Mitigation Through Simulation: An Evaluation of the Somulator Social Media Training Tool in the Norwegian Armed Forces

Silje Lensu Dåbakk
Instituttveien 20
2007 Kjeller
NORWAY

silje-lensu.dabakk@ffi.no

ABSTRACT

This paper presents key findings from an evaluation of the first-time use of a social media simulator in a military exercise in the Norwegian Armed Forces. The purpose is to explore the training opportunities that including social media simulation into a military exercise can provide, and how these training opportunities can be expanded and enhanced to advance training to mitigate and respond to Cognitive Warfare. As it presents some findings from a first-time use of a social media simulator in a military exercise, the paper may also contribute with practical advice to NATO partners aiming at including such simulation into their training practices.

1.0 INTRODUCTION

Having become imperative in the 21st century information environment, social media platforms have added new layers of complexity to modern conflicts, confrontation, and war. The emergence of social media platforms as important communication infrastructure represents a watershed in how people receive and perceive information, while allowing for anyone with a device, including adversaries, to participate in and shape the information environment through producing, editing, and sharing content in real time. Social media provides fast and broad access to target audiences, enabling the delivery of attacks that can impact and influence both civilian and military decision-making. Social media platforms are therefore regarded as powerful technological enablers of Cognitive Warfare (CogWar) [1] actualizing the need to mitigate and respond to attacks where cognition is the target.

Current conceptualizations of CogWar have in common that the activity targets individual or collective cognition, aiming to influence or modify behaviour or decision-making [2], [3], [4]. In CogWar, social media platforms represent a multitude of potentialities to be exploited by an adversary for such purposes. The instant connection formed by a multitude of trust-based networks provides opportunities to manipulate perceptions and beliefs, with little cost or effort [5], [6]. Indeed, social media has been weaponized by adversaries for such activities, and common examples include infiltrating domestic conversations and heated debates using fake accounts [7], [8] and coordinated inauthentic behaviour to amplify certain narratives or content [9].

While the common examples of adversarial exploitation of social media include attempts at manipulating public debates and discourse, social media poses specific challenges for the military. An adversary may take advantage of the "strategic "informational" architecture" of social media, by using it to create effects that influence the perception, behaviour or capabilities of a specific target audience to reach a desired end-state[10].The potential synergies between social media and military activities are manifold, ranging from using social media data to collect and exploit information about target populations, to using social media platforms as vessels to deliver effects. Nissen [10] presents six ways social media can support military activity, which when used by adversaries create vulnerabilities that need to be managed: intelligence collection; targeting; psychological operations; operations; command and control; and defence [10]. For instance, adversaries may use social media platforms for *intelligence collection*, collecting and analysing information about military personnel, operations, or exercises. They can use social media platforms to *target* accounts and profiles of military personnel to monitor, influence or hack. The platforms can be exploited to deliver *psychological operations*, attempting to influence a target audiences' perceptions, beliefs, motives, reasoning, and behaviour through content such as messages or video. This includes deception, and such manipulation of the information environment can lead to wrongful conclusions, comprehension, and predications [11] for decision-making, as they will be based on inaccurate data. Adversaries can also perform *operations* through targeting certain profiles with the purpose of breaching or altering the content of a profile or disabling it. And as social media platforms offer the possibility to coordinate, facilitate and synchronize actions through internal communication and information dissemination, or, *command and control*, they can be efficient tools that assist in the delivery of effects all the while *defending* one's own systems against competing actors. There are thus multiple ways in which social media can be exploited by adversaries in CogWar when military personnel are the target.

In an experiment conducted by the NATO Stratcom Center of Excellence, researchers demonstrated some of the ways in which social media can support military activity, when they used social media platforms to collect information about personnel on exercise in an allied country [12]. During the experiment, they were able to identify a significant number of participants, pinpoint exact locations of several battalions, discover the dates of the active phases of the exercise, and gain knowledge about troop movements on their way to and from exercise. They were also able to collect detailed personal information about the exercise participants using social media, which were then used to tailor influence operations aiming at instilling behaviour detrimental to the conduct of military operations among the participants. Some of these attempts were successful, demonstrating the multifaceted enablers of CogWar inherent in social media platforms, specifically when military personnel are the target.

However, social media also provides opportunities to mitigate and respond to cognitive attacks in the information environment, for instance through responding to adversarial narratives or disinformation through efficient strategic communication. They also offer opportunities to improve Situational Awareness (SA) [13], and the accurate and competent defence of one's own systems can offer competitive advantages [14].

Social media thus represents opportunities, vulnerabilities, and challenges for military personnel, that demand competencies for ensuring operational readiness and efficient and secure handling of social media in the 21st century battlefield. Building such competencies ensures better preparation for mitigating and responding to cognitive attacks delivered through social media. This includes, but is not limited to, ensuring aspects such as Operations Security (OPSEC) and Information Security (INFOSEC); building and maintaining situational awareness; mitigating the effects of adversarial influence operations, and responding to them; coping with the emotional stress induced by cognitive attacks delivered through social media; efficient strategic communications, and evaluating the credibility of online information. Developing and improving such competencies supports the enhancement of cognitive superiority and layered resilience, two of the five long-term warfighting imperatives to accomplish NATO's core missions [15].

To build such competencies, there is a need to train on the secure handling of social media using tools that simulate the information environment as naturalistically as possible, following the "train as you fight" concept. Training in simulated environments allows for scripting events and actions to target desired learning objectives in a systematic manner [16] and is a recommended action to build knowledge needed to counter CogWar efforts and effects [17]. Including social media simulators into military training practices may assist in building competencies required to respond to and mitigate CogWar.

This article will examine how the military can benefit from adding social media simulators into their exercises. The basis for the paper is key findings from an evaluation of the first-time use of a social media simulator, *The Somulator*, in an exercise in the Norwegian Armed Forces. The evaluation identified concrete training opportunities that can be further enhanced to advance training to mitigate and respond to CogWar.

2.0 THE SOMULATOR: A SOCIAL MEDIA SIMULATOR

At the Cognitive Warfare Workshop in Oslo, Norway, 2022, The Norwegian Defence Research Establishment (FFI) presented *The Somulator*, a social media simulator for education and training purposes. The Somulator was in part inspired by earlier NATO Joint Warfare Center (JWC) efforts to simulate social media during exercises, specifically Trident Juncture in 2019. In that exercise, the JWC used a commercial software package that emulated features from Twitter and Facebook [18]. Encouraged by these results, FFI initiated a research activity with the aim of providing an interactive virtual environment for social media simulation [19].

After a broad needs assessment followed by a review of existing solutions, FFI developed a tool to emulate four different social media platforms: Twitter, Facebook, Instagram and YouTube, as well as a fictitious news site that allows for multiple newspaper simulations, using open-source clones. In the Somulator, an exercise control panel provides the opportunity for Directing Staff in an exercise to stage and manage different scenarios that may occur in the information environment, creating simple or complex training sessions. Somulator is intended to be used by anyone who requires social media simulation in their training practices, for instance intelligence staff, cyber operators, government departments and NGOs, and it does not require expert IT skills [19].

2.1 Comprehensive Shield: First-time use of the Somulator in a Military Exercise

In spring 2023, the Norwegian Armed Forces University College (FHS) included the Somulator into their annual capstone exercise, *Comprehensive Shield [20]*. Specifically, the Twitter clone and emulations of newspapers were used. The aim of the exercise is for future Staff level officers to develop knowledge about how politics, strategy, and military operations interrelate. The scenario consists of themes and issues that aim at triggering training opportunities in planning, execution, leadership, and support of NATO operations on strategic, operational, and tactical levels. Thus, the exercise is designed to advance the competencies of future staff officers for military leadership and defence planning, to prepare them for more advanced roles in joint operations.

In previous years on this exercise, the media-play has entailed sending scenario-specific news articles on email [only] to the students that are training on strategic communication, aiming to trigger training opportunities and decision-making. Social media has not been simulated in these exercises before. As such, the information environment has been a training aspect only for the three or four students who have been explicitly tasked to work with strategic communication and handling the press, and it has not simulated the omnipresence of social media nor the different dynamics in the operational environment that are mirrored in social media content. For this exercise, the Somulator enabled a different way of conducting media-play. Yet precisely because it is different, it had to be integrated into the logics and praxis of a military exercise, and FHS saw this as an opportunity both to test this new tool and to offer knowledge and experience on how it can be best integrated into other military exercises. FFI thus conducted an evaluation of the use of the Somulator in the exercise.

2.1.1 Exercise Scenario

The scenario during exercise Comprehensive Shield entails simulating a NATO headquarters in a fictious geographical area of geopolitical relevance to both NATO and adversarial actors. This area is characterized by historical and current ethnic tensions, political instability, armed conflicts, and global competition of access to newly discovered natural resources. Underlying this development is a great power rivalry between a rising power, Vulpecula, that is highly aggressive towards NATO, and Aquila, a former member of a federation of several countries that was dissolved in the late eighties. In the Eastern regions of Aquila, Pro-Vulpeculan separatists aim at integrating three provinces into Vulpecula, which is welcomed by Vulpecula through military and political support. As tensions have risen in the region, the UN has discussed the situation, but it has not adopted a resolution that can trigger a UN operation. In the absence of this, Aquila has solicited political and military support from NATO for an operation aiming at stabilising the situation in the eastern provinces of Aquila. In the exercise, the students are tasked to establish and run a NATO headquarters in this region and context.

2.1.2 Exercise Setup

In total, there were 110 participants in the exercise, that is, students under Staff education. The exercise also included Directing Staff, trainers, and facilitators. The entire media-play and simulation of the information environment occurred in the Somulator.

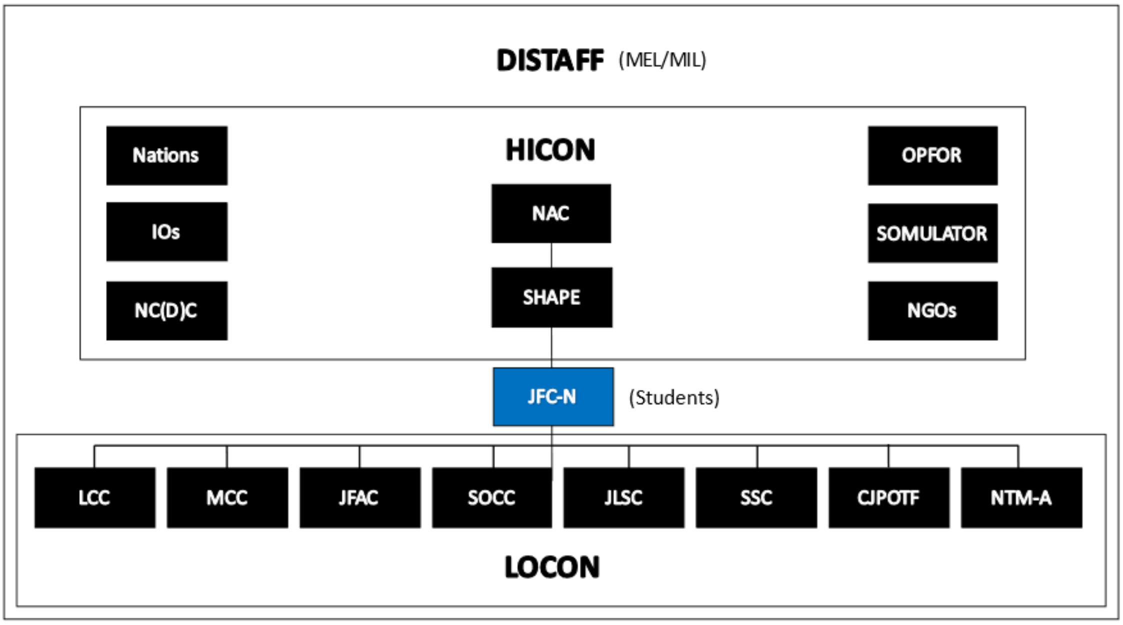
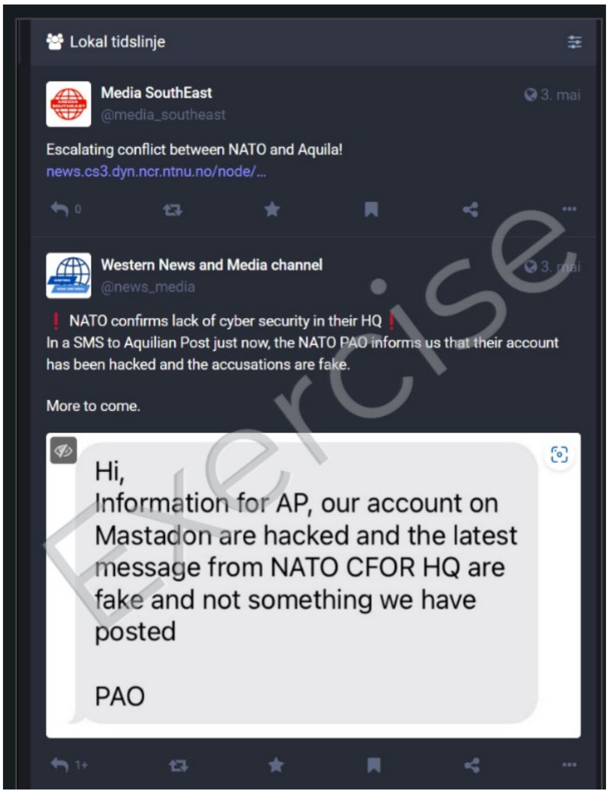


Figure 1. Illustration of the exercise setup, Norwegian Armed Forces Defence University College.

Figure 1 shows the exercise setup, with the students (main training audience) situated between High Command (HICON) and Low Command (LOCON). In the exercise, the students ran the headquarters (JFC-N), with mentors present to guide and evaluate them. The Directing Staff (DISTAFF) is responsible for the Main Event List/Main Incident List, which guides the overall scenario and the learning objectives. In HICON, DISTAFF played actors such as nations, international organisations (IOs), NATO Cyber Defence Command (NCDC), opposing force (OPFOR) and NGOs.

The Somulator staff was situated in HICON, simulating both the OPFOR and the general operation environment, including civilians, “trolls” (that for instance were spreading disinformation and amplifying content) and three different news media. Figure 2 shows a screen shot of what the Somulator could look like during the exercise. It depicts two different media channels in the wake of a simulated attack, where the Somulator staff hacked the NATO CFOR HQ account and disseminated narratives and false information detrimental to the cooperation efforts with Aquila, the country in which the headquarters was situated.



Lokal tidslinje

Media SouthEast
@media_southeast
3. mai

Escalating conflict between NATO and Aquila!
news.cs3.dyn.ncr.ntnu.no/node/...

Western News and Media channel
@news_media
3. mai

❗ NATO confirms lack of cyber security in their HQ ❗
In a SMS to Aquilian Post just now, the NATO PAO informs us that their account has been hacked and the accusations are fake.

More to come.

Hi,
Information for AP, our account on Mastadon are hacked and the latest message from NATO CFOR HQ are fake and not something we have posted

PAO

Figure 2: Screen shot from the Somulator during the exercise.

The group in DISTAFF that managed the Somulator, that is, that populated it with personas and produced content is shown in Table 1.

In the Somulator staff, there was one leader, who had the function of being the editor in chief, tying the content to the scenario and communicating with the rest of the Directing Staff and mentors, one blue team player, one read team player, two journalists, and one technical support person who also created content where needed. DISTAFF who played nations and NGOs, such as the UN and the Red Cross, had their own profiles in the Twitter clone, and were not managed through the Somulator cell.

Table 1: The Somulator staff set-up.

	Role	Function
1	Leader	Editor in chief, ties the content with the scenario, coordinate with the rest of the Directing Staff
2	Blue Team lead	Simulate blue actors in the information environment
3	Red Team Lead	Simulate red actors in the information environment
4	2 x Journalists	Simulate three newspapers with distinct perspectives
5	Technical Lead	Ensuring an agile implementation of the Somulator
6	Directing Staff	Nations and NGOs, such as the UN and the Red Cross

3.0 APPROACH

In the following, I will describe how we collected and analysed the data for the evaluation of the Somulator in the exercise Comprehensive Shield.

3.1 Research Questions

Social media simulators have, up until now, not been part of training scenarios in the Norwegian Armed Forces. Thus, when FHS included it into their exercise, it was the first time a social media simulator in general, and the Somulator in particular, was operationalized in a military exercise in Norway. This offered an opportunity to observe, evaluate, and to learn from the experience to inform and advance the use of social media simulation in military training. The following two research questions were identified:

RQ1: What training opportunities did the social media simulator enable in the exercise?

RQ2: How can these training opportunities be enhanced to optimize training to mitigate and respond to CogWar?

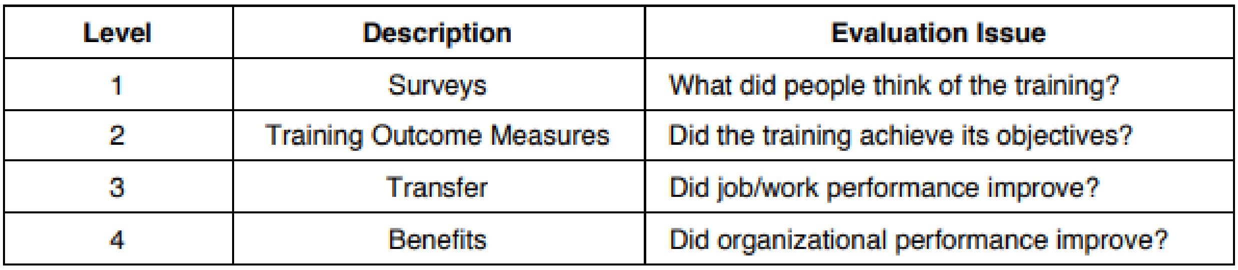
3.2 Method

The exercise presented several "firsts", as this would be the first time FHS applied a social media simulator in their training practice, while also being the first time the Somulator would be used at this scale. This meant that there were many "unknowns" regarding the integration of the Somulator into the exercise. For instance, we did not know whether the students would, in fact, sign in to the Somulator, as participation was voluntary, but encouraged. We did not know whether the Somulator staff would successfully use the Somulator and create content that catalysed training opportunities, or if both content and the Somulator itself would be regarded as a realistic simulation of the information environment in a military context for the students. Furthermore, research on the use of social media simulators in military training is scarce.

For these reasons, we opted for an exploratory approach. In social science, exploratory approaches are used when there is little knowledge about the group, process, or activities one wants to examine, and where the main goal is to produce inductively derived generalizations about said group, process, or activity [21]. In this case, an exploratory approach assists in identifying interesting areas for further inquiry and helps determine future research priorities to further advance the knowledge on how best to integrate social media simulation into military training.

Kirkpatrick [22] launched four different steps or levels of evaluation frequently applied in the evaluation of military training [23] as shown in Table 2, of which different levels can be applied depending on the objectives of the evaluation.

Table 2: Kirkpatrick's four levels of evaluation (Fletcher, 2000).



Level	Description	Evaluation Issue
1	Surveys	What did people think of the training?
2	Training Outcome Measures	Did the training achieve its objectives?
3	Transfer	Did job/work performance improve?
4	Benefits	Did organizational performance improve?

Including the Somulator into the exercise was related to an overall learning objective that aimed at deepening the knowledge of how different factors in the operation environment influence the possibilities and limitations of the armed forces. However, specific learning objectives involving social media had not yet been defined. Indeed, to date, there is no consensus on how to train military personnel to defend against CogWar [24]. As there were no specified training outcomes for the social media simulation, it sufficed to conduct the evaluation on step 1 in an exploratory manner. However, to gain as much insight into the training opportunities enabled by the Somulator as possible, instead of using only surveys, we also conducted semi-structured interviews. The ambition is to use this exploratory data to identify training opportunities offered by the Somulator in the exercise, which can contribute to developing training objectives and creating knowledge on how to mitigate and respond to CogWar [25]. Once the concrete training objectives for social media simulation have been defined, steps 2, 3 and 4 can be applied to evaluate their success in the next iterations of Comprehensive Shield or other exercises.

We were interested in the experiences from four different perspectives on the exercise, which were thus our data sources:

- The perspective of the exercise planner, who oversaw the overall scenario.
- The perspective of the Somulator staff, i.e., the team that created content and simulated the information environment.
- The perspective of the mentors, i.e., the personnel who guided and evaluated the students during the exercise.
- The students, who were the training audience.

In total, four group interviews were conducted: One with the leader of the exercise and the leader of the Somulator staff, one with the red lead and blue lead in the Somulator staff, one with a trainer, and one group interview with seven students. Out of the 110 students in the exercise, 37 answered survey questions about the Somulator.

The interviews and the surveys included questions about the general experience of using the Somulator, whether it was perceived as relevant and realistic, how it was compared to earlier simulations of the information environment, whether and how it supported the training during the exercise, questions about resource management, and technical aspects. The interviews were semi-structured. Semi-structured interviews are conversations which are focused on a certain theme and questions but where there is leeway to follow up on angles and experiences that may show up during the conversation [26]. This is a useful method when the approach is exploratory and gave us room to capture any interesting information relating to the use of the Somulator during the interviews. The survey questions were yes/no questions with the possibility to elaborate experiences and opinions in text boxes. The text responses were included in the analysis.

The data was analyzed using a reflexive thematic approach developed by Clarke et al. [27]. Thematic analysis is an umbrella term for methods that aim at capturing patterns ("themes") across qualitative datasets" [27]. These themes can synthesize experiences of using, interacting with, or learning from, the Somulator, and provide a basis for analysis that help us understand how the Somulator was used and perceived during the exercise. Specifically, *reflexive* thematic analysis means developing these themes from the data and is thus a method that is focused on inductive reasoning [27]. This is a strength for this study, as it is an evaluation of the experiences and perspectives of the Somulator users in the exercise. This is especially helpful as we wanted to map the training opportunities that occurred but did not have any defined training objectives. The emphasis that reflexive thematic analysis places on creating themes that are empirically developed aligns with the exploratory nature of an evaluation where we are open to whatever experiences or perspectives the research subjects might have within the categories of inquiry. The coding process yielded 53 codes. Next, these codes were used to infer themes or patterns, or "coherent clusters of meaning that tell a story about a particular aspect of the dataset" [27]. This resulted in 17 themes, which ranged from experiences with technical aspects, content, operationalisation (that is, the practical integration of the Somulator into the exercise structure), pedagogical value (that is, the training opportunities the Somulator created), overall experience and resource management. In the following, a summary of the key themes related to training opportunities and the possibility to enhance them, is presented.

4.0 RESULTS

In the following, themes that answer RQ1, namely what training opportunities the social media simulator enabled in the exercise, are presented.

4.1 The Somulator Adds an Additional Layer of Information About the Operational Environment that Can Help Build SA

The exercise leader reported that the Somulator assists in reaching the overall learning objective of understanding how different factors in the operational environment influence the opportunities and limitations of the armed forces, as influence through media is a central aspect that can be both such a limitation and opportunity. Both the trainer, the exercise leader, and the Somulator staff leader reported that simulating social media in the exercise provided an extra layer of information about the operational environment that the students had to consider in their practice. Compared to previous ways of simulation, the Somulator allowed for a mirroring of social and political sentiments and currents which created a closer interaction with the realities in the operational environment. Thus, it enabled more variables to consider in analysis and decision-making:

> *The Somulator was good at simulating the sentiment in an environment. I think this mirrors social and political conflicts and currents in society, both locally, nationally, and globally, but also between those levels. What's unique about social media is that it ties the human and personal dimension to the public debate, the military reality, and when they're tied together, it creates a different expression [of the operational environment]. In an exercise where you don't include the Somulator, you don't get the human perspective, you don't get pictures from the conflict and from the political discourse in your face in the same way. Without the Somulator, there is another distance; Somulator shoves the societal sentiment in the face of the students.* (Trainer, Comprehensive Shield)

4.2 Somulator can Demonstrate the Effects of Decision-Making and Strategic Communication

The Somulator creates a better interaction between the media-play and HICON and LOCON actors, compared to the previous ways of simulating the information environment, the Somulator staff leader reported. HICON actors were able to participate independently, that is, without being part of the Somulator staff, in the information environment. When actors such as "the UN" or "the Red Cross", and fictitious nations had their own profile in the Twitter clone, they were able to contribute to a much more realistic simulation. With HICON activity, the Somulator staff were able to use and further simulate the operation environment. This created a simulation of an interactive and diverse information environment, that could also be unpredictable, which mirrors real social media.

> *[…] it's much easier to activate HICON especially. That used to be a difficult thing, […], it disappears, but now we could, to a much larger extent, pull them in as actors in the information environment, which is far more realistic.* (Somulator staff leader)

Using the Somulator to instigate increased participation into the media-play added a new dimension to the simulated headquarters. The fact that the information environment was interactive made it possible to probe and sense, that is, to conduct small, fail-safe experiments and sense what happens, before making important decisions. The Somulator staff did this to adjust the media-play, but in general, this is an important feature that enable the students to train on efficient strategic communications, for instance.

For the students, this meant getting an extra layer of information about the operational environment to consider before and after making decisions. The interactive and pluralistic nature of social media simulation creates a feedback mechanism that can enhance the training to acquire competencies within strategic communication, according to the informants. Specifically, simulating the reactions to a certain narrative or decision can stage how that narrative or decision affected the operational environment:

> *An interesting aspect that Somulator can contribute to is demonstrating effects of decisions made in the headquarters for example, so that you can use the reactions in the Somulator to evaluate whether it [the decision] was effective, or if there were some negative side effects that you hadn't thought of. This is a feedback mechanism- when evaluating that feedback, important learning happens.* (Trainer, Comprehensive Shield)
>
> *I think that the Somulator demonstrates the necessity of considering [what happens in the information environment] and have a plan for one's own presence (or not). If you're going to be active; how will you do that? Does that create new problems for you? That is a difficult balance to strike, but it is necessary that we train on it, and then we need something to train on, like the Somulator. Simply training on effective STRATCOM.* (Trainer, Comprehensive Shield)

Some of the students who were active on the Somulator reported that they did in fact use the Somulator to understand civilian parties and reactions during the exercise, and that they used it to see how their strategic communication was received by audiences.

4.3 The Somulator Adds the Possibility to Navigate and Make Sense of a Complex Information Environment, Including One with Adversarial Activity

The trainer emphasized that the Somulator can create an excess of information, including disinformation and deception, which is an additional aspect that the students must handle together with other tasks. This creates a training opportunity in which it is necessary to separate trustworthy from untrustworthy, and relevant from irrelevant, content in the information environment. It also enables the possibility to simulate potential adversarial modus operandi, and train on mitigating and responding to that in the information environment:

> *[The Somulator] especially added the possibility to create uncertainty for the students, for instance through disinformation. […] If you have [the Somulator], loads of reports coming from below and from the side… it creates a more realistic exercise which is imperative to high learning outcomes.* (Trainer, Comprehensive Shield)

The previous paragraphs presented a summary of themes that help answer RQ1, *what training opportunities did the social media simulator enable in the exercise?* In the following, themes that answer RQ2, that is, *how these identified training opportunities can be enhanced to optimize training to mitigate and respond to CogWar*, are presented.

4.4 There is a Need to Define the Training Audience

The students were asked whether they were active on the Somulator during the exercise, and why/why not. Several of them expressed that they were not active on the Somulator because they did not see how it was relevant for their position in the exercise. Furthermore, some participants expressed that they used it for entertainment during dead time. Indeed, some of the DISTAFF had also expressed beforehand that having every student participating in the Somulator would not be realistic, as many groups of students would not have access to the internet in their positions in the headquarters. This indicates that there is a need to define who the training audience of the Somulator is and communicate this to the students. This necessity was explicitly expressed from the Somulator staff and from the leader of the exercise.

4.5 Content Needs to be Voluminous, Personas Realistic, and they Need to have a History

The students expressed that the content produced for the Somulator was sometimes a bit "flaky". An incident in which the Somulator staff used an image of a member of the DISTAFF, familiar to the students, to impersonate a fictious character, was mentioned as one aspect contributing to said "flakiness". Similarly, some names chosen for the simulated personas in the information environment were reported to be somewhat caricatural.

Furthermore, the students expressed a need for the simulated personas to have a history on the social media platform. This was particularly important when trying to determine the credibility of a source of information. The students pointed out that without the persona's history on social media, it becomes difficult evaluating the credibility, and as such, the information in the Somulator can't really be considered as relevant. To increase realism, and to create situations in which the credibility of information needs to be evaluated, one suggestion was for the Somulator staff to build a history for each of the personas in the information environment in the form of earlier posts.

The students also expressed a need for a higher volume of content in the Somulator, to trigger the possibility to train on sorting irrelevant from relevant information. It was reported that there was too little content to do so. One idea that occurred was to prefabricate content and publish this twenty-four seven.

The previous points imply a need for more resources to create content and was also highlighted by the leader of the Somulator staff. It was emphasised that simulating the information environment with the Somulator required more resources than previous ways of doing it, which of course translates to more staff and higher costs. Specifically, it is creating the content that simulates the pluralism of an information environment, including content that is scenario-specific and noise that is costly, according to the Somulator staff leader. It was, however, concluded that in a cost-benefit assessment, the Somulator offers more benefits than costs, despite the resources needed to create a realistic information environment.

4.6 Coordination between Directing Staff, Trainers, and Somulator Staff Needed to Enhance the Training Opportunities

Members of the Somulator staff and the trainer team expressed the need for better coordination between the trainers, Somulator staff, and the overall Directing Staff throughout the exercise:

> *On the exercise, I wish there had been more coordination between the three: Directing Staff, trainers, and Somulator [staff]. Because then you would have the possibility from the DISTAFF side to say "now these developments [in the scenario] are happening, and we will focus on disinformation."* (Trainer during Comprehensive Shield)

They identified a need for a shared mental model regarding how the different social media incidents would be played out, i.e. what kind of content would lead to triggering an event in the scenario, and what the training objective is. Specifically, it was noted that mutual planning and coordination should occur to ensure that beneficial training opportunities arise:

> *Then DISTAFF could seek input from the trainers, to make it [the inject] as specific as possible, and then through sparring with the Somulator staff, where they provide their competence. Trainer requests what is needed to create the training opportunities. DISTAFF provides the overall perspective in the scenario.* (Trainer during Comprehensive Shield)

The trainer emphasised that a better coordination between HICON, LOCON, and the Somulator staff, can also allow for training opportunities in which the Somulator staff can simulate the effects and reactions of strategic communication coming from the headquarters. There is a potential to learn from this, and to create such situations, there needs to be better coordination between the Somulator staff and DISTAFF:

> *And we were like sitting in our own little bubble, with different profiles [in the twitter clone]. I think we were able to integrate many factors. I wish we got more feedback from the players.* (Somulator staff member)

Central in this theme was also how the Somulator staff would have benefitted from concrete feedback on how the content was perceived by the students, and how it contributed to their learning:

> *Whether HQ were able to [use the content to probe and sense]- I don't know. I didn't feel that we got a direct response that said they did. [...] How did they perceive [the content]? Did it contribute to them discussing concrete things [that were injected into the Somulator]? Or was this something that just passed them by, and they didn't care about?* (Somulator staff leader).

5.0. DISCUSSION

The current understandings of CogWar have several basic tenets in common. These are techniques that aim to manipulate, distort, influence or bias thinking and decision-making [28], [29], [30]. In a military headquarters, and indeed in any situation of crisis, decisions may have to be made at haste and based upon input from, and accurate analysis of, a highly complex multi-domain operational environment. These situations are vulnerable to adversarial cognitive attacks in the information environment. The findings of this evaluation indicate that adding a social media simulator to a military exercise provides opportunities to train on decision-making in the face of such context. The following draws out a few key discussion points that the author recommends are considered when introducing social media simulation into a training environment.

5.1 Identified Training Opportunities

Analysis of the results revealed four notable ways the Somulator provided training opportunities compared to earlier ways of conducting media-play in the exercise:

1) Social media simulation creates possibilities to improve the understanding of the multidomain operational environment, which, with accurate assessment of input data, can contribute to better situational awareness [31]. For SA to lead to a level of understanding that can enable better decision making, it requires trusted data input and evaluation of meaningful information [32]. In CogWar, SA can be targeted through manipulating input data. Social media enables training to improve and maintain Situational Awareness (SA), which is vulnerable to adversarial attacks in CogWar.
2) With social media simulation, reactions to, and effects of, decision-making can be simulated. This enables an improved assessment and evaluation of the impact of the decisions made by the headquarters. This offers a more interactive and realistic way to train on strategic communication, which may provide a competitive advantage in CogWar.
3) Social media simulation enables a simulation of threat actors whose modus operandi includes taking advantage of the digital information environment to manipulate, distort, influence or bias thinking and decision-making of their adversary or strategic competitor. This enables training to mitigate and respond to the effects of such activities.
4) Simulating a pluralistic information environment requires a training audience to separate irrelevant from relevant, untrustworthy from trustworthy content, and evaluate the credibility of information. This can build competencies that strengthen the resilience against disinformation or other cognitive attacks on social media.

These were potential opportunities for training that social media simulation enabled in the exercise Comprehensive Shield. The evaluation also showed that these aspects can be further enhanced to ensure better training situations, which are discussed in the following.

5.2 How to Enhance These Training Opportunities

Firstly, in an exercise, there is a need to define who the training audience of the social media simulator is. The students who were not active in the Somulator said it was due to being unsure of how it was relevant to them or their position. This raises a discussion concerning the role of military personnel and social media: Who, in a headquarters, should be trained to handle social media? And is there a difference between students who explicitly work in the information environment, for instance in the form of strategic communication, and students who don't, considering the omnipresent nature of social media? Indeed, some members of the Directing Staff commented that all students being active in the Somulator would not be realistic, as some would be working in classified areas with no access to the internet. Yet, this can be countered with the fact that some students reported that they used the Somulator during "dead time" or during breaks. This implies that in theory, almost everyone can be targeted through social media, regardless of position and tasks. In a military exercise, it must thus be agreed and defined who the training audience of a social media simulation is, and a rationale given by the exercise planners for including and excluding participants. When considering this, factors worth considering are:

- Should the social media simulation only apply to and concern exercise participants who would for operational reasons only, encounter social media during an operation, or should there be an ambition to have all exercise participants take part in the social media simulation? Worth noting here is the experiment conducted by the NATO Stratcom Centre of Excellence that showed the potential ways a threat actor can take advantage of social media data to influence military personnel, with the intention of inducing behaviour detrimental to their military activity [33]. The researchers targeted all participants on the exercise, not only those who for operational reasons worked in the information environment.
- As CogWar can target entire populations [34] the implication is that it can target a soldier both on and off duty. If one goal of including a social media simulator into an exercise is to simulate a more realistic operational environment, then having as many as possible participate in the social media simulation adds to said realism.
- Whether the training audience of the social media simulator is the students working with, for instance, strategic communications, or whether it's all the exercise participants, must be set during the planning and execution of the exercise as it has implications for how the exercise is shaped to train on mitigating and responding to CogWar.

Secondly, for social media simulation to realistically enhance training outcomes, the quality and quantity of content and its creation needs to be high on the planning agenda:

Quality: Firstly, lessons learned from this evaluation suggest that the emulated personas and the content in the simulation must be realistic, and the Somulator staff must avoid creating caricatures. Doing so might incite 'a fight against the white' situation. This is a phenomenon that occurs in [military] training when the assumptions and instructions delivered (often on white paper) become the centre of focus instead of the assignment itself. Secondly, the findings indicate that there is a need to ensure that personas have a history, or back story, on the social media platform, as this assists in determining the credibility of posts and can contribute to a more comprehensive understanding of the information and the wider operational environment.

Quantity: There is a need to scale-up the content. In this exercise, although there were six people creating content for the social media simulator, the students reported that it was not enough to create an information environment that was unclear, confusing, and ambiguous. To better emulate a real information environment, there will be a need to integrate AI tools that can produce high volumes of realistic content. “Realistic” means content that convincingly emulates the political, social, and cultural aspects of an information environment, but perhaps more importantly, accurately mirrors the potential modus operandi of an adversary. The latter is especially important, as to ensure that the training in the social media simulator is based on the correct assumptions.

Thirdly, while the evaluation showed that social media simulation enables a feedback mechanism in the form of simulated reactions and comments that are especially useful for strategic communication, there is a need to coordinate among the Directing Staff. In this exercise specifically, that meant a coordination between HICON, LOCON, trainers, and Somulator staff. This coordination is vital to ensure that scenarios are played-out in ways that enhance learning. Generally, this means that the Somulator staff must coordinate with the trainers and the remaining Directing Staff to tailor the content they create.

Fourth, the training opportunities identified by the evaluation can be formulated into concrete training objectives for social media simulation. Currently, there is no consensus on how to train and defend against CogWar [35]. Following Kirkpatrick’s four levels of evaluation [36] the training objectives must be defined so that concrete skills and competencies to respond and mitigate CogWar can be enhanced. The evaluation evidenced four such skills and competencies that a social media simulator can assist in developing: Building and maintaining situational awareness through assessing more layers of the operational environment; strategic communication; understanding, navigating, and responding to adversarial influence in the information environment and the assessment of the validity of information on social media. For instance, since the Somulator allowed for a better understanding of the multidomain operational environment, should there be training objectives that explicitly create scenarios that target the situational awareness of a decision-maker through social media? Or, should one training objective be to simulate reactions to a decision or strategic communication, for instance a “Twitter-storm”, that is, a spike in activity regarding a theme or topic, that the students then have to handle? Because the Somulator also allowed for a simulation of threat actors’ modus operandi and a pluralistic information environment that can contain both disinformation, deception, and trustworthy content; should one training objective be to try and separate these? Defining concrete training objectives for social media simulation will require state- of the art knowledge about the continuous development of social media, and how these developments create new threats and opportunities for military personnel. Once defined, the skills and competencies needed to mitigate and respond to CogWar can be further enhanced through continuous evaluation after exercises.

Lastly, there are other theoretical possibilities for training when using social media simulators that were not identified during this evaluation. As Nissen’s [37] conceptualisation of how social media can support military activity shows, intelligence collection and targeting are two possible ways in which social media can pose threats to military personnel and has also been evidenced by [38]. Training on these aspects in a social media simulator may entail a focus on OPSEC and INFOSEC. One training scenario could be adversarial monitoring, hacking, and leaking of information from the different profiles, which can be simulated using the Somulator. Furthermore, to outline training objectives for defending against CogWar on social media, systematic scenario development may assist [39].

To ensure the full potential of the training opportunities enabled by social media simulation in a military exercise, there is a need to prioritise resources to this new way of doing media-play. The Somulator staff did report that adding the Somulator to the exercise was a more resource exhaustive approach than previous ways of simulating the information environment, especially for content creation. Indeed, it represents a different way of doing media-play, precisely because the information environment has changed with the emergence of social media. Notwithstanding the need for more resources than before, both the exercise leader and the Somulator staff leader agreed that, in a cost-benefit analysis, the benefits of simulating social media outweighed the costs. Simulating the 21st century information environment requires resources both in the planning cycle and execution of the exercise. This includes content creation ahead of the exercise and requires expert knowledge in the production of content, to ensure that it accurately mirrors adversary modus operandi based on state-of-the-art knowledge. AI tools can assist in such, but need to be critically assessed to ensure that content used for training is as close to reality as possible, and not based on biased assumptions built into the software. Investing in social media simulation (and indeed other types of training to mitigate and respond to CogWar) will ensure a better preparedness for handling the battlefields of cognition.

6.0 CONCLUSION

This paper has examined the training opportunities that including a social media simulator into an exercise in the Norwegian Armed Forces enabled. Through evaluating the first-time use of the Somulator, a social media simulator developed by FFI, four main areas of training that can enhance the response to and mitigation of CogWar using social media simulation were identified:

1) The Somulator added more layers of complexity and information about the operational environment to the exercise, compared to previous media-play. This enables training to improve and maintain Situational Awareness (SA), which is vulnerable to adversarial attacks in CogWar.
2) It created a feedback mechanism that can simulate the effects of decision-making and strategic communication. This offers a more interactive and realistic way to train on strategic communication.
3) It enabled a simulation of adversarial potential modus operandi in the information environment, for instance in the form of disinformation. This offers possibilities to train on mitigating and responding to their effects.
4) It created a pluralistic information environment in which the students had to assess the credibility of various pieces of information. This can build competencies that strengthen the resilience against disinformation or other cognitive attacks on social media.

Our data shows that to enhance these situations, there is a need to define the target audience in an exercise, provide resources for content creation, include the social media simulator into the planning cycle of the exercise, and develop concrete training objectives for social media which can be evaluated and enhanced as CogWar in social media develops. Investing in social media simulation for military training ensures a better preparedness for handling the battlefields of cognition and provides a better environment for training to mitigate and respond to CogWar.

7.0 REFERENCES

[1] Masakowski, Y & Grendahl Sivertsen, E (2022). Defence Against 21st Century Cognitive Warfare: Considerations and Implications of Emerging and Advanced Technologies, in Mitigating and Responding to Cognitive Warfare. NATO STO Technical Report HFM-ET-356. AC/323(HFM-356)TP/1120

[2] Claverie, B., & Du Cluzel, F. (2022). “Cognitive Warfare”: The Advent of the Concept of “Cognitics” in the Field of Warfare. FM 356

[3] NATO (2022). NATO Allied Command Transformation (ACT): Cognitive Warfare Exploratory Concept Draft, Version: December 2022: 1-48. Svetoka (2016)

[4] Blatny, J and Masakowski, Y (2022). Mitigating and Responding to Cognitive Warfare. NATO STO Technical Report HFM-ET-356. AC/323(HFM-356)TP/1120

[5] Svetoka, S. (2016). Social media as a tool of hybrid warfare. NATO Strategic Communications Centre of Excellence.

[6] Nissen, T. E. (2015). The Weaponization Of Social Media: Characteristics of Contemporary Conflicts. Royal Danish Defence College.

[7] Golovchenko, Y., Buntain, C., Eady, G., Brown, M. A., & Tucker, J. A. (2020). Cross-platform state propaganda: Russian trolls on twitter and YouTube during the 2016 US Presidential Election. The International Journal of Press/Politics, 25(3), 357-389.

[8] Bastos, M., & Farkas, J. (2019). "Donald Trump is my President!": the internet research agency propaganda machine. Social Media+ Society, 5(3), 2056305119865466.

[9] Nimmo, B. (2022). Removing coordinated inauthentic behavior from China and Russia. Meta report: https://about.fb.com/news/2022/09/removing-coordinated-inauthentic-behavior-from-china-and-russia/

[10] Nissen, T. E. (2015). The Weaponization Of Social Media: Characteristics of Contemporary Conflicts. Royal Danish Defence College, p. 58.

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

[12] Bay, S., Biteniece, N., Bertolin, G., Christie, E. H., Dek, A., Fredheim, R. E., ... & Marchenko, T. (2019). The Current Digital Arena and its Risks to Serving Military Personnel. NATO STRATCOM COE, 7-18.

[13] Masakowski, Y & Grendahl Sivertsen, E (2022) Defence Against 21st Century Cognitive Warfare: Considerations and Implications of Emerging and Advanced Technologies, in Mitigating and Responding to Cognitive Warfare, HFM 356 Exploratory Team Report.

[14] Nissen, T. E. (2015). The Weaponization Of Social Media: Characteristics of Contemporary Conflicts. Royal Danish Defence College.

[15] NATO's Warfighting Capstone Concept: anticipating the changing character of war, Admiral John W. Tammen 09 July 2021.

[16] Hancock, P. A., Vincenzi, D. A., Wise, J. A., & Mouloua, M. (Eds.). (2008). Human factors in simulation and training. CRC Press.

[17] Blatny, J and Masakowski, Y (2022). Mitigating and Responding to Cognitive Warfare. NATO STO Technical Report HFM-ET-356. AC/323(HFM-356) TP/1120.

[18] Tomlin, G.M. (2016). #SocialMediaMatters: Lessons Learned from Exercise Trident Juncture. Joint Force Quarterly.

[19] Bergh, A (2022) SOMULATOR: Developing CogWar Resilience Through Social Media Training, in Mitigating and responding to Cognitive Warfare, NATO STO Technical Report HFM-ET-356. AC/323(HFM-356)TP/1120.

[20] Sønsthagen, M (2023) Comprehensive Shield er i gang, https://www.forsvaret.no/aktuelt-og-presse/aktuelt/comprehensive-shield-er-i-gang

[21] Stebbins, R. A. (2001). Exploratory research in the social sciences (Vol. 48). Sage.

[22] Kirkpatrick, D.L. (1987). Evaluation. In R.L. Craig (Ed.), Training and development handbook (Third Edition). New York, NY: McGraw-Hill, 301–319.

[23] Fletcher, J. D., & Chatelier, P. R. (2000). An overview of military training. Institute for Defense Analyses.

[24] Koerteling, H (2022) Education and Training for Cognitive Warfare, in Mitigating and responding to Cognitive Warfare, NATO STO Technical Report HFM- ET-356. AC/323(HFM-356)TP/1120.

[25] Blatny, J and Masakowski, Y (2022). Mitigating and Responding to Cognitive Warfare. NATO STO Technical Report HFM-ET-356. AC/323(HFM-356)TP/1120.

[26] Brinkmann, S. (2014). Unstructured and semi-structured interviewing. The Oxford handbook of qualitative research, 2, 277-299.

[27] Clarke, V., Braun, V., & Hayfield, N. (2015). Thematic analysis. Qualitative psychology: A practical guide to research methods, 3, 222-248.

[28] Claverie, B., & Du Cluzel, F. (2022). "Cognitive Warfare": The Advent of the Concept of "Cognitics" in the Field of Warfare. FM 356.

[29] Blatny, J and Masakowski, Y (2022). Mitigating and Responding to Cognitive Warfare. NATO STO Technical Report HFM-ET-356. AC/323(HFM-356)TP/1120.

[30] NATO (2022). NATO Allied Command Transformation (ACT): Cognitive Warfare Exploratory Concept Draft, Version: December 2022: 1-48. Svetoka (2016).

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

[32] Knox, B & Masakowski, Y (2022) Situational Awareness, Sensemaking and Future NATO Multinational Operations, in Mitigating and Responding to Cognitive Warfare. NATO STO Technical Report HFM-ET-356. AC/323(HFM-356)TP/1120.

[33] Bay, S., Biteniece, N., Bertolin, G., Christie, E. H., Dek, A., Fredheim, R. E., ... & Marchenko, T. (2019). The Current Digital Arena and its Risks to Serving Military Personnel. NATO STRATCOM COE, 7-18.

[34] Blatny, J and Masakowski, Y (2022). Mitigating and Responding to Cognitive Warfare. NATO STO Technical Report HFM-ET-356. AC/323(HFM-356)TP/1120.

[35] Koerteling, H (2022) Education and Training for Cognitive Warfare, in Mitigating and responding to Cognitive Warfare, NATO STO Technical Report HFM- ET-356. AC/323(HFM-356)TP/1120.

[36] Kirkpatrick, D.L. (1987). Evaluation. In R.L. Craig (Ed.), Training and development handbook (Third Edition). New York, NY: McGraw-Hill, 301–319.

[37] Nissen, T. E. (2015). The Weaponization Of Social Media: Characteristics of Contemporary Conflicts. Royal Danish Defence College.

[38] Bay, S., Biteniece, N., Bertolin, G., Christie, E. H., Dek, A., Fredheim, R. E., ... & Marchenko, T. (2019). The Current Digital Arena and its Risks to Serving Military Personnel. NATO STRATCOM COE, 7-18.

[39] Bjørgul, L., Sivertsen, E. G., & Sellevåg, S. R. (2022). Scenarioer for uønsket påvirkning i forbindelse med norske valg.