Expert Interview Guide: Cybersecurity and Hybrid Warfare Research Validation

1 Introduction

Thank you for taking the time to review my research on digitization's role in hybrid warfare campaigns and the challenges to Denmark's cybersecurity governance frameworks. Your expertise is invaluable in helping me understand the impact and utility of this work. This interview will take approximately 20-60 minutes.

2 Background Context

- **Research focus:** Examining how digitization facilitates hybrid warfare campaigns against Denmark and analyzing the cybersecurity governance challenges in response to these threats.
- **Key findings:** Regional disparities in threat perception, critical infrastructure vulnerabilities, human factors in cybersecurity, and governance fragmentation.
- **Geopolitical context:** Tensions with Russia, China, and other actors influencing Denmark's cybersecurity posture.

3 Interview Questions

3.1 Research Scale Assessment

1. **Digitization Vulnerability:** "My research suggests Denmark's high digitization level creates unique security vulnerabilities. How might this perspective be incomplete or misguided? What counterarguments should be considered?"
2. **Trust-Security Paradox:** "I've identified a tension between Denmark's trust-based culture and cybersecurity requirements. What nuances or alternative interpretations might I have overlooked in this analysis?"
3. **Infrastructure Design:** "My findings suggest centralized digital systems represent significant vulnerability points. What evidence or cases might contradict this conclusion or suggest a more complex reality?"
4. **Human Factors:** "The research emphasizes employee awareness as a critical security factor. What other perspectives might challenge the primacy of human factors in cybersecurity outcomes?"
5. **Multi-Vector Threats:** "I've documented patterns in hybrid warfare tactics against digital infrastructure. What alternative explanations might account for these patterns, or what important dimensions might be missing from my analysis?"
6. **Governance Frameworks:** "My research identifies fragmentation in Danish cybersecurity governance. What strengths might exist in the current approach that my critical assessment may have undervalued?"

7. **Foreign Dependencies:** "The findings highlight risks associated with dependency on foreign technology providers. What countervailing benefits or mitigating factors might make this concern less significant than presented?"
8. **Ukraine Comparison:** "I've suggested Denmark should adopt specific lessons from Ukraine's cybersecurity experience. What limitations or contextual differences might make this transfer of approaches problematic?"
9. **Threat Attribution:** "The research makes certain assumptions about threat actors and their motivations. What biases or oversimplifications might exist in these attributions?"
10. **Resilience Strategies:** "My conclusions advocate for specific resilience measures. What trade-offs, limitations, or alternative approaches deserve greater consideration?"

3.2 Future Directions

1. Based on this research, what emerging threats do you believe warrant further investigation in the Danish context?
2. How might Denmark better leverage international cooperation based on the findings of this research?
3. What follow-up studies would be most valuable to build upon this work?

3.3 Concluding Reflections

1. How would you summarize the contribution of this research to Denmark's cybersecurity posture?
2. What recommendations would you make to strengthen the impact of this research?
3. Is there anything else about the research that you'd like to discuss that we haven't covered?

4 Thank You

Thank you again for your time and insights. Your expertise is invaluable in helping refine this research and enhance its practical utility for Denmark's cybersecurity community.