Interview Guide: Cybersecurity and Cyberwarfare in Denmark

1 Introduction

Thank you for participating in this research study on cybersecurity and cyberwarfare in Denmark. This interview explores how digitization enables hybrid warfare and challenges Denmark's cybersecurity governance, and how geopolitical tensions reshape cyberwarfare threats facing Denmark. Your insights as an expert in your field are invaluable to this research.

Before we begin, I want to confirm your consent to participate and record this interview. All information will be handled confidentially, and your identity will be anonymized in any publications or reports. You may withdraw from this study at any time without consequence.

2 Tailored Questions by Expert Category

2.1 For Healthcare IT Security Specialists

2.1.1 Current Threat Landscape and Operations

- How does your company ensure the security and integrity of hospital IT infrastructure against evolving cyber threats?
- What are the biggest cybersecurity challenges facing Danish hospitals, and how does your company mitigate these risks?
- How has your approach to security changed since the increased geopolitical tensions in Europe?

2.1.2 Digitization Impacts on Healthcare

- How does digitalization in hospitals impact data security, particularly regarding sensitive patient information such as CPR numbers?

- What security challenges arise when integrating new digital solutions into hospital IT systems?

- How has the transition from NemID to MitID affected security operations in healthcare environments?

2.1.3 Governance and Compliance

- How does your company collaborate with national and international cybersecurity agencies to protect hospital infrastructure?

- What are the key considerations when ensuring compliance with GDPR and other data protection regulations in hospital digitalization efforts?

- How effective do you find Denmark's current cybersecurity governance frameworks for healthcare institutions?

2.1.4 Geopolitical Factors and Hybrid Warfare

- Have you observed changes in attack patterns following Denmark's support for Ukraine?

- How vulnerable are Danish healthcare systems to hybrid warfare tactics that combine cyberattacks with disinformation?

- What specific threats do you believe are targeting healthcare infrastructure due to geopolitical tensions?

2.1.5 Future Challenges and Preparedness

- How does your company balance the need for accessibility and usability with strong cybersecurity measures?

- What future trends do you foresee in hospital cybersecurity?

- What additional resources would strengthen healthcare cybersecurity against state-sponsored threats?

2.2 For Academic Researchers (Example: Dan, Professor specializing in election security and cyberwarfare)

2.2.1 Research Perspectives on Danish Cybersecurity

- What are the most significant cyberwarfare threats facing Denmark today, and how do they compare to global trends?
- How do your research findings on election system vulnerabilities translate to other critical infrastructure in Denmark?
- What methodologies do you use to evaluate cybersecurity risk in national infrastructure?

2.2.2 Digitization and National Security

- How has Denmark's rapid digitization affected its vulnerability to cyberwarfare?
- What cryptographic or security protocol developments from your research are most relevant for protecting Denmark's digital infrastructure?
- What theoretical frameworks best explain the relationship between digitization and hybrid warfare vulnerability?

2.2.3 Election Security and Critical Infrastructure

- Based on your research into US election system vulnerabilities, what potential weaknesses exist in Denmark's digital voting processes?
- What parallels exist between election system vulnerabilities and risks to other critical digital infrastructures, such as healthcare?
- How would you assess Denmark's preparedness for cyber threats during election periods?

2.2.4 International Dimensions

- What role does Denmark play in international cybersecurity research and collaboration against cyberwarfare?
- Which hacker groups or nation-states pose the biggest cyberwarfare threats to Denmark?

- How does Denmark's position within NATO and the EU influence its cybersecurity strategy and threat profile?

2.2.5 Academic Contributions to National Security

- How should academic research inform Denmark's cybersecurity policy development?
- What gaps do you see in Denmark's approach to cybersecurity education and awareness?
- What research directions would most benefit Denmark's cyber resilience in the next five years?

2.3 For Private Sector Cybersecurity Professionals (Example: Lukas, Infrastructure Specialist)

2.3.1 Private Sector Experience and Challenges

- How does your industry's cybersecurity approach differ from public sector approaches?
- Can you describe your experience dealing with cyberattacks in critical infrastructure environments?
- What has been the most challenging cybersecurity incident you've handled, and what lessons did you learn?

2.3.2 Technical Approaches and Incident Response

- How do you assess and prioritize threats in your infrastructure environment?
- What tools and systems do you rely on for intrusion detection and prevention?
- Walk us through your approach to managing a ransomware attack on critical systems.

2.3.3 Digitization Impacts on Business Security

- What digitization-related vulnerabilities concern you most for Danish businesses?

- How has the transition from NemID to MitID affected your security operations and user experience?

- How do you secure legacy systems that can't be easily patched or updated?

2.3.4 Geopolitical Factors and Business Impacts

- How has the threat landscape changed since the Russian invasion of Ukraine?

- Have you observed changes in attack patterns that might indicate geopolitically motivated targeting?

- What hybrid warfare tactics targeting private infrastructure have you seen or anticipate?

2.3.5 Public-Private Collaboration and Future Trends

- How effective is information sharing between private companies and government cybersecurity entities in Denmark?

- Where do you see cybersecurity for critical infrastructure evolving in the next 5 years?

- What emerging threats do you think are currently underestimated by Danish enterprises?

3 Follow-up Questions for All Participants

- Based on your experience, what cybersecurity recommendations would you prioritize for Denmark's national strategy?

- What lessons could Denmark learn from Ukraine's cybersecurity experiences during the ongoing conflict?

- How do you see Denmark's cybersecurity landscape evolving over the next 5 years?

- What additional resources or governance frameworks would strengthen Denmark's cyber resilience?

- How do you evaluate the security implications of Denmark's digital authentication evolution (NemID to MitID)?

4 Closing

- Are there any other aspects of cybersecurity or cyberwarfare affecting Denmark that we haven't discussed?
- Would you be willing to review your interview transcript for accuracy?
- Who else would you recommend I speak with about these topics?
- Thank you for your valuable insights and time.

5 Implementation Notes

This interview guide is designed to be semi-structured, allowing for:

- Follow-up questions based on participants' responses.
- Adjustment of questions based on the participant's specific expertise and experience.
- An average interview duration of 20-60 minutes.
- Recording with consent and later transcription.
- Removal of identifying information from transcripts.
- Creation of a conversational atmosphere where participants feel comfortable sharing detailed insights.

The questions are tailored to each expert's background while ensuring all interviews contribute to the core research questions about digitization's role in enabling hybrid warfare and how geopolitical tensions are reshaping cybersecurity threats facing Denmark.