Cyber Crisis Management Roles – A Municipality Responsibility Case Study

Grethe Østby, Basel Katt

Cyber Crisis Management Roles – a Municipality Responsibility Case Study

Grethe Østby and Basel Katt

Norwegian University of Science and Technology, Gjøvik, Norway
{grethe.ostby;basel.katt}@ntnu.no

Abstract. In this paper we propose a role model that can be applied in societal cyber crisis management to build safety and standard procedures during cyber security crisis. We define societal cyber crisis as the cyber crisis which affect the society in which disaster is or might be the consequence. The process to create our model started by analyzing regulations and responsibilities in Norwegian municipalities, and we used steps of a design science research (DSR) research approach to create our suggested artifact. A combination of conventional crisis management and cyber crisis management is proposed to identify the interrelationships among diverse stakeholders when managing the preparation for and reaction to a cyber crisis incident. We present a cyber incident handling role model (CIHRM) which is usable for visualizing cyber crisis in a diversity of organizations. After our model has been reviewed by the cyber security research community, we plan to implement the model when analyzing crisis management in various organizations to prepare for instructions, training and exercises at our training environment - The Norwegian Cyber Range.

Keywords: Cyber crisis, Cyber management, Management roles, Crisis management, Societal cyber crisis.

1 Introduction

Bruer research has shown that the current competence levels on digitalization process among leaders in public sector in Norway has led computer security activities to be isolated from strategic planning daily operation [1]. Consequently, upper management leaders is focused on efficiency, rather than society readiness and emergency preparedness [2]. This is also supported by the Norwegian Auditor General's administration study nb 1, 2018 about digitalization in governmental sector, which concluded that the digitalization among departments and directorates is going too slow [3]. Cyber security and safety are not mentioned in any part of the report, only personal information in the matter of how to transfer these data from one department to another, and consequently the managers are forced to focus on the digitalization.

However, NOU 2015: 13 Digital vulnerability – safe society (Lysne committee), is describing how the civil protection system also should include the handling of cyber-incidents, both system failures and malicious attacks [4]. At the same time the Lysne committee also observed that there is lack of a cyber-security arena within the sector of

the municipalities. They described that many municipalities have an increased need of counselling and education to make good risk- and resilience analyses, and to establish control-systems to handle cyber-incidents. In addition, a municipality CERT is recommended in the study of municipalities common need of competence-center to deal with handling cyber-security incidents made by NorSIS 2017 [5].

In general, between an individual and an organization, there are teams, and more specifically, crisis management groups. Groups of people and teams from different worlds, with very different cultural responses to risk and emergency, having often very distinct prejudices about the threats to be dealt with and the goals to be met, and whose individual and corporate interests lend themselves poorly to broader cooperation. And they are all expected to work together under pressure [6].

In Norwegian (and other countries) traditional emergency-organizations, as for example the military forces, the police forces, the civil defense forces and others, roles have been defined to avoid dependency on individuals and to have a long-time rollover in these roles. Norwegian governmental regulations and guidance on municipalities' responsibilities is still suggesting tasks to be managed, and crises to be led by the municipality management. For several years, roles in such crisis responsibilities have been suggested in a number of municipality crisis management courses run by the Norwegian Civil defense national competence center, which those municipalities have adopted and have used with success during crisis.

The Norwegian municipality guidance suggests establishing a crisis staff to sup-port the crisis management, but it does not define the roles of the staff. A lot of tasks are outlined, but they are not regulated in roles to deal with them [7]. Thus, it is easy to understand why decision makers responsible for crisis management want ways to respond to these challenges. It is important to recruit competent individuals, but it is also crucial to build teams and organizations that compensate for moments of individual weakness [6]. In this paper, we try to tackle these issues by studying two com-parable crises with different causes. These crises could be analyzed within organizational tiers and thereby model roles and tasks to handle a variety of crisis, specifically societal cyber crisis. We use the municipality crisis management responsibility as a case to combine this responsibility with cyber crisis which affects municipality society. We aim to combine traditional incident command system roles with the organization–governed networks responsibilities.

Based on the analyzed crises, we suggest a model to best implement roles in management teams of societal cyber crisis on how to handle the crisis. We define societal cyber crisis as cyber crisis which affect the society in such a context of which disaster is or might be the consequence. We discuss the cyber incident management in all phases of the crisis on strategic, tactical and operational tiers in organizations to sup-port other/overall crisis management decisions. Cyber-incidents require vast knowledge on all tires, and there will be a need of bringing in diverse experts in management-teams on the different tires, such as experts from SOCs, CERTs and other real-life stakeholders. These vast tasks require excellent capabilities to manage such teams and will be one of the most important ranges of roles to frame for managing societal cyber crisis.

The paper is structured as follows: After the introduction in section 1, in section 2 the background and relevant literature is presented. In section 3, our research approach

is discussed together with the use of municipalities crisis management responsibilities. In section 4, we present the municipality management roles, and discuss how to bring in cyber crisis roles. In section 6 we exemplify the outcome of our model and outline our prospects for further research.

2 Background and relevant literature

In the literature on social–ecological systems, the term 'resilience' is used to de-scribe the ability of a system to absorb or withstand changes inflicted onto the system from the outside [8]. Walker et al. [8] define the resilience of a system as: the capacity of a system to absorb disturbance and reorganize while undergoing change to still retain essentially the same function, structure, identity, and feedbacks. Resilience research is also interested in studying what kind of interactions can occur in complex interdependent infrastructures, but not with the aim to only identify the most critical relations. Rather, the aim is that operators and middle managers learn about complex system behavior to enable them to perform real-time resilience, or "operating at the edge of failure without falling off" [9]. Risk analysis, business continuity management and crisis management training are often performed within the context of a single organization or sector and are seldom addressing the holistic analysis of multiple infrastructures [9].

The process of disaster management is commonly visualized in several phases. The disaster management cycle illustrates the ongoing process by which governments, businesses and civil society plan for and reduce the impact of disasters, react during and immediately following a disaster, and take steps to recover after a disaster has occurred. The significance of this concept is its ability to promote a holistic approach to disaster management as well as to demonstrate the relationship between disasters and development. The pre-disaster activities are done before the hazard interacts with the vulnerable community to cause a disaster, usually referred to as mitigation and preparedness, which includes major activities such as preparedness through response, from prevention, mitigation and readiness, through relief, recovery and rehabilitation [10].

Disaster management is dealing with the immediate aftermath of the disaster, including short-term relief and response. This relates to activities such as evacuation, search and rescue and medical care. Post-disaster is the period of recovery until community returns to a normal condition. The concept of sustainable development is frequently associated with long-term recovery, which strongly aligns to the multiple-state definition of resilience, whereby a community should maximize the capacity to adapt and focus on long-term growth to a state of reduced vulnerability [11].

The NIST Framework for Improving Critical Infrastructure Cybersecurity, commonly referred to as the NIST Cybersecurity Framework, provides organizations with a structure for assessing and improving their ability to prevent, detect and respond to cyber incidents. Version 1.0 was published by the US National Institute of Standards and Technology (NIST) in 2014 and was aimed at operators of critical infrastructure. The framework guides cybersecurity activities and considers cybersecurity as a part of an organization's risk management processes. In this paper we present a model for the response and recovery phase as suggested in figure 1.

Fig. 1. NIST Cyber security framework [12]

From a cyber security incident perspective Kulikova et. al. [13] suggests four steps in crisis management comparable to NIST's framework, and FEMA suggests four stage activity cycle of mitigation, preparedness, response and recovery [15]. These approaches are comparable to NIST, and response and recovery are important in all suggestions.

As mentioned before, there should be roles pre-defined to cope with the response and recovery. When an emergency is unfolding, the people and systems involved in watching it unfold must determine what has already happened, what is currently happening, and what is likely to happen in the future; then, they make recommendations for reaction based on their situational awareness [15]. To be able to understand the situation, the responsible staff role should be able to visualize the incident.

As van der Aalst pointed out, event data is the major source of information [16]. Therefore, all these available events are numerous and the data and information they contain is more or less reliable, comes from varied sources, in various types and formats, and are time-dated. Incident Command Systems (ICS) is used to coordinate multiple response organizations under a temporary central authority with a hierarchical structure [17]. It is better understood as a highly centralized mode of network governance, designed to coordinate interdependent responders under urgent conditions. The contrast between a network governance and hierarchical view of the ICS is illustrated in figure 2. The left-hand side of the figure represents the dominant view of the ICS [18]. In this figure, a hierarchy allows the incident commander to direct the crisis functions of logistics, operations, planning, and finance/administration. But if we consider the ICS in terms of its members, we see it as a network, albeit a highly centralized one (on the right-hand side). The incident commander is at the center of the network, surrounded by organizations that have ongoing inter-crisis dyadic relationships, as illustrated by the right-hand side of figure 2.

When it comes to roles, the National Institute of Standards and Technology (NIST) has ranged three different tiers in the framework of risk management, which can help organize roles in these tiers. These tiers are strategic, tactical and operational [19] (figure 3).

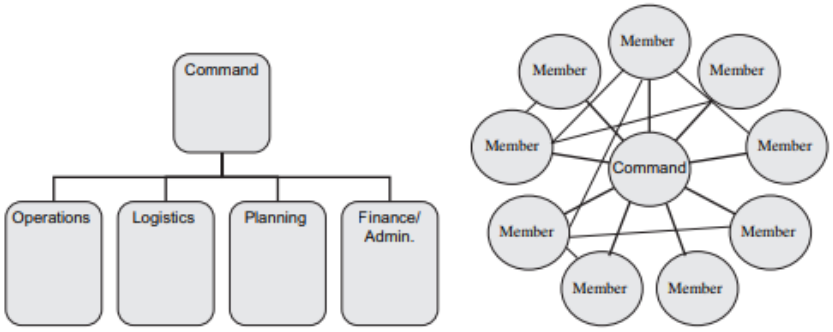

Fig. 2. Traditional incident command system and organization–governed networks [17]

Fig. 3. Tiers in framework of risk management (NIST)

Every tier is led by managers, and different crises require different management roles on each layer. This can be transferred into diverse organizations on national, sectorial and local public responsibilities.

Boeke investigates how different models of public–private partnerships shape cyber crisis management in four European countries: the Netherlands, Denmark, Estonia, and the Czech Republic. Using Provanand Kenis's modes of network governance, an initial taxonomy of cyber governance structures, he presents two suggestions: First, national CERT/CSIRT teams are to be embedded inside or outside the intelligence community. Second, if cyber capacity can be centralized in one unit or spread across different sectors [20].

In this paper, we use the municipality crisis management responsibility as a case to discuss cyber crisis which affects municipality society to argue for a solution which combine Boeke's suggestions. We aim to combine traditional incident command system roles with the organization–governed networks responsibilities as outlined in this section.

3 Research approach

In this paper, we approach the cyber security challenges using what can be referred to as a naive inductivist approach. The naïve inductivist approach starts by first observing a phenomenon and then generalizing the phenomenon which leads to theories that can be falsified or validated [21]. This approach will use the methodology out-lined by design science research in information systems (DSRIS) [22]. This methodology uses artifact design and construction (learning through building) to generate new knowledge and insights into a class of problems.

DSRIS requires three general activities: (1) construction of an artifact where construction is informed either by practice-based insight or theory, (2) the gathering of data on the functional performance of the artifact (i.e., evaluation), and (3) reflection on the construction process and on the implications the gathered data (from activity (2)) have for the artifact informing insight(s) or theory(s) [22].

How to work on these steps was presented in a thesis written by Karokola [23]. He visualized this approach as outlined in figure 4. As we are approaching our work in a naive inductivist approach, we modified the logical formalism in the model from abduction to induction.

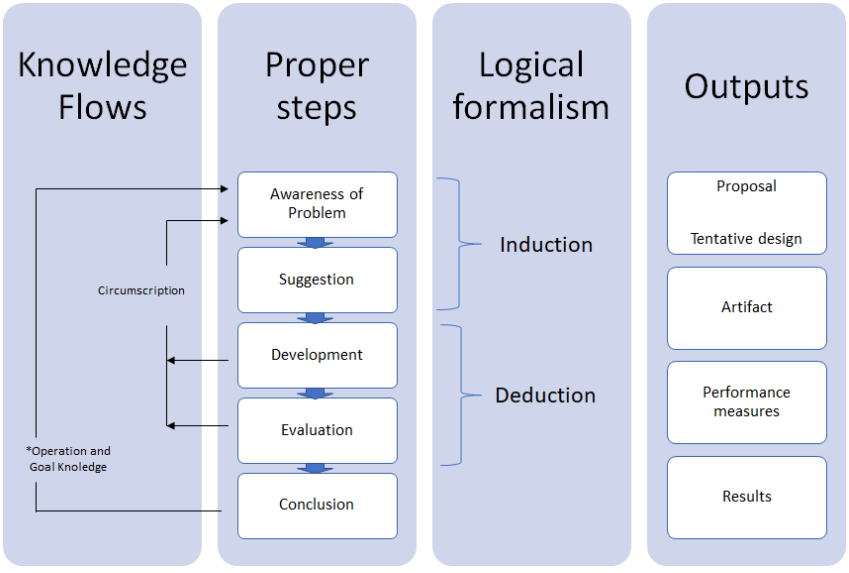

Fig. 4. Design research methodology - modified

To propose an artifact in an inductive approach we started up by analyzing municipalities responsibilities when handling crisis in general and cyber-incidents in special (first step in the 2nd column). For the next step we suggest a model to deal with the problem in crisis management when handling cyber incidents (second step in the 2nd column). The goal of the paper is to propose a tentative design (first step in the 4th

column), in which we want to present and test when executing cyber training and exercises in our training environment.

Apply the case of municipalities crises management responsibilities

The Norwegian law concerning the municipality's emergency duty, civilian preparedness and the Civil defense organization outlines the municipality's responsibility to analyze and make emergency preparation based on risk and resilience in their geographical designated area [24].

The municipalities should outline prepared societal emergency work that will [25]:

- Protect the population and contribute to uphold critical infrastructure.
- Give an overview of knowledge and awareness of societal critical challenges and what effect these challenges would have on the society and communities.
- Reduce risk and vulnerability through preventive work.
- Ensure good emergency preparedness and crisis contingency.
- Attend to ensure collaboration and coordination with internal and external societal emergency partners in the municipality.

In this idea-paper, we start by presenting as-is crisis-management roles that are defined and evolved based on the guidelines and try to combine this with roles needed in a cyber crisis.

4 Cyber incident handling role model – a municipality case study

In this chapter we propose a cyber incident handling model to best implement roles in management teams of societal cyber crisis on how to handle the crisis. We discuss the cyber incident management in the respond and recovery process of the crisis on strategic, tactical and operational tiers in a municipality case. We suggest bringing in diverse experts in management-teams on the different tires, such as experts from SOCs, CIRTS and other real-life stakeholders. We present the as-is responsibilities in the municipality's regulations and guidance on crisis management as introduction to our arguments and the modelling and give a summary of the roles in the end.

4.1 Municipality regulations and guidance

DSB's guidance recommends that the roles and responsibilities should be described in the contingency plan, the municipalities crisis management is to be understood as a critical societal function, and is supposed to be maintained throughout any event, no matter of time, both in peace, security political crises and in armed conflicts. The guidance also suggests that the municipalities crisis management can be expanded by supporting personnel and subject responsibilities, dependent on the crisis nature and extent.

Our experience in this matter is that it takes too much effort not to start out with the necessary experts to begin with, and that it is better to call out subject responsibilities

which will adapt to the incident, and then dismiss staff as the crisis is going into pre-crisis phase. We suggest key personnel to be on predefined roles-lists, to quickly do replacement in the specific subject role.

The guidance suggests that the municipality should consider the need of safety-clearance of key personnel in the crisis management. To be able to consider who needs this clearance, roles must be defined, and what personnel can fill the roles. This also supports our suggested role-modelling.

The guidance suggests the crisis management to be prepared on the following:

- Quickly decide efforts within the municipality's responsibilities, i.e. public information establishes evacuation center and psycho-social support teams.
- Be the public "face" and ensure good communication with the population, inter-nal employees and media.
- Attend to coordinate local handling of the crisis through internal and external societal security organizations.
- Provide recourses to handle crises based on contractual agreements.
- In special cases – discuss priorities and diffusion of limited recourses in collaboration with other societal critical organizations, and neighboring municipalities.
- Communicate needs of resources to the county or/and other regional security organizations.
- Surveillance of the situation, and dialogue with other emergency organizations affected by the crisis.
- Develop and communicate gathered understanding of the situation based on information from the responsible department in the municipality.
- Inform the political parties on a regular timeline
- Inform county on collaboration channel
- Make sure substitute/deputy personnel is in place in case of regular members absence.

The guidance suggests establishing a crisis staff to support the crisis management, but it does not define the roles of the staff. As you can see a lot of tasks is outlined, but they are not regulated in roles to deal with them. We suggest the diversity of crisis responsibilities roles should be defined on strategic level, tactical level and operational level.

4.2 Different crises, comparable roles

Typically, the strategic level consists of the municipality's management, the tacti-cal levels consists of the managers running the different local municipality elderly homes, schools, kindergartens, water-supply departments etc., while the operational level consists of staff and employees on the ground, like doctors, nurses', teachers and engineers. When the incident is an elderly home on fire, the roles in the organiza-tion based on regular crisis, and crisis management regulated in contingency plans. When the incident is an elderly care-taker system out of order, the need of ICT-expert teams is necessary, and regular crisis management roles does not cover experts need-ed. There is a need to

include these roles, as regular municipality crisis management might not have the competence to handle those crises. However, the crisis still must be handled manually by the regular crisis management. This means that a cyber crisis will need additional management and will thereby be more challenging to handle. Our discussion is visualized in figure 5.

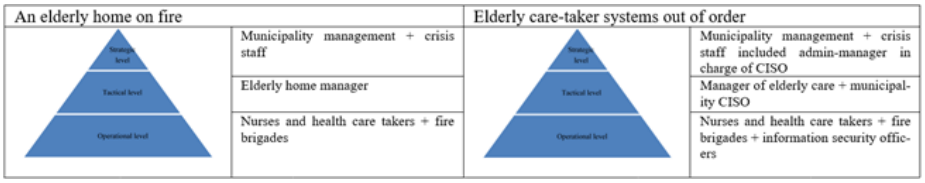

Fig. 5. Regular crises vs. cyber security crises

As suggested in the guidance it is the municipality management with their responsibilities which should take the roles as crisis management. In a crisis as suggested – fire at the elderly home, some managers will be more affected than others, and it is of course the health and elderly manager that will follow up on the employees, elderlies and their situation. The chief municipal executive will take the role as the crisis manager and will make sure that other members of the crisis management less influenced by the incident contribute with necessary supply and logistics. The major will follow up on media information, meet the elderlies and their next of kin. To get necessary support on media tasks, the major typically get support from a press coordinator. In such a crisis both the police contact, a fire brigade officer and the chief municipal medical officer will be a part of the crisis management to bring situational awareness into the group. They will get updates from forces alarm centrals and the forces alarm centrals get update from operative teams at the elderly home.

Crisis management and/or staff management is set up as a team working together in a safe environment to ensure the contingency of the management throughout the crisis. The regulations require a plan to move the crisis management if necessary [26]. The crisis management is therefore in need of the right information about the situation to make the right decisions. On the other hand, the information needs outside the crisis management is also not just pushing boundaries to the regular organization but are vast and mixed as visualized in figure 6.

These information needs require extra focus and handling during crises, and we have chosen to define information roles as requested in the regulations, as separate roles in the crisis management [26]. These roles are also specifically outlined in figure 7, on both strategic, tactical and operational levels.

On the tactical level the health and elderly manager team will support the elderly home manager with regulations from the contingency plans, more specific evacuation and necessary health support from next door municipalities etc. On operational level the elderly home manager will follow up on drilled tasks in such an incident.

As mentioned before, information in such crises is vital, and the tactical information team will monitor information in the crisis management systems, in newspapers and social media. They will also publish information both external in social media, and

internal to the employees in the municipality. And of most importance: support and gather information back and forth to the 1st line service desk personnel. 1st line service desk personnel are commonly strengthened with more personnel in such crises. This regulated way of handling crisis is presented in figure 7.

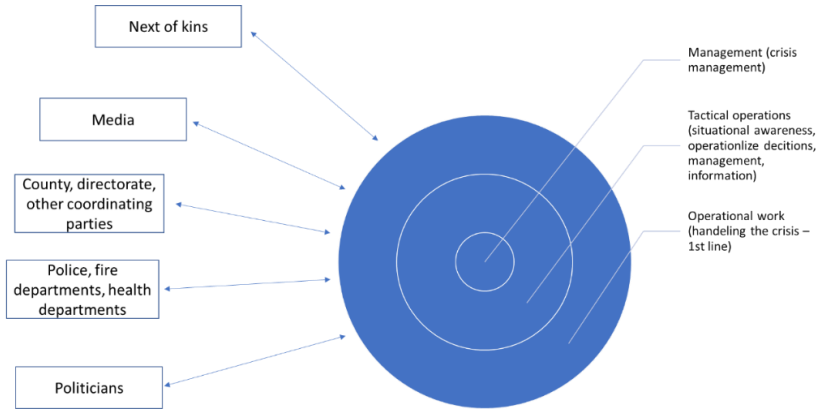

Fig. 6. Needs of crisis information

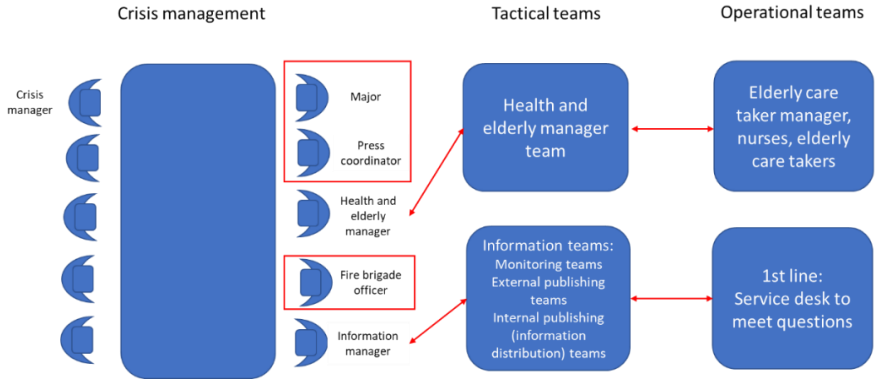

Fig. 7. Incident handling roles in conventional crises management

As previously stated regarding our other suggested crises: an elderly care-taker system out of order, that will require additional tasks. We have discussed which other roles could have incorporated these tasks, but as the principle of nearness and likeness is the foundation of crisis management, we suggest new roles to support the crisis.

First, we suggest that the municipality ICT-manager should be a part of the crisis management. In such a case the timeline to provide redundant systems or get the system back up and running is crucial information to the crisis management decisions. Next a tactical ICT management team should coordinate information between the management and the operational teams and get the responsibility to communicate with municipality

CERT and organizations like National security authorities if necessary. Third, at operational level, investigation and recovery operations like suggested by NIST cyber security framework (figure 1) should take place.

Additionally, the operational cyber team should collaborate with police investigators and system users. The other tasks during the crisis remain the same as in any other crisis. Our suggested additional roles during cyber incident crisis is visualized in figure 8.

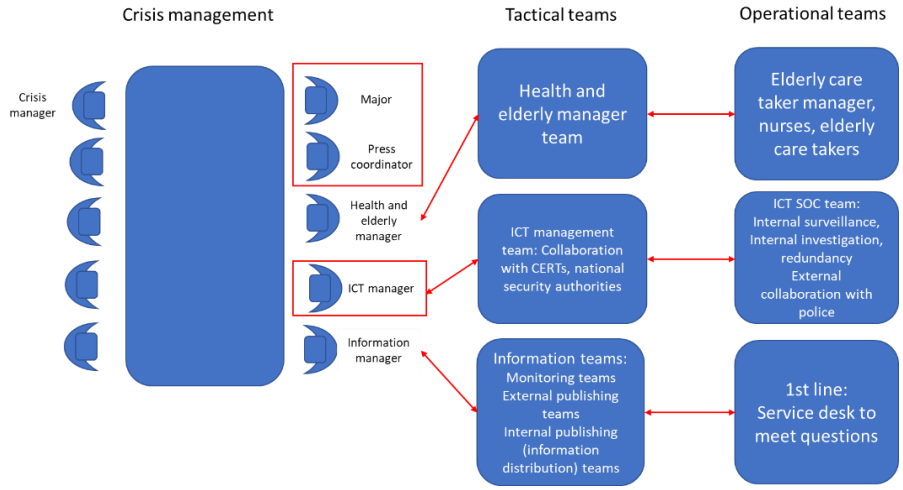

Fig. 8. Incident handling roles in cyber security crisis

As the mentioned digitalization is increasing, one may also argue the necessity of this type of organization in any societal crisis. To exemplify this, we argue the need of ICT personnel in the mentioned fire at the elderly home were an evacuation will take place, but also in conventional crises like forest fires, floods, hurricanes and others.

All information flow in such crisis is today digitalized, and to follow up information security and prepare for redundant information flow during any crisis, we suggest the ICT-roles as an essential part of the crisis management on a regular basis, regulated in contingency plans.

4.3 Summary

Using well known crises to visualize and implement cyber crises in municipality crises management appear useful in understanding and defining roles as it gives us a good indication about relevant tasks and information sharing on both strategic, tactical and operational level.

An overview of municipality crisis management roles when cyber crisis occur is presented in table 1.

Table 1. Tasks and roles in societal cyber crises: an overview

	Management roles	Internal team tasks	External team tasks
Strategic	Chief municipal executive Municipality management Major Press coordinator Information manager ICT-manager:	Chief municipal executive leading the crisis Municipality management = crisis management handling crisis in departments Major and press coordinator meet media, elderlies and next of kin Information manager coordinates all information ICT-manager: Managing ICT-crisis	Might be coordinated by county governor and directorate
Tactical	Department manager team Information teams ICT management team	Health and elderly manager team: Follow up on the employees, elderlies and their situation Information teams: Monitoring teams External publishing teams Internal publishing (information distribution) teams ICT management team: Collaboration with CERTs, national security authorities	Other municipalities CERT NSM
Operational	Operational manager and employees ICT SOC Team Municipality service desk	Elderly care-taker manager, nurses, elderly care takers: ICT SOC team: Internal surveillance, Internal investigation, redundancy External collaboration with police 1st line: Service desk to meet public questions	Police investigators

5 Conclusion and future research

The cyber incident handling roles model (CIHRM) presented in figure 8 is usable to visualize both regular crisis and cyber crisis. We propose to name this crisis handling visualizing model a cyber incident handling role model (CIHMR).

Visualizing crisis tasks and roles enables us to introduce more holistic and near-to-life elements needed to be factored in handling crisis. We need to verify and validate the findings suggestions we have made, and to enhance and improve the cyber inci-dent management roles in more detail. To validate the framework, we plan to test suggested roles model when setting up exercises in our training environment, the Nor-wegian Cyber Range (NCR). NCR will be an arena where testing, training, and exer-cise are tools to expose people, businesses, and units to realistic events and situations in a realistic but safe environment. The arena ensures efficient transfer of knowledge and building of real-world competence, that links together the strategic, operational, tactical and technical levels of decision making, by simulating the impacts of cyber security events on the levels of society, digital value chains and cyber infrastructure without harming the entities involved and their critical infrastructure.

In this paper we propose roles by using only one specific example of cyber crisis. In future work we will test if these roles are transferable to other societal emergency cyber crises. We intend to use the cyber incident handling role model (CIHRM) pre-sented in figure 8 to visualize cyber crisis in various aspects of cyber crisis.

To ensure the best possible effect in the NCR, current suggested roles and tasks will be facilitated as most accurate comprehension of exercises fitted the different roles. Additionally, there will be need of preparedness learning based on real life incidents. We plan the preparedness learning as instruction for adults using action research by instructors with reflection throughout lectures.

When analyzing the outlined definitions of roles, we found that there is no clear definition of cyber crisis management roles. We based the suggested roles on NIST management tiers and will also need to consider NATO management tiers. Moreover, as mentioned before, there are examples of real-life incidents roles which might be analyzed to compare best practices. We consider this as an area, which can be devel-oped better in combining role-definitions and scenarios and have a long-time work in progress in this matter.

References

1. Bruer, A.: Ny undersøkelse: Stort etterslep på mellomlederes IT-kompetanse i offentlig sector. digi.no, 09-Aug-2017.
2. Baugerød Stokke, O. P.: Advarer it-sjefer mot effektivitet. Computerworld.no, 23-Mar-2009.
3. Office of the Auditor General of Norway, “admin report nb. 1, (2018).
4. NOU 13 Lysne commitee, “Digital vulnerability – safe society,” (2015).
5. NorSIS: The study of municipalities common need of competence-center to deal with handling ICT-security incidents, (2017).
6. Lagadec, P.: PREVENTING CHAOS IN A CRISIS Strategies for prevention, control and damage limitation Preface : tools for thinking about, preventing, and managing crisis ix. (1993).
7. DSB: Municipality guidance, emergency duty. (2017).
8. Walker, B. Holling, C. S. Carpenter, S. R. and Kinzig, A.: Resilience, Adaptability and Transformability in Social–ecological Systems. Ecol. Soc., (2004).

9. De Bruijne, M. and Van Eeten, M.: Systems that Should Have Failed: Critical Infrastructure Protection in an Institutionally Fragmented Environment. (2007).
10. De Guzman, E. M.: Towards Total Disaster Risk Management Approach. (2002).
11. Haigh, R. and Amaratunga, D.: An integrative review of the built environment discipline's role in the development of society's resilience to disasters. International Journal of Disaster Resilience in the Built Environment, 1(1), pp. 11–24, 26-Feb-2010.
12. Anderson, E.: How to Comly with the 5 Functions of the NIST Cybersecurity Framework. Forecoun, (2017). [Online]. Available: https://www.secmatters.com/blog/how-to-comply-with-the-5-functions-of-the-nist-cybersecurity-framework.
13. Kulikova, O. Heil, R. Van Den Berg, J. and Pieters, W.: Cyber crisis management: A decision-support framework for disclosing security incident information. in Proceedings of the 2012 ASE International Conference on Cyber Security, CyberSecurity 2012, pp. 103–112 (2013).
14. FEMA: The Federal Emergency Management Agency Publication 1. (2016).
15. S. L. Pfleeger and D. D. Caputo: Leveraging behavioral science to mitigate cyber security risk. Comput. Secur., (2012).
16. van der Aalst, W. M. P.: Data Scientist: The Engineer of the Future. (2014).
17. Moynihan, D. P.: The network governance of crisis response: Case studies of incident command systems. Journal of Public Administration Research and Theory, 19(4), pp. 895–915, (2009).
18. Fema: National Incident Management System. (2017).
19. Locke G. and Gallagher, P. D.: Managing Information Security Risk Organization, Mission, and Information System View Joint Task Force Transformation Initiative Nist Special Publication 800-39, (2011).
20. Boeke, S.: National cyber crisis management: Different European approaches. Governance, vol. 31, no. 3, pp. 449–464, (2018).
21. Kowalski, S.: IT Insecurity: A Multi-disiplinary Inquiry: Stockholm University. 1994.
22. Kuechler, W. and Vaishnavi, V.: A Framework for Theory Development in Design Science Research: Multiple Perspectives. (2012).
23. Karokola, G. R.: A framework for Securing a-Government Services, The case of Tanzania: Stockholm University, (2012).
24. Justis- og beredskapsdepartementet, "Lov om kommunal beredskapsplikt, sivile beskyttelsestiltak og Sivilforsvaret (sivilbeskyttelsesloven)." Norwegian Government, (2010).
25. DSB, Guidance to holistic risk and vulnerability assessment in the municipality. DSB, (2019).
26. Norwegian government, FOR-2011-08-22-894. Norwegian Government, (2011).