Educating New Military Leaders to be Robust against Influence Operations: A Case Study

Knut Østby[1], Kirsi Helkala[1] and Ole Joachim Aasen[2]
[1]Norwegian Defence University College / Norwegian Defence Cyber Academy, Lillehammer, Norge
[2]Accenture, Oslo, Norge

knostby@mil.no
khelkala@mil.no
ole.Joachim.aasen@accenture.com

Abstract: Influence operations and cognitive warfare are part of the new complex threat picture that Norway and other nations face. In general, military education and leadership education have traditions in place to build robustness against war demands, but how to build robustness against influence operations is still almost non-existing. In this case study, we show how an educational module on influence operations was conducted at the Norwegian Defence University College's Cyber Academy department and how this module contributed to strengthening robustness against cognitive warfare. The impact of the educational module was evaluated by a questionnaire and a short group interview, and the results are shown in this paper. The findings indicate a positive development in the cadets' own perceived robustness. In addition, we also discuss and suggest some personal and organizational factors that can strengthen military leaders' robustness against influence operations. The findings and the discussions can be used as inspiration when educational modules are designed both in military and civilian education.

Keywords: Influence Operations, Military Education, Leadership Education, Robustness, Resilience

1. Introduction

Both mental and physical resilience to cope with the demands of war has been and is an important part of the training of military forces. The military profession is inherently stressful, and if the stress factors are not handled it can lead to a persistent reduction in performance and health challenges (Bartone et al. 2009). Lack of information or ambiguous information are examples of the many military stress factors (Bartone et al. 2009). These two stress factors can be reinforced by an adversary through influence operations, psychological operations, and propaganda, which are often intended to inhibit and influence decision-making.

Disinformation directed at military forces is nothing new. However the emergence of the digital domain and the extensive use of digital information to influence people has led to discussions of a sixth war domain, the cognitive domain (Ottewell 2020). Today's examples can be found in the Ukraine war, where several actors have used disinformation to strengthen their narrative (ENISA 2022, Singer and Johnson 2021). Regardless of whether the cognitive is defined as a separate warfare domain, the digital battle for narratives, truth and information has created a growing need for resilience against influence operations.

In a series of articles, the Norwegian Defence Research Establishment (FFI) has looked at how states use social media as one of many means in their influence operations. The reports highlight how foreign states have contributed to creating division and polarization within Western democracies, with examples such as the handling of COVID-19 and the election in the USA in 2016. The reports emphasize that it is essential and necessary that society becomes more robust facing such operations, and that this is made more accessible by reducing the effect of such operations rather than stopping the operations themselves (Sivertsen et al. 2021). FFI puts forward several proposals for measures to reduce the effect of these operations. One of the proposed measures is to increase the resilience of ministries, agencies, and actors in total defence through training and awareness-raising. Several other articles and reports also promote the importance of strengthened education in the military to reduce the effect of information operations and propaganda (Fitzpatrick et al. 2022, Kacała 2015, Mobley 2011). "Digital Literacy" competence is often mentioned, but it is not specified how this can be raised. Nor has any attempt been made to measure the effect of such education. Singer and Johnsen (2021) also agree that education against disinformation should be included in military training. They indicate that military forces should look to civilian education programs and introduce disinformation awareness training similarly to cyber situational awareness training. Several articles refer to the effects achieved by education in Finland, which is ranked at the top among 35 European countries in robustness against disinformation (Lessenski 2021, Singer and Johnson 2021), mainly due to increased competence from an early age in the entire population.

As there is little information on how such training can be carried out as part of military leadership training and studies on the effect of the training, this research project aims to contribute to precisely this. By studying the

effect of an educational experiment on a military leadership education, the study intends to create a deeper understanding of how resilience against cognitive warfare in general and influence operations in social media can be created among military leaders. This study contributes to the development of best practice in the area. The project is based on FFI's hypothesis. It measures if robustness and resilience can be created through training and awareness raising, including practice in handling the impact on exercises. Military training and exercises, including constructive feedback, have previously been mentioned (Helkala and Rønnfeldt 2022) to strengthen self-regulation and cognitive robustness.

This hypothesis was tested on cadets at the Norwegian Defence Cyber Academy. Ahead of the closing exercise at the school, the cadets received training in how states use influence operations to promote their narrative and how social media can be used as part of these operations. The cadets were then tasked to design influence operations in social media based on the scenario of the following military exercise. The actors in the scenario were involved in a fictitious military conflict in Europe. The influencing operations were developed with a simulation tool called Somulator[1]. This tool, developed by the FFI in collaboration with the Norwegian University of Science and Technology (NTNU), can be used to simulate posts on Twitter, websites, image sharing and video sharing.

1.1 Problem Statement

This case study contributes to understanding of how future military leaders feel equipped to deal with influence operations and how education and training could strengthen their resilience.

2. Theory

2.1 Resilience/Robustness

Mental robustness is closely related to psychological or cognitive robustness, which are terms that are often used to explain the same sets of mental qualities that military leaders should have to cope with the pressures and stress. We define robustness as the ability to withstand strain and stress, similar to Aven's definition (Aven 2022).

Resilience is an alternative term that is used to describe many of the same characteristics as robustness and is increasingly used within social security (Stavland and Bruvoll 2019). Resilience focuses more on the process of recovering from demanding situations, while robustness is more about not being affected by the demanding situations. The American Psychological Association defines resilience as both a process and a result of being able to adapt to demanding situations in life (APA 2023).

Although we focus specifically on robustness against influence operations, several characteristics that contribute to resilience can also contribute to increased robustness. Bartone and Armstrong (Bartone et al. 2009) show that resilience in military forces is influenced not only by individual characteristics and training but also by organizational and societal factors.

2.2 Information and Influence Operations

An individual is a part of information systems as we collect, analyse, store, edit and share information in the same way as other parts of information systems do (Whitman and Mattord 2012). The difference between a human and other parts is that humans are also influenced by non-linguistic information, for example, colours, sounds, touches, tastes, and smells. Moreover, this is what makes us vulnerable to influence operations.

Sensory marketing (Erenkol and Merve 2015, Rathee and Rajain 2017), for example, is based on the perceptive capabilities of our senses, and it is used not only by sales organisations, but also by others who want to influence us (Helkala and Rønnfeldt 2022). Marketing campaigns, election campaigns, vaccination campaigns, and mass-produced phishing emails are examples of campaigns were sensory marketing techniques are used (Helkala and Rønnfeldt 2022). Even though not all goals are political, they still influence decision-makers overall, for example, to make one emotionally aroused and angry, which is not necessarily positive when decisions must be made.

[1] https://www.ntnu.no/ncr/somulator

The participants in this study, like the rest of Norway's population, are daily exposed to digital information that is intended to influence them. A very small part of this information is considered information operations or influence operations in a military context, which is a form of a campaign with the purpose to influence decision-makers in such a way that one achieves one's own political and military objectives (Johnsen and Eid 2018). However, we do not make a difference between miliary and non-military operations in this paper.

The Ministry of Defence in Norway sees influence operations as part of the complex threat to the country (Forsvarsdepartementet 2020). Robustness against influence means that military leaders do not change decisions because of an adversary's influence.

2.3 Cognitive Warfare

Cognitive warfare is another new and debated term with several different definitions. Several environments in NATO claim that this must be seen as a new war domain, on an equal footing with the other war domains of sea, land, air, cyber, and space (Claverie and Du Cluzel 2022).

Cognitive warfare opens a possibility that a wide range of methods, including technological methods categorized as cyber tools, could influence how we think. By making military leaders more robust against digital influence operations, it will also be possible to increase robustness against cognitive warfare.

2.4 Robustness Against Influence Operations

In this case study, we explore the concept of robustness in the context of influence operations. Robustness against influence operations can be defined as the ability to withstand informational influences without losing ability to carry out tasks.

At the individual level, there is no generally accepted list of characteristics that contribute to this resilience. However, research points in the direction that the ability of critical reflection, analytical thinking, and a higher level of knowledge contribute to a better ability to distinguish between fake and factual news in social media (Lessenski 2021, Pennycook et al. 2020). Furthermore, a well-developed short-term memory and good word comprehension have been shown to have a positive impact on resistance to spear-phishing attacks via e-mail (Ebner et al. 2020). There is also research that indicates that a higher level of education reduces the likelihood that individuals will be attracted to conspiracy theories (Douglas et al. 2016). These measures have also been proposed by FFI to strengthen robustness against the influence of social media (Sivertsen et al. 2021).

2.5 Situational Awareness

The Norwegian defence leadership philosophy is based on mission-based leadership, where military units must be able to interpret overall intentions and objectives and find the best solutions. This philosophy requires that the individual unit or leader is able to understand surroundings and adapt plans in line with them. The core of the challenge lies in the ability to distinguish between information that should influence decisions and actions and information that should not.

The process of gaining situational awareness can be divided into three parts: perception, understanding, and foresight (Endsley 1995). Endsley (1995) presents several characteristics that are important in achieving good situational awareness. Since a solid understanding of the situation also requires a correct response to information, these characteristics can also contribute to strengthening resistance to influence operations. Endsley highlights the individual's ability to process information, which is influenced by characteristics, experience, and training. Research conducted on cyber operators (Jøsok et al. 2019) shows that individual characteristics such as self-regulation, metacognition and communication skills strengthen the development of good situational awareness.

3. Method

This paper presents a case study of an educational module carried out at the Norwegian Defence Cyber Academy in 2023. The cadets' subjective understanding of robustness against foreign states' influence operations was mapped through a questionnaire and a group interview. The questionnaire was answered by 33 respondents on a scale from "a very small extent" to "a very large extent", and the group semi-structured interview was conducted with ten cadets. The questionnaire and interview were approved by the Norwegian Agency for Shared Services in Education and Research and the Norwegian Defence Research Board. Both data collection methods

were carried out in Norwegian. For this paper, the questions have been translated to English, as well as the direct quotes from the cadets.

3.1 Case Description

Cyber Academy offers a combined leadership, soldier, and engineering education with a bachelor's degree. The bachelor's education includes a subject called Cyber Power, which aims to create an understanding of how to exercise power between states in the cyber domain. In 2023, the cadets participated in an educational model on influence operations as part of this subject. This module lasted a total of 12 school hours spread over two days. On the first day, the cadets had a 120-minute lecture about influence operations given by external researchers from the Norwegian Defence Research Establishment. After this, the cadets, in teams of 4-5 people, developed influence operations in the Somulator[2] (social media simulator). Each group got to be a different actor in a fictitious military conflict in Europe. The military conflict scenario was the same that the cadets faced in their final military exercise later that spring.

In Somulator, the cadets had the opportunity to create different social media users accounts and add content to the accounts. Several of the groups used generative artificial intelligence applications such as ChatGPT to generate their content. The influence campaigns were presented to the other cadets and later used as part of the final military exercise. The module also included reflection breaks.

In addition, the cadets took part in another investigation where they were asked to distinguish between AI and human-generated a low-resource language, Norwegian, Twitter messages. This investigation was part of a master thesis which results are presented in (Aasen 2023). The master thesis explored the use of language models in Norwegian.

The educational module follows Kolb's learning circle (Kolb 1984, Kolb and Kolb 2013) which have four modes: Concrete experience, reflective observation, abstract conceptualization, and active experimentation. In our module, the first mode was the cadets involving themselves in the disinformation operations. During the second mode, the cadets reflected on their new experience from different political, legal, ethical, technical, and tactical perspectives. Further on, the cadets were to integrate these perspectives in the military context and the theories presented during the Cyber Power course. This would be the third mode: conceptualization. The final mode, active experimentation, was when the cadets presented their disinformation operations to other cadets, as well as when some of the operations were used in the final military exercise.

A weakness of the survey is that it was completed immediately after the second day of education. The long-term effect on the changes in robustness is, therefore, uncertain.

4. Results

4.1 Survey

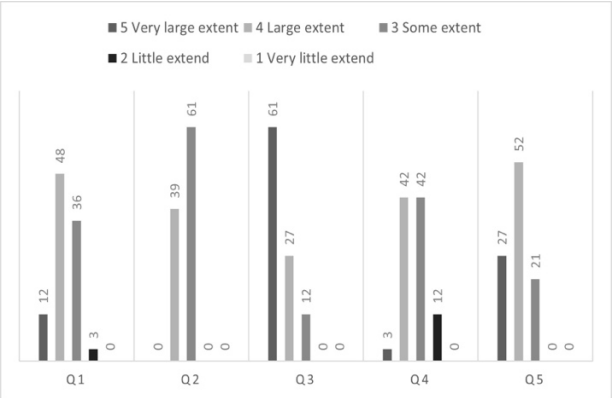

Figure 1. Survey results in percents.

[2] https://www.ntnu.no/ncr/somulator

Figure 1 shows the results for the survey. The questions are as follows. “To what extent …

1. …has the education about influence operations changed your understanding of how information operations can be used by states to achieve their interests?
2. … do you feel that this education module has made you more robust to face cognitive warfare and influence operations conducted by a foreign state?
3. … do you feel that education on this topic should be part of military leadership training?
4. … has this education module led to changes in your understanding of the digital information domain?
5. … has this topic engaged you?

As Figure 1/Q5 shows, the cadets engaged in the module (79% of the cadets answered either large or very large extent). As explained, both traditional lectures and group work were used. This makes the teaching student-centred, which can also support commitment to the teaching in addition the topic itself. Most of the cadets (88% of the cadets answered either large or very large extent, Figure 1/Q3) also thought that today's military leadership training should include influence and cognitive warfare as mandatory themes.

After the module (lectures, presentations of influence operations, investigations, and discussions with both instructors and researchers who participated in both the investigations and the teaching) the cadets felt more confident in dealing with the influence operations. Figure 1/Q2 shows the results stating that the cadets “to some extent and to large extent” feel more robust against cognitive warfare.

We also asked the cadets how this module, especially creation of their own influence operations, has changed their views. Figure 1/Q4 shows results for the question about changes in the understanding of the digital information domain, and Figure 1/Q1 shows results for changes in understanding how states can use the digital influence on their own advantage. As the results show, most of the cadets have changed their understanding from some degree to a large degree.

4.2 Interview

4.2.1 Own Understanding of Influence Operations

The cadets emphasized learning how little resources are required to initiate such campaigns and how difficult it is to detect such campaigns. The module also made them to understand that campaigns have an impact. The role of AI was also highlighted. A cadet summarized the issue as follows:

"With AI, it lowers the threshold for being able to do such operations. Before, you had to have a nation state with many people to be able to do such an operation and employ people to write. However, now all you need is a Python script and an API for ChatGPT, then you can create the same effects."

There are several measures the cadets see that should be taken to strengthen the understanding and robustness of the Defence Forces. One important measure is raising awareness of such operations. The following was said during the interview:

"The most important thing is what we do now. We talk about it and learn. You create an understanding of why the adversary does it, what is the purpose of the operation."

The cadets did not see this as a unique problem for the Armed Forces but a challenge that affects society as a whole. Thus, the counter measures should be introduced to a greater extent and preferably start at school at an early age. One cadet stated the following during the interview:

"If the Defence Forces are to have any effect from this, they [the kids] must be taught from an early age and learn to use technology that is coming. It is perhaps easier to recognize the models that are used if you learn to use them. You get training in this for a long time and from an early age. Getting a person who is familiar with it from the start.”

Some Defence-specific measures were also seen as beneficial, such as introducing influence operations as an element in military exercises and focusing on providing verified information about geopolitical happenings for the leaders in order to prevent the effects of influence operations of foreign states.

4.2.2 Own Robustness

The cadets believed that many people think that they are better at recognizing influence operations than they actually are. An example of this is the following statement during the interview:

"I think many people are self-righteous that they are able to discover this themselves, but that there are others who can be affected".

The cadets thought that resilience against such operations is difficult to develop. They said that important qualities are being curious about what is going on in the world and being able to be critical of information that is presented to you. The cadets thought it is difficult to build resilience as they reflected on their own acquired knowledge after the educational module. An example statement from the interview is as follows:

"I might not say that I am more resilient, but that I am more aware that it can happen. But will still not be able to distinguish something that is fake from something that is real. The robustness may lie in the fact that one is aware of it, but being able to directly identify that someone is trying to influence me, that ability has not appeared now. It's perhaps more that I know I don't have it, which is just as important."

5. Discussion

To put the results of this study in a larger context, we discuss development of individual resilience, engagement across topics, and organizational and societal factors.

5.1 Development of Individual Resilience

This study provides limited insight into which personal characteristics promote resistance to influence. However, some of the respondents claimed that they have achieved increased resilience by taking time to reflect on influencing factors and being aware that something is influencing them.

Being able to reflect on one's own thinking is called metacognition. Jøsok et al. (2016) have previously shown how the ability for metacognition strengthens the ability to form a good situational awareness among cyber operators. This, together with the findings from this study, suggests that the ability for metacognition could increase resistance to influence operations. However, this should be further studied.

5.2 Engagement Over a Theme Creates Robustness

This survey also shows that over 50% of the cadets believed that the topic and the way it was delivered engaged them "to a large" or "to a very large extent". Based on previous research that studied a connection between commitment, resilience, and further performance (Luthans et al. 2016, You 2016), a commitment to the topic of influence operations could also help to build resilience against such operations.

The educational module was a student-active approach where the cadets had to use a social media simulator to create their own influence operations that were then used in later exercises, as FFI recommends. No specific investigation has been carried out into whether it is the form of teaching or other reasons that can explain the high level of commitment. This is a topic that further research could investigate in more detail to contribute to developing best practices within education and training of resilience against influence operations.

5.3 Organizational And Societal Factors That can Strengthen Resilience

Bartone et al. (2009) pointed out several organizational and societal factors that can contribute to strengthening resilience in military forces. The study highlighted the importance of educating and training on source criticism and critical thinking in the school system. Furthermore, it is pointed out that the Defence Forces as an organization could contribute by having leaders regularly disseminate updated and verified situational information. Such updates can help to create an understanding that limits operations' influence on decision-making.

The cadets are also relatively united in their views on whether education on the topic should be included as part of military leadership training. Over 85% of the respondents believe that the topic should be included to a large and very large extent in military leadership training. This teaching experiment was carried out as an intensive two-day teaching/practice programme; probably other ways of setting up the teaching will give more effect. The interviews emphasize that creating resilience is a long-term process, which should preferably be started in the school system long before the military career begins. This agrees with findings from Finland, which has included

education on the topic already from primary school. The country is considered to be the most robust in Europe against disinformation (Lessenski 2021).

Fact checking services such as faktisk.no in Norway have been established to contribute to correct mis/disinformation. Also, comparing social media news to information provided by the governmental intelligence services in Norway and in other countries could reveal mis/disinformation. Making a habit of using these services could increase societal resilience towards influence operations.

Nevertheless, today's threat picture, which is described, among other things, in the long-term plan for the Norwegian Armed Forces (Forsvarsdepartementet 2020), and this survey suggest that the educational process of creating robust military leaders and soldiers should include the development of robustness against influence. Further research should examine how such robustness should be developed and measured. This would set the foundation for forming a best practice for developing resilience against influence operations by military leaders.

6. Conclusion

This case study contributes to creating a better understanding of how future military leaders feel that they are equipped to deal with influence operations and how education and training could strengthen their resilience.

Understanding of how to design and carry out influence operations changed during the educational module. When the cadets were allowed to design their own operations, it became clear how easily it was done and how little resources actually were required to create an advocacy campaign. After the module, it also became clear how difficult it can be to discover an influence operation.

The study shows that young military leaders see a great need to include training on influence operations in military leadership training. Education, training, and practice could help strengthen military leaders' resilience against such operations. 39% of the cadets who participated in a two-day educational module report that the module has greatly strengthened their own robustness against such operations. This agrees with other research indicating that resistance and robustness against operations can be trained.

Furthermore, the study gives indications that the robustness is based on the increased awareness that such operations are taking place, as well as exercising reflection and metacognition whenever dealing with the information. Further research should map how these factors could be further empowered.

Acknowledgements

We thank Silje Lensu Dåbakk from FFI for giving lectures on influence operations.

References

APA (2023) 'Resilience', *APA Dictionary of Psychology* [online], available: https://dictionary.apa.org/resilience [Accessed 10 November 2023].

Aasen, O. J. A. (2023) *Small languages and big models - Using ML to generate social media content for training purposes*, https://hdl.handle.net/11250/3107222: Norwegian University of Science and Technology.

Aven, T. (2022) 'Robusthet', *Store Norske Leksikon* [online], available: https://snl.no/robusthet [Accessed 10 November 2023].

Bartone, P. T., Barry, C. L. and Armstrong, R. E. (2009) 'To build resilience: Leader influence on mental hardiness', *Defense Horizons* 69.

Claverie, B. and Du Cluzel, F. (2022) '"Cognitive Warfare": The Advent of the Concept of "Cognitics" in the Field of Warfare. ' in Claverie, B., Prébot, B., Buchler, N. and Du Cluzel, F., eds., *Cognitive Warfare: The Future of Cognitive Dominance*, NATO Collaboration Support Office.

Douglas, K. M., Sutton, R. M., Callan, M. J., Dawtry, R. J. and Harvey, A. J. (2016) 'Someone is pulling the strings: hypersensitive agency detection and belief in conspiracy theories', *Thinking & Reasoning,* 22(1), 57-77.

Ebner, N. C., Ellis, D. M., Lin, T., Rocha, H. A., Yang, H., Dommaraju, S., Soliman, A., Woodard, D. L., Turner, G. R., Spreng, R. N. and Oliveira, D. S. (2020) 'Uncovering Susceptibility Risk to Online Deception in Aging', *J Gerontol B Psychol Sci Soc Sci,* 75(3), 522-533.

Endsley, M. R. (1995) 'Measurement of situation awareness in dynamic systems', *Human factors,* 37(1), 65-84.

ENISA (2022) *Threat Landscape 2022*.

Erenkol, A. D. and Merve, A. K. (2015) 'Sensory Marketing', *Journal of Administrative Sciences and Policy Studies,* 3(1), 1-26.

Fitzpatrick, M., Gill, R. and Giles, J. F. (2022) 'Information Warfare: Lessons in Inoculation to Disinformation', *Parameters,* 52(1), 105-118.

Forsvarsdepartementet (2020) *Prop. 14S (2020-2021) Langtidsplan for forsvarssektoren*,

Helkala, K. M. and Rønnfeldt, C. F. (2022) 'Understanding and Gaining Human Resilience Against Negative Effects of Digitalization' in Lehto, M. and Neittaanmäki, P., eds., *Cyber Security: Critical Infrastructure Protection*, Cham: Springer International Publishing, 79-91.

Johnsen, B. H. and Eid, J., eds. (2018) *Operativ psykologi,* 2 ed.*,* Fagbokforlaget.

Jøsok, Ø., Lugo, R., Knox, B. J., Sütterlin, S. and Helkala, K. (2019) 'Self-regulation and cognitive agility in cyber operations', *Frontiers in Psychology*.

Kacała, T. (2015) 'Military Leadership in the Context of Challenges and Threats Existing in Information Environment', *Journal of Corporate Responsibility and Leadership,* 2(2).

Kolb, A. Y. and Kolb, D. A. (2013) 'The Kolb Learning Style Inventory 4.0: Guide to Theory, Psycho-metrics, Research & Applications', [online], available: https://learningfromexperience.com/downloads/research-library/the-kolb-learning-style-inventory-4-0.pdf [Accessed 10 November 2023].

Kolb, D. A. (1984) *Experiential learning: experience as the source of learning and development,* Englewood Cliffs, NJ, Prentice Hall.

Lessenski, M. (2021) *Media Literacy Index 2021, Double Trouble: Resilience to Fake News at the Time of Covid-19 Infodemic*, Open Society Institute - Sofia.

Luthans, K. W., Luthans, B. C. and Palmer, N. F. (2016) 'A positive approach to management education: The relationship between academic PsyCap and student engagement', *Journal of Management Development,* 35(9), 1098-1118.

Mobley, J. (2011) *Study to Establish Levels of Digital Literacy for Soldiers and Leaders in the U.S. Army*.

Ottewell, P. (2020) 'Defining the Cognitive Domain', [online], available: https://overthehorizonmdos.wpcomstaging.com/2020/12/07/defining-the-cognitive-domain/].

Pennycook, G., McPhetres, J., Zhang, Y., Lu, J. G. and Rand, D. G. (2020) 'Fighting COVID-19 Misinformation on Social Media: Experimental Evidence for a Scalable Accuracy-Nudge Intervention', *Psychological Science,* 31(7), 770–780.

Rathee, R. and Rajain, P. (2017) 'Sensory marketing - investigating the use of five senses', *International Journal of Research in Finance and Marketing,* 7(5), 124–133.

Singer, P. W. and Johnson, E. B. (2021) 'The need to inoculate military servicemembers against information threats: the case for digital literacy training for the force', [online], available: https://warontherocks.com/2021/02/we-need-to-inoculate-military-servicemembers-against-information-threats-the-case-for-digital-literacy-training/].

Sivertsen, E. G., Hellum, N., Bergh, A. and Bjørnstad, A. L. (2021) *Hvordan gjøre samfunnet mer robust mot uønsket påvirkning i sosiale medier*.

Stavland, B. and Bruvoll, J. A. (2019) *Resiliens – hva er det og hvordan kan det integreres i risikostyring?*

Whitman, M. E. and Mattord, H. J. (2012) *Principles of Information Security,* 4 ed.*,* Cengage Learning.

You, J. W. (2016) 'The relationship among college students' psychological capital, learning empowerment, and engagement', *Learning and Individual Differences,* 49, 17-24.