased mandate through the "anti-terror law" of July 24th, 2005, and can, once operational, assist in restoring critical infrastructure[9]. The Prime Minister assumes political responsibility.

The system of Civil Protection can assist in the manual restoring of order, but is not appositely equipped to handle an ICT crisis. A reform of the system is under way to better prepare for this kind of crisis[10].

Operators restore the systems after a crisis, and the Police's Postal and Communication Service manages the investigation of the causes. The Police have access to data logs and can benefit from wider competences in, amongst others, the already mentioned anti-terror law.

[9] The Cnaipic centre ("Centro nazionale anticrimine informatico di protezione infrastrutture critiche) is formally established but not operational by September 2005. Ref. Roberto Setola, (Gruppo di lavoro sulla Protezione delle Infrastrutture Critiche Informatizzate), 1.09.05.

[10] Motivating factor for an adjustment were the severe consequences of the 2003 Swiss power failure causing a blackout in the Italian power supply, and the subsequent failure in the communication systems when emergency power supply failed to suffice.

Several actors in Italy have expressed a wish to use *exercises* as a method to better prepare for an ICT crisis in Italy. So far, this method has not been applied. The future role of Cnaipic could lead to a better management of all critical infrastructure and the mutual dependencies in the ICT sector, and Cnaipic could potentially conduct exercises with relevance for the ICT sector.

Another interesting feature of Italian management is the Civil Protection system, which has proven very efficient in for instance the handling of the Tsunami catastrophe in South-East Asia in December 2004[11]. If the Italian government manages to readjust this system to prepare also for assistance in an ICT crisis, this could represent an important example also for other countries. Coordinating ICT in general could be simplified by the new organisational structure suggested by the ICT technical committee[12] in 2004. So far, only the project GovCERT.IT has been realised, but still needs to be made fully operational.

In-depth analysis on ICT knowledge in public and private sector, as well as a general awareness rising is still lacking in Italy.

3.2 ICT management in France[13]

ICT management and the national plan on information security[14] in France, is based on the OECD guidelines. The management is shared between the PMO, more exactly the Central Direction of Security in the Information systems (DCSSI)[15], and the ministries, principally the Ministry of the Interior.

Before the crisis is a fact, the national early warning system for cyber attacks, CERTA, provides the public sector enterprises with information and assistance. If the crisis is severe enough, the Vigipirate plan of 2004 will indicate the level of alert.

The Ministry of the Interior, Head Office for the Fight against ICT-crime (OCLCTIC)[16], will manage the crisis. If the crisis escalates, the overall coordination will be transferred to the Secretariat-general for National Protection (SGDN) under the PMO, while a specialised centre reporting to the SGDN, COSSI[17], will lead the

[11] Further information at the Department of Civil Protection Homepage: http://www.protezionecivile.it/sistema/index.php.
[12] Comitato tecnico nazionale per la sicurezza ICT (2004)*"Proposte concernenti le strategie in materia di sicurezza informatica e delle telecommunicazioni per la pubblica amministrazione,* www.governo.it/GovernoInforma/Dossier/sicurezza_informatica/proposte.pdf.
[13] This study is mainly based on Internet-research, and could therefore have some shortcomings.
[14] ADELE (2004) *"Plan de renforcement de la sécurité"* , and DCSSI (2004) *"Guide pour l'élaboration d'une politique de sécurité.*
[15] DCSSI: "Direction centrale de la sécurité des systèmes d'information"
[16] OCLCTIC: "Office Central de Lutte contre la Criminalité liée aux Technologies de l'Information et de la Communication".
[17] COSSI: "Centre Opérationnel de la Sécurité des Systèmes d'Information".

operational coordination. In 2003, COSSI organised two exercises in order to test the efficiency of the existing plans for ICT crisis management.

The operators have responsibility for the operational management and restoring of the systems, but if the crisis is considered grave, several 24/7 operational centres will be established in both the SGDN and in the affected sectors[18]. The OCLCTIC will take on the investigative task.

The CERTA provides insufficient warning to the private sector[19]. Improving this could turn the CERTA into an instrument of trust and cooperation between private and public sector, but this is currently not at an advanced stage. On the other hand, a thematic server[20] provides both the public and private users with relevant information and a useful "who's who" in ICT-security.

3.3 ICT on a European level

As mentioned above, European actors vary in the handling of ICT challenges. In some countries the Prime Minister's Office is in charge of the sector, in other it is the Ministry of the Interior. Such differences are reflected when trying to agree on common standards and policies of cooperation on ICT in Europe.

Three EU initiatives are of special interest[21]. The 2004 "European Network and Information Security Agency" (ENISA), the "European Programme for Critical Infrastructure Protection" (EPCIP) and the "Critical Infrastructure Warning Information Network" (CIWIN), the two latter to be implemented and operational by the end of 2005[22].

ENISA is about to become fully operational. It will have 30 employees and an initial mandate for five years. ENISA will advise and coordinate the European Commission as well as the member states on ICT-related matters, conduct risk analysis and promote cooperation between private and public sector.

The EPCIP-programme will assist industry and the EU member states' governments in the analysis and the protection of all critical infrastructures. The EPCIP will continue to "...identify critical infrastructure, analyse vulnerability and

[18] ADELE (2004) *"Plan de renforcement de la sécurité"*.
[19] CERTA informs the private sector "..just a few days after" the public sector. DCSSI (2004), *"Mise en oeuvre en France des lignes directrices de l'OCDE"*, page 2.
[20] Thematic server: Serveur Thématique sur la sécurité des systèmes d'information, http://www.ssi.gouv.fr/fr/index.html.
[21] The "European Governments CERTS-group" (EGC) is an interesting non-EU initiative. It has developed from bilateral collaboration and now has 7 member-states, with Norway's NorCERT joining in Sept.2005.
[22] Ref communication with Marcelo Masera (Joint Research Centre), 28.07.05.

interdependence"[23] with an "all-hazards approach", and is, amongst other tasks, to elaborate an emergency plan for ICT.

The CIWIN network will build on the corresponding American institution, CWIN. Its exact functions and range of activities remain to be decided, and as the above-mentioned initiatives, the main challenge is that the member states might be reluctant to cooperate closely, because ICT vulnerability is considered to be of vital national interest. Hence, state sovereignty is preferred.

4 DISCUSSION

After having described the management of an ICT crisis in Norway and other European countries, the three main points of the analysis are summarized: who is responsible in an ICT crisis, what are the tools available, and finally, does the management differ according to the severity of the crisis?

4.1 Who has overall responsibility in a given ICT crisis in Norway?

It has been said that in Norway, the responsible ministry should be the one that has most "at stake" in a crisis; i.e. the sector or department in which the crisis occurs should determine the responsible ministerial actor. However, in an ICT crisis, the challenge is its cross-ministerial nature. The findings imply that when it is difficult to detect the ministry that should take responsibility, the Ministry of Justice and the Police intervenes. An escalation of the crisis calls for the Government's emergency council to be constituted.

The analysis based on our scenarios suggests that the Ministry of Modernisation, which is responsible for governmental ICT in general, will not have a role in an ICT crisis. It was several times suggested that the Government's emergency council be summoned at an early stage, and this was particularly expressed at lower levels of administration. The council's intervention depends on the severity of the crisis. It would naturally be convened in scenario three, where national security is at stake, less certainly so in scenario one and two, although its constitution would be evaluated constantly. The lack of practical experience in ICT crisis management seems to leave an uncertainty as to what should happen, and actors often call for a "super-ministry for safety and security".

The organisational readjustments made both in Norway and Italy underscore the many parallel processes going on in the ICT sector. The constitution of the Cnaipic centre in Italy might require a reconsideration of the competences appurtenant to the Italian

[23] European Commission (2004), *"Critical Infrastructure Protection in the fight against terrorism"*, COM(2004)702F.

PMO and the Ministry of the Interior, which outcome can prove interesting also for Norway. The ongoing creation of national CERTs in both countries can provide better organisation, as well as increased cooperation between public and private sector. Norway is in a special situation with regard to such cooperation, as there is already widespread exchange of information through the NorCERT and the VDI, creating an environment of trust. France has had a national CERT since 1999, but still struggles to provide cooperation between the sectors. The CERTs also have different tasks as the national CERT in Italy and France provides both warning and response. In Norway, these tasks are separated between VDI and NorCERT, but as they share the physical office premises, it leads to a salient degree of cooperation.

4.2 Which policy instruments are available in a given crisis scenario?

Among the tools available are the use of law and governmental financial resources. The most efficient tool is said to be emergency plans as well as the rehearsal and evaluation of these through exercises. The advantage of such plans is to better prepare for an emergency situation, but it has been claimed that the use of exercises could prove both closer to reality as well as a more interesting learning activity for the participants. Particularly in the case of Italy, the use of exercises in the field of ICT crisis management seems to be lacking.

The question of financial resources was not considered to be a major problem in ICT crisis management. According to the actors interviewed and the participants at the workshop, the mentality is dominated by the need for immediate action: "…build up and find the financial resources later". Whether or not this is the case in a real situation remains to be seen.

An additional instrument could be information to the public through a set of "do's and don'ts". This was not mentioned during the interviews or the workshop, but could prove vital in an actual crisis situation[24].

4.3 Is the crisis managed differently according to the kind of crisis scenario?

As described in chapter 2.3.4, it seems that the actors involved have the same responsibility in all three scenarios, both at the operational level and the coordinating level. A major question can be raised as to in which scenario, and at what point in time, will the Norwegian emergency council be established.

[24] This was one of the recommendations in the BBC terror-scenario in London, "London under attack", BBC Panorama, one year before London was hit by a real terror attack in July 2005 (broadcasted on BBC One on Sunday, 16 May 2004 at 22:15 GMT).

Specific challenges arise in an ICT crisis, such as the question of political ownership of the crisis, and the problem of sectoral interdependencies leading to domino effect breakdowns in other sectors. While there are some differences between an ICT crisis and other crises, the consequences rapidly become the same.

In Italy and France it is clearly the concern of life and health that determines the management of the crisis. If life and health is endangered, the management is escalated to a national level. If it is a simpler crisis, the operators manage with the assistance of the national CERT. So far, in Norway and Italy these CERTs are still not fully operational, and the role of the French CERT is weakened by its less ambitious action towards the private sector.

5 CONCLUDING REMARKS

Throughout this analysis, the main actors and roles in an ICT crisis have been identified. Potential for improvement in the Norwegian ICT management suggests that one should not consider ICT as a "sectoral issue", and that overall responsibility should be more clearly defined. It is relatively easy to define the lines of responsibility in the *management* of the crisis, but more insecurity exists as to who has the overall "*ownership*". Since the crisis is to be resolved at the lowest possible level, one can discuss the relevance of such a distinction. The challenge is to think of ICT as an issue that stretches across the departments, and not to focus only on the sectoral principle. In Italy, responsibility is clearer. It is in the hands of the Ministry of the Interior, unless life is in danger. In that case, it is transferred to the Prime Minister's Office.

When more than one sector experiences the effects of an ICT crisis in Norway, placing the responsibility becomes more difficult. On the other hand, interviewees stated that this does not cause a problem as long as the responsibility for the operational management is clearly defined to the lowest possible level of administration.

The authorities have few policy instruments at hand in such a crisis, but as the handling is made mainly at the operators' level, it is more important for the government to assure that good practice is in place, including emergency plans and regular exercises. The use of simulations and exercise could be a useful supplement and means of correction of crisis management in Italy. Desire has been expressed also in Norway for more large-scale exercises specifically with regard to an ICT crisis. In general, an ICT crisis is considered as any other crisis. Several initiatives at the international stage look promising, but chances are that they remain "paper tigers" unless practical testing and exercising are used to better assess the preparedness for an

ICT crisis. The issue of sovereignty will also influence the success of the efforts on an international and especially a supranational level of cooperation.

Due to the short timeframe of this report, not all areas have been sufficiently explored. A report on the Norwegian government's efforts to secure ICT infrastructure has been released by the Office of the Auditor General[25], and will make a useful contribution to the results of this analysis. The OECD report "Review of Risk Management Policies in Norway Concerning Information Security" will be available early 2006. Furthermore, it is of interest to follow the Norwegian government's emergency council once it becomes fully operational. The Italian national CERT and the Cnaipic centre, as well as the future use of large-scale exercises to better the crisis preparedness also need to be further analysed. Exploring the existence and use of emergency plans could prove beneficial, especially with regard to critical infrastructures. Lessons might be drawn from reports following the recent hurricane Katrina in the USA, and finally, the question of public information would need more analysis, as it is especially difficult in a crisis where the communication systems are damaged.

[25] The Office of the Auditor General of Norway ("Riksrevisjonen") is the controlling agency of the Norwegian Parliament. Riksrevisjonen (2006), *"Riksrevisjonens undersøkelse av myndighetenes arbeid med å sikre IT-infrastruktur"*, Document no. 3:4 (2005-2006).

APPENDIX

A LIST OF ABBREVIATIONS

BAS	Protection of the Society (”Beskyttelse av Samfunnet”)
CERT	Computer Emergency Response Team
CIRC	Computer Incident Response Capability
CIWIN	Critical Infrastructure Warning Information Network
Cnaipic	Centre for national anticrime and the protection of critical infrastructure (“Centro nazionale anticrimine informatico di protezione infrastrutture critiche”)
COSSI	Centre Opérationnel de la Sécurité des Systèmes d'Information”
DCSSI	Central Direction of Security in the Information systems (“Direction Centrale de la Sécurité des Systèmes d'Information”)
DSB	Directorate for Civil Protection and Emergency Planning
ENISA	European Network and Information Security Agency
EPCIP	European Programme for Critical Infrastructure Protection
EU	The European Union
FD	Norwegian Ministry of Defence
HOD	Norwegian Ministry of Health and Care
ICT	Information and Communication technology
JD	Norwegian Ministry of Justice and the Police
MOD	Norwegian Ministry of Modernisation
NATO	North Atlantic Treaty Organisation
NVE	Norwegian Water Resources and Energy Directorate
OCLCTIC	Ministry of the Interior, Head Office for the Fight against ICT-crime (“Office Central de Lutte contre la Criminalité liée aux Technologies de l'Information et de la Communication”)
PMO	Prime Minister’s Office
PST	The Police Security Service
PT	Norwegian Post and Telecommunications Authority
SCADA	Supervisory control and data acquisition systems
SD	Norwegian Ministry of Transport and Communications

SGDN	Secretariat-general for National Protection
VDI	Early Warning Unit for Digital Infrastructure (”Varslingssystem for Digital Infrastruktur”)
UD	Norwegian Ministry of Foreign Affairs

B BIBLIOGRAPHY

B.1 Bibliography

ADELE (2004), *"Plan de renforcement de la sécurité des systèmes d'information de l'Etat (2004-2007)"* (PRSSI), 10.03.2004 SMK/ ADELE, France
http://www.ssi.gouv.fr/site_documents/PRSSI/PRSSI.pdf

BBC Panorama (2004), Great Britain *"London under attack"*, documentary film broadcasted on BBC One on Sunday, 16 May 2004 at 22:15 GMT.

Bogen, L. og Mørkestøl, K. *"Håndtering av IKT-kriser - Aktører og roller"*, FFI/Rapport-2005/03536

Comitato tecnico nazionale per la sicurezza ICT (2004)*"Proposte concernenti le strategie in materia di sicurezza informatica e delle telecommunicazioni per la pubblica amministrazione"*, March 2004 Italy
www.governo.it/GovernoInforma/Dossier/sicurezza_informatica/proposte.pdf

DCSSI (2004), *"Mise en oeuvre en France des lignes directrices de l'OCDE régissant la sécurité des systèmes et réseaux d'information adoptées le 25 juillet 2002"*, France
http://webdomino1.oecd.org/COMNET/STI/IccpSecu.nsf/viewHtml/index/$FILE/fiche%20application%20lignes%20directrices%20-%20mars%202004.pdf

Dipartimento della Protezione Civile, Italy
http://www.protezionecivile.it/sistema/index.php

Masera, Marcello, Joint Research Centre, Italy, electronic communications, 28.07.05

Serveur Thématique sur la sécurité des systèmes d'information, France
http://www.ssi.gouv.fr/fr/index.html

Setola, Roberto, Gruppo di lavoro sulla Protezione delle Infrastrutture Critiche Informatizzate, Italy, electronic communications 1.09.05.

B.2 Suggested readings

AEEG (2004), *"Resoconto dell'Attività Conoscitiva in Ordine alla Interruzione del Servizio Elettrico Verificatasi il 28 Settembre 2003"*, Report, AEEG Autorità per l'energia elettrica e il Gas, 9 June 2004, Italy
www.autorita.energia.it/com_stampa/index.htm

Buzan, B., Waever, O., de Wilde, J. (1998), *Security: A New Framework for Analysis*, Lynne Rienner Publishers

CRN (2004), *International CIIP Handbook – An Inventory and Analysis of Protection Policies in Fourteen Countries*
http://www.isn.ethz.ch/crn/_docs/CIIP_Handbook_2004_web.pdf

Daclon, Corrado Maria (2004), *"Intervista con Vincenzo Merola"*, *Analisi Sicurezza*, Nr. 47/48, July-August 2004, Italy www.analisidifesa.it/articolo.shtm/id/4375/IT

DCSSI (2004) *"Guide pour l'élaboration d'une politique de sécurité de système d'information"*, SMK/SGDN/DCSSI, France
http://www.ssi.gouv.fr/fr/confiance/documents/Methodes/PSSI-Section4-ReferencesSSI-2004-03-03.pdf

ENEL (2004) *"Energia e Ambiente"*, Report 2004, Italy
http://www.enel.it/attivita/ambiente/energiaelettrica/doc/tab_dipendenza_importazioni.pdf

European Commission (2004), *"Critical Infrastructure Protection in the fight against terrorism"*, COM(2004)702F
http://europa.eu.int/comm/justice_home/doc_centre/criminal/terrorism/doc/com_2004_702_en.pdf

Gruppo di lavoro sulla Protezione delle Infrastrutture Critiche Informatizzate (2004), *"Protezione delle infrastrutture critiche informatizzate"*, Report, March 2004, Italy

Hagen, J. og Fridheim, H. (2005), *Hva er kritisk infrastruktur?*, FFI/notat-2005-00363

IDABC European Commission eGovernment Observatory (2005a),*"e-Government in Italy"*, Periodical Report June 2005,
http://www.innovazione.gov.it/ita/ministro/dpcm_050506.shtml

IDABC European Commission eGovernment Observatory (2005b),*"eGovernment in France"*, Periodical Report June 2005,
http://europa.eu.int/idabc/servlets/Doc?id=21009

ISCOM (2005)*"La Sicurezza delle Reti: dall'analisi del rischio alle strategie di protezione"*, March 2005, Rome, Italy

Johansen, I. (2004), *Cyberspace som slagmark: Refleksjoner omkring Internett som arena for terrorangrep*, FFI/Rapport 2004/01666

Kjølberg, A. (2003), *Når Religionen Blir Truet: årsaker til og konsekvenser av islamistiske gruppers sikkerhetisering av religion*, FFI/Rapport 2003/00330

La Repubblica (2003), *"Italia avamposto dei terroristi"*, 3 April 2003, Italy
http://www.repubblica.it/online/politica/italiairaqtredici/frattini/frattini.html

Ministero delle Communicazioni (2005), *"Decreto 6 Maggio 2005"*, Italy,
http://www.innovazione.gov.it/ita/ministro/dpcm_050506.shtml

Ministero dell'Interno (2005) *"decr.legge 144/24 Luglio 2005, art. 7bis"*, Italy http://www.interno.it/legislazione/pages/pagina.php?idlegislazione=648

Ministero dell'Interno (2005),*"Lo stato della sicurrezza in Italia"* Report, 16.08.2005, Italy http://www.interno.it/assets/files/8/20058141464.pdf

OECD (2003) *"Survey on the Implementation of the OECD guidelines for the security of Information systems and Networks: Towards a culture of Security"*, DSTI/ICCP/REG(2003)8/FINAL, July 2003, (downgraded 2004) http://webdominio1.oecd.org/COMNET/ST/IccpSecu.nsf?OpenDatabase

Perrow, C. (1984), *Normal Accidents – living with high-risk technologies*, Basic Books, Inc., Publishers, New York

St.meld. nr. 17 (2001-2002), *Samfunnssikkerhet – veien til et mindre sårbart samfunn*, Det Kongelige Justis- og Politidepartement, Norway

St.meld. nr. 37 (2004-2005), *Flodbølgekatastrofen i Sør-Asia og sentral krisehåndtering*, Det Kongelige Justis- og Politidepartement, Norway

St.meld. nr. 39 (2003-2004), *Samfunnssikkerhet og sivilt-militært samarbeid*, Det Kongelige Justis- og Politidepartement, Norway

Svenska Kraftnät Beredskapsstaben (2005), *"Erfarenheter av krisehanteringsarbetet efter Gudrun"*, PM 25.04.2005, Sweden

Vulpiani, Domenico, (2002)*"L'esperienza italiana nel contrasto al crimine informatico"*, International conference on Cybercrime, Palermo, Italy, October 2002