TALLINN UNIVERSITY OF TECHNOLOGY
School of Information Technologies

Crystella Sokk 232647IVGM

Disinformation as a Scenario Element in Cyber Exercises

Master's thesis

Supervisor: Kaido Kikkas

Tallinn 2025

TALLINNA TEHNIKAÜLIKOOL
Infotehnoloogia teaduskond

Crystella Sokk 232647IVGM

Desinformatsioon küberõppuste stsenaariumielemendina

Magistritöö

Juhendaja: Kaido Kikkas

Tallinn 2025

Author’s declaration of originality

I hereby certify that I am the sole author of this thesis. All the used materials, references to the literature and the work of others have been referred to. This thesis has not been presented for examination anywhere else.

Author: Crystella Sokk

12.05.2025

Abstract

This master's thesis examines the use of disinformation as a scenario element in cyber exercises, focusing primarily on the experience from large-scale exercises. The research is based on a literature review and expert interviews, with the aim of understanding how disinformation is understood, implemented and perceived in the context of technically focused cyber exercises. The results of the study show that although disinformation is increasingly included through strategic communication and media simulations, its impact on exercises remains modest. The main reason is its weak connection to the evaluation systems and substantive objectives of the exercises. It also revealed shortcomings in cooperation between technical and communication strands - especially where cognitive threats are treated as an extraneous addition. The work also points out the possibilities of how disinformation can be adapted to smaller exercises. The analysis supports the understanding of cyber exercises as socio-technical systems and emphasizes that cognitive and narrative threats should not be mere decorative additions, but a central part of the exercise. In order for exercises to better reflect the reality of hybrid threats, the paper recommends the conscious and systematic integration of disinformation into scenario design, assessment models, and inter-role cooperation.

This thesis is written in English and is 62 pages long, including seven chapters, two figures and four tables.

Keywords: cybersecurity, cyber exercise, disinformation, strategic communication, hybrid threat

Annotatsioon

Desinformatsioon küberõppuste stsenaariumielemendina

Antud magistritöö uurib desinformatsiooni kasutamist küberkaitseõppuste stsenaariumielemendina, keskendudes eelkõige kogemustele suurõppustelt. Uurimistöö tugineb kirjanduse analüüsile ja ekspertintervjuudele, eesmärgiga mõista, kuidas desinformatsiooni mõistetakse, rakendatakse ja tajutakse tehnilise fookusega küberõppuste kontekstis. Uuringu tulemused näitavad, et kuigi desinformatsiooni kaasatakse üha enam strateegilise kommunikatsiooni ja meediasimulatsioonide kaudu, jääb selle mõju õppustel tagasihoidlikuks. Peamiseks põhjuseks on selle nõrk seotus hindamissüsteemide ja õppuste sisuliste eesmärkidega. Samuti ilmnesid puudujäägid koostöös tehniliste ja kommunikatsioonisuundade vahel – eriti seal, kus kognitiivseid ohte käsitletakse kõrvalise lisana. Töö toob esile ka võimalused, kuidas desinformatsiooni saab kohandada väiksematele õppustele. Analüüs toetab arusaama küberõppustest kui sotsio-tehnilistest süsteemidest ning rõhutab, et kognitiivsed ja narratiivsed ohud ei tohiks olla pelgalt dekoratiivsed lisandid, vaid õppuse keskne osa. Selleks, et õppused peegeldaksid paremini hübriidohtude tegelikkust, soovitab töö desinformatsiooni teadlikku ja süsteemset lõimimist stsenaariumi ülesehitusse, hindamismudelitesse ja rollidevahelisse koostöösse.

Lõputöö on kirjutatud inglise keeles ning sisaldab teksti 62 leheküljel, seitset peatükki, kahte joonist ja nelja tabelit.

Märksõnad: küberkaitse, küberõppus, desinformatsioon, strateegiline kommunikatsioon, hübriidoht

List of abbreviations and terms

BT	Blue Team
CCDCOE	Cooperative Cyber Defence Centre of Excellence
CERT	Computer Emergency Response Team
CIB	Coordinated Inauthentic Behavior
CNI	Critical National Infrastructure
COE	Centre of Excellence
DFIR	Digital Forensics and Incident Response
ENISA	European Union Agency for Cybersecurity
Expo	Exercise platform for technical status update and scoring
GT	Green Team
IO	Information Operations
NATO	North Atlantic Treaty Organisation
OLEx	Operational-Level Exercise
RT	Red Team
SLEx	Strategic-Level Exercise
SNT	Strategic Narrative Theory
StratCom	Strategic Communications
TLEx	Technical-Level Exercise
WT	White Team
YT	Yellow Team

Table of contents

1 Introduction 11
1.1 Problem statement 12
1.2 Motivation for the study 13
1.3 Research questions 13
1.4 Value and contribution 14
1.5 Thesis outline 14
2 Literature review 16
2.1 Cognitive security and resilience 16
2.2 Strategic communications in cybersecurity 18
2.3 Cyber exercises and integration of cognitive threats 18
2.4 Disinformation, information operations and hybrid threats 20
2.5 Disinformation tactics in cyber operations 21
2.6 Disinformation in cyber exercises 23
2.7 Research gaps 24
3 Theoretical framework 26
3.1 Strategic Narrative Theory 26
3.2 Cognitive security and epistemic vigilance 27
3.3 Cognitive resilience in adversarial information environments 28
4 Methodology 30
4.1 Research design 30
4.2 Data collection 31
4.3 Sampling strategy and interviews 32
4.4 Limitations 34
4.5 Data analysis 35
5 Research results 36
5.1 Importance of disinformation in cyber exercises 36
5.2 Integration with technical tracks 37
5.3 Content design: scripted vs reactive injects 38
5.4 Participant engagement and scoring 39

5.5 Exercise scale and coordination challenges 40
5.6 Strategic communication as a learning objective 41
5.7 Lessons for smaller-scale exercises 42
5.8 Key findings and implications 44
6 Discussion 46
6.1 Integration and purpose of disinformation tracks 46
6.2 Operational constraints and trade-offs in exercise design 47
6.3 Implications for smaller-scale exercises 49
6.4 Theoretical reflection and framework alignment 50
6.5 Key insights with recommendations 51
6.6 Future work 52
7 Conclusion 54
References 56
Appendix 1 - Non-exclusive licence for reproduction and publication of a graduation thesis 60
Appendix 2 - Interview questions 61

List of figures

Figure 1. Theoretical framework dual lens breakdown 29
Figure 2. Overview of the research process 31

List of tables

Table 1. Differences between misinformation, disinformation and malinformation 20
Table 2. Linking strategic narrative theory concepts to disinformation tactics in cyber exercises..... 27
Table 3. An overview of the interview participants 33
Table 4. Key dimensions of disinformation integration in cyber exercises 44

1 Introduction

Over time cybersecurity exercises have evolved from traditional technical simulations into also mirroring the complexity of modern world digital threats. As cyberattacks become more embedded within information warfare along with psychological operations, training simulations now include such hybrid reality (ENISA, 2023). One of the most significant additions to this development has been the inclusion of disinformation as a scenario element (NATO ACT, 2024). These imitate information campaigns that distort different narratives in the public domain, exploit information gaps, and emphasize decision-making under uncertainty (Pantazi et al., 2021).

Exercises like Locked Shields by CCDCOE and NATO organisations have had an assortment of disinformation injects ranging from deepfakes to applying media pressure (CCDCOE, 2022; NATO StratCom COE, 2024). The injections present the contemporary crisis scenario where attacks are not only launched in technical networks but also on information environments that are vital for public trust (NATO StratCom COE, 2024).

These cognitive and narrative threats are truly growing challenges for government organisations which run critical digital services, such as e-government technologies and services (Wirtz & Weyerer, 2016). Disinformation during crises can mislead public perception of service dependability or break confidence in digital governance, even if the technical systems remain secure (Schünemann, 2022).

Cyber exercises now not only aim to test technical capabilities of the participating teams but also to toughen coordination and mental preparedness against attacks that aim to destroy trust (Knox, Lugo, & Sütterlin, 2019). That raises a question: does adding disinformation to exercises sharpen participating teams' overall preparedness and realism, or does it make focus on technical training more complicated and surrounds participants with ambiguity?

Some of the texts from the author's essays and research proposal in the "E-Governance Technologies and Services Master's Project" (ITE4310) and "Research Methods"

(ITE4260) courses have been used in this thesis because the author has been associated with the topic of this research throughout her master's studies. Also, limited use of ChatGPT-4o (OpenAI, 2025) primarily to improve phrasing and language clarity, with all outputs carefully revised by the author to ensure academic integrity.

1.1 Problem statement

With the increased inclusion of disinformation injection into cyber training, little is known about how such fragments affect technology-oriented participant teams learning goals. Information operations and narrative warfare scholarship are well established in political and military environments (Wardle & Derakhshan, 2017), whereas detailed review of disinformation as a designed scenario feature within cyber training protocols remains limited, especially concerning technical team exposure.

Exercises like Locked Shields (CCDCOE, 2022) demonstrate how the addition of disinformation injects can make it more realistic without drowning technological objectives (NATO StratCom COE, 2024). Yet as cyber exercises become increasingly fine-tuned to smaller organisations and more technically challenging scenarios, then the question becomes: how are cognitive threats brought in without producing confusion of role, decision exhaustion, or diluting technical capability?

In this thesis, smaller-scale exercises refer to cyber simulations conducted by individual organisations or agencies with limited resources, personnel, or scenario scope. These are typically focused more on a single sector or technical goal. An understanding of this balance is necessary in order to appropriately insert scenario-based information pressure into exercises of different sizes, especially for groups tasked with managing core services such as e-government infrastructures (Maennel et al., 2023).

Therefore, the controversy is not about whether disinformation scenarios must be part of cyber exercises, but how to balance cognitive injects with technical transparency and role play by exercisers. Although large exercises such as Locked Shields attempt to merge cognitive and technical challenges, it is questionable whether total integration always produces better training outcomes (Maennel et al., 2017). In addition, smaller exercises are usually under stricter resource limitations and lower training objectives, which create

the distinction between technical and cognitive elements - even though in actual crises, these elements are necessarily combined.

1.2 Motivation for the study

The motivation for the thesis comes from the work experience of the author in cyber training related organisations providing the technical environments of international cyber exercises. From professional experience, it was assumed that exercises on a larger scale appear to be successful in incorporating StratCom and disinformation scenario elements, whereas smaller and more technical oriented exercises are struggling with incorporating these cognitive threats. This resulted in growing interest in how disinformation narratives affect cyber training and whether such elements could be integrated even better.

In addition to work experience, the education within the master's programme in e-Governance Technologies and Services also increased the interest of the author in cyber defence integration and information management. Active participation in exercises, including collaboration with experts from the NATO Strategic Communications Centre of Excellence (StratCom COE), further strengthened the motivation to develop knowledge in these hybrid threat tracks of cyber training.

The research seeks to merge theoretical knowledge, experience, and cognitive security insights based on organisers and participants knowledge and experience. In an effort to eventually be able to help in developing stronger cyber security trainings and exercises.

1.3 Research questions

This thesis analyses the design, implementation, and perceived impact of disinformation as a scenario element in cyber security exercises. Also, their impact on the cognitive threat influence on technical training simplicity, role coordination, and performance of participants. Thesis is meant to also find out about the transferability of cognitive exercise tracks from large scale exercises to smaller scale exercises.

This thesis will answer the following research questions:

- RQ1: Why are cognitive threat elements being incorporated into cyber exercise scenarios?

- RQ2: How are disinformation elements developed and implemented within different exercise tracks?

- RQ3: What are the challenges in balancing technical learning objectives with cognitive injects, especially in highly technical or small exercises?

- RQ4: Which are best practices that inform better incorporation of disinformation injects without undermining essential learning goals?

- RQ5: How may successful strategies from large exercises be scaled down to smaller-scale or organisation-specific cyber exercises?

1.4 Value and contribution

This study provides practice-based knowledge on the evolving design of cyber exercises to imitate some hybrid threats. It directly contributes to operational planning for different organisations such as CCDCOE, ENISA, NATO StratCom COE, national CERT teams and cyber exercise companies which support critical infrastructure and digital public services.

Rather than recommending a specific technical tool or methodology, this thesis offers experience-based guidance for integrating disinformation scenario elements while maintaining technical clarity. For organisations tasked with securing e-government environments, where continuity and public trust are essential, then such specificity is increasingly critical (ENISA, 2023).

1.5 Thesis outline

There are seven chapters in total in this master's thesis. Introduction gives a short overview of the topic, states the problem, explains motivation behind the study, introduces research questions and possible value. It is then followed by the second chapter, which is the literature review that also defines some conceptual terms like disinformation, cognitive security, and cyber exercise scenario design. Third chapter discusses the theoretical framework where the author outlines the key concepts and theories that underpin this research. Chapter four presents methodology, explaining the data collection procedures and research design part. Empirical findings based on

document triangulation and interviews with technical and strategic communication stream participants are shown in the fifth chapter. Chapter six offers an explanation of the findings in relation to the current literature and formulates design guidelines for the introduction of disinformation as a scenario content into exercises. The final chapter summarises the thesis by encapsulating responses to the research questions and hypothesising potential areas for further research.

This thesis applies a qualitative exploratory research design. It includes semi-structured interviews with exercise planners, technical participants, and StratCom/media cell planners along with document analysis of playbooks and after-action reports. The analysis follows thematic analysis methodology (Braun & Clarke, 2006) to uncover recurrent tensions, value perceptions, and key learning lessons.

2 Literature review

Cybersecurity training has evolved beyond just technicalities to increasingly address cognitive challenges as well, such as disinformation and strategic manipulation (NATO StratCom COE, 2024). In the modern hybrid threat environment, cyber incidents rarely affect only infrastructure, these also over time have started to simultaneously target public trust, decision-making processes, and narrative control (Steingartner, Galinec, & Kozina, 2021). Understanding how disinformation tracks are constructed, deployed, and experienced is therefore needed to strengthen technical and cognitive resilience among participating teams. This literature review explores the theoretical and practical background necessary to situate the role of disinformation in cyber exercises, drawing from different sources.

The chapter is organised into several thematic sections beginning with a broad overview and gradually narrowing towards the specific topic of disinformation in cyber exercises. It starts by introducing the concept of cognitive security and resilience, followed by an examination of strategic communication in cybersecurity contexts. This chapter then explores how cyber exercises have begun to incorporate cognitive threats, before turning to the foundations of disinformation, including its definitions, tactics, and role in hybrid operations. The final sections address specific methods of disinformation in cyber operations and conclude with an analysis of how such elements are integrated into modern cyber exercises. Ends with defined research gaps based on the found literature.

2.1 Cognitive security and resilience

Cybersecurity field now sees more and more cognitive security as part of its core, just like the security of digital infrastructure (Andrade & Yoo, 2019). Defending human decision-making from misdirection, manipulation, and information overload (Buzzell, 2024). Cognitive security tries to defend individuals and groups from efforts by opposing actors to change beliefs by using damaging information (Pierce, 2021).

Cognitive threats exploit vulnerabilities not in hardware but in human psychology: trust, biases, emotional responses, and information processing habits (Kirdemir, 2019). In the context of hybrid warfare, securing the cognitive domain is seen as essential, as adversaries deploy disinformation and influence tactics to weaken societal resilience without necessarily breaking physical infrastructure (Wells, 2017).

This is supported by cognitive resilience that prioritises the capacity of an individual or an organisation to exercise critical thinking and scepticism in the face of cognitive manipulation (Fazey, 2010). Cognitive resilience is developed through the cultivation of vigilance - cognitive mechanisms which human beings employ to determine the trust value of information (Sperber et al., 2010).

Research points out that increased cognitive load and information overload decrease epistemic vigilance and because of that people are more prone to accepting lies (Pantazi et al., 2021). For instance, in time pressure during crisis simulation, decision-makers use intuitive heuristics instead of cautious thinking and so the potential to accept disinformation is heightened (Pantazi et al., 2021). Plus, strengthening cognitive resilience includes training participants to critically assess incoming information, resist emotional manipulation, manage attention, and maintain scepticism even in stressful environment (Pantazi et al., 2021). In the cyber exercise context, these skills are also increasingly vital because technical defenders must also operate in an information environment which is shaped by these disinformation injects and media manipulation.

Effective cognitive security training may include teaching media literacy and training against simulated cyber crises involving controlled disinformation campaigns (Dame Adjin-Tettey, 2022). Such interventions aim to increase the users sensitivity to recognising efforts at manipulation at an early stage and having sound operational judgment when encountering conflicting or fake inputs (Kont, Elving, Broersma et al., 2024).

Overall, defense against cognitive attacks involves both systemic capabilities - monitoring content and verification in media, and also individual abilities like critical thinking and awareness of strategic communication. Training defense teams to face contemporary threats therefore needs attention to both technical and cognitive aspects.

2.2 Strategic communications in cybersecurity

As cognitive complexity increases then states and organisations have developed strategic communications capabilities to defend their information spaces (Nicholson, 2012). Strategic communication coordinates public messaging, media outreach, and narrative development to counter adversary influence activities (Heap, Hansen, & Gill, 2021).

Strategic narratives are stories narrativized for which the events unfold and public attitudes are shaped (Schmitt, 2018). The operators try to legitimise their actions and delegitimise their competitors via narration of conflicts or crises (Heap, Hansen, & Gill, 2021). Institutions of NATO, as well as the EU, increasingly understand that communication is a battlefield territory, viewing influence operations as a national defense threat (NATO, 2020).

During cyber exercises such as Locked Shields, StratCom personnel mimic actual world media situations (NATO Allied Command Transformation, 2024). These are mainly offering disinformation injects, monitoring public opinion assignments, and exposing participants to unexpected information attack tests (NATO Allied Command Transformation, 2024). Strategic communications, in the context of this thesis, implies active defense against cognitive threats by establishing and maintaining information space in these cyber defense environments.

2.3 Cyber exercises and integration of cognitive threats

Recent years have witnessed cyber exercise developers incorporate information warfare topics into scenarios. This is a reflection of the realisation that real cyber crises in the real world tend to entail concurrent battles in the information space. Attackers can now employ false news reports alongside technical attacks, so some training now have both the technical and cognitive aspects of security incidents (ENISA, 2018).

Some cybersecurity exercises have evolved from being strictly technical drills towards complex simulations involving strategic, operational, and cognitive evaluation (Skopik & Leitner, 2021). In the past, these mainly only concentrated on testing technical resiliency - the speed and ways of which participants could identify, isolate, and recover from a cyber attack. However, realising that the new dimension of information operations in

contemporary wars, some of the larger exercises these days include disinformation topics and cognitive tests in their design in order to better represent hybrid attacks (ENISA, 2018; CCDCOE, 2022).

Cyber exercise participants are generally organised into teams within a color-coded structure. Blue Team (BT) defends systems and reacts to incidents, and the Red Team (RT) plays the role of the adversary and performs simulated intrusions and disruptions (Seker & Ozbenli, 2019). White (WT) and Yellow Team (YT) are responsible for scenario management, tracks performance, and manages exercise flow, e.g., injects events to challenge participants (Seker & Ozbenli, 2019). Green Team (GT) takes care of the technical infrastructure and ensures the simulated environment and networks run smoothly (Seker & Ozbenli, 2019). More and more, exercises also include a dedicated StratCom or Media Cell (sometimes integrated into the WT, or separately), whose task is to mimic external communications environments, manage media coverage, and incorporate disinformation (CCDCOE, 2022).

The scope of cyber exercise goals has increased proportionally. Beyond the development of technical competencies, they now seek to legitimise crisis management procedures, conduct communication planning exercises, and develop decision-making in stress and uncertainty (Karpiuk, 2017). For example, exercise like Locked Shields requires BTs to not just defend their networks but also address scripted news articles, social media rumors, and pressurised media questions when simulating persistent technical incidents (NATO Allied Command Transformation, 2024). This two-layered problem illustrates the need for overall cognitive and operational resiliency.

Cyber exercises differ in terms of focus level. Technical-level exercises (TLEx) are hands-on exercises like malware analysis, vulnerability management, and real-time network defense (Gavrila, Ogée, Trimintzios et al., 2015). Operational-level exercises (OLEx) prepare participants to coordinate incidents, share information, and manage crises processes (Gavrila et al., 2015). Strategic-level exercises (SLEx) model senior leadership decision-making, public communication, and policy response in crises (Gavrila et al., 2015). Some exercises of a more holistic nature, such as Cyber Europe 2018, trying to involve all three levels by combining technical containment activities with public communication challenges, linking tactical action with strategic thought (ENISA, 2018).

The addition of cognitive threats to cyber exercises is catalysed by an awareness that attacks today are not just on systems but on public trust, decision-making, and institutional credibility (NATO ACT, 2021). Present-day cyber exercises now simulate real scenarios where communities have to deal with cyber attacks and misinformation. Examples include false reporting of attacks against some communities, arranged breach incidents implying insider attacks, deepfakes aimed at frightening the public, and coordinated social media to disseminate misinformation in order to erode trust.

Handling such conditions demands actors to rapidly verify accepted information, reconcile internal and external communications, respond against misinformation, and maintain the trust of stakeholders. All this under intense time pressure and without much situational context. Cyber war nowadays happens at the same time both in the "network and narrative domains," therefore, the defense must succeed both. (Veksler et al., 2018) Introducing cognitive challenge into cyber drills adds realism, encourages thoughtful action, and constructs resilience against hybrid threats, but also creates tension.

2.4 Disinformation, information operations and hybrid threats

In cybersecurity and information security studies, the differences between malinformation, disinformation, and misinformation are clearly defined. Misinformation is false information spread without the purpose of deception, like spreading a false rumor out of ignorance (Princeton Public Library, n.d.). Disinformation is intentionally false information spread with the aim of doing harm (Princeton Public Library, n.d.). Malinformation is accurate information spread in a damaging manner, like leaking classified papers to harm a public figure (Princeton Public Library, n.d.). Table 1 below brings out the differences between these three.

Table 1. Differences between misinformation, disinformation and malinformation

Type	**Truthfulness**	**Intent to harm**	**Key characteristic**	**Example**
Misinformation	False	No	Shared unknowingly, perceived as true	A user sharing an incorrect health tip on social media

Disinformation	False	Yes	Deliberately created or spread to deceive	Created news article to influence elections
Malinformation	True	Yes	Truthful information shared with malicious intent	Leaking private emails with want to damage a public figure's reputation

Disinformation is the focal point of information operations (IO) (Murphy, 2024). Information operations are coordinated efforts against information channels to disrupt and affect opponents decision-making process (Pierce, 2021). Hybrid war tactics use information operations as a blend of cyberattacks, propaganda, and psychological operations to destabilise opponents (NATO, 2024). For example, Russian invasion of Ukraine in 2014 both incorporated military actions and massive campaigns of disinformation (Bilal, 2021). This policy has been pursued and amplified in the current conflict. Russia actively used information operations to discredit Ukraine, using disinformation to legitimise military intervention and conceal its planning activities (Atlantic Council, 2024). Disinformation has therefore become a central tool of cognitive warfare, seeking to break confidence and disable decision-making ability (Reding & Wells, 2022).

2.5 Disinformation tactics in cyber operations

Disinformation campaigns utilise different techniques for the production and distribution, of disinformation (Morgan, 2018). They are usually deployed together with tech attacks in cyberspace to undermine trust, increase uncertainty, or sway people's opinions whenever there are crisis situations (Sultan, 2019). Knowledge of such tactics is required so that cyber exercises can be properly designed so as to appropriately simulate defenders cognitive threats.

Deepfakes are very realistic created videos, images, or audio recordings made with the technique of deep learning (Tammekänd, Thomas, & Peterson, 2020). These are even able to generate realistic visual proofs of statements or incidents that didn't happen and, as a result, will lead to disbelieving the audio-visual media (Tammekänd et al., 2020). For

example, during a conflict the political figures can make inciting remarks that could cause public unrest or loss of credibility of crisis leaders. Vaccari and Chadwick (2020) observe that small-scale deployment of deepfakes can cause disproportionate disturbance by taking advantage of the inherent trust individuals place in visual data.

Robot automated scripts where computer codes are programmed to mimic human activity online are broadly used to spread disinformation (Bessi & Ferrara, 2016). Network bots can post synchronised posts as a way of creating the illusion of genuineness for social media handles (Bessi & Ferrara, 2016). These leverage psychological heuristics like the "illusory truth effect," where repeated presentations of information boost subjective truthfulness (Udry & Barber, 2024). Bot amplification strategy was greatly noted in critical influence campaigns like the ones that occurred close to the United States election in 2016 (Bessi & Ferrara, 2016).

Coordinated Inauthentic Behavior (CIB) refers to organised activities by groups of imitative accounts or pages to deceive audiences regarding their identity and intention (Murero, 2023). Social media platforms define CIB as coordinating more than one asset to artificially amplify stories and overwhelm public debate (Murero, 2023). CIB hides its organised activities by labeling them as people's spontaneous movements or people's ordinary opinions.

Besides technical strategy, disinformation is typically implanted within larger strategic narratives - coherent stories that are built to frame how audiences consider past, present, and future events. For instance, during war, strategic narratives can present enemy states as illegitimate, situating any future action within an ideologically embedded context. (Miskimmon, O'Loughlin & Roselle, 2018).

Larger cyber exercises now not only simulate technological intrusions, but also disinformation operations a criminal would conduct to disrupt cognitive spaces. Exercises such as Locked Shields (CCDCOE, 2022), Cyber Europe (ENISA, 2018), and Cyber Coalition (NATO ACT, 2021) now include media injects, disinformation narratives, and public messaging challenges in a bid to better model the hybrid nature of cyber crises of our era. Invented news reporting and designed disinformation in drills test situational awareness, critical thinking, and public communication in manipulated information environments (ENISA, 2018). Their recognition and opposition now constitute a critical

component of cognitive resilience training, merging technical defense with strategic communication skills in cybersecurity education (ENISA, 2018; CCDCOE, 2022).

2.6 Disinformation in cyber exercises

There is plenty of literature on cognitive security, disinformation, and cyber exercises. Yet, how these are interconnected, particularly from the point of view of participants perceptions during exercises, has not been examined enough. In other words, we know a lot about what disinformation tactics exist and how exercises are run, but we know far less about how participants process and respond to disinformation within exercises, and how that training translates to real-world readiness.

As the understanding of hybrid threats has matured, major cyber exercises have increasingly incorporated disinformation scenarios to simulate the full spectrum of modern crises (CCDCOE, 2022). Recognising that cyber incidents are rarely limited to technical failures, exercise designers now frequently integrate media manipulation, narrative disruption, and public trust erosion challenges alongside traditional network attacks (ENISA, 2018).

One great example again is Locked Shields, organised annually by the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE). Originally focused purely on network defense, the exercise has evolved to include strategic communications challenges. Defending teams are currently expected to handle not only technical crises but also orchestrated disinformation campaigns on the social media platforms, where they have to ensure not only service availability but also trust among people (CCDCOE, 2022). Likewise, ENISA Cyber Europe exercises have placed cognitive threats within technical crisis scenarios. Cyber Europe 2018, for example, brought together mass technical disruptions and manipulated media narratives, requiring collective technical and communicative action at the industry and national level (ENISA, 2018). Cyber Coalition exercise has also incorporated information warfare dimensions through media cell, focusing on cross-national cooperation in order to share correct information and counter adversary influence operations (NATO ACT, 2021). These examples demonstrate a trend that disinformation is no longer addressed as a secondary objective but integrated as a central training objective.

The addition of disinformation simulations increases the validity of exercises via the recreation of the disorienting and media perplexity that in most instances have followed cyber crises in the external environment, i.e., the NotPetya attack (2017) in Ukraine and the SolarWinds hack (2020) (Beyond Identity, 2021). An education of exercisers in responding to disinformation improves critical analysis, situational awareness, and synchronisation of technical, legal, and communications pathways (ENISA, 2018). Effective engagement builds the communications preparedness of an organisation, testing vulnerabilities less likely to surface in technical only training (ENISA, 2018).

2.7 Research gaps

This review has confirmed the rise in sophistication in disinformation tactics, the growth of cognition-oriented security thought, and the enhanced incorporation of information operations into cyber defense education. But some research and practice gaps still exist.

Firstly, while exercises like Locked Shields, Cyber Europe, and Cyber Coalition illustrate the injection of disinformation into crisis simulation, participant-centred cognitive analysis is not typical. Post-event analysis and assessment mainly focuses on technical results like system availability or the rate of attack detection - instead of how participants experience and learn from disinformation injects during stressful conditions.

Secondly, there is no standardised measuring system for cognitive performance. Efficiency measurement criteria of incident response are set but regularised systems of measuring cognition resilience, situation awareness, and narrative control in the context of disinformation operations are not there (Silva et al., 2014; ENISA, 2018). Due to the absence of any standardised frameworks being set, it is difficult to benchmark or boost the capability of the participants against hybrid threats.

Thirdly, empirical evidence on the training value of disinformation scenarios is limited. While exercise designers increasingly believe that simulation of cognitive threats improves readiness, few researches investigate systematically whether trainees who train on media injects are improved performers in actual events or follow-on exercises. Such feedback that exists is qualitative in nature.

Lastly, the majority of the research and exercise design nowadays is directed at huge, national-scale exercises. Less has been done in applying cognitive threat components to

scale to technical exercises of smaller size, corporate training exercises, or industry-based simulations. It is a need to learn how to scale and translate cognitive threats correspondingly for various environments.

This thesis seeks to fill these gaps by critically analysing how disinformation components are crafted, executed, and understood in cyber exercises, specifically with regard to balancing cognitive complexity and technical learning clarity. Along the way, it adds practice-based knowledge to the use of cognitive threats in cybersecurity training.

Most documented disinformation training exercises take place in large-scale national or international exercises with government agencies, military groups, or critical infrastructure sectors. Smaller-scale technical exercises, especially in private sector firms or SMEs, hardly comprise cognitive threat elements. This leaves organisations, which are still at risk of hybrid attacks, with an unacceptably low readiness level. Exploring how cognitive elements might be reallocated to smaller or technical-hypervigilant exercises, without overloading participants, is a needed research area and exercise design innovation for the future (ENISA, 2018).

3 Theoretical framework

This thesis is composed with two related theoretical models: Strategic Narrative Theory and the concepts of Cognitive Security and Cognitive Resilience. Together, these two offer a dual lens through which to examine how disinformation serves both as strategic tool and cognitive disruptor in cyber exercises.

3.1 Strategic Narrative Theory

Strategic Narrative Theory (SNT), which Miskimmon, O'Loughlin, and Roselle (2018) built, illustrates how states and non-states project themselves in the international system by generating and disseminating significant narratives. Strategic narratives are narratives used for altering target audiences perceptions, identities, and behaviors by re-framing events, actors, and ends into a specific ideological narrative (Miskimmon et al., 2018).

In cyber war, strategic narratives serve to legitimise aggression, delegitimise enemies, and shape public perception of complex events (Dowse & Bachmann, 2022). Disinformation, in this context, does not appear as discrete lies but as part of larger campaign efforts.

Disinformation injection in cyber exercise replicates the same dynamic by exposing exercise participants to uncertain attributions, dysfunctional narratives, and fabricated media environments (Miskimmon et al., 2018). These kinds of exercises are representative of real-life missions where strategic information disruption is paired with technical attacks, and participants must operate in contested narrative space.

Drills such as Locked Shields and Cyber Europe expose participants to simulated public criticism, adverse media coverage, and scripted news broadcasts (CCDCOE, 2024; ENISA, 2018). These narrative tests challenge the teams capacity to respond to both the factual event and the public interpretation of it, affirming strategic communication as a core defense resource. Strategic Narrative Theory forms the foundation for analysing how disinformation injects are developed and how participants respond to enemy narrative pressure (Miskimmon et al., 2018). Table 2 indicates how disinformation strategies most

effectively utilise the most important strategic narrative theory concepts in cyber training and how, in turn, these affect patterns of participant behaviour and response.

Table 2. Linking strategic narrative theory concepts to disinformation tactics in cyber exercises

Partially taken from Miskimmon, A., O'Loughlin, B., & Roselle, L. (2018).

Strategic narrative concept	**Example disinformation tactic in exercise**	**How affects participants**
Framing the incident	False news reports blaming an ally for carrying out cyber attack	Challenges in participant trust and alliance coordination
Identity construction	Deepfakes showing a leader making false claims	Undermines public trust and leadership integrity
Attribution ambiguity	Multiple contradictory social media rumors regarding the attacker	Compels participants to work in a state of uncertainty
Crisis narrative management	Leaked (fake) insider emails implying incompetence	Requests for rapid strategic communications to defend reputation
Legitimacy delegitimisation	Fake protests by citizens against cyber defenders	Employs test of people's capacity to preserve authority and narrative under pressure

3.2 Cognitive security and epistemic vigilance

Whereas SNT is concerned with how the information is displayed externally, cognitive security is concerned with how the information is received, processed, and interpreted internally (Miskimmon et al., 2018). Cognitive security refers to protecting human mind processes like perception, reasoning, and memory from manipulation, especially in difficult times such as cyber attacks (Pierce, 2021).

Disinformation takes advantage of cognitive vulnerabilities by using processes such as repetition, affective priming, and visual realism that are capable of fracturing under pressure judgment. Research indicates even politically active individuals are unable to differentiate fact from fiction when given misinformation under conditions of high stress. (Pantazi et al., 2021)

In order to counteract these weaknesses, epistemic vigilance helps by critically assessing whether information and its source are trustworthy (Sperber et al., 2010). Cyber exercise simulates environments where technical failures and information manipulation are

present. Participants are tested with their capacity to question, authenticate claims, and be resilient under operations pressure. Plus, cognitive security is not only about identifying imitation content, but also about having critical thinking and clear-headed judgment in noisy information environments (ENISA, 2018).

3.3 Cognitive resilience in adversarial information environments

For the aspect of cognitive security, cognitive resilience values adaptability, deep critical thinking, and psychological resistance when facing the informational pressure from an adversary (Bjola & Papadakis, 2020, pp. 642–645). Cognitive resilience enables individuals and groups to soundly make choices regardless of information divergence, emotive stimuli, and uncertainty (Silva et al., 2014).

Cognitive resilience is put to the test in cyber exercises when the players are subjected to concurrent technical interferences and story-based attacks. For example, when false rumours on social media accuse an organisation with crisis management failure, the team will need to rush to check if the rumour is true or false, formulate an appropriate response, and stay focused within limited time frames. (ENISA, 2018).

These exercises replicate actual hybrid threat situations in the world, such as ransomware with combined information operations against public trust. Cognitive resilience is absent, and even technically competent teams can break apart because of misunderstanding, role confusion, or stress (Silva et al., 2014, p. 3).

By integrating Strategic Narrative Theory and models of cognitive security and resilience, this research constructs an integrated analytical framework. It assists in determining the strategic objectives of disinformation campaigns and their psychological impact on participants. It also provides better understanding of how narrative exposure, cognitive tension, and strategic communication interact with each other during cyber exercise. Figure 1 illustrates this double-lens theoretical model, showing how narrative processes and cognitive responses are both treated together.

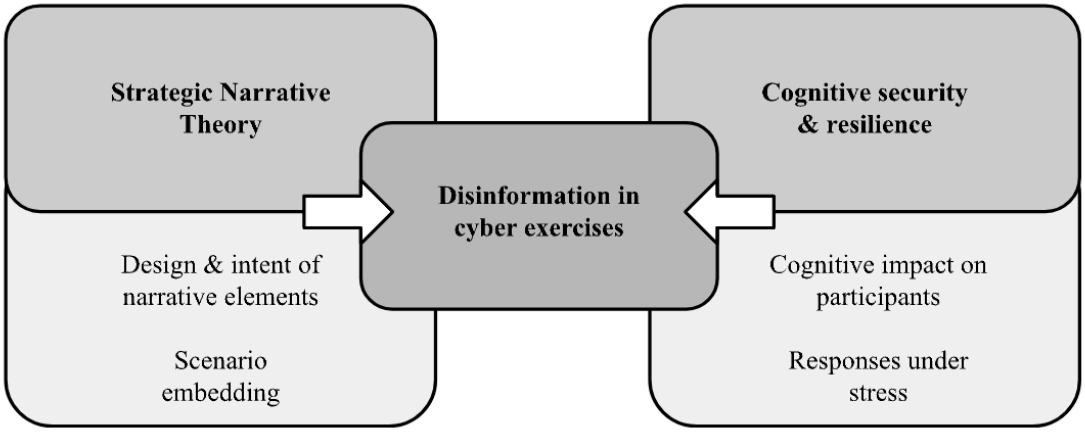

Figure 1. Theoretical framework dual lens breakdown

4 Methodology

This chapter outlines the approach employed in examining how disinformation is incorporated in cyber defense training simulations and influences participant experience, perceived value, and learning performance. Inquiry applies exploratory and qualitative approaches based on the extent of complexity of the study problem and the need to comprehend human subjective realities in structured simulated situations.

4.1 Research design

The study employs a qualitative, exploratory case study design. It is suitable method for studying social phenomena in their natural setting (Yin, 2018), especially when it is hard to determine the boundary between the phenomenon and its setting. This thesis investigates the influence of disinformation on training within cyber exercises, which are scenarios with complex environments and numerous stakeholders. Figure 2 provides a general overview of the research process, demonstrating the order of case selection, data collection, analysis, and interpretation within this sophisticated context.

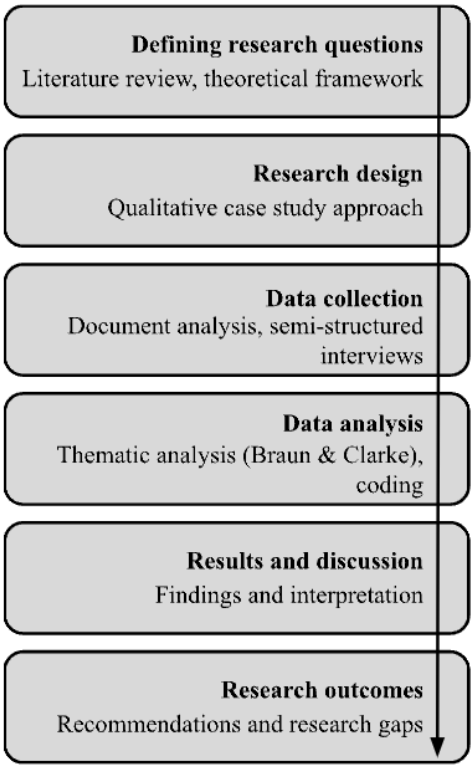

Figure 2. Overview of the research process

A case study method is used in offering various views of the process, interactions, and perceptions. Cases being explored involve high-visibility exercises such as Locked Shields and ENISA's Cyber Europe that have become more interwoven with media manipulation and strategic communication injects to exercise scenarios (CCDCOE, 2024; ENISA, 2018).

4.2 Data collection

The research relies on two empirical sources of evidence: document analysis and semi-structured interviews. These two will be complementary. Interviews are dense with information regarding organisers and participant attitude, while document examination offers contextual understanding and cross checks these results.

Five interviewees who have been directly involved in cyber exercises with disinformation aspects will be interviewed using semi-structured interviews. Interview participants will consist of exercise planners, StratCom or media cell creators, and evaluators. The interviews were structured around the research questions but with room for the individual

changes and ideas with reference to the roles of the participants. Questions were written in terms of searching for information on the motivation behind introducing disinformation, perceived effect on role clarity and concentration, team coordination problems, and mental stress in scenarios.

Parallelly to this, publicly available reports such as ENISA's Best Practices for Cyber Crisis Management (ENISA, 2023), after-action reports from Cyber Europe 2018 (ENISA, 2018), and strategic communication briefs from NATO StratCom COE (NATO StratCom COE, 2024) were reviewed. These documents were valuable for understanding how disinformation is integrated into cyber exercise design, how cognitive injects are used to simulate real-world influence operations, and how narrative management is approached as part of crisis response training. They also gave some information about communication management and coordination elements under cognitive stress.

4.3 Sampling strategy and interviews

The interviewees were sampled to select those who have relevant, hands-on experience with exercises, so applicable to the research question. A good and representative range of positions were invited: technical participants, exercise organizers, communications experts, evaluators and scenario writers. Snowball sampling was also to be used to refer other participants by the initial contact persons.

To be eligible, participants needed to have participated in a cyber exercise within the last two years that contained a disinformation component. Participants are in a position to provide opinions about how these components were perceived, how groups responded, and how such cognitive injects impacted technical performance, learning, or coordination. Participants were informed of the educational purpose of the study, their right to withdraw at any time, and anonymity.

After preliminary document examination and literature review, expert interviews were undertaken in order to verify results and inform about actual experience. Interviews served as a primary method for understanding how the disinformation elements in cyber exercises are conceptualised, implemented, and experienced by key stakeholders.

Five interviews (see Table 3) were carried out with subject matter experts who had direct experience in major cyber exercises such as Locked Shields, Cyber Europe and Cyber Coalition. As well as smaller-scale or national-level simulations. Respondents represented a balanced cross-section of professional roles, including exercise leadership, technical planning, StratCom cell design, and evaluation team member. This selection allowed the study to gather different perspectives from both strategic and technical layers of exercise planning and implementation.

Before each interview, participants received written information explaining the purpose of the research, the voluntary nature of participation, and guarantees of anonymity and data protection. Consent was obtained for recording the interviews and using anonymised quotes in the final thesis. No classified materials were collected or processed and all of the audio recordings are securely kept until the thesis defense in June 2025.

The interviews length ranged from 32 to 63 minutes (see Table 3) depending on the role, response level and rate of speech. Four were conducted online using Microsoft Teams application, and one was face-to-face with the help from smartphones voice recording app. Sessions were recorded for transcription purposes. Anonymity was maintained throughout transcriptions, and participant identities are referenced only by role (separate), organisation and exercise connection.

Table 3. An overview of the interview participants

Organisation	**Exercise connection**	**Interview format**	**Date and length**
CCDCOE	Locked Shields	Microsoft Teams online recording	14 April 2025; 62 minutes
NATO StratCom COE / CERT LV	Cyber Europe; Locked Shields	Microsoft Teams online recording	25 April 2025; 57 minutes
CCDCOE	Locked Shields	Microsoft Teams online recording	28 April 2025; 32 minutes
CR14	Locked Shields	On-site voice recording	30 April 2025; 46 minutes
CR14	Cyber Coalition	Microsoft Teams online recording	30 April 2025; 63 minutes

The interviews followed a semi-structured format based on a prepared questions script aligned with the research questions. Participants were encouraged to elaborate freely and offer additional reflections or examples. The full list of the used questions is provided in the appendix. Recordings were transcribed using the Microsoft Teams transcription tool, after which the author manually reviewed and corrected the transcripts for accuracy. These formed the primary data source for the thematic analysis described above and provided the foundation for the findings presented in Chapter 5.

4.4 Limitations

There are a few constraints to this research. First, the access is to publicly available and non-classified records that might constrain understanding of internal exercise design protocols. Second, participant perspectives are susceptible to contamination of memory, interpretation, or organisational culture and are subjective. Third, though qualitative methodology provides richness of understanding, it restricts generalisability. However, it is not the aim of this research to generate results that are generally applicable, but to study the less studied imbalance between cognitive realism and technical coherence in cybersecurity training from the insider's point of view.

Alongside these, there is a further limitation within the number of the sample interview. Although chosen experts included a satisfactory balance of roles (scenario leads, judges, planners, and support staff), the low number of interviews means that some viewpoints, especially from novice players or lesser-known national teams - may not have been completely attained.

In addition, the StratCom, media, and disinformation lines tended to be nested within other structural headings in exercises (e.g. media cell, white cell injectors), adding inconsistency to the use of terms and role definition. This may impact the frequency with which specific concepts were referenced or coded.

In spite of these limitations, the work is empirically based, relying on expert sources and professional practice. It is valuable in bringing to the fore the practical tensions and tacit

gaps in the way disinformation and information-based threats are instantiated into technically oriented training environments.

4.5 Data analysis

Six steps of Braun and Clarke's (2006) thematic analysis were used. These include familiarisation with data, generation of initial codes, developing the theme, reviewing themes, naming and defining the themes, and producing the final report.

The coding followed a two-dimensional approach: it was informed by existing theories such as strategic narrative framing (Miskimmon et al., 2018) and epistemic vigilance (Sperber et al., 2010), but it remained open to new concepts that emerged directly from participants words.

For organisation and presentation of data, qualitative coding tool Excel matrixes was used. Codes were grouped under broader themes, including perceived realism, role clarity, distraction or misunderstanding, value-added content, and affective or cognitive load. Representative experts from exercise documents and transcripts were integrated to triangulate key findings and examine consistency between participant experience and intended scenario design.

The discussion was thematic in its approach, focusing on three wide areas: the justification of incorporating disinformation into exercises, modes of implementation, and the challenge of finding the balance between technical clarity and cognitive realism. These dimensions mirrored the structure of the research questions and helped guide the interpretation of data.

5 Research results

In this chapter, the empirical research findings based on five semi-structured expert interviews are presented. The interviews examined the integration, implementation, and acceptance of disinformation and StratCom aspects into cyber exercises. Participants represented diverse functions, including scenario planning, technical coordination, judging StratCom, and national CERT participation. The objective was to understand how StratCom and disinformation are treated in large cyber exercises, what problems arise, and what best practices are developing. The analysis is organised thematically, bringing out similarities and differences between the exercises as well as experts experiences.

5.1 Importance of disinformation in cyber exercises

All the interviews substantiated that aspects of StratCom and disinformation are becoming essential elements of successful cyber exercises However, the justifications varied based on their specific roles. Coordination roles emphasized that exercises lacking cognitive or strategic levels currently fail to reflect real-world complexity. One respondent noted: *"A purely technical exercise that doesn't have a result is frankly useless… Ultimately, it's the decision-maker who makes the call on how or what is going to happen."*

The value is in the integrative nature of the training process, especially since new conflicts are becoming more hybrid. A number of the respondents brought up that disinformation is not a theoretical issue anymore but an operational fact that overlaps with technical breakdowns, political decision-making, and public trust. One of the interviewees stated that large-scale cyber-attacks inevitably demand public affairs, crisis communication, and strategic messaging competencies. To make the inclusion of disinformation elements in cyber training a matter of practical exigency and not as an adjunct.

Although StratCom was once seen as an *"add-on,"* exercises are now incorporating it more formally. One large exercise, for example, began as a technical exercise but has evolved to include operational and strategic levels, with components such as media simulation, role-playing, and narrative coordination.

Still, interviews identified a persistent gap in practice. While cognitively focused elements are acknowledged in theory, they often receive less planning time and fewer resources than technical components. Particularly in competitive settings, StratCom tracks are frequently underused unless they are tied directly to scoring or seen as helpful in achieving a win condition. This results in StratCom being practically deprioritised by many teams during live play.

5.2 Integration with technical tracks

A central question across the interviews was how to incorporate StratCom and disinformation aspects into technical cyber exercise components effectively. While there is strong conceptual support for integration, its practical implementation remains inconsistent.

Some interviewees described how disinformation scenarios were often overlooked, misinterpreted, or treated as secondary to the "real" technical game. As one noted: *"Expo showed your systems are down - energy 100 down - and they go like 'fake news'."* This shows a coordination gap within BT cells. Particularly between StratCom and technical operators. Ideally, these cells would collaborate to confirm incident realities and construct coherent public narratives. In practice, however, resource constraints (like access restrictions, limited accounts, scoring incentives) often prevent such cooperation.

Competitive environment also impedes integration further. Teams compete to maximize scoring points, which tends to lead them to prioritise technical defence functions over strategic communication track. Limited account availability reinforces this behaviour, as teams allocate resources to functions most directly tied to scoring outcomes, sidelining roles that are seen as lower priority despite their relevance to real-world crisis response.

In contrast, other exercise's non-competitive format provides more room for multi-level integration. There, the overlap between media and StratCom injects with technical incidents is designed to enable coordinated decision-making. Still, achieving full synchronisation is difficult due to the large number of participants and differing levels of StratCom maturity across nations.

An innovative suggestion from the interviews was to incorporate a small number of pre-agreed, cross-track injects (such as a nationwide power outage or a hospital data breach)

that would simultaneously trigger responses from technical, legal, and communication teams. Interviewees proposed that these shared scenario anchors could enhance narrative cohesion and realism by creating coordinated pressure points across all participating cells, ensuring that no team could disregard or sideline the scenario's core developments.

Overall, integration is looked for but currently unequal. Technical training continues to dominate in scale and character, while media and communication cells are gradually gaining more focus in planning and operations.

5.3 Content design: scripted vs reactive injects

The technique of injecting disinformation elements into cyber exercises differs significantly across platforms, from completely pre-scripted injects to reactive, moment-by-moment content generation. The balance between these approaches was a recurring design tension across all interviews.

Exercise participants characterised scripted injects as the foundation for most StratCom play. They are precomposed news articles, simulated social media updates, and adversary messaging - all composed to align with technical events and larger-scenario themes. As one scenario lead put it: *"You can do 100% pregen with an expectation, but there will always be something that occurs that drives you straight off the track."*

Both exercises use inject libraries as pools of pre-designed content for pertinent scenario elements. But at the same time, both exercises do concede that dynamic injects are needed. These get called when in response to live play, such as when a blue team (BT) is visibly struggling or has missed key developments. As described: *"If teams don't pick up a lesson, we hammer them a little bit more. That's what the reserve injects are for."*

This on-the-fly or active scripting enables white teams to stress-test participants' procedural and cognitive reactions under pressure. If a team claims their systems are okay when Expo indicates 100% breakdown, StratCom can introduce media questions to challenge their response. This creates realism and unpredictability, reflecting real-world information environments.

While useful, reactive scripting is problematic. It requires a high resource overhead, as it means expert StratCom operators have to be kept on standby around the clock and

available to improvise on demand. It also risks compromising scoring consistency, most obviously in competitive exercises, where unbalanced or improvised injects could compromise fairness. Aside from that, there is the risk of narrative drift: with loose management, reactive material can inadvertently ruin deep narratives or contradict large exercise themes.

In order to control these risks, one exercise depends on official controls like "*encouraging injects*" and "*reserve injects.*" They are initiated only under tight conditions, for example, when teams do not respond to earlier events. This enables exercise planners to maintain the integrity of the master narrative without compromising in reaction to player activity.

Simply put, while pre-scripted injects offer structure and control, reactive on-call content is necessary to offer realist testing and player response. Best exercises are between both - locating scenarios within scripted narrative but granting white teams room for improvisation as a response to altered performance and player choices.

5.4 Participant engagement and scoring

A theme that ran throughout all of the interviews was how participant behaviour is shaped by scoring mechanisms, especially in competitive simulations. Whether incentives are in place significantly affects whether StratCom tracks are taken seriously, how consistently teams stay engaged, and whether they focus on multi-domain coordination or only technical tasks.

In exercises where points are given for strategic communication activities (such as answering press questions, drafting press releases, or coordinating across roles) participants tend to allocate more effort toward those actions. Several interviewees noted a clear shift in engagement before and after StratCom scoring was formally introduced. One expert observed: *"When there was no scoring, people were more relaxed and more willing to try things… Now they really need points."* This shift highlights how gamification influences prioritisation and alters the seriousness with which communication elements are approached.

However, scoring also distorts behaviour. Teams are seeking to maximize their points ad sometimes emphasize outputs that align with scoring rubrics over those that reflect real-world. Interviewees noted that some participants would deny obvious system failures and

label them as misinformation, even when technical data showed otherwise. This kind of response prioritises narrative control over operational truth and undermines the training value of the disinformation track.

Smaller teams or those less familiar with exercise structures struggled more. Without clear understanding of how StratCom responses would be evaluated, they either underperformed or deviated from expectations. This led several organisers to call for better preparatory materials (mandatory videos, briefings, or clearer guidance) particularly for participants not coming from core technical communities.

In non-competitive environments, the absence of scoring allows greater room for exploratory learning but can also lead to reduced participation. Without the pressure of scoring, teams may disregard StratCom tasks in favour of more concrete technical objectives. To address this, some planners have introduced softer incentives such as "*training rewards*" or simulated audience reactions to encourage involvement and realism.

5.5 Exercise scale and coordination challenges

The scale of a cyber exercise heavily influences the ability to merge disinformation and strategic communication tracks with technical play. Across all interviews, people mentioned that large exercises offer more potential for sophisticated, multi-layered scenarios. However, they also introduce a higher risk of misalignment and siloed participation.

Some of the interviewees clarified that technical teams have well-defined tasks and deliverables, whereas StratCom teams rely on timely coordination, situational information, and narrative consistency. In reality, though, such coordination is not always present. StratCom players do not necessarily know technical information or a complete situational context, thus receiving disconnected or incredulous messaging.

An innovative suggestion from the interviews was to design shared scenario anchors that affect all tracks simultaneously. These cross-functional injects would trigger coordinated technical and communication responses, increasing cohesion. As one scenario lead explained, *"If you have that universe, many universe scenarios, different levels encompassing that strategic political operational levels and Stratcom and everything as*

a library, then yes, it's easier because you take those events from library… and link it with some cyber incidents".

Coordination is further complicated by time zone differences, mixed team composition, and uneven experience levels. In exercises involving geographically dispersed or unfamiliar partner organisations, miscommunication is more likely - especially in "partner runs" or smaller national versions of major exercises, where teams tend to be leaner and less prepared. Without clear role definitions or direct communication channels, inter-cell coordination can easily break down.

To address this, planners emphasized early scenario alignment and joint scripting. Shared operational tools like the Expo dashboard, structured pre-briefings, and routine coordination meetings during the exercise were all mentioned as helpful. Within Cyber Coalition, the "*national scripting conference*" was praised as a good model, enabling nations to tailor injects while still aligning with the broader storyline.

Scale can be perceived at the same time as both an asset and a challenge. Big exercises can better approximate the complexity of cyber-enabled crises, but without deliberate coordination mechanisms in place, they can mimic the very stovepipes they are meant to prepare against.

5.6 Strategic communication as a learning objective

Although cyber exercises have historically emphasized technical competence, recent iterations of large exercises show growing interest in including strategic communication as a distinct learning objective. Interviewees confirmed this trend, though the extent of integration remains uneven. Some exercises embed StratCom or media cell into the scenario from the start, while others continue to treat it as optional or secondary.

It was commented that even if StratCom is part of the planning exercise, its instructional process is also shallow. The participants can also not have a formalised set of objectives, measurable evaluation criteria, or adequate role preparation. One planner noted that the success of this track largely depends on how much initiative the participants take themselves: *"We're hoping that the blue teams will really run with what's going out from the StratCom team and it will enable this bigger story."*

This lack of clarity leads some StratCom participants to treat the track less seriously, often perceiving it as a form of performance or entertainment rather than a structured learning activity. One interviewee described how this mindset results in participants being unprepared when confronted with serious scenario elements, such as high-stakes crisis questions, which they had not expected to be treated with real-world gravity.

Without clear framing, StratCom risks being reduced to performance instead of a serious tool for developing cognitive resilience, pressure communication, and inter-team coordination. Several interviewees advocated for stronger educational framing, such as setting explicit expectations, offering structured feedback, and requiring mandatory briefings. One interviewee pointed out that mismatched expectations can lead to disengagement: *"They come to have fun, then ask: why is everyone so mean to me?"*

In contrast, exercises have evolved incrementally by putting StratCom players into virtual or real headquarters positions. Although these positions are not necessarily formally managed as part of the training audience, their operations more and more resemble actual military communications procedures. Interviewees characterised this evolution as a move toward eventually formalising StratCom learning objectives, particularly for NATO-related training consistent with policy frameworks.

Despite this momentum, assessment practices remain inconsistent. In competitive environments, StratCom scoring is often based on human judgment and subjective criteria. One interviewee pointed out that in some cases, the same individual both posed the questions and evaluated the responses (without teams being aware of this dual role) which led them to respond differently than they might have under more transparent conditions.

In summary, strategic communication is gaining ground as a key part of cyber resilience, but its role as a structured learning objective is still not consistent. Without clear goals, proper instruction, and evaluative feedback, StratCom risks being sidelined. Then it can be perceived more as background performance than as a meaningful training signal.

5.7 Lessons for smaller-scale exercises

Whereas large exercises offer multi-track, large-scale simulations, some of the interviewees highlighted the fact that high-quality disinformation and StratCom training

is attainable on a smaller scale, provided that one is well planned. This directly applies to national CERTs, private sector companies, or crisis response units by a single organisation.

Exercise designers highlighted that disinformation scenarios are extremely reproducible in lower-resource environments. Those fundamental principles such as narrative coherence, cross-functional communication, and timely media injections can still be maintained in tabletop or hybrid exercises. One interviewee described a national-level setup: "*We didn't need a full media simulator. We just used people in different rooms. One was the comms team, another legal, another technical. It worked. You just need the story to be strong.*"

The greatest challenge is not technology, though, but attitude and planning. Small-format buildings far too often are missing articulated interaction between cognitive and technical functions. This can lead to disconnected gameplay: technical groups are fixing systems and StratCom groups around in circles or isolated. Without tight linking of scenarios (articular decision nodes and cross-functional triggers) groups run the risk of becoming disconnected or inventing their own discrete narratives, destroying the intended learning value.

Another problem in small-scale exercises is one of a lack of realism. StratCom tasks often feel abstract or disconnected from actual responsibilities - especially in private sector or non-governmental contexts. When scenarios focus purely on technical breakdowns without societal or narrative context, cognitive engagement tends to drop. As one respondent noted, *"If you have just incident related with some technology, but there is no context, it limits training opportunities."* Participants may not take the scenario seriously unless they can connect it to familiar or recent events. If the narrative reflects something that has been witnessed on TV or happened around the location, engagement and presence are enhanced. Incorporating realistic and pertinent cues into the scene description can therefore greatly enhance cognitive immersion and cross-role interaction.

Importantly, small-scale exercises don't need complex platforms or full inject libraries. A single well-timed challenge (such as a fake media inquiry during a technical incident) can prompt real coordination and reveal procedural gaps. Several respondents emphasized that it's not about quantity but strategic placement. Smaller formats also

benefit from greater agility. With compact, co-located teams, facilitators can apply active scripting more responsively and pause the scenario for discussion or adjustment. As one interviewee put it: "*In small settings, you can stop the game, talk it through, and restart. You can't do that in Locked Shields*."

5.8 Key findings and implications

From each of the five expert interviews, there was a set of recurring issues and opportunities for incorporating disinformation and strategic communication aspects into cyber exercises. What these are indicate that success depends on careful design of scenarios, defined roles to teams, active scripting measures, and sufficient incentivisation. Although more complex exercises such as Locked Shields and Cyber Coalition provide sophisticated multi-layer coordination models, smaller exercises might be better served by less complicated and modular approaches to prevent cognitive overload and team disaffection.

The following table (see Table 4) synthesizes the main domains that were determined through open coding and thematic synthesis of interview data. For each domain, it outlines major findings and implications for exercise planning, scripting, and participant engagement.

Table 4. Key dimensions of disinformation integration in cyber exercises

Dimension	**Observed practice**	**Implications**
Relevance	Disinformation recognised as critical by organisers but often understood only by higher-level participants.	Realistic simulation depends on multi-level understanding; technical-only focus limits impact.
Integration with technical tracks	StratCom and technical teams rarely exchange information directly; few formal collaboration mechanisms.	Silos hinder narrative realism and reduce the value of technical contributions to public messaging.
Content design (scripted or reactive)	~70% of content is scripted, ~30% depends on participant behaviour. Reactive injects often improvised.	Reactive scripting adds realism but increases coordination burden and risk of narrative derailment.
Participant allocation and resources	Teams prioritise technical roles due to scoring bias; StratCom and legal roles understaffed.	Strategic communication are underutilised, reinforcing a tech-dominant bias.

Scoring incentives	Technical scores dominate evaluation frameworks; StratCom scores are more subjective and inconsistently applied.	Lack of standardised metrics undermines engagement and perceived legitimacy of StratCom contributions.
Scenario cohesion and narrative control	Lack of shared timeline across teams causes mismatched interpretations of unfolding events.	Reduces immersion and leads to confusion.
Coordination in large exercises	Difficulty aligning teams from different nations and sectors (gov, private, military).	Highlights need for exercises to mirror real-life stakeholder diversity but adds complexity.
Learning objectives	StratCom tracks often lack defined outcomes and feedback mechanisms.	Without objectives, it's hard to measure success or improve year-to-year. Lowers strategic learning value.
Participant perception	Some StratCom participants expect light play and are surprised by intensity or criticism.	Shows a need for expectation-setting and a pre-exercise briefing that clarifies tone and stakes.
Exercise preparation	Some StratCom planners report not being included early; key injects created by a single organiser.	Limits diversity of input, risks bias and reduces scalability. Stronger early-stage collaboration needed.
Small-scale exercises	Most smaller exercises omit disinformation; lack time, staff, or context-building capability.	Lost opportunity to test crisis comms in lower-stakes settings. Could use simplified versions.
Information environment design	Simulated social media often lacks emotional realism.	Weakens cognitive stress testing. Need richer personas, language, and emotional tone in content.
Exercise documentation	Teams often unaware that evaluators are also scenario participants (e.g., judges also playing red team).	Reduces transparency in evaluation. Teams may overestimate performance in self-assessments.

6 Discussion

In this chapter, findings presented in Chapter 5 are explained with respect to research context of the thesis, theory bases, and research approach. In interviews conducted with exercise planners, judges, and scenario leaders, this research scrutinized the concept, enactment, and embodied life of disinformation components of cyber exercises. Analysis has further discussed the impact of these elements on technical components of the player-game interaction, team dynamics, and training goals - under competition or operation-style training conditions specifically.

One of the most significant findings from the interviews is that although disinformation and strategic communication are being more and more integrated into large-scale cyber exercises, they remain viewed as marginal or add-ons to the technical core. This aligns with earlier research on cyber training environments, which indicates that cognitive and communicative challenges fall behind when scoring and structure prioritise technical performance. But role players all around emphasized that information pressure decision-making is impossible to separate from cyber realism - the issue of balancing simulation fidelity against training value. In addition, disinformation element integration was not just a scenario content issue but institutional design. Areas for coordination shortfall between technical, legal and communication roles were identified as persistent problems, in particular where StratCom elements existed in a silo from the technical gameplay or had no situational awareness in real-time. These conclusions corroborate the general argument that cross-functional cooperation, rather than role-based competence is a core building block of resilience for cyber crisis scenarios.

6.1 Integration and purpose of disinformation tracks

One of the most noticeable trends in the results is the continued struggle to see disinformation trails as addition to narratives and not core training elements. As a matter of scenario design, the StratCom elements have dual purposes: they contextualise technical events, role-play public opinion, and probe decision-making within uncertainty. However, as became apparent through the interviews, what the participants consider these

elements involves widely diverging interpretations. This section addresses the first research question by showing that disinformation is included in cyber exercises to mirror the complexity of hybrid threats. It also illustrates the ambiguity in how different roles perceive its relevance, especially when not tied to scoring.

For example, interviewees went out of their way to repeatedly emphasize that technical teams are likely to de-prioritise or overlook disinformation injects so long as they are not tightly connected to scoring metrics or operating implications. That was typical of a larger problem of misalignment between training goals and participant incentives. Even when StratCom scoring was being experimented with, respondents suggested that restricted access to accounts or team prioritisation workflows meant little involvement with non-technical roles. This detracts from the scenarios purpose of simulating real-world interdependencies between information and infrastructure.

By comparison, another exercise incorporated media cell into national-level scenario customisation. Permitting states to be authors of media stories for their specific purposes was asserted to provide increased buy-in and realism. Even here, strategic communication specialists were discovered to operate with limited training objectives or formal feedback. The implication is that as integration mechanisms are being enhanced, the putative objective of the disinformation track still remains behind its potential value as training.

Theoretically, this supports the argument that tasks which are essentially technical in character tend to structure non-technical areas as secondary. From a sociotechnical perspective, the results indicate that cognitive, organisational, and communicative layers need more intentional design integration – not just additive content.

6.2 Operational constraints and trade-offs in exercise design

The research also identifies structural and operational limitations on the extent to which disinformation components are represented in practice. Both Locked Shields and Cyber Coalition both use some type of cognitive injects, though these are time, team capability, and exercise format constrained. For example, as many respondents noted, the number of participating accounts is often what decides if, and how, a team can expend resources on non-technical functions like StratCom or media cells. In competitive settings teams will

optimise for point-earning categories, which makes playing tracks that are seen as low-impact in the overall grading less appealing.

Methodologically, this is what Braun and Clarke (2006) refer to as "contextual meaning-making" where the participants behave in accordance with the institutional logics that are embedded in the exercise. In this case, the logic is technical performance, which by definition precludes elements that do not directly have technical advantage. Meanwhile, interviews indicated that the exercises most likely to induce response and reflection in team roles were those providing tiny but effective doses of disinformation injections, most notably those requiring cross-functional coordination. This indicates that cognitive pressure can be an effective training vector, but only if tied to a tangible operational consequence or decision path.

These tensions reveal a larger design issue: how to add cognitive injects without overloading limited team capacity or sacrificing the technical integrity of the exercise. Scenario writers described using "*reserve injects*" or "*encouraging injects*" as methods for maintaining audience engagement without overloading teams with information. This resonates with systems thinking in sociotechnical design, whereby resilience is not an outcome of optimised complexity, but coordinated flexibility across functions. The strategic application of media pressure, oppositional messages, or attributional dilemmas is thus therefore an organisational challenge not of media literacy as such, but of an organisation's coordination in conditions of ambiguity.

This discussion contributes to the second research question, which focused on how disinformation is implemented in practice. It highlights the operational and structural trade-offs that affect whether and how cognitive elements are embedded. Methodologically, these findings legitimise the use of qualitative interview and thematic analysis as suitable methods for deconstructing multi-layered experiential data within role limits. Triangulating organisers, judges, and technical support staff' perspectives allowed the research to chart both structural and cultural forces that shape disinformation's construal and management in training.

6.3 Implications for smaller-scale exercises

One of the ongoing themes in the interviews was the clear advantage of transposing cognitive aspects such as disinformation across big exercises and organisational or national-level training exercises on a lesser scale. The strategic justification for incorporating disinformation is simple, particularly its applicability to narrative influence and public trust, and yet lower-scale exercises usually do not have the resources, personnel, or scenario sophistication to effectively simulate it.

Several interviewees noted that within constrained environments, technical teams usually have to carry out a variety of tasks with little role specialisation. Within these environments, disinformation injects risk being diversions unless highly scripted and associated with critical incident response procedures. This operational limitation was seen in both partner-conducted national exercises, where media injects were occasionally ignored completely unless backed by scoring pressure or forced coordination.

Yet, the research also offers some encouraging design strategies for bridging this gap. Large and small format experienced interviewees alike suggested scenario convergence which are operating on one event to generate both technical and communicative repercussions, an effective means of incorporating disinformation without loading up the roles. A hospital network cyber attack, for instance, can be followed by the inject of a breaking news report of failing systems that will generate communication and decision-making activity even in a leaner staffing. These findings relate to the fifth research question, exploring how practices from large-scale exercises might be adapted for smaller training formats with limited capacity.

From a theoretical perspective, this supports the idea that realism does not require scale, but salience. Well-timed, scenario-linked disinformation injects can still offer cognitive value even in minimal configurations, provided they are tied to operational consequences. In this regard, modularity and narrative coherence appear more critical than media volume.

In terms of methodology, the interviews identified a pragmatic knowledge gap: there are many organisers of smaller-scale events who do not have access to StratCom professionals or reusable content storage banks that can reduce the exclusion barrier. This indicates a potential institutional opportunity for actors such as CCDCOE, ENISA to

create and share scalable StratCom modules or inject kits tuned into limited training environments. Notably, this is a reflection of a cycle of feedback between tactical action and strategic planning, increasing the usability of sociotechnical integration in exercise planning.

6.4 Theoretical reflection and framework alignment

The results of this research are in line with the sociotechnical view of reference that structured its theoretical context. As discussed in Chapter 3, cyber defence cannot be reduced to technical systems alone but must be understood as a layered interplay between infrastructure, institutions, communication, and cognition. Disinformation, while not necessarily defined as an exercise track, solidified in interviews as an operational scenario variable of concern to several facets of cyber readiness.

This is supported by the literature that positions cognitive security as being within digital resilience, precisely where public opinion, decision-making, and trust in digital service are undermined (Wirtz & Weyerer, 2016). Introducing elements of disinformation into circumstances, training scenarios replicate the kind of information noise and uncertainty with which defenders have to deal in actual events. But as the interviews proved, these variables only become meaningful if tied to decision and job points of action.

The diverse participant views exhibit a stratified divide between design intention and participant engagement. Technical determinism (focus on quantifiable technical achievement) is nevertheless the criterion governing groups' work with scenario sophistication. This is indicated in the low take-up of what StratCom injects unless they have tangible impact upon scoring or de-escalating incidents. Such results find echo with issues in literature that technical training unwittingly excludes softer, yet equally vital, competencies like communications and psychological readiness.

The theoretical framework also accounts for institutional inertia: Locked Shields training is maximized for high-pressure performance, while Cyber Coalition seems to be more narrative-driven but less immediate in evaluation. Both models contribute, but neither satisfies the gap between cognitive scenario-building and integrated learning outcomes. Cognitive threats such as disinformation are therefore structurally close at hand rather than embedded, though with conceptual pertinence.

This section reinforces the theoretical basis of the thesis, supporting the idea that disinformation and cognitive injects are key elements in sociotechnical training systems. It also strengthens the conceptual answer to RQ1 and RQ4 by framing these threats as part of resilience-building.

What filters through is an appeal for more highly interwoven design: where attacks on cognition are not only simulated but made functional as part of cyber defense mechanisms. This is in line with the thesis' key argument: that disinformation must be treated not as an extra layer but as an active scenario element with some training value and implementation need. From a systems theory point of view, one cannot guarantee full-spectrum cyber resilience unless one completes the loop between technical action, coordination, and perception.

6.5 Key insights with recommendations

This research aimed to explore the integration of disinformation components into cyber defense training exercises and their effects on participant motivation, scenario realism, and training utility. Based on expert interviews and document analysis, some main findings were established

First, although disinformation is increasingly seen as a plausible element of cyber crisis scenarios, it is unevenly integrated into training. Locked Shields and Cyber Coalition both include strategic communications elements, but their utility as training hangs precariously on their use, placement, and context in relation to incentives for participants. Lacking direct linkage to scoring mechanisms or results in simulations, disinformation is at risk of being dismissed by technologically oriented participants more interested in protecting infrastructure than engaging with narrative.

Second, inter-role coordination (specifically technical, legal, and communication cells) is an issue. Most of the participants reported having siloed implementation, where StratCom players do not know the operating picture, or technical individuals work without regard to the information environment. The gap compromises the realism of exercises that try to replicate hybrid threats.

Third, both large exercises and small exercises grapple with resource management and scenario complexity. Locked Shields is better at pressure-testing, but Cyber Coalition is

more adaptable when it comes to national-level scenario customisation. Neither, though, has been entirely able to effectively balance cognitive realism with technical simplicity. Injects need to be dynamic enough to simulate real-time threat environments, but also well-structured enough to provide consistency and fairness.

Lastly, the results demonstrate there is a definite need to reconsider how cognitive scenario elements like disinformation are handled in overall design. Instead of being variable options or overlay tracks, they need to be designed in as scenario cues that inform operational choices. Suggestions include:

- Linking StratCom outputs more directly to scenario milestones and scoring mechanisms.
- Clear role definitions and interdependencies in scenario briefings.
- Co-location or structured interaction between technical and narrative cells.
- Creation of reactive injects that force cross-domain coordination under time pressure.

This synthesis pulls together the study's core findings in relation to RQ3 and RQ4. It highlights the practical gaps between technical clarity and cognitive realism, and points to necessary design changes for better integration.

These are conclusions affirming the notion that disinformation, though usually peripheral, is centrally pertinent in contemporary cyber defense, particularly where public confidence and collective crisis management are concerned. To offer cognitive resilience as an actual product of cyber training, it must be considered a design imperative. Not a narrative extra, but a functional component of the scenario.

6.6 Future work

Based on this study's findings, a number of directions for future research are opened. Firstly, follow-up studies may use quantitative measurement in combination with qualitative interview. And observational data, for example, participant response time, inject uptake, or coordination frequency between groups responding to cognitive challenge like disinformation.

Second, additional study of smaller-scale or sector-specific exercises, national CERT drills, crisis communication simulation, or private sector incident response scenarios might cast some light on how exercises with limited resources embrace (or eschew) narrative complexity. A comparative analysis might expose divergent adaptation strategies based on institutional purpose, stakeholder pressure, or audience maturity.

Third, as automated content generation technologies like AI-generated media gain more uses, future research must examine the influence of synthetic disinformation on participants' action, message believability, and training outcomes. This involves issues of ethics in realism versus manipulation, as well as technical possibility of effectively simulating influence operations plausibly without overwhelming participants.

Finally, scenario planning framework design may be refined to improve alignment between technical and cognitive objectives. Studies may be conducted for refining templates or modular inject sets aligning infrastructure incidents with scripted or reactive media stimuli so the process of adaptation can be smoother at different scales of exercises without reducing narrative coherence.

7 Conclusion

This thesis aimed to investigate how disinformation as a scenario element is introduced in cyber exercises. Particularly targeting technically advanced formats like multinational cyber exercises. Through qualitative analysis based on literature review and expert interviews, the research examined both the narrative logic of disinformation injects and the institutional processes by which they are introduced and responded to during cyber exercises.

The research addressed the first question by showing that disinformation is increasingly seen as a necessary reflection of modern hybrid threats. It is used to simulate attacks on public trust, decision-making, and legitimacy (rather than only technical systems). However, the study also found that disinformation is not envisioned as a standalone training stream. Rather, it serves as a scenario component within broader communication and narrative roles, typically delivered through Strategic Communications (StratCom), media simulation, or cognitive injects.

This addressed the second research question of how the components of disinformation are deployed. While their deployment has increased in recent years, especially in prominent NATO-led exercises, their development and integration are still inconsistent. Injects are typically pre-scripted, with minimal use of reactive components, and are commonly out of phase with technical tracks unless scoring rewards are involved. This makes disinformation play an unintended function with regard to its perceived intent among players, especially those who perform technical roles.

In relation to balancing technical training with cognitive injects (RQ3), the findings revealed that disinformation is often viewed as peripheral unless clearly connected to operational consequences or point-based rewards. Teams tend to prioritise roles that contribute directly to measurable outcomes, which leaves communication cells underused. This is a reflection of structural imbalance in meeting cognitive and technical goals.

Fourth research question tested best practice in the use of disinformation without taking away from learning outcomes. This thesis highlighted that success depends on how well disinformation injections are integrated into important scenario events and decision points.

Exercises that use shared scenario anchors (such as national outages or public-facing crisis narratives) see more meaningful engagement. Coordination between technical and communication cells was another strong predictor of impact. Wherever limited situational awareness or structural separation existed, disinformation components were often completely overlooked, even if technically present.

Lastly, the study tested to what extent best practices of exercises which are large in scale can be transferred to the smaller ones (RQ5). The outcome was that realism does not require complex tools, but rather salience and clear narrative structure. Small exercises can incorporate cognitive challenge very well with low-tech techniques (such press questions, plain injects, or room-divided role teams) if scenarios are planned with keeping coordination and simplicity in mind.

This thesis adds to our knowledge of cyber exercises as sociotechnical training systems, where success is not just in infrastructure defense, but in effective decision-making under stress. It shows that disinformation injects, if properly designed and meaningfully incorporated, add scenario realism and strategic value. But their impact is usually limited by siloed roles, poorly defined goals, and unbalanced evaluation practices.

In favor of stronger cyber crisis response capability, this thesis recommends that planners treat disinformation not as an optional narrative layer, but as on of the core components. Something that influences all levels of play - from technical operations to strategic leadership. As a result, cyber training environments can better mirror the complexity of today's hybrid threat environment with providing participants in all roles with a more realistic learning experience.

References

Atlantic Council's Digital Forensic Research Lab. (2024). *Undermining Ukraine: How Russia widened its global information war in 2023*. Atlantic Council. https://www.atlanticcouncil.org/in-depth-research-reports/report/undermining-ukraine-how-russia-widened-its-global-information-war-in-2023/

Beyond Identity. (2021, October 28). *Software supply chain attack methods behind SolarWinds, Kaseya, and NotPetya and how to prevent them*. https://www.beyondidentity.com/resource/software-supply-chain-attack-methods-behind-solarwinds-kaseya-and-notpetya-and-how-to-prevent-them

Bessi, A., & Ferrara, E. (2016). Social bots distort the 2016 U.S. presidential election online discussion. *First Monday, 21*(11). https://doi.org/10.5210/fm.v21i11.7090

Bilal, A. (2021). Hybrid warfare – New threats, complexity, and 'trust' as the antidote. *NATO Review*. https://www.nato.int/docu/review/articles/2021/11/30/hybrid-warfare-new-threats-complexity-and-trust-as-the-antidote/index.html

Bjola, C., & Papadakis, K. (2020). Digital propaganda, counterpublics and the disruption of the public sphere: The Finnish approach to building digital resilience. Cambridge Review of International Affairs, 33(5), 638–666. https://www.tandfonline.com/doi/full/10.1080/09557571.2019.1704221

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology, 3*(2), 77–101. https://doi.org/10.1191/1478088706qp063oa

Buzzell, A. W. (2024). *The ethics of cognitive security* (Doctoral dissertation, York University). YorkSpace Institutional Repository. https://yorkspace.library.yorku.ca/items/413453c5-490c-4052-ad50-1a769f0f0b10

CCDCOE. (2022). *Locked Shields 2022 Exercise*. NATO Cooperative Cyber Defence Centre of Excellence. https://ccdcoe.org/locked-shields/

CCDCOE. (2024). Locked Shields Exercise. NATO Cooperative Cyber Defence Centre of Excellence. https://ccdcoe.org/locked-shields/

Dame Adjin-Tettey, T. (2022). Combating fake news, disinformation, and misinformation: Experimental evidence for media literacy education. *Cogent Arts & Humanities, 9*(1). https://doi.org/10.1080/23311983.2022.2037229

Dowse, A., & Bachmann, S. D. (2022). Information warfare: Methods to counter disinformation. Defense & Security Analysis, 38(4), 453–469. https://doi.org/10.1080/14751798.2022.2117285

ENISA. (2018). *Cyber Europe 2018 After Action Report*. European Union Agency for Cybersecurity. https://www.enisa.europa.eu/publications/cyber-europe-2018-after-action-report

ENISA. (2023). *Best Practices for Cyber Crisis Management.* European Union Agency for Cybersecurity. https://www.enisa.europa.eu/publications/best-practices-for-cyber-crisis-management

Fazey, I. (2010). Resilience and higher order thinking. *Ecology and Society, 15*(3). http://www.jstor.org/stable/26268183

Gavrila, R., Ogée, A., Trimintzios, P., & Zacharis, A. (2015). *ENISA CE2014 after action report*. European Union Agency for Cybersecurity (ENISA). https://www.enisa.europa.eu/publications/ce2014-after-action-report

Heap, B., Hansen, P., & Gill, M. (2021). *Strategic Communications Hybrid Threats Toolkit: Applying the principles of NATO Strategic Communications to understand and counter grey zone threats*. NATO Strategic Communications Centre of Excellence. https://stratcomcoe.org/publications/strategic-communications-hybrid-threats-toolkit/213

Karpiuk, M. (2022). Crisis management vs. cyber threats. *Sicurezza, terrorismo e società, 2*(16), 113–123. https://www.sicurezzaterrorismosocieta.it/wp-content/uploads/2022/12/SicTerSoc16.pdf#page=114

Kirdemir, B. (2019). *Hostile influence and emerging cognitive threats in cyberspace*. Centre for Economics and Foreign Policy Studies (EDAM). https://edam.org.tr/wp-content/uploads/2019/12/Hostile-Influence-Emerging-Cognitive-Threats-in-Cyberspace-by-Baris-Kirdemir.pdf

Knox, B. J., Lugo, R. G., & Sütterlin, S. (2019). Cognisance as a human factor in military cyber defence education. *IFAC-PapersOnLine*, *52*(19), 163–168. https://doi.org/10.1016/j.ifacol.2019.12.168

Kont, J., Elving, W., Broersma, M., & Bozdağ, Ç. (2024). What makes audiences resilient to disinformation? Integrating micro, meso, and macro factors based on a systematic literature review. *Communications*. https://doi.org/10.1515/commun-2023-0078

Maennel, K., Brilingaitė, A., Bukauskas, L., Juozapavičius, A., Knox, B. J., Lugo, R. G., Maennel, O., Majore, G., & Sütterlin, S. (2023). A Multidimensional Cyber Defense Exercise: Emphasis on Emotional, Social, and Cognitive Aspects. *SAGE Open*, *13*(1). https://doi.org/10.1177/21582440231156367 (Original work published 2023)

Maennel, K., Ottis, R., & Maennel, O. (2017). Improving and measuring learning effectiveness at cyber defense exercises. In Secure IT Systems: 22nd Nordic Conference, NordSec 2017, Tartu, Estonia, November 8–10, 2017, Proceedings 22 (pp. 123-138). Springer International Publishing. https://link.springer.com/chapter/10.1007/978-3-319-70290-2_8

Morgan, S. (2018). Fake news, disinformation, manipulation and online tactics to undermine democracy. *Journal of Cyber Policy*, *3*(1), 39–43. https://doi.org/10.1080/23738871.2018.1462395

Murero, M. (2023). Coordinated inauthentic behavior: An innovative manipulation tactic to amplify COVID-19 anti-vaccine communication outreach via social media. *Frontiers in Sociology, 8*, Article 1141416. https://doi.org/10.3389/fsoc.2023.1141416

Murphy, B. (2024). In defense of disinformation. *Journal of Homeland Security and Emergency Management, 21*(3), 441–466. https://doi.org/10.1515/jhsem-2022-0045

Miskimmon, A., O'Loughlin, B., & Roselle, L. (2018). Strategic narrative: 21st century statecraft. *Revista Mexicana de Política Exterior, 113*, 43–63.

NATO. (2020). *NATO 2030: United for a new era*. https://www.ndc.nato.int/news/news.php?icode=1509

NATO. (2024). *Hybrid threats and hybrid warfare: Reference curriculum*. NATO Headquarters Brussels, Partnership for Peace Consortium. https://www.oranoua.ro/wp-content/uploads/2022/03/Understanding-global-disinformation.pdf

NATO ACT. (2021). *Cyber Coalition Exercise Overview*. NATO Allied Command Transformation. https://www.act.nato.int/cyber-coalition/

NATO Allied Command Transformation. (2024). *Decoding the information environment: NATO's Strategic Communications Centre of Excellence*. https://www.act.nato.int/article/stratcom-coe-2024/

Nicholson, M. M. (2012). The cognitive battlefield: A framework for strategic communications. https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=332dd8b61c6041c35420f8582d2240d73b10ef7f

OpenAI. (2025). ChatGPT (GPR-4o) [Large language model]. https://chat.openai.com

Pantazi, M., Kissine, M., & Klein, O. (2021). Social and cognitive aspects of the vulnerability to political misinformation. *Political Psychology, 42*(S1), 277–299. https://doi.org/10.1111/pops.12797

Pierce, B. M. (2021). Protecting people from disinformation requires a cognitive security proving ground. *Defense News*. https://www.c4isrnet.com/opinion/2021/02/10/protecting-people-from-disinformation-requires-a-cognitive-security-proving-ground/

Princeton Public Library. (n.d.). *Misinformation, disinformation & malinformation: A guide*. https://princetonlibrary.org/guides/misinformation-disinformation-malinformation-a-guide/

Reding, D. F., & Wells, B. (2022). Cognitive warfare: NATO, COVID-19 and the impact of emerging and disruptive technologies. In Gill, R., & Goolsby, R. (Eds.), *COVID-19 disinformation: A multi-national, whole of society perspective* (pp. 25–45). *Advanced Sciences and Technologies for Security Applications*. Springer. https://doi.org/10.1007/978-3-030-94825-2_2

Schmitt, O. (2018). When are strategic narratives effective? The shaping of political discourse through the interaction between political myths and strategic narratives. *Contemporary Security Policy, 39*(4), 487–511. https://doi.org/10.1080/13523260.2018.1448925

Schünemann, W. J. (2022). A threat to democracies?: An overview of theoretical approaches and empirical measurements for studying the effects of disinformation. Cyber security politics, 32-47.

Seker, E., & Ozbenli, H. H. (2019). The concept of cyber defence exercises (CDX): Planning, execution, evaluation. In *International Conference on Cyber Conflict*. https://arxiv.org/pdf/1906.03184.pdf

Silva, A., McClain, J. T., Sundaram-Stukel, R., & Albert, A. (2014). Factors impacting performance in competitive cyber exercises. *U.S. Department of Energy*. https://www.osti.gov/servlets/purl/1315132

Skopik, F., & Leitner, M. (2021). Preparing for national cyber crises using non-linear cyber exercises. In *2021 18th International Conference on Privacy, Security and Trust (PST)* (pp. 1–5). IEEE. https://doi.org/10.1109/PST52912.2021.9647795

Sperber, D., Clément, F., Heintz, C., Mascaro, O., Mercier, H., Origgi, G., & Wilson, D. (2010). Epistemic vigilance. *Mind & Language, 25*(4), 359–393. https://doi.org/10.1111/j.1468-0017.2010.01394.x

Sultan, O. (2019). Tackling disinformation, online terrorism, and cyber risks into the 2020s. *The Cyber Defense Review, 4*(1), 43–60. https://www.jstor.org/stable/26623066

Tammekänd, J., Thomas, J., & Peterson, K. (2020, October). *Deepfakes 2020: The tipping point*. Sentinel. https://thesentinel.ai/media/Deepfakes%202020:%20The%20Tipping%20Point,%20Sentinel.pdf

Udry, J., & Barber, S. J. (2024). The illusory truth effect: A review of how repetition increases belief in misinformation. *Current Opinion in Psychology, 56*, 101736. https://doi.org/10.1016/j.copsyc.2023.101736

Veksler, V. D., Buchler, N., Hoffman, B. E., Cassenti, D. N., Sample, C., & Sugrim, S. (2018). Simulations in cyber-security: A review of cognitive modeling of network attackers, defenders, and users. *Frontiers in Psychology, 9*, Article 691. https://doi.org/10.3389/fpsyg.2018.00691

Wardle, C., & Derakhshan, H. (2017). *Information disorder: Toward an interdisciplinary framework.* Council of Europe. https://rm.coe.int/information-disorder-toward-an-interdisciplinary-framework-for-researc/168076277c

Wells, L. (2017). Cognitive-emotional conflict: Adversary will and social resilience. *PRISM, 7*(2), 4–17. http://www.jstor.org/stable/26470514

Wirtz, B. W., & Weyerer, J. C. (2016). Cyberterrorism and Cyber Attacks in the Public Sector: How Public Administration Copes with Digital Threats. *International Journal of Public Administration*, *40*(13), 1085–1100. https://doi.org/10.1080/01900692.2016.1242614

Appendix 1 - Non-exclusive licence for reproduction and publication of a graduation thesis[1]

I Crystella Sokk

1. Grant Tallinn University of Technology free licence (non-exclusive licence) for my thesis “Disinformation as a Scenario Element in Cyber Exercises”, supervised by Kaido Kikkas
   1.1. to be reproduced for the purposes of preservation and electronic publication of the graduation thesis, incl. to be entered in the digital collection of the library of Tallinn University of Technology until expiry of the term of copyright;
   1.2. to be published via the web of Tallinn University of Technology, incl. to be entered in the digital collection of the library of Tallinn University of Technology until expiry of the term of copyright.
2. I am aware that the author also retains the rights specified in clause 1 of the non-exclusive licence.
3. I confirm that granting the non-exclusive licence does not infringe other persons' intellectual property rights, the rights arising from the Personal Data Protection Act or rights arising from other legislation.

12.05.2025

1 The non-exclusive licence is not valid during the validity of access restriction indicated in the student's application for restriction on access to the graduation thesis that has been signed by the school's dean, except in case of the university's right to reproduce the thesis for preservation purposes only. If a graduation thesis is based on the joint creative activity of two or more persons and the co-author(s) has/have not granted, by the set deadline, the student defending his/her graduation thesis consent to reproduce and publish the graduation thesis in compliance with clauses 1.1 and 1.2 of the non-exclusive licence, the non-exclusive license shall not be valid for the period.

Appendix 2 - Interview questions

Below is the master list of interview questions used for this study. Questions were modified from this list to suit each participant's role and experience in the exercise setup. Not every participant was queried on all issues. Rather, appropriate subsets were chosen to reflect to their responsibility in planning, technical coordination, communication role, or assessment.

Role

1. Please describe your current role in cyber exercises.
2. How long have you been involved in exercises like Locked Shields, Cyber Coalition, or others?

Disinformation purpose

3. Why is disinformation included in cyber exercises?
4. What are primary learning outcomes or training goals intended with disinformation or StratCom injects?

Inject design and implementation

5. How are disinformation injects designed (are they mostly pre-scripted, reactive, or mixed)?
6. What factors influence the timing and delivery of these injects?
7. What challenges arise in balancing scripted content with real-time reactions?

Cross-track integration

8. How are disinformation and StratCom elements coordinated with technical gameplay?
9. Do StratCom/media cells interact with technical teams during play?
10. What difficulties have you observed in aligning cognitive and technical objectives?
11. How does the presence or absence of scoring influence StratCom participation?

Exercise scale and realism

12. How does the scale of an exercise affect disinformation integration?
13. What lessons can be applied when scaling down StratCom tracks for smaller exercises?
14. How realistic do participants perceive the simulated media or public environment to be?
15. What methods are used to simulate emotional tone, audience pressure, or narrative stakes?

Recommendations

16. What would you improve in future exercises regarding the design and delivery of disinformation tracks?
17. What recommendations would you give to new planners wanting to introduce these elements?
18. Is there anything else you would like to add about this topic?