Interviewer: Thank you so much for taking time to review my research on digitalization'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 20-40 minutes. What were your first thoughts after reviewing my research on Denmark's cybersecurity posture and hybrid warfare vulnerabilities?

Expert: After reading what I read, I feel that we are on thin ice. The feeling that we are on much thinner ice than I realized. We have a lot of complexity built into our society that is very vulnerable.

Interviewer: Which findings or insights from my research resonated most strongly with your professional experience?

Expert: What I was often thinking about was the centralization of IT competencies at the university. You get more and more a single point of attack, in my view. What you describe is that we have many different systems. That's good in a way, but in another way it's not. It's a dilemma - if everybody had their own security system, it would be harder for an enemy to have a widespread attack. But all those small systems are not well developed and must have lots of errors, so they are weak. Somehow you have to find a balance, and I'm not sure what the right balance is.

In some places you used the word "proportional" - as the complexity of our systems grows, the dangers grow proportional to that, or the security measures that have to be taken grow proportionally. I wondered if that's actually true. Could it be that the amount of measures you have to take grows much faster than proportional? Every addition to our already complex system might exacerbate the security problem much more, so perhaps we should think twice before using that extra component.

Interviewer: What aspects of the research surprised you or contradicted your previous understanding of Denmark's cybersecurity landscape?

Expert: I wasn't particularly surprised or contradicted by anything. But there is an interesting point about our trust-based society. The trust doesn't go so far that we get informed by everybody because they trust us. We do not get information from our IT department about the threats they have seen, which I think would be very interesting for us lower in the pyramid to know. Instead, the policy is to ask all employed people to take a course every now and then in security measures, to learn rules about how to keep your data safe. The information that they have closer to the dangers doesn't trickle down to us. So there's a lack of trust in a way, but perhaps there's a risk in sharing that information with us. That's the contradiction, I think.

Interviewer: How useful do you find this research for understanding Denmark's current cybersecurity challenges?

Expert: I think it's very useful because the researcher is both close to the hot spot in Europe and this hyper-digitized society. So that's a very nice place to be for a researcher. It makes it relevant.

Interviewer: How does this research complement or challenge existing knowledge about the hybrid warfare tactics targeting Denmark?

Expert: I think it was unwise for postal services to stop bringing letters around because you need something to fall back on. If our digital systems fail, we need letters again. We need this parallel system. The breakdown of lower technology things is concerning. Earlier there was talk about abolishing FM radio, and even earlier we had medium wave. I still have this radio from the 50s that was the Cold War era radio. You could always fall back on long wave and medium wave, but now it's impossible because those systems don't exist anymore.

Russia and the Soviets were flying jets with equipment that had tubes instead of transistors. That seemed very backwards, but their jets were not as sensitive as Western jets to electromagnetic pulse (EMP) from atomic bombs in the atmosphere. So perhaps that was a deliberate tactic they had.

Interviewer: Did the comparison between Denmark and Ukraine provide any valuable insights toward hybrid warfare?

Expert: Yes, we know that Ukraine has made a tiger jump in knowledge about hybrid warfare and that we have to learn from Ukraine. You pointed that out clearly.

Interviewer: What was your opinion about hybrid warfare tactics before you read my research? Did your opinion change after?

Expert: I hadn't thought much about it before, honestly.

Interviewer: Are there any specific threats or vulnerabilities that you believe deserve more attention than they received in the research?

Expert: What I was thinking about is parallel systems or backup systems. To keep things online, you could have parallel systems doing exactly the same thing but developed by completely different unrelated groups. That's very expensive - everything is twice as expensive - but it could tremendously improve security. In spacecraft, it's normal to have redundant systems. If one computer fails, we use the other one because there's always danger of cosmic rays hitting some transistors. You need this fallback.

I don't have the impression that our society has such fallbacks. Here on earth we are depending on digital methods, and if the app doesn't work, then many people suddenly have a problem. What are the procedures? Are we informed about them? Is it possible to get informed? There's a lack of information.

We have nice websites that pose everyday practical questions, like whether I'm allowed to cut my neighbor's tree that's hanging into my garden. It's interesting to read even if you're not in that situation. Websites like that could also address security problems, but you don't see it anywhere. Perhaps they exist, but they're not advertised as places you go to for security information. A place where you could learn about security problems that other people have experienced would be nice.

Interviewer: What would be your opinion about a bug bounty program for people who find problems in government systems but don't have proper channels to report them?

Expert: That would be very nice, yes.

Interviewer: What lessons from this research could be applied to enhance incident response capabilities in your organization?

Expert: We've been thinking about moving away from software packages from Microsoft, for example. I think that's something we have to do at the university, where we are Microsoft and Oracle dependent, along with other foreign providers. You pointed out the risks involved.

Interviewer: What's your opinion about Microsoft-based solutions as affected by geopolitical situations? How do politics affect your opinion on the software you use?

Expert: The political situation has changed my perspective. Before, I trusted Google, Dropbox, and a few other American companies. I know they make good products. But now I'm thinking perhaps we should use a European cloud system like NextCloud instead of Microsoft OneDrive. I use OneDrive for my workstation; we cannot use Dropbox at the university. But personally, on another computer, I use Dropbox. I'm now thinking more about switching to something else because of the political situation. But I also have my own backup system with hard drives at home.

Interviewer: Do you see the potential for the insights about foreign technology dependencies to influence strategic planning in Denmark's public or private sectors?

Expert: Yes, and I think that's already happening. I hope so, at least.

Interviewer: As you mentioned before, a lot of public infrastructures are equipped with Windows-based solutions. If you were in charge, how would you change it?

Expert: That's hard. There are countries that use European office-based solutions. I use LibreOffice, and it has a long history already, but it's still not stable. I've had crashes with it lots of times, so there are hiccups in the software. It's challenging. But perhaps the debugging could be accelerated if a whole nation decided to use it. There are software systems that are hard to replace, so in that sense, Microsoft has a de facto monopoly.

Interviewer: How might Denmark better leverage international cooperation based on the findings of this research?

Expert: I think Denmark must keep this tradition of trust, but must also be more wary about becoming independent of other countries. Even Ukraine could turn on us. We like what Ukraine can do, but we should not become too dependent on them. The political situation in Ukraine is not stable. There's still a lot of corruption as far as I know. They are our friends and we have to learn from them, but we always need to be cautious and keep our eyes open.

This applies to many EU countries as well. We are perhaps a more vulnerable country than others because of our degree of digitization. As a small country, we have to be dependent on other countries; we have to cooperate, perhaps with countries of about the same size as Denmark, because they probably face similar situations.

Interviewer: How would you describe the current political stance of Denmark and how it affects the overall public opinion?

Expert: We are clearly in a kind of COVID-like period where people tend to support the government more than they did just a few months ago. We more or less agree about what the government is doing. We trust the government.

Interviewer: Would you confirm the research findings that Asia and the US right now are Denmark's main threats in hybrid warfare?

Expert: No, I think Russia is the worst threat, not the US and not China. China is interested in theft of information and technology, which is criminal. Russia is trying to influence elections secretly, while America does it more openly. I think Russia is the biggest threat.

Interviewer: Given the current political situation when Russia closely cooperates with the US, would you say this alliance creates a threat for Denmark?

Expert: Sure. Then we stand alone. But we are aware that they are allied, and that's partly why we're thinking of moving away from American software systems. It's not because we want to boycott, but it's also related to the confrontation between Denmark and the US about Greenland, which makes it clear that Denmark cannot trust too much on US systems.

But there's another layer - they already have our data from Facebook and other social media. Whether we move away from those systems or not, they still have that data. We can request that it's deleted, but they can simply refuse.

Interviewer: Would you say Danish society is sufficiently aware of the damage that digitalization can bring?

Expert: Obviously not enough. Because if people were aware enough, they wouldn't just use those systems. I don't use them, but I disagree with most Danish people on this.

Interviewer: How would you say cultural differences affect Danish society?

Expert: I'm not sure cultural differences mean that much in this context. If you're thinking about immigrants and non-immigrants, I don't think that makes much difference.

Interviewer: What recommendations would you make to strengthen the impact of this research?

Expert: A very short version that could appear in newspapers would be relevant. Perhaps a double-page article about this research, or being interviewed for the radio.

Interviewer: Which points would you recommend I emphasize when presenting my research? In my research, I discussed how hybrid warfare affects Danish society and Danish cyber warfare in relation to Ukraine's experience. Would you recommend expanding the research to other areas, for example using a different country?

Expert: Being Dutch, I've thought about extending this to other countries that aren't as far progressed in digitization. Germany would be very relevant because they're not as advanced with digitization. This research focuses on healthcare for a significant part, and I think going to the doctor in most countries south of Denmark is more complicated than in Denmark. But perhaps they have some approaches they should maintain nonetheless.

Interviewer: Would you say that the Danish healthcare system is overly digitalized?

Expert: No. My first experience with Denmark being different from the Netherlands was when I came here and had to get a CPR number. In the Netherlands, we didn't have personal identification numbers, which was a lesson from World War II where resistance fighters burned down population registries to make it harder for Germans to find Jews. So they destroyed these community offices, and for many years, introducing a personal number system was completely unthinkable.

Nowadays, due to digitization, we have a number when you turn 18, connected to taxes for example. So the principle has been eroded. I initially frowned upon having a CPR number - I have to keep it secret, but it's not very secret. Already there, I wondered if it was really safe, even before considering digitization.

What you describe in your text is that for immigrants, they're often assigned the same date - January 1st - which causes the system to malfunction because there are too many people on a single date. So exceptions have to be made, and you can't properly verify the number. As a software developer, I would say they should have modified the number system, perhaps added extra digits.

Interviewer: You mentioned the lesson that the Netherlands learned from World War II. Would you say countries that were differently affected by the war have different approaches to societal development?

Expert: Yes, it is a factor, though I cannot quantify it. There are many other relevant factors too. When Denmark introduced the CPR number, there was already movement toward European integration. The Netherlands, Belgium, Luxembourg, Germany, Italy, and France started what would become the EU, with the Benelux cooperation even predating that. They came together saying "never again this kind of war."

Denmark, however, wanted to stay outside. To this day, Denmark has exceptions to EU regulations. Denmark doesn't participate in the euro currency or in some military cooperation.

There were four exceptions made, and only because of those exceptions did the Danish population vote to join the EU. The Netherlands was much more willing to cooperate. I think that's a consequence of lessons from World War II. And we will draw lessons from the current war as well.

Interviewer: As a user of public transportation, especially the train system in Europe, how would you describe differences between the Danish train system and other countries? Are they more or less digitalized?

Expert: I think they're mostly the same nowadays. They've had an upgrade of signal systems in Denmark, and the same happens in other countries. Trains cross boundaries, so there must be some standardization of protocols. A few years ago, there was an issue with the train from Copenhagen to Hamburg that couldn't connect with the German control system, but that was just a hiccup.

Interviewer: Which challenges, in your opinion, are facing the Danish security systems?

Expert: The costs. That's something you wrote about that I hadn't thought about. The costs of hardening your systems can be higher than your budget allows. As users of IT systems, we don't get this information. We don't know how feeble the systems we are using actually are.

Interviewer: As an end user not directly involved in cybersecurity management and risk management, how would you describe your preparedness for a system collapse? How are you prepared for emergency situations?

Expert: I'm in a relatively easy situation because in our small group, we don't handle much personal data - mostly just texts. We do have some personal data like Zoom interviews that need to be anonymized, but it's not high-risk.

I think I could continue working without internet because I have lots of materials on my computer itself. If the university's system breaks down, I still have source code on GitHub. Of course, that system would also need to be down for me to be in trouble, but we have complete copies of the repositories on our workstations. I make backups of work-related data at home too. I think I have enough of a "prepper mentality" not to be worried about my work situation.

Interviewer: Would you say that Denmark is well prepared for hybrid warfare?

Expert: I'm afraid it's not. I would like to know what preparations exist, but we don't have that information as ordinary citizens.

Interviewer: Would you say that the government should inform society more about the risks that Denmark faces?

Expert: Yes, if it doesn't compromise security. If it's not too secret. We get basic information about emergency preparedness, like keeping some water at home. We're also advised to keep some physical cash, but they don't explain how to use it in case of system failure. I think we should have more information. For example, if I have 1000 kroner in banknotes, how do I effectively use them at shops if digital payment systems are down? I'd be out of money in a couple of days.

Interviewer: So you're saying the government should provide instructions for emergencies?

Expert: Yes, including guidance on how to access healthcare if systems are down.

Interviewer: In my thesis, I described experiencing system downtime myself.

Expert: Yes, you mentioned they called out names of people who weren't there. There should be fallback options, like using your passport or identity card. But if the computer is down and they can't see anything on the screen, it's still challenging.

I don't know much about health systems, but perhaps the web applications are too sensitive to breakdowns. If we had standalone apps, doctors might have a small database of their own patients, so they could still access patient history locally. But now the database isn't on their computer.

At the university, Microsoft's Office system is becoming more web-based. I have the 2010 version on my computer, and I think it works perfectly. Why should I change? Why should I have my documents on the internet? It's crazy.

Interviewer: How would you describe the development of artificial intelligence posing a threat for identity protection? My research discusses deepfakes and different AI tools that can compromise your identity. How can you know for sure that your identity hasn't been stolen and used against you?

Expert: You can't know for sure. We might be in a period of a few years where AI systems are being trained on real data but will become poisoned because there will be so much fake data that you can't be sure about what you're seeing or hearing. As a society, we will learn to distrust anything we see - any image will be distrusted. But right now, we're not fully aware and we're confused. It's definitely a threat. Personally, I don't want to work with AI.

Interviewer: You don't use ChatGPT?

Expert: I experimented with it when it first came out. I asked questions and requested sonnets and limericks, but it doesn't interest me anymore.