Preparing for cyber crisis management exercises

Grethe Østby[1] [0000-0002-7541-6233], Stewart James Kowalski[1] [0000-0003-3601-8387]

[1]Norwegian University of Science and Technology, Gjøvik, Norway

{grethe.ostby;stewart.kowalski}@ntnu.no

Abstract. In this paper the authors discuss how to create a preparation schedule for exercises (PSE) to support EXCON-teams and instructors for full-scaled combined crisis management and cyber-exercises. The process to create the preparation schedule starts by performing vulnerability analysis to identify the most relevant and likely threats to the organization, before
processing historical threats and attacks to further focus our simulation scenario development by planning and designing a socio-technical scenario. Moreover, a plan for simulation that are realistic and based on the organization's maturity will be considered, and finally, in terms of a societal crisis impact exercise necessary lectures will be prepared.
After this framework has been reviewed by the HCI International 2020, we plan to test the model when planning for exercises at the Norwegian Cyber Range (NCR) environment. NCR will be an arena where testing, training, and exercise will be used to expose individuals, public and private organizations, government agencies to simulate socio-technical cyber security events and situations in a realistic but safe environment.

Keywords. Exercices, cyber exercices, cyber management exercices, cyber crises, cyber crises management exercices

1 Introduction

The Norwegian Directorate for Civil Protection (DSB) recommends that full scale crisis management exercises consist of two major components: an exercise directive, and a scenario (DSB, 2016). An exercise directive sets the framework for the exercise, whilst the scenario sets the content and timeline for the exercise.

The *ENISA Good Practice Guide on National Exercises* outlines in the initiation and planning phases of exercises that an organization should prepare an exercise directed to the needs of the organization but does not give guidelines how these needs should be identified (ENISA, 2009).

The authors have from years of experience of planning for crisis management exercises, done vulnerability analysis on the organizations, and prepared and executed lectures beforehand the exercises based on such analyses. Recent research has also

suggested the need to use maturity modelling to prepare for exercises, to plan the exercise for an appropriate level for the participating organizations (Østby & Katt, 2019). Additionally, other recent research suggests preparing scenarios in a socio-technical root cause analytical context to prepare for different types of exercises (Østby, Berg, Kianpour, Katt, & Kowalski, 2019).

By providing a clear step-by-step guide to follow, the authors suggest that such planning framework can provide a more effective and efficient learning environment for exercises.

After the introduction we present background and relevant literature in section 2, before presenting the research approach in section 3. In section 4 we present the suggested preparation schedule for exercises, and in section 5 we conclude and present our future plans on the topic.

2 Background and relevant literature

The scope of the authors' research is to investigate information security awareness and cyber security preparedness in society and public organizations like municipalities and counties and to investigate cyber-management in the public emergency organizations in both the organizations themselves and cyber-operations centers. To meet the scope, we will arrange cyber-incidents exercises at the Norwegian Cyber Range (NCR) (NTNU, 2019).

At the NCR, we want to develop and offer near to real life exercises, i.e. full-scaled exercises in a secure environment, to train organizations on strategic, tactical and operational levels together. We plan to copy – paste the organizations socio-technical control structure into a safe environment at the cyber range, and train the teams on system incident handling, incident information escalation and crisis management.

To prepare for such exercises, we plan to test our suggested Preparation Schedule for Exercises (PSE) - framework as presented in this paper. Preparation for cyber exercises often centers around the cyber test bed and a fictive scenario (Micco, Ed, & Rossman, 2002; Vykopal, Vizvary, Oslejsek, Celeda, & Tovarnak, 2017), and the cyber exercises are often executed as competitions (Bei, Kesterson, Gwinnup, & Taylor, 2011; Patriciu & Furtuna, 2009). The author's approach is however, to focus on status in the organization that will be trained, to make the exercise as realistic as possible, but also aligned with the organization's level of awareness and knowledge.

In Jason Kick's Cyber Exercise Playbook (2014), the training audience is divided into 5 different challenge levels, and suggest impact and resolution on how to address the audience based on these challenges. In this paper the author suggests using vulnerability analysis and maturity modelling to find the training audiences/organizations level of expertise or lack of expertise.

System vulnerability analysis involves discovering a subset of the input space with which a malicious user can exploit logic errors in an application to drive it into an insecure state (Sparks, Embleton, Cunningham, & Zou, 2007). Vulnerability analysis in this paper also includes physical/material, social/organization and motivational/attitudinal analysis similar to those presented by Twigg (2001), and will be compa-

rable with Norwegian guidelines for risk – and vulnerability analysis made by The Norwegian Directorate for Civil Protection (DSB) (DSB, 2014). The author also consider Shah and Mehtre's Vulnerability Assessment and Penetration Testing (VAPT) relevant for some organizations of which is competent to consider and relate to such approach (Shah & Mehtre, 2013).

In preparation for full-scale exercises it is also relevant to investigate the organization's experience with crisis in general and cyber-crisis in particular. Additionally, societal trends of which may impact the organization should be considered. To run such investigations, the use of threats - and opportunities analysis can be justified. In a study by Jackson & Dutton (1988) designed to investigate the use of threats and opportunities analysis among decision makers, the authors suggests that managers are being more sensitive to issue characteristics associated with threats than to those associated with opportunities. We suggest however, that by combining threat and opportunity analysis with vulnerability analysis like those previously presented, or together with a vulnerability functional assessment analysis as presented by Depoy et al. (2005), opportunities and vulnerabilities can be presented together.

According to Liao et al., Gartner define Cyber Threat Intelligence (CTI) as "evidence-based knowledge, including context, mechanisms, indicators, implications and actionable advice, about an existing or emerging menace or hazard to assets that can be used to inform decisions regarding the subject's response to that menace or hazard" (Liao et al., 2016). Research on managing CTI by CTI-sharing (Brown, Gommers, & Serrano, 2015; Burger, Goodman, Kampanakis, & Zhu, 2014), and use of SIEM's systems to present and evaluate threats (Al Sabbagh & Kowalski, 2015), are relevant practice to consider when preparing for cyber exercises. The authors consider in this paper how to bring this information from ICT-management to the organizations top management to prepare for cyber incidents and exercises which affects the organizations ability to still run their daily business or activity and thereby require top management involvement.

Since the beginning of 2011 DSB has published annual description of possible crisis scenario that could have major impact on Norway (DSB, 2019). There are three major developments in the society, which are presented in the 2019 analysis, and one of these is the security consequences from rapidly increasing digitalization. Such development has led to a number of security analysis and techniques (Mahmood & Afzal, 2013), and it is difficult for organizations which do not have ICT-security as their main tasks, to keep track with these trends. As a preparation for cyber incidents and exercises, the author suggests conducting trend analysis targeting the organizations to be trained as a part of the overall CTI-analysis.

In previous research Østby et al. suggests that socio-technical scenario building can be useful in understanding and defining training scenarios as it gives a good indication on both social and technical challenges from real life cases (Østby, Berg, et al., 2019). A socio-technical system considers both social and technical aspects of change as presented in figure 1.

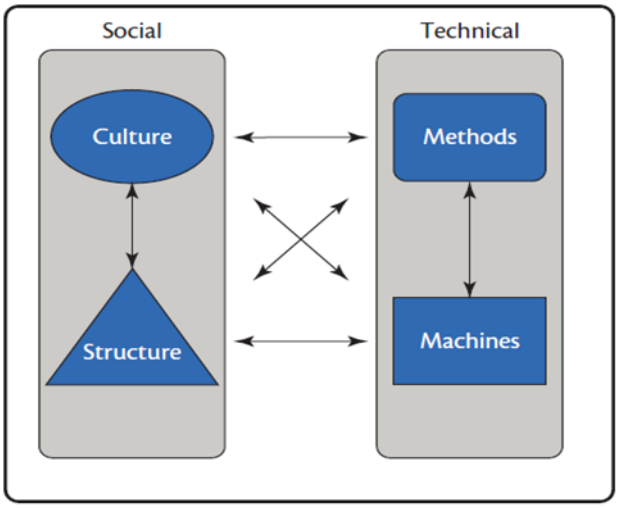

Fig. 1. Socio-technical approach (Kowalski, 1994)

In preparation for exercises the socio-technical approach is useful for making scenarios to highlight possible imbalance between the component and may give the organizations directions of how to bring their system back into balance. On the social side of the approach ISO standards like ISO 27005 (ISO 27005, 2018) and ISO 27035 (ISO, 2016) can be used to investigate culture and structure, and on the technical side standards like presented by the Telecommunication Standardization sector of ITU (ITU-T) (ITU-T, 2019) about protection assurance (chapter 5) can be used to investigate the methods and machines in the organization.

Recent research by Walhgren and Kowalski in Sweden indicates that there is a lack of cyber security incident readiness and that most organizations are at such a low level of maturity to deal with information security incidents that it may not even be beneficial for the organization to start off by running full scale exercise (Wahlgren & Kowalski, 2016). Østby & Katt (2019) recently tested Wahlgren & Kowalski's model (Wahlgren & Kowalski, 2016) in the Norwegian Inland Hospital trust, and the results indicated a diversity in needs and knowledge on strategic, tactical and operational layers in the organization.

Van Laere and Lindblom (2018) suggest theoretical education sessions via table-top discussions to role-playing, to give the trainees a fair chance of building skills and confidence before the exercise starts. This is also supported by the authors experience of running crisis management exercises both with and without theoretical lectures beforehand the exercises, and we suggest better learning from the exercise when preparing with lectures.

The Poorvu Center for Teaching and Learning at Yale (Yale, 2019) presents how to write intended learning outcomes from lectures, and suggests that by writing specific, measurable takeaways, learning outcomes improves (Richmond, Boysen, & Gurung, 2016). This is from a cyber security perspective also supported by ENISA's guidelines on assessing key objectives for operators of essential services (OES) and

for the digital service providers (DSP) (ENISA, 2018). The assessment is presented in the order of 1) security measures, 2) questions and 3) evidence.

In this paper we present an adaption of the Backward Design framework, presented by The Porvu Center for Teaching and Learning at Yale (Yale, 2019).

3 Research approach

In this paper, we approach the cyber security exercise design and execution challenge by using the design science research in information systems (DSRIS) (Kuechler & Vaishnavi, 2012). Design science research (DSR) is a methodology which can be conducted when creating innovations and ideas that define technical capabilities and product through which the development process of artifacts can be effectively and efficiently accomplished (Kuechler & Vaishnavi, 2012).

How to work on DSR was presented in a thesis written by G. R. Karokola (Karokola, Kowalski, & Yngström, 2011). He visualized this approach as outlined in figure 2.

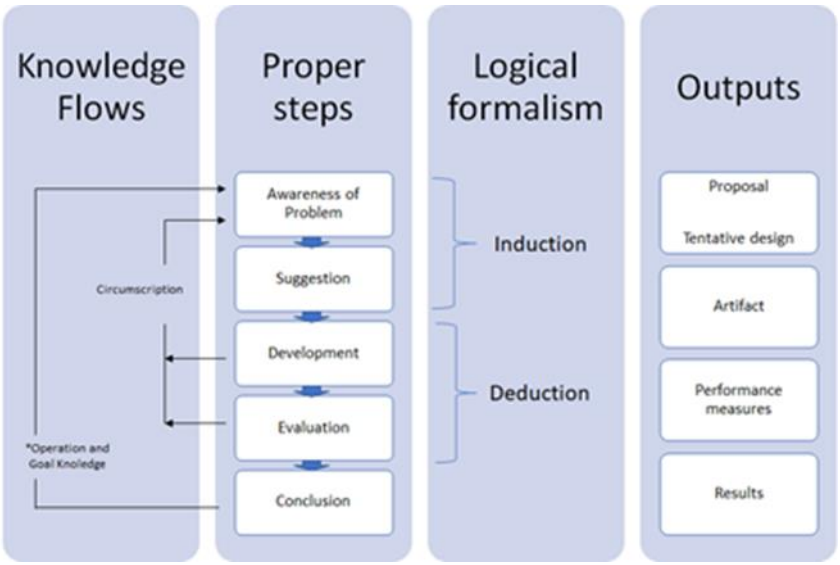

Fig. 2. Design research methodology - modified

The main goal of the research is to develop a step by step preparation framework for planning for cyber full-scale exercises.

The authors approach the goal by what can be referred to as a naive inductivist approach. The naive inductivist approach starts by first observing a phenomenon and then generalizing about the phenomenon which leads to theories that can be falsified or validated (Kowalski, 1994).

Our proposed artifact in this paper is a framework to prepare for exercises which involves

1) vulnerability analysis to identify the most relevant and likely threats to the organization, both from an overall perspective and those specific to the organization,

2) work with the cybersecurity teams to understand historical threats and attacks to further focus our relevant simulation scenario development,

3) plan and design a socio-technical scenario for the exercise,

4) plan for simulation that are realistic and based on the organization's maturity,

5) and finally, in terms of a societal crisis impact exercise; look into the organization's responsibility (laws and regulations), crisis management roles and responsibilities, and suggested escalation continuity plans (involving information continuity plans), to prepare for exercise lectures.

4 Preparation schedule for exercises (PSE)

The proposed artifact is based on relevant literature presented and practical experience in planning for exercises. In this section we present the five-step preparation schedule for exercises (PSE) for full-scale cyber-incident exercises that will be executed for both strategic, tactical and operational participants from the organizations that are being trained.

4.1 Vulnerability analysis

To identify the most relevant and likely threats to the organization, both from an overall perspective and those specific to the organization, the authors suggest using an overall SWOT-analysis (strengths and weaknesses, opportunities and threats) together with information from SIEMS systems and systems architecture overviews. Additionally, we want to investigate existing risk- and vulnerability analysis or prepare such if none exist. The suggested vulnerability analysis is presented in figure 3.

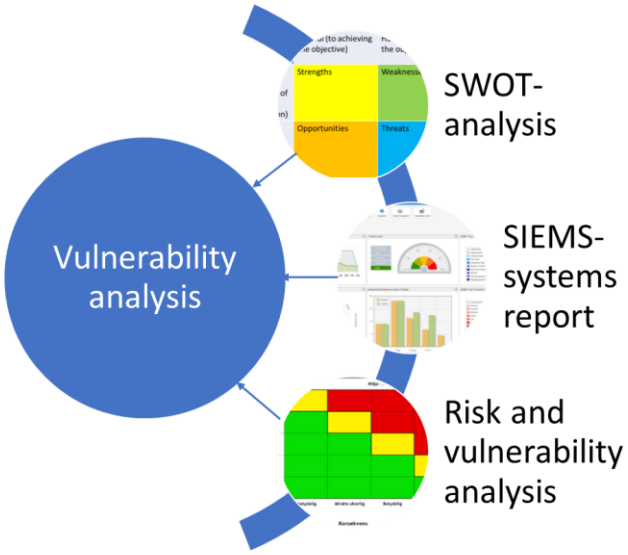

Fig. 3. Vulnerability analysis before exercises

We also suggest executing penetration testing as a part of the vulnerability analysis before exercises. Such reports will outline all the system and cyber vulnerabilities in a more detailed context and will give the organization more detailed results to work with after the exercise.

4.2 Historical threats and attacks

To approach analysis of historical threats and attacks both from within and from the outside of the organization, the authors suggests implementing reporting escalation processes from Security Incident and Event Management Systems (SIEMS) - to improve information flow and indicate what relevant information should be provided from a cyber incident to the crisis information management systems used.

In future research, a socio-technical escalation framework (STEF) to support synchronizing Security Incident and Event Management Systems (SIEMS) and Crisis Information Management Systems (CIMS) as suggested in Østby, Yamin and AlSabbagh (2019) could be implemented.

It is also important to evaluate trends in threats both within the organization and in the society in a national and international context similar to the DSB's incidents analysis (DSB, 2019).

4.3 Socio-technical scenario building

In Østby, Berg, et al. (2019), different socio-technical models are suggested for different types of exercises. In our planning for exercises at the NCR, we will test how

this approach works compare them to other scenario-building models. The socio-technical models, however, needs measurement standards when setting up the scenarios. We intend to use learning outcomes as described in section 4.5 as measurement. We want to use ISO-standards to measure the status of the social part of the organization, and the ITU-T-standards to measure the technical part of the organization. Our approach can be visualized like presented in figure 4.

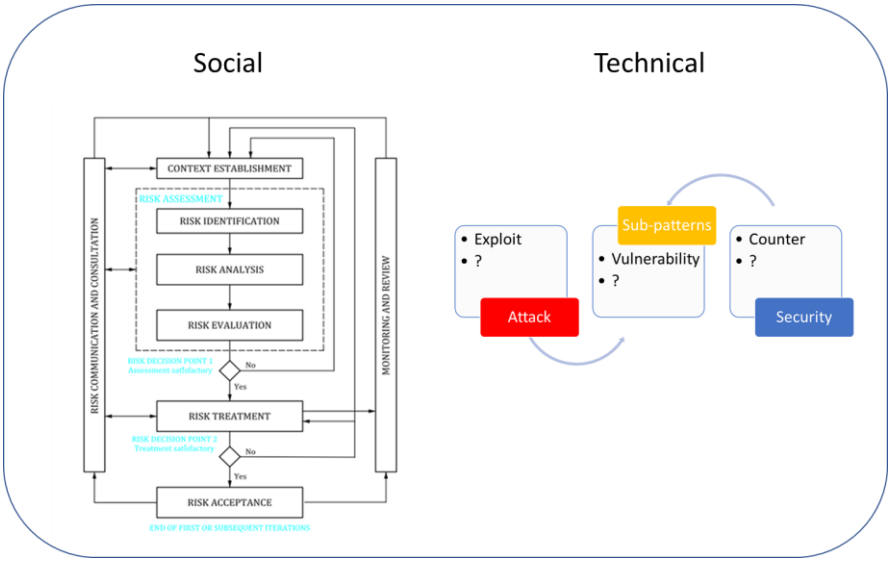

Fig. 4: Socio-technical standardization scenario measurement

The scenario will combine the results from the social and technical measurements to provide a total-concept scenario for the full-scale exercises. By this approach it will be possible to also measure the scenario incident handling process during the exercise.

4.4 Escalation maturity analysis

When analyzing the mentioned maturity escalation study executed at the Inland Hospital trust in Norway (Østby & Katt, 2019), the authors focused on the weakest scores. However, the authors suggest that it is also important to focus on the high scores, to find the organization's strengths, and find the prioritization to the management to find an action strategy within the regulations of crisis management in the organization.

This is especially important when preparing for the exercise, to give the participants the possibility to perform successfully on their strengths. In planned research we want to suggest improvement-work during and after the exercise (Østby & Katt, 2019).

It is however important to give the participants the possibility to train on their maturity weaknesses, and when preparing for the exercises, there will be a need to pro-

vide suggestions on how to handle the organizations biggest challenges on both strategic, tactical and operational layers. This process can be presented as in figure 5.

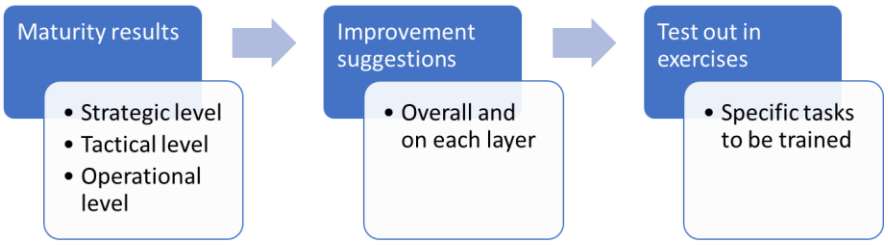

Fig. 5. Maturity results to be trained

For the exercise itself it can be organized with time-outs when these specific tasks are put in focus. That is, time to reflect on specific tasks and to document lessons learned experiences.

4.5 Lectures

In an evaluation after a recent table-top exercise for the tactical/emergency ICT-management team at our university, most of the participants answered relevant, very relevant and huge relevance when asked about relevance in lectures beforehand the exercise. The results are presented in table 1.

Table 1. Relevance in lectures beforehand exercises[1]

	No relevance	Some relevance	Relevant	Very relevant	Huge relevance
Regulations in security and emergency at Universities and Colleges (laws, regulations and guidance's), and other tasks crises management should be prepared for.	0%	16,7%	50%	16,7%	16,7%
Crisis management and work in crisis staff: Situational analysis, need of recourses (personnel and material), roles in crises and operative management.	0%	0%	33,3%	50%	16,7%

[1] 6 out of 10 participants answered the evaluation form

Information in emergencies, crisis management brief, crises communication and CIM.	0%	0%	16,7%	66,7%	16,7%
Emergency plans, task lists for roles in crisis (critical analysis of the team's emergency plan).	0%	0%	33,3%	50%	16,7%

When planning the lectures for the organization participating in exercises at the Norwegian Cyber Range, it will be necessary to plan the lectures to support both the strategic, tactical and operational teams. However, the focus in the lectures will still be responsibilities, roles and escalation procedures. In this research we suggest preparing lectures as executed in this mentioned exercise, of which is a modified version of Backward Design, in a socio-technical context, as presented in figure 6.

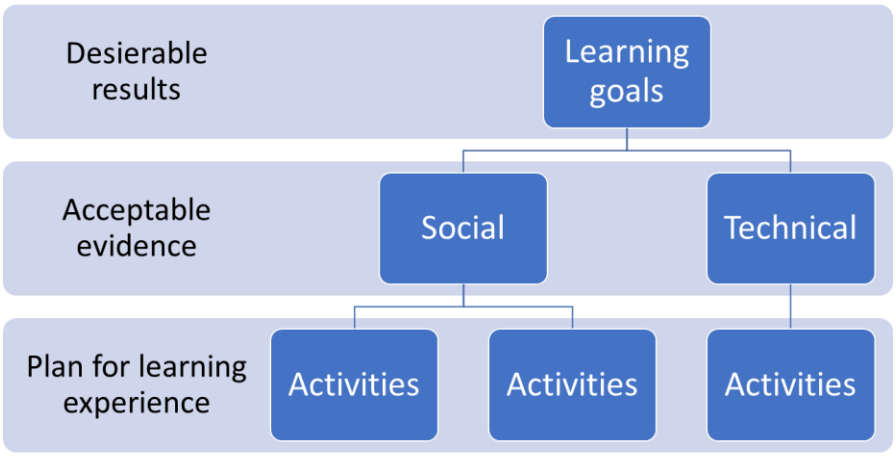

Fig. 6: Backward Design, modified in a socio-technical context (Wiggins, Wiggins, & McTighe, 2005)

By using this approach, the learning experience may flow into the exercise. That is that we don't need to "stop" the lectures when starting the exercise, as much of the learning experience will take place in the actual exercise in so called teachable moments.

5 Conclusion and future research

In this paper the author discusses a work in progress, to create a preparation schedule for exercises (PSE) to support exercise control (EXCON) teams and instructors for full-scaled combined crisis management and cyber-exercises.

After this framework has been reviewed and presented at the HCI International 2020 we plan to implement, test and evaluate the framework when setting up cyber crises exercises in the Norwegian Cyber Range (NCR) environment. We shall test the relevance of the framework for different types of organizations in Norwegian public sector and help develop interoperability standards so that scenario and exercises can be exchange both with in Norway and around the world.

6 References

Al Sabbagh, B., & Kowalski, S. (2015). *MULTIDISCIPLINARY SECURITY*. Retrieved from www.computer.org/security

Bei, Y., Kesterson, R., Gwinnup, K., & Taylor, C. (2011). *CYBER DEFENSE COMPETITION: A TALE OF TWO TEAMS **.

Brown, S., Gommers, J., & Serrano, O. (2015). From cyber security information sharing to threat management. In *WISCS 2015 - Proceedings of the 2nd ACM Workshop on Information Sharing and Collaborative Security, co-located with: CCS 2015* (pp. 43–49). Association for Computing Machinery, Inc. https://doi.org/10.1145/2808128.2808133

Burger, E. W., Goodman, M. D., Kampanakis, P., & Zhu, K. A. (2014). Taxonomy model for cyber threat intelligence information exchange technologies. In *Proceedings of the ACM Conference on Computer and Communications Security* (Vol. 2014-November, pp. 51–60). Association for Computing Machinery. https://doi.org/10.1145/2663876.2663883

Depoy, J., Phelan, J., Sholander, P., Smith, B., Varnado, G. B., & Wyss, G. (2005). *RISK ASSESSMENT for PHYSICAL AND CYBER ATTACKS on CRITICAL INFRASTRUCTURES*.

DSB. (2014). *Veileder til helhetlig risiko og sårbarhetsanalyse i kommunen*. Retrieved from https://www.dsb.no/globalassets/dokumenter/veiledere-handboker-og-informasjonsmateriell/veiledere/veileder-til-helhetlig-risiko-og-sarbarhetsanalyse-i-kommunen.pdf

DSB. (2016). *VEILEDER I PLANLEGGING, GJENNOMFØRING OG EVALUERING AV ØVELSER Metodehefte: Fullskalaøvelse*.

DSB. (2019). *Analyser av krisescenarioer*. Retrieved from https://www.dsb.no/globalassets/dokumenter/rapporter/p1808779_aks_2018.cleaned.pdf

ENISA. (2009). *Good Practice Guide on National Exercises Enhancing the Resilience of Public Communications Networks Good Practice Guide on Exercises 2 Good Practice Guide on National Exercises*. Retrieved from http://www.enisa.europa.eu/act/res

ENISA. (2018). Guidelines on assessing DSP and OES compliance to the NISD security requirements. https://doi.org/10.2824/265743

ISO. (2016). *ISO 27035 - 1*. Retrieved from https://www.standard.no/nettbutikk/sokeresultater/?search=ISO+27035&subscr=1

ISO 27005. (2018). *ISO 27005*. Retrieved from www.iso.org

ITU-T. (2019). *ITU-T FG-DFC TELECOMMUNICATION STANDARDIZATION SECTOR OF ITU Protection assurance use case for a payment transaction Security Working Group Deliverable Focus Group Technical Report*. Retrieved from https://www.itu.int/en/ITU-T/focusgroups/dfc/Documents/DFC-O-009_Security deliverable_Report_Protection Assurance Use Case for a Payment transaction.pdf

Jackson, S. E., & Dutton, J. E. (1988). *Discerning Threats and Opportunities*. *Source: Administrative Science Quarterly* (Vol. 33).

Karokola, G., Kowalski, S., & Yngström, L. (2011). Secure e-government services: Towards a framework for integrating IT security services into e-government maturity models. In *2011 Information Security for South Africa - Proceedings of the ISSA 2011 Conference*. https://doi.org/10.1109/ISSA.2011.6027525

Kick, J. (2014). *Cyber Exercise Playbook*.

Kowalski, S. (1994). *IT Insecurity: A Multi-disiplinary Inquiry*. Stockholm University.

Kuechler, W., & Vaishnavi, V. (2012). *A Framework for Theory Development in Design Science Research: Multiple Perspectives*. *Journal of the Association for Information Systems* (Vol. 13).

Liao, X., Yuan, K., Wang, X., Li, Z., Xing, L., & Beyah, R. (2016). Acing the IOC game: Toward automatic discovery and analysis of open-source cyber threat intelligence. In *Proceedings of the ACM Conference on Computer and Communications Security* (Vol. 24-28-October-2016, pp. 755–766). Association for Computing Machinery. https://doi.org/10.1145/2976749.2978315

Mahmood, T., & Afzal, U. (2013). *Security Analytics: Big Data Analytics for Cybersecurity A Review of Trends, Techniques and Tools*. 2nd National Conference on Information Assurance (NCIA). Retrieved from https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6725337

Micco, M., Ed, D., & Rossman, H. (2002). *Building a Cyberwar Lab: Lessons Learned. Teaching cybersecurity principles to undergraduates*. Retrieved from http://penguin.nsm.iup.edu/security.

NTNU. (2019). The Norwegian Cyber Range. Retrieved from https://www.ntnu.no/ncr

Østby, G. ;, Berg, L. ;, Kianpour, M. ;, Katt, B. ;, & Kowalski, S. (2019). A Socio-Technical Framework to Improve cyber security training: A Work in Progress. Retrieved from https://ntnuopen.ntnu.no/ntnu-xmlui/handle/11250/2624957

Østby, G., & Katt, B. (2019). Maturity modelling to prepare for cyber crisis escalation and management. Retrieved from https://orcid.org/0000-0002-7541-6233

Østby, G., Yamin, M. M., & Asabbagh, B. (2019). SIEMS in Crisis Management: Detection, Escalation and Presentation – A Work in Progress. Retrieved from

https://www.researchgate.net/profile/Stefan_Suetterlin/publication/334139727_Team_learning_in_cybersecurity_exercises/links/5d1a241e299bf1547c8eec06/Team-learning-in-cybersecurity-exercises.pdf#page=40

Patriciu, V.-V., & Furtuna, A. C. (2009). Guide for Designing Cyber Security Exercises. In *WSEAS International Conference on Information Security and Privacy*. WSEAS Press. Retrieved from http://www.wseas.us/e-library/conferences/2009/tenerife/EACT-ISP/EACT-ISP-28.pdf

Richmond, A. S., Boysen, G. A., & Gurung, R. A. R. (2016). *AN EVIDENCE-BASED GUIDE TO COLLEGE AND UNIVERSITY TEACHING*.

Shah, S., & Mehtre, B. M. (2013). *A Modern Approach to Cyber Security Analysis Using Vulnerability Assessment and Penetration Testing*. *International Journal of Electronics Communication and Computer Engineering* (Vol. 4). Retrieved from www.ijecce.org

Sparks, S., Embleton, S., Cunningham, R., & Zou, C. (2007). Automated vulnerability analysis: Leveraging control flow for evolutionary input crafting. In *Proceedings - Annual Computer Security Applications Conference, ACSAC* (pp. 477–486). https://doi.org/10.1109/ACSAC.2007.27

Twigg, J. (2001). *SUSTAINABLE LIVELIHOODS AND VULNERABILITY TO DISASTERS*. *Disaster Management Working Paper* (Vol. 2).

van Laere, J., & Lindblom, J. (2018). Cultivating a longitudinal learning process through recurring crisis management training exercises in twelve Swedish municipalities. *Journal of Contingencies and Crisis Management*. https://doi.org/10.1111/1468-5973.12230

Vykopal, J., Vizvary, M., Oslejsek, R., Celeda, P., & Tovarnak, D. (2017). Lessons Learned From Complex Hands-on Defence Exercises in a Cyber Range. In *FIE Frontiers in Education*.

Wahlgren, G., & Kowalski, S. (2016). A Maturity Model for Measuring Organizations Escalation Capability of IT-related Security Incidents in Sweden. *Assosiation for Information Systems*.

Wiggins, G., Wiggins, G. P., & McTighe, J. (2005). *Understanding by Design*. ASCD. Retrieved from https://books.google.no/books?hl=no&lr=&id=N2EfKlyUN4QC&oi=fnd&pg=PR6&dq=Wiggins+GP,+McTighe+J.+(2005).++Understanding+by+Design.&ots=gpcyn4UH5x&sig=HmWITitQ3nVTu1XKcvtKGTibJfA&redir_esc=y#v=onepage&q&f=false

Yale. (2019). Intendent learning outcomes. Retrieved from https://poorvucenter.yale.edu/IntendedLearningOutcomes