Interviewer: I'm working on research about the impact of hybrid warfare on Danish cultural aspects, with a focus on healthcare security. I've already conducted interviews with healthcare professionals in Denmark and received questionnaire responses from Ukrainian specialists. It's interesting to compare Danish and Ukrainian digitalization progress.

Expert: That makes sense. It's better to focus on a specific area like healthcare since it limits how much you can cover. I'm curious what you'll ask since I don't see myself as a cyber expert specifically, but I'm happy to help.

Interviewer: How do you think Denmark could defend against the hybrid warfare tactics that Russia is currently using in Ukraine?

Expert: The interesting thing about hybrid warfare is that it's not necessarily connected to other types of warfare. You can have hybrid warfare during peacetime or during hot conflicts like the current situation in Ukraine. Cyber attacks continue regardless of the conflict's intensity.

Ukraine is obviously a big target for Russia, but Denmark is also under constant cyber attacks. Danish cybersecurity professionals are continuously working to address these threats.

One of the interesting challenges is the problem of attribution in cyberspace. It's not always clear who is behind an attack, even when it appears to come from Russia. Is it state-sponsored or a criminal group? There's a blurring of lines with private actor involvement in warfare, which is very clear in cyber warfare.

Some private groups even benefit financially from attacks on Danish companies. The conflict in cyberspace is much more active than many people realize.

Interviewer: How would you comment on Russia's simultaneous hybrid warfare tactics? They attacked Ukraine's digital systems first and then physically invaded a few hours later.

Expert: It's often discussed that in modern warfare, the first wave of attack will be in cyberspace. It makes sense as an easy way to create chaos before exploiting that opportunity with physical forces.

Ukraine seemed quite prepared for this approach, so I don't think it had the effect Russia hoped for. This is likely due to Ukraine's eight years of prior conflict with Russia, during which they experienced severe cyber attacks. The Ukrainian cyber defense was prepared for the situation.

Overall, the effects of cyber warfare have been more limited during the full-scale invasion than many predicted. People expected devastating effects, but we haven't seen that materialize. Ukraine has managed these threats quite well, showing that proper preparation can mitigate cyber threats.

It's been interesting to see Ukraine also engage in offensive activities, with private actors and groups being encouraged to participate. We've witnessed quite a battle playing out in the cyber domain.

Interviewer: How would you assess Denmark's preparedness level for hybrid warfare?

Expert: It's difficult to evaluate cybersecurity readiness without being an insider, and those with knowledge are understandably reluctant to discuss details.

My impression is that Denmark's cybersecurity is primarily driven by concerns about criminal activity rather than state actors. However, the distinction isn't always clear, and being prepared for criminal threats may also help defend against state-sponsored attacks.

I believe cybersecurity is taken seriously in Denmark, but it would not surprise me if we have substantial security vulnerabilities that Russia could exploit if determined.

When discussing hybrid warfare beyond just cyber aspects, it's important to note that the number of vulnerabilities is so high that it's impossible to defend against everything. Resilience becomes crucial—the ability to quickly restore systems after an attack or have redundant alternatives in place. For example, if the electricity grid is compromised, having alternative power sources is essential.

I suspect some attacks on Denmark already come from Russia, but authorities may not publicize this. When transportation systems experience "malfunctions," there's a likelihood that some are actually cyber incidents. My impression is that Danish cybersecurity professionals feel constantly challenged and take the Russian threat seriously.

Interviewer: How would you comment on how digitalization supplements hybrid warfare and general military tactics?

Expert: Information technology is changing warfare on many levels. It's the technology driving drones, enabling battlefield management systems like Delta in Ukraine, and allowing ordinary citizens to contribute to warfighting efforts.

In the early days of the Ukraine conflict, civilians could take pictures of Russian tanks and send them through telegram bots. This technology involves all of society in warfare, raising questions about who's a combatant versus a civilian.

Smartphones function as multipurpose tools in modern warfare—they're computers for running military applications, cameras for intelligence gathering, communication devices, and news sources. This technology is fundamentally changing how wars are fought and contributing to the current stalemate where both sides have exceptional situational awareness.

Interviewer: Are people in Denmark aware of the risks that digitalization brings to both cyberspace and physical space?

Expert: I think there's generally a good understanding of these threats in Danish society and the military, which is a fairly digital, modern force.

However, I'm not sure people fully understand the consequences. In my recent video about drones on the battlefield, I discussed how people still see technology as enhancing rapid maneuver warfare, when in reality, what we're seeing in Ukraine is the opposite effect. The technology creates a situation where mobility becomes dangerous because detection leads to immediate targeting.

In Danish society, my greater concern is the dependency on American technology. These discussions about digital sovereignty are important, as we saw with the recent Microsoft outage that affected systems nationwide. When an entire country essentially runs on Windows, that creates significant vulnerabilities.

Interviewer: How would you comment on the geopolitical tensions between Denmark and formerly friendly nations like the US? How is the military responding to these developments?

Expert: Most people probably haven't fully understood the consequences of these changing relationships. Danes have taken the American security guarantee for granted for so long that it will take time to comprehend what it means if the US no longer protects us, which would embolden Russia in dangerous ways.

It's difficult when geopolitical situations are changing so rapidly, but these developments significantly increase the risk of conflict for Denmark and other NATO countries.

Interviewer: How do you view Denmark's collaboration with other European nations to prevent threats from countries like China and North Korea?

Expert: North Korea is actively fighting in Ukraine now, so they're clearly a concerning actor. Much depends on how relations develop with the United States. If American support wanes, European countries might look elsewhere for security arrangements, potentially opening up new discussions with China.

For Europe, I don't see China as the primary threat—it's quite clearly Russia. How we respond will depend on how the situation develops.

Interviewer: Has the Russia-Ukraine conflict changed your understanding of the relationship between conventional military operations and cyber warfare?

Expert: These domains overlap significantly. Modern information technology is transforming warfare, and cyber operations will play an important role in creating localized, time-limited effects.

For example, if Russia wanted to launch a major attack at a specific point, it might be advantageous for them to temporarily disable Ukraine's Delta system for 30 minutes. While Ukraine would likely restore the system quickly, that window might be sufficient for Russia to achieve tactical objectives.

We'll likely see increased attempts to coordinate actions across domains. The military concept of "multi-domain operations" addresses this coordination across different spheres, including cyber. It's about fighting in a way where you can leverage technology while denying that capability to your enemy at critical moments.

Interviewer: Which critical infrastructure sectors in Denmark would likely be targeted first based on patterns observed in the Ukraine conflict?

Expert: The obvious targets include electricity and telecommunications. However, attackers often focus on wherever they find vulnerabilities. If that's the water supply, that's what they'll target. I think target selection is largely vulnerability-driven.

Interviewer: What threats do you consider most dangerous for Denmark right now?

Expert: It's a very dangerous time overall. The risk that current tensions could develop into a wider war involving Denmark is higher than it has been for many years.

We're entering a period of perhaps the next ten years where Europe will still be struggling to build the necessary forces, as we neglected making proper investments for decades. Those investments are being made now, but they take time to materialize.

The next decade is particularly dangerous, especially while Putin remains in power. How the Ukraine conflict ends could either embolden or restrain Russia's future actions toward NATO.

Interviewer: How has the Russia-Ukraine war affected Europe and neighboring countries?

Expert: The war in Ukraine has revolutionized and permanently changed Europe's security landscape. The previous security order no longer exists. NATO is in its deepest crisis in 75 years, with some arguing that the alliance is becoming worthless.

These developments wouldn't have happened without the war in Ukraine. We don't know where this will lead, but hopefully we'll see a new European security structure emerge where Europeans take responsibility without depending on the United States. This should include greater focus on digital sovereignty and bringing technology under European control.

Europe isn't fully ready for this transition yet, but I hope we'll develop this new security structure, which should include Ukraine.

Interviewer: As a military analyst, what recommendations would you give researchers regarding which aspects of warfare to focus on?

Expert: There's currently significant focus on learning from Ukrainian experiences, which is appropriate. Referring to my latest video about drones, we're witnessing something that's changing the character of warfare fundamentally.

We need to understand that we can't fight the next war using NATO's current doctrine because it won't work against the technology Russia now possesses. We urgently need to determine how to deal with these technological changes, what our forces should look like, and what investments are needed to prepare properly.

Interviewer: What specific indicators should Denmark monitor that might signal an impending hybrid attack, based on patterns observed in Ukraine?

Expert: Hybrid attacks happen continuously, not as discrete events. Kilcullen's model for "liminal warfare" is useful here, describing different thresholds in hybrid space:

1. Detection threshold - Recognizing that something is happening
2. Attribution threshold - Gathering enough information to identify who is responsible
3. Response threshold - Having sufficient information for politicians to make decisions

We need to build systems that quickly elevate incidents through these thresholds. The detection and attribution thresholds require technical solutions, while the response threshold is organizational—requiring government agencies to communicate effectively, understand implications, and implement proper procedures.

We need both technical solutions and organizational readiness, with regular exercises to practice these responses.