SELF REFLECTION UPON BACHELOR THESIS

Yuliia Storm Larsen

Bachelor Project: Investigation of Emerging Cyberwarfare in Denmark - BIBAPRO1PE

https://github.com/jsolomkk0/Bachelor-Project---Yuliia-Larsen-

IT UNIVERSITY OF COPENHAGEN

Investigation of Emerging Cyberwarfare in Denmark
S25BIBAPRO1PE757

Yuliia Storm Larsen
Student, IT University of Copenhagen
yuls@itu.dk

Oksana Kulyk
Supervisor, IT University of Copenhagen
okku@itu.dk

May 14, 2025

With steadfast steel and unyielding will, Denmark stands by Ukraine - not just in arms, but in spirit, defending freedom where it burns brightest[60; 174].

The landscape of modern warfare has evolved dramatically with the rise of digital technologies.

Cyberwarfare refers to coordinated digital assaults targeting nation-states, inflicting damage comparable to traditional military
conflicts by compromising essential computer networks.

For the more detailed information please use this GitHub repo that contains the Research Project and all the Supplementary Materials :
https://github.com/jsolomkk0/Bachelor-Project---Yuliia-Larsen-

WHY DID I CHOOSE THIS TOPIC FOR MY BACHELOR RESEARCH?

I undertook this topic regarding cyberwarfare research after witnessing how technological vulnerabilities directly endanger patient safety, exemplified by my personal experience where a clinic's system failure created chaos and raised disturbing questions about data integrity. My research specifically examines digitization's role in hybrid warfare campaigns against Denmark's healthcare sector and how geopolitical tensions influence cyberwarfare evolution against my country. Through my interviews with Danish security experts, I discovered concerning variations in preparedness, constrained budgets forcing impossible choices between system upgrades and security measures, and troubling patterns of unexplained system outages without proper incident response protocols. When hospital networks experience attacks, I believe the impact transcends conventional cybercrime classification into something uniquely dangerous as real patients suffer when doctors cannot access critical data or life-saving equipment malfunctions.

CYBERWARFARE – PERCEPTION OF THE EMERGING CYBERWARFARE

Key points in my research:

- Healthcare is among the top 10 most targeted sectors according to CrowdStrike's 2025 Report
- Denmark's extensive digitalization creates both opportunities and unique vulnerabilities
- My research focuses on the human impact of compromised healthcare systems rather than just financial or data protection concerns

Research Questions:

- **RQ1**:How digitization aids hybrid warfare campaigns and challenges Danish cybersecurity governance?
- **RQ2:**How geopolitical tensions influence cyberwarfare evolution against Denmark?

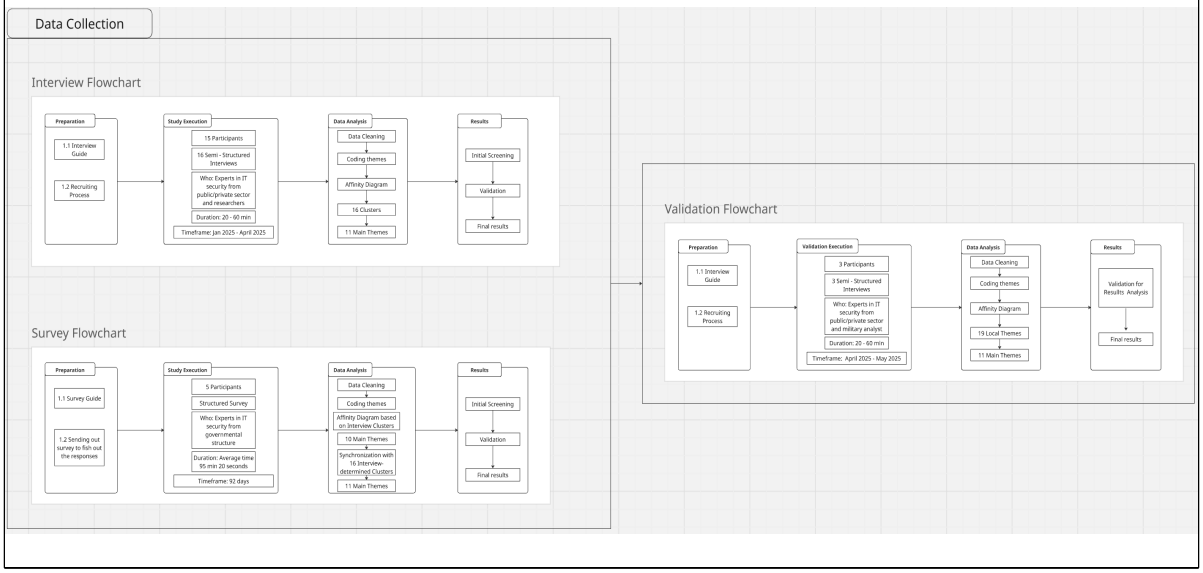
Main findings:

- Significant variations in preparedness and incident response capabilities
- Budget constraints forcing difficult choices between system upgrades and security
- Troubling patterns in security incident reporting, with some facilities experiencing unexplained outages without proper protocols to determine their cause

The blurred boundary between cybercrime and cyberterrorism when healthcare systems are attacked, suggests that the impact on human life should be a key consideration in how these attacks are classified and addressed.

Cyberwarfare refers to coordinated digital assaults targeting nation-states, inflicting damage comparable to traditional military conflicts by compromising essential computer networks. It can be considered hybrid warfare tactics - navigating technology with intention of spying and destroying valuable assets. These digital offensives pursue various strategic aims, from intelligence gathering and infrastructure sabotage to manipulation of public opinion.

METHODOLOGY FLOWCHART:



DATA COLLECTION:

Key Questions for the Interviewees:

For Healthcare IT Security Specialists:
•How vulnerable are Danish healthcare systems to hybrid warfare tactics that combine cyberattacks with disinformation?

For Academic Researchers:
•How has Denmark's rapid digitization affected its vulnerability to cyberwarfare?

For Private Sector Cybersecurity Professionals:
•What hybrid warfare tactics targeting private infrastructure have you seen or anticipate?

Follow-up Question for All Participants:
•What lessons could Denmark learn from Ukraine's cybersecurity experiences during the ongoing conflict?

Validation Questions for My Study:

1.Theory Validation Question:
1. "Based on my research hypothesis that digitization increases vulnerability to hybrid warfare tactics, do you find this framework accurately reflects the cybersecurity challenges Denmark faces? What elements might be missing or overstated?"

2.Methodology Validation Question:
1. "This study approaches cybersecurity threats through the lens of expert interviews across healthcare, academia, and industry. What additional perspectives or data sources would strengthen the conclusions about Denmark's cybersecurity posture against geopolitically-motivated threats?"

Survey was focused on the cyberwarfare tactics that Russia employes in Ukraine and how Ukraine fends from their attacks. With focus on Ukraine's experience that should be implemented in Danish systems.

My research uncovered significant data selection bias in how experts assess cybersecurity risks.

I noticed regional experts reported different threat perceptions than university researchers, and information asymmetry widened perception gaps between practitioners and researchers.

I found practitioners possess knowledge of incidents that never reach academic literature due to confidentiality agreements and operational constraints.

Operational priorities clearly shaped which threats received attention - private sector facilities prioritized different threats than public institutions. Resource allocation decisions also influenced which threats were emphasized in their reporting.

This divergence likely stems from several interconnected factors I identified. Regional security experts operate within specific operational contexts, responding to immediate threats, while academic researchers approach security from broader theoretical frameworks.

INVESTIGATION OF EMERGING CYBERWARFARE IN DENMARK

Outcomes of Qualitative analysis:

Digital Paradox: Denmark's position as one of the world's most digitized societies creates both unprecedented opportunities and significant national security vulnerabilities, especially through centralized systems like MitID that represent single points of failure.

Trust-Security Conflict: Denmark's high-trust culture fundamentally clashes with effective cybersecurity practices that require skepticism and verification, creating a unique vulnerability that technical solutions alone cannot address.

Evolving Geopolitical Threats: The shifting geopolitical landscape has transformed Denmark's security environment, with nation-states employing distinct threat patterns: China focusing on intellectual property theft, Russia on geopolitical disruption, and North Korea on economic cybercrime.

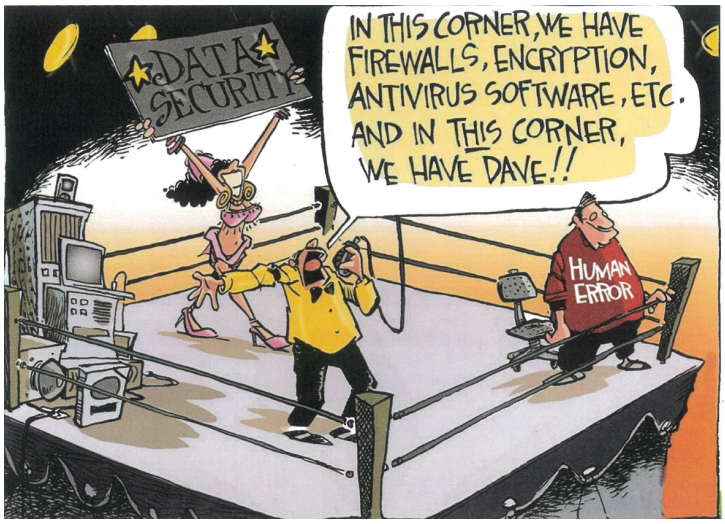
Balanced Resilience Approach: Future cybersecurity in Denmark requires balancing continued digital innovation with enhanced security resilience through technological solutions, organizational adaptations, professional education, and public awareness.

Dynamic Security Ecosystem: Digitization represents a continuous trade-off where security vulnerabilities coevolve with opportunities, requiring adaptive frameworks that preserve digital benefits while effectively mitigating emerging risks in an unstable geopolitical environment.

DIGITALIZATION – IS SALVATION OR DEMISE?

Emerging vulnerabilities and threats caused by digitalization followed by human error?

My evidence shows that digitization creates neither salvation nor demise exclusively, but instead forms a dynamic ecosystem where opportunities and vulnerabilities coevolve.



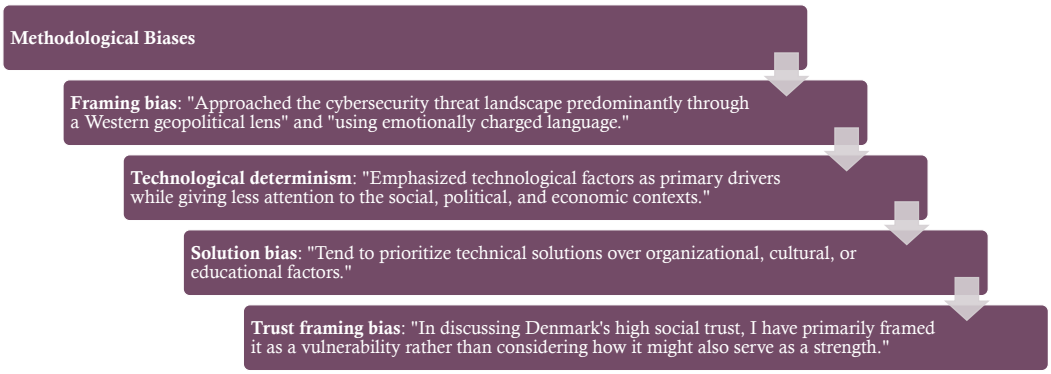
During the reflection upon the insights harvested by my research, a very provocative question emerged, demanding
deeper contemplation: "Digitization - is salvation or demise?" in the context of Danish cyberwarfare. Based on
my comprehensive interview and survey data, I can now conclude that this question captures the complex reality
revealed through my research. The evidence demonstrates that digitization creates neither salvation nor demise
exclusively, but rather establishes a dynamic security ecosystem where opportunities and vulnerabilities coevolve.
My findings reveal that Danish digital transformation has created a specific security environment where increased
connection between simultaneously enhances service delivery and expanded attack surfaces the effective response.
The accelerated digitization of society presents a double-edged paradigm: while it undeniably enhances operational
efficiency and creates innovative solutions which address arising challenges, at the same time it introduces systemic
vulnerabilities through increased technological dependencies. The significant

increase of digital frameworks aiding
the infrastructure across various sectors has skyrocketed the delivery of substantial benefits for both social and
financial solutions, yet this transformation has created an expansion in attack surface that sophisticated adversaries
can exploit through evolving cyberwarfare tactics. As digital systems become integrated into essential infrastructure
and services, following the emerging traits, the potential impact of successful cyberattacks grows proportionally
to it. This creates asymmetric advantages for adversaries who can leverage relatively modest resources to achieve
significantly disruptive effects. This technological integration creates a fundamental security paradox where digital
innovations that strengthen economic competitiveness and enhance quality of life also generate new vulnerabilities
while these systems are targeted with malicious intent. Consequently, policymakers and security professionals
must carefully evaluate the strategic tradeoffs between digital advancement and security resilience. Particularly
when cyberwarfare capabilities continue to evolve and become sophisticated. This tradeoff in assessment requires a
profound understanding of how digital dependencies shape national security with consideration and how protective
measures can be implemented without undermining the social benefits that digitization offers. Strategic security
frameworks must, therefore, incorporate both technical safety strategies and organizational resilience to effectively
manage the inherent tensions between digital innovation and vulnerability mitigation in an environment where
cyberwarfare represents an enduring security challenge.

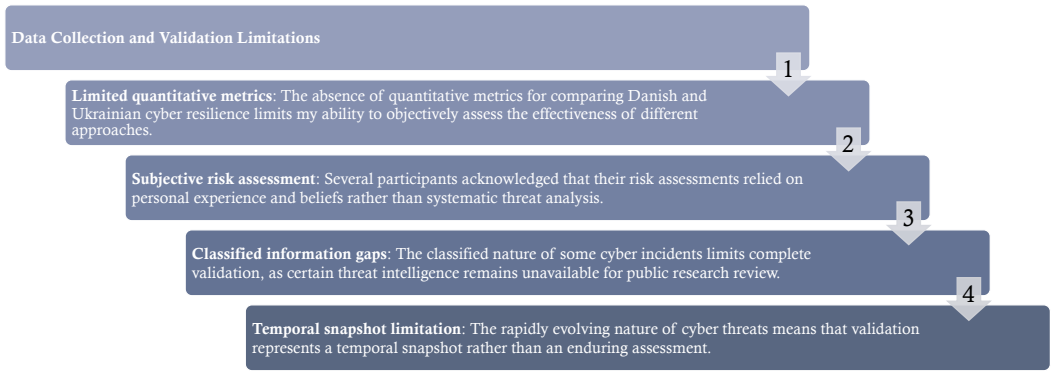
FINDINGS

- I found that my initial research on human-factor vulnerabilities was strongly validated by all participants, confirming that the human element represents the primary vulnerability across systems and organizations. My validation interviews revealed that "employees are both the greatest strength and greatest weakness of any organization," with studies showing 85-90% of cyber attacks resulting from human error. I documented concrete examples of security lapses, including approximately 40% of employees failing to lock computer screens when leaving workstations - equivalent to leaving a home's front door wide open. My research identified that CEO scams and phishing emails remain highly effective tactics, comparable to catchy advertisements that exploit personal information. I observed some organizations implementing innovative approaches like reward systems offering candy to employees who follow security protocols, though these efforts are hampered by limited training time, with some companies allowing only 40 minutes annually for security awareness training. This significant gap between identified vulnerabilities and mitigation efforts presents clear opportunities for developing more robust awareness campaigns and modern threat education.
- I also discovered that Denmark's position as one of the world's most digitized societies creates a dual complex of opportunities and vulnerabilities in the face of emerging hybrid warfare threats. My research revealed how centralized authentication systems like MitID represent single points of vulnerability, while legacy systems persist in healthcare due to budget constraints rather than technical limitations. I found that Denmark's trust-based culture creates unique cybersecurity challenges that conventional security frameworks struggle to address, as this cultural factor often contradicts cybersecurity practices emphasizing skepticism and verification. My analysis showed how the evolving geopolitical landscape has transformed former allies into potential adversaries, with different nation-states presenting distinct threat patterns requiring tailored defensive approaches. Looking forward, I conclude that Denmark must balance digital innovation with enhanced security resilience through technological solutions, organizational adaptations, ethical policies, and international cooperation, recognizing that digitization represents a dynamic trade-off where opportunities and vulnerabilities coevolve in an unstable geopolitical environment.

METHODOLOGY BIAS:



DATA COLLECTION BIAS



BIAS IN RESULTS:

Cognitive Biases

- **Expert bias**: "Expert bias is unavoidable - particularly when professionals have institutional interests or are constrained by confidentiality requirements regarding specific security incidents."
- **Confirmation bias**: Reflected in "echo chamber effect where similar viewpoints reinforce one another" when relying heavily on Danish and Ukrainian experts only
- **Availability bias**: "The availability of statements likely influenced how threats were prioritized, with participants emphasizing incidents like the water facility attack mentioned by P12 over more common but less sensational threats."
- **Optimism bias**: "Particularly pronounced in organizations that had not yet experienced significant security incidents, potentially skewing their risk assessments."
- **Crisis amplification bias**: Emphasizing dramatic worst-case scenarios, such as "the panic of not being able to get personal documents, use healthcare benefits, or receive emergency help" potentially "completely ruin[ing] the whole system."
- **Recency bias**: "Analysis focuses heavily on current and emerging threats with less historical context about how Denmark's cybersecurity posture has evolved."

Social Data Biases

- **Sampling bias**: "The relatively small sample size, particularly of participants from Ukraine, limiting the generalization of findings."
- **Representation bias**: "The study's focus on senior decision-makers may have overlooked important perspectives from technical practitioners and end-users."
- **Cultural bias**: "My proposed solutions often reflect Western cybersecurity paradigms and practices" and "Danish cultural context may limit generalizability of some findings to other national contexts."
- **Temporal bias**: "My research captures perceptions at a single points' time rather than tracking how they change in response to new threats or experiences."

BIAS BASED ON PERSONAL BACKGROUND

As a Ukrainian citizen conducting this study during an ongoing full-scale war with Russia, I acknowledge that my personal experiences and perceptions have unavoidably shaped this research. Having directly witnessed cyber attacks and hybrid warfare tactics deployed against Ukrainian infrastructure, institutions, and citizens, I bring a particular perspective to the interpretation of data that should be transparent to readers.

My firsthand exposure to cyber terror incidents - including disinformation campaigns, critical infrastructure disruptions, data breaches, and coordinated hybrid warfare tactics that include cyber attacks followed by physical damage. This experience provided me with practical knowledge that influenced how I approached this study, from the formulation of research questions to data analysis and interpretation of findings. While this experience offers valuable insights that might not be accessible to researchers without similar exposure, it also introduces potential interpretation bias.

OPPORTUNITIES FOR FUTURE RESEARCH

Longitudinal studies: Cohort studies that could track how perceptions of digitization's risks and benefits evolve over time.

Multi-stakeholder approach: Future studies should expand the participant pool to include more diverse perspectives from both practitioners and researchers.

Empirical analysis: Future studies which can incorporate data regarding security breaches, attack patterns, and response effectiveness would complement the qualitative insights.

Structural geopolitical approach: Broaden the perspective of the research to study more structural approach by connecting the cyberattacks to the emerging geopolitical conflicts.

THANK YOU FOR YOUR ATTENTION!