Interviewer: So basically I'm more interested in your opinion towards how political aspects affect cybersecurity and cyber warfare in Denmark. Did you notice any drastic changes since the Russia-Ukraine war started or, for example, the election in the US?

Expert: It does affect us a lot, actually. The US election, not so much. That's more on a day-to-day basis. Of course, Trump's current policies are affecting everyone. But the US election was not a big deal for our part of the industry at least.

Expert: The Russian-Ukrainian war was a big deal because like Ukraine, we're also a target for cyber warfare. We have seen attacks, some from Russia and some deniable ones, from the gas main line incident to damaged cables, which involve Russian cyber fleet ships for the more physical damages.

We are seeing many attacks. Our water facilities had some Russian attacks recently. We're worried about attacks on power production. We had closed access from Ukraine and Russian websites way back, but when the invasion started, we decided to block all known Russian IP addresses and Ukrainian ones too. Not because we dislike Ukraine, but because Russia might try to blame them by using Ukrainian IP addresses to launch attacks.

We don't expect accessing specific Russian or Ukrainian IPs, but by blocking certain countries, we dropped a lot of attacks. Currently, I think our block list includes 47 countries we don't allow

Expert: I think we need a good way to block new Chinese AI systems like Deepsea Eagle, DeepMind, and a few others because the second someone starts putting data into them, it all goes to the Chinese. The AI race right now is quite scary because you have no clue what's going to happen and what data they steal. People don't think before they put data into AI just because they think they're using something friendly - but they're not.

Interviewer: What laws would be beneficial to introduce to protect citizens and users of AI systems and secure companies?

Expert: For AI, the European Union will have to make some general law decisions about how to handle AI in the European Union. I don't think that should be on a country basis - it will have to be European Union deciding, and that takes a while. It's going to take years, probably.

What we can do is implement some regulations on a country scale. For example, we had a massive problem with Chinese cameras because they might have backdoors. Most government functions in Denmark are not allowing official Chinese cameras and probably others. But again, that should probably be a European decision for EU/EEA member states.

Smaller things will be country-based, of course. Laws against attacking our power production or water production already apply, but I don't think we need to make new laws to protect us because the attackers don't care about the laws. We just need to secure our systems.

Interviewer: Would you say there is a distinction in the victimology of cyber attacks? Do people usually target women or men, or is there a specific demographic that suffers cyber attacks more?

Expert: It depends on the attack. If it's the normal "I'm a Nigerian prince, I have some money for you" scam, it doesn't matter. But other attacks target men or women differently depending on the type of attack and what they want to accomplish.

If they want money from men, they'll typically use tactics like "Hey, I have big breasts, I'm in a bikini, want to talk to me?" If it's women, they're often targeted by love scams. It's effective - I think last year the numbers showed they got around 17 million Danish kroner in 2023 from love schemes alone, and those mainly target women.

The attacks related to blackmail about what people are doing typically target men, saying "I recorded what's on your PC," or even worse, they actually talk to what seems to be a nice woman that turns out to be not so nice. That's a targeted attack on men.

I assume, and I'm guessing here based on news reports, that in a battle zone like Ukraine, they probably use destabilizing attacks mainly against women because the men are at war. If you can start saying "Let's attack the women, send them emails about their houses, and show them pictures of their children" to demoralize the population, that would be targeted against women.

Interviewer: What about children? Usually cyber attackers target hospitals - one reason could be the number of patients and creating disturbance in society. What is the main reason for attacking hospitals and critical infrastructure? Is it to create terror and scare people?

Expert: What we've seen with hospitals is, from what I've observed, mainly ransom-based ransomware attacks. Originally, criminals figured out that hospitals were a bad idea to target, and that lasted until about three years ago, because hospitals were only targeted as collateral damage.

The European Union and Interpol go quite hard against people who attack hospitals. There was an incident years ago when they attacked a German hospital by accident - they were supposed to target the local college or university but hit the hospital instead. A woman died during the transfer to another hospital, and Interpol clearly told the press that this was not investigated as a random attack but as manslaughter, which carries a quite different penalty. That was meant to discourage targeting hospitals.

That has changed because some attackers now don't care about direction - they just want the easiest target. But that's the ransomware part. I assume that if Russia or China were to seriously target us, they would find it more beneficial to target power plants and water infrastructure because that affects everyone, not just hospitals.

As for blackmail, that's probably more interesting for most countries - can they steal health information to use for blackmail? In the US, they use it for insurance fraud because cancer treatment can cost half a million USD. In Denmark with free healthcare, that's not as interesting - here it's more about blackmail potential.

Regarding children, I haven't heard about anyone targeting children specifically. Most attackers probably wouldn't do that, but of course, if someone in a children's ward clicks on the wrong email, it would affect that ward too. We're actually more focused on influencers targeting children for advertisements, which causes problems in the press occasionally.

Interviewer: What impact has the Ukraine conflict had on NATO's cybersecurity policies and international cooperation?

Expert: We have stood quite united against Russia. Since Russia frequently engages in cyber attacks and hybrid warfare, we've all had to improve our cybersecurity. Denmark is more of a target because we have supported Ukraine with quite a lot of money per capita compared to other countries, but we're all targets.

The European Union has worked to block Ukrainian and Russian funding, and we've confiscated Russian holdings where possible. Yes, we've all had to improve our cybersecurity, and we consider Russia a major threat. But I think most countries and companies in Denmark right now are assessing whether Russia can actually hit them, what they should worry about regarding Russia, and what they can do beyond blocking them and training employees to be vigilant.

Interviewer: What lessons can other nations learn from Ukraine's cyber defense strategies? Did you learn something from the cyber warfare between Russia and Ukraine, especially after last year's incident where the mobile network was down for days and people couldn't call doctors or access private institutions?

Expert: From my perspective, we haven't learned much from Ukraine's cyber defense specifically, because what you're describing is more about attacks on physical infrastructure rather than purely cyber threats. Of course, we've emphasized having backup systems, generators in case we lose power, and water supplies.

Our government has advised people to ensure they have food and water for three days, a radio, and so on, just in case something similar happens here. Personally, I would be just as worried about a major ransomware attack as I would be about Russia attacking our infrastructure. But that's more about physical preparedness. I don't have detailed knowledge of what Ukraine is doing regarding cyber protection specifically.

Interviewer: How would you say the political stance affects cyber warfare in Denmark? What is your opinion about Danish cybersecurity, since the level of cybersecurity risk was raised from low to medium in June 2024? Can you comment on recent cyber activity?

Expert: Interestingly, it hasn't changed much for our sector because you're referring to the general security warnings, but for our sector, the threat level has actually been high to very high for years before the conflict. It hasn't really changed for us because we were already at the maximum level. When you're already at the highest level, there's no higher to go when Russia invades Ukraine.

The official designation hasn't changed for us, but the focus from politicians has changed. Four years ago, we had just two people in the security department here. We've scaled up significantly, and our politicians have recognized that cyber attacks and security are serious problems. They're investing money in it, and everyone is doing that - not just the hospital sector.

Russia is not the only concern. The pressure from China is also a problem for our infrastructure. For companies, cyber security concerns are more about Chinese intellectual property theft or damaging attacks.

Interviewer: How does conflict in Asian countries affect global stability? Since there's conflict between China and Taiwan, China and the US, China and Russia - how does it affect the whole world?

Expert: It affects us greatly. There are many concerning countries in that region. North Korea, due to all the embargoes against them, basically only gets outside money from cyber warfare, and they have many skilled people doing it. They mainly focus on attacks in East Asian countries, including ATM attacks where they can extract large sums during a single night.

China is problematic because they're trying to partially support Russia while maintaining flexibility. North Korea is giving soldiers to the Russians, likely because they need money. China is in a halfway position, saying they might support Russia but could back out at a moment's notice.

If the US manages to broker a peace treaty where Ukraine essentially loses territory and Russia backs off - as Trump suggested recently - we're sending a clear signal to China that they can move on Taiwan without consequences. If the US and NATO back out of commitments, many nations will see an opportunity to take what they want. China will take Taiwan if allowed; they'll also pressure the Philippines and take some of their territory if permitted. It's not that they need more land, it's about power.

Interviewer: So you're saying that the stronger the need, the stronger the danger from Russia and China cooperating and creating new attack methods. But what's the reason behind these attacks? Is it income from ransomware or something else?

Expert: For North Korea, it's money. For Russia, it's land, power, and prestige. Putin wants to recreate the old USSR - he wants more land and all the former Soviet countries. For China, it's about intellectual property - they want to copy whatever they can get their hands on. If they can steal research on a new technology and produce it themselves, that's perfect for them. It's money in the form of intellectual property.

But if they can cause destabilization along the way, it increases their chances. If NATO falls apart, if Russia intimidates neighbors, if the US leaves international agreements - all of this signals weakness. If they can influence public opinion, for example, by boosting right-wing parties in Germany through false news and misinformation campaigns, they will do it because it increases their chances of success. Those parties would be less likely to support Ukraine or stand up to aggression later.

Interviewer: If NATO starts falling apart, what will unite countries or drive them apart? Will it be political issues or interests?

Expert: If NATO falls apart, Russia will, at minimum, try to reclaim all former Soviet countries. That's Putin's dream. He might be limited because he's expended so much in Ukraine, losing many soldiers and resources. But North Korea just sent 10,000 soldiers, and China has a million-person military - one of the largest in the world. If Russia can rent Chinese soldiers for invasions, they'll have enough manpower that no one could stop them.

China likely wouldn't invade Russia's territory like Siberia since that would be counterproductive while supporting Russia. They also wouldn't go after India or Pakistan since both have nuclear weapons. Instead, they'd expand in other directions toward the Philippines, Malaysia, and similar areas. Russia would be the major land grabber in this scenario.

Interviewer: You mentioned the German election. How do political stances in different countries affect Denmark? For example, Trump came to power and proposed buying Greenland. How does this affect Denmark and Danish security?

Expert: It affects us greatly because when one country makes questionable decisions, it impacts everyone. Right now, Germany is talking about reinstating border controls, which means everyone commuting between Denmark and Germany will face greatly increased travel times. To be fair, we did the same a few years ago during the Syrian refugee crisis.

If far-right parties gain more power in Germany, they'll start pushing anti-immigrant policies and try to force other countries to take asylum seekers. We see this pattern everywhere. Look at Erdogan in Turkey, who essentially blackmails Europe by threatening to open the gates and let all refugees into Europe unless he gets money or concessions.

Even within the European Union, countries create problems like this. If some Eastern European EU countries start looking more toward Russia, that also affects us because it could begin the collapse of the European Union. If member states start leaving, it creates a domino effect. Look at the UK after Brexit - they suffered economically, which was a wake-up call for everyone else. Before that, there were many people in Denmark saying we should leave the EU, but that discussion stopped shortly after the UK left because we saw the consequences.

If Russia can influence public opinion through misinformation campaigns, it might affect some populations negatively.

Interviewer: You mentioned how if a population is somewhat "brainwashed," it's easier to control the nation. How would you comment on the situation in Russia where they don't have much access to the outside world and are locked in their own information bubble?

Expert: That is a problem because when you control information, you control the population. Russia is a good example. To be fair, they do have some internet access - they're not completely locked off. They're more controlled in the sense that people who complain tend to "fall out of windows" - there was a musician who reportedly fell out a window just two days ago.

Countries like North Korea don't allow their citizens any access to outside information - they're completely in a bubble. In such cases, the only way people can change things is through rebellion. Since the military is controlled by the government, this is extremely difficult.

In Russia, we saw the Wagner Group attempt something like that, marching halfway to Moscow before they were stopped. That scared the government because it showed what could happen if other military factions rebelled. This means the government must rely on military power and population suppression.

The general population doesn't have access to weapons, so they can't do much against military forces. In Denmark, we don't have access to arms either - if our government decided to establish a dictatorship with military support, we couldn't do much. The US would likely start a civil war in such a situation because the population is armed. It depends on the country.

But yes, if you can block people from getting reliable news or influence the news they receive, it creates serious problems. The Philippines is a good example. The Marcos family ran the country under martial law for about 20 years and stole billions of dollars before being ousted. But now, through misinformation campaigns, especially on platforms like Facebook that many Filipinos access for free on mobile phones, they've managed to rehabilitate their image. The average Filipino teenager thinks the Marcos family did great things and doesn't believe they imposed martial law for over two decades. This is despite the fact that it takes about five minutes on Wikipedia to learn what actually happened. But they managed to hide that history successfully.

Interviewer: How would you comment on the effect of Facebook and other social media on populations?

Expert: It's enormous. With the current political climate in the US, where Trump and tech media are essentially aligned, it's a problem. Even Musk's Twitter (now X) basically says "If we don't want something on the platform, we don't care." Last week there was a government agency that was not allowed to make public announcements on X.

In Italy during Berlusconi's time, he owned all the TV stations and controlled what they reported. The US is heading in that direction now - the more you can influence media, the worse things get.

In Denmark, people complain all the time about bias in media, but I don't think we're that bad. We have laws requiring truth in reporting. Of course, the depth of research varies by outlet, but generally we have relatively unbiased media in Denmark. The serious newspapers do okay, and most online or TV-based news is acceptable.

The problem is that social media makes it so easy to confuse people, and many have lost their critical thinking skills. People don't fact-check information anymore, and Russia is actively exploiting that weakness right now.

Interviewer: So basically, how does it interfere with cyber warfare? Is it one way of criminals to contact the society or one way of manipulating?

Expert: It's not affecting cyber warfare directly. These are more disinformation campaigns to affect public opinion. Criminals are abusing it in some way to try to steal money—for example, creating fake stories about political figures to get people to click malicious links.

But generally, they're using traditional methods. The bigger concern is nation-state attacks or information campaigns. It depends on how you define criminal gangs. Russian state actors, for instance, don't conduct cyber warfare directly. Instead, they use criminal groups to do it for them. Technically, the Russian state doesn't do much cyber warfare themselves—they just use groups that have this capability. So if you define those groups as cyber criminals, then yes, they conduct massive information campaigns, but these are state-sponsored and state-directed in practice.

Interviewer: You mentioned state-owned cyber groups. Are there any existing in Denmark?

Expert: In practice, yes, a little bit. Our defense center (CCA) and our military are recruiting cybersecurity specialists. We had one completely counterproductive situation a few years ago where an official went to the press and essentially said, "We're so advanced in cyber defense that we don't get attacked." That's basically inviting hackers to test our systems.

But yes, our military is recruiting cybersecurity talent, as they should. We need people who understand cyber defense. We also have both red and blue teams in our department. We need to understand what would happen if we were attacked.

We don't attack other nations, but we do defend ourselves. However, I'm confident some of our military engages in offensive operations in limited ways. For example, if we discover Russian hackers using servers in the Netherlands, we might work to take down that service or coordinate with Dutch police. That's technically a counterattack to defend ourselves, but not directly targeting critical infrastructure in other countries.

Interviewer: So you mentioned cyber gangs in Denmark. Do you have any members in the hospital who can help with cyber attack defense? Who are the main people who take care of it?

Expert: We don't have cybersecurity specialists among the regular hospital staff. You rely on our security department to handle this. When I asked one of our best programmers if he would join our security team, he said he'd be too paranoid—which I told him is exactly what we need! If you're not paranoid, you shouldn't be in our department.

We provide general security awareness training to staff, teaching them to be vigilant and cautious. But we monitor for suspicious activity. If one of our doctors, nurses, or other staff starts using hacking tools, we get notified and investigate immediately. We're implementing systems to detect this type of activity and will isolate machines from the network until we can talk to the user, because regular staff aren't authorized to use such tools.

We had an example yesterday where we detected one of our medical systems using PowerShell scripts to capture screenshots. Our supplier stores their data in Houston on their servers, so this could potentially involve sensitive patient data, which would be illegal. I contacted the department to investigate and discovered one of our doctors was documenting errors by taking screenshots. We had to explain this wasn't acceptable and would be blocked.

Interviewer: Who are the first responders to a cyber attack? Who is the first wave of emergency response team?

Expert: In our case, it's our Security Operations Center (SOC), which provides 24/7 surveillance and receives alerts. If someone reports a problem, they get the call and then contact our team during daytime hours. We recently discontinued our 24/7 on-call duty. After 4 PM, if an issue isn't urgent enough, it waits until the next morning when a designated person arrives and coordinates the response.

Interviewer: Were there any recent cyber attacks at the hospital?

Expert: Attempted attacks happen all the time—we block them continuously. We deal with the usual scams and phishing attempts. But we haven't had any major attacks affecting operations in quite a while. The last significant incident was in 2018.

When I started at the regional level, we had emergency response drills weekly. Last year we improved considerably, addressing not just cyber attacks but also infrastructure failures like power outages. We don't have many emergencies anymore.

The last notable incidents were DoS attacks where attackers used new techniques to flood our routers, preventing external connections. We had about 30 minutes of disruption before resolving the issue. But we haven't had anything significant in well over six months.

Interviewer: Can you tell me more about the major cyber attacks during your career? You mentioned the 2018 incident.

Expert: It wasn't a sophisticated attack—just basic ransomware. Our problem was that our enterprise security wasn't adequate at the time. Despite all our warnings, hospital staff continued to click on suspicious links.

From 2015-2017, we were attacked weekly. My boss and I would be restoring data constantly. Back then, antivirus software would simply check if a file was known to be dangerous—if it was new, it was assumed safe. Now enterprise security includes ransomware detection that identifies when processes are rapidly encrypting or modifying many files. That has prevented ransomware attacks since then, and we haven't experienced any major cyber incidents apart from that.

Interviewer: What were the key components of the emergency response plan?

Expert: You've already seen our basic plan. When an incident occurs, we gather in a designated room with all relevant personnel: communications staff to handle press inquiries, administrative directors, my department, and representatives from clinical departments. We coordinate tools and emergency procedures.

We work on two tracks simultaneously: a technical track focused on containing damage, investigating the cause, and restoring systems; and a communications track focused on keeping the press, users, and patients informed. We also implement emergency procedures so clinical work can continue.

We never stop treating patients. There are contingency procedures for almost every scenario. Of course, if there's a complete power failure because, for instance, a foreign actor compromised the power grid, we would need to evacuate patients. But with backup generators, we prioritize what services can continue operating.

Interviewer: You mentioned patients potentially being victims of cyber attacks. Can we discuss the specific hospital incident you mentioned last time?

Expert: Yes, there was a ransomware incident where one of our doctors was using network drives. The ransomware not only encrypted local files but also mapped network drives, including a connection to two Azure servers containing blood analysis results. The recent blood test data was encrypted.

We were able to restore it, but the server was unavailable during recovery. The biggest impact was on blood analysis—we couldn't access previous results temporarily and had to slow down processing new samples. Staff had to record results manually rather than uploading to the server while systems were being restored.

If there were critical blood tests needed immediately, we still had the physical samples and could repeat the analysis. So no patient care was compromised—we just had to spend extra time redoing some tests. Nothing was permanently lost.

Interviewer: Were there any similar incidents?

Expert: None that I'm aware of. We've been lucky, honestly. But realistically, with 50,000 users, many of whom aren't security-conscious, something will eventually happen despite our best efforts. The question is how we handle it and how prepared we are with emergency procedures.

We practice these procedures yearly at the executive level, and individual departments should conduct their own emergency training. Unfortunately, not all departments do this consistently. My wife's department recently did an emergency drill and discovered that all their backup materials were outdated and unusable. They realized they needed to implement procedures to update these materials every six months. Many departments don't have proper controls in place, but that's not exclusively an IT problem—it's a hospital-wide responsibility. We can advise them, but we can't force compliance.

Interviewer: You mentioned yearly training. Is there a better way to prevent people from clicking suspicious links? How would you advise someone who's been hacked on social media and doesn't know what to do?

Expert: Educating people through awareness training is critical. We require an annual IT security course for all staff. We create a new course each year, but we don't have enough resources to make it as comprehensive as we'd like.

We're limited in how much time we can require from staff. Currently, we're allowed 40 minutes per year for security awareness training. With 50,000 employees, if we asked for one hour, that would be 50,000 person-hours annually. Our leadership has to decide if that's justifiable given the impact on patient care.

Every time we hire someone new in my department, they ask why we don't conduct phishing simulation exercises. Technically, we know how to do this, but there are practical challenges. Even if we target just 5,000 employees (less than 10% of our workforce), many won't see the test emails. Some roles, like cleaning staff, rarely check email.

Of those who do see the phishing test, let's say 500 become concerned and call our helpdesk. That creates a sudden surge in the queue, potentially delaying assistance for nurses with actual clinical problems. We could staff up the helpdesk, but we operate with minimal personnel. Training temporary staff takes months, creating a cyclical staffing issue. To conduct a proper phishing campaign, we'd need to hire workers three months in advance—which won't happen without political approval.

Interviewer: Is there any threat hunting report that can be used in my bachelor thesis?

Expert: No, I'm not allowed to share those with you because they would reveal many of our internal vulnerabilities. These reports are not public. We would never be allowed to release this information.

The reality is that we're significantly behind in securing many systems. Our medical devices are especially vulnerable. Any public report detailing our weaknesses could be exploited. I can't share those documents, but I can confirm we conduct security assessments and are working to address the issues we find, though we can't fix everything.

Expert: For example, we have a pressure chamber used for treating diving sickness and difficult-to-heal wounds. Patients with complex wounds spend a few hours weekly in these pressure tanks with oxygen masks to accelerate healing. These chambers aren't replaced frequently—they last 30-40 years.

The vendor might support Windows 11 now, which is fine for new purchases, but what happens in 5-10 years? What about the following 20 years? We have equipment with a 30-year lifecycle, which means we need to find security solutions that work within those constraints. These challenges are substantial, and while we do what we can, we can't address everything.

Interviewer: So you're saying that outdated software and medical equipment with expired licenses are security threats?

Expert: It's both licensing issues and lack of technical support. License violations might result in fines from suppliers, but the bigger problem is when you're running Windows XP and can't update it.

We had a researcher who, due to EU requirements, needed to use specific software for genealogy and inherited disease research. This software was last updated in 1999 and only ran on Windows XP. We couldn't fix or update it—we had to provide an isolated XP machine.

The medical industry is improving, but they're only now waking up after 30 years of neglect regarding cybersecurity. We probably have about 2,000 medical devices in the hospital, and we don't always know what they are, how they're running, who's responsible for them, or if updates even exist. We lack the budget to upgrade even if upgrades were available. All of these are potential attack vectors.

The trend toward wireless connectivity complicates matters. Equipment manufacturers want everything on Wi-Fi—pacemakers sending data to servers to monitor patient health and adjust treatment remotely. This provides valuable capabilities but also introduces risks. If a pacemaker connects wirelessly, there's potential for unauthorized access. How do you patch a pacemaker? I don't know if you even can, and we can't run security scans on implanted devices.

Interviewer: For example, if someone gets a heart implant that connects wirelessly, is there a risk of unauthorized access to this medical equipment?

Expert: I haven't heard of actual attacks like that, but it's absolutely a potential risk. It's honestly just a matter of time—there have probably been some incidents somewhere already.

Let me give you a simpler example: I have sleep apnea and use a CPAP machine with built-in connectivity that reports data back to the hospital. Potentially, that could be hacked. If someone were to adjust the airflow settings on my CPAP machine, it could affect my sleep quality. Sleep apnea can lead to heart problems and even heart attacks, so tampering could potentially be dangerous.

I haven't heard of such attacks occurring, but they're certainly possible. The issue isn't just about likelihood—it's about possibility. "Unlikely" doesn't mean "safe"—it just means no one has figured out how to exploit it yet.

Consider another scenario: what happens when a terrorist group discovers vulnerabilities in common hearing aids that are now online and controlled by specific companies? Could they exploit these to cause malfunctions or generate massive sound pulses that damage hearing, then demand ransom to stop attacking customers? It's not an implausible scenario. It would be technically challenging, but something similar will happen eventually.

The security level on devices like infusion pumps is so low that these concerns can't simply be dismissed.

Interviewer: Should I mention this in my project or is it better left out?

Expert: You're welcome to mention medical device security risks in your thesis—it's a significant issue. If you Google "medical devices security," you'll find hundreds of pages of information. When discussing hospital cybersecurity, unsecured medical devices should definitely be addressed. It's well-documented and remains largely unresolved.

Interviewer: What's your technical opinion on the situation when the pagers were blown up in that terrorist attack?

Expert: It was a concerning development. I read somewhere that Israel has acknowledged responsibility, though I need to verify that information, so don't quote me on it. But what they did was essentially open the door to physical supply chain attacks.

Now we have to question whether any device has been tampered with or contains explosives. That applies to every piece of hardware you might give to any company or person in the world. Can anyone guarantee that Apple hasn't installed something dangerous in their devices? What we witnessed demonstrates that such attacks are now considered acceptable tactics.

This is particularly troubling because the next major attack might not resemble something like 9/11 with planes. Instead, it might target supply chains or infrastructure. The pager attack wasn't just someone intercepting a shipment—they infiltrated the entire production line. This is state-sponsored level activity.

Many electronic components come from countries like China. While I'm not specifically worried about consumer companies, government involvement could change that equation. If China decided to place malicious components in products manufactured in their factories, they could potentially do so. Israel's actions have essentially normalized this type of attack, and we'll likely see more similar incidents from various countries and terrorist groups in the future.

Interviewer: How did this affect the situation in Denmark? Have Danish hackers or terrorists been inspired by this, or is the threat still theoretical?

Expert: It doesn't directly affect individual hackers in Denmark because a single hacker can't execute these types of physical attacks. This is firmly in the domain of nation-states or very large, well-organized groups. Russia with state support could potentially do it, but we're currently blocking imports from Russia. China could also have this capability, as could certain other countries.

For us, it's more about limiting potential damage. For example, we're already concerned about Chinese cameras with potential backdoors. Now we have to consider whether devices might contain explosives or other harmful components. It raises questions about trust in the entire supply chain. I'm cautious about purchasing electronics from certain online marketplaces because there's no telling what might be inside them.

If someone wanted to create widespread disruption and destroy consumer trust globally, they could potentially sell compromised devices through popular platforms like AliExpress, Amazon, or Wish, and activate them a year later. That would severely damage consumer confidence. Tampered charging devices could be particularly concerning.

Interviewer: What do you think are the main threats to Danish society right now?

Expert: The primary threat is a cyber attack from Russia.

Interviewer: What exactly are the targets? What is the reason for them, and what are the main consequences that could arise?

Expert: My best guess is that if Russia wants to escalate, several scenarios could unfold. If the war doesn't stop and we keep supplying Ukraine while Russia becomes more desperate, Russian troops will likely target critical infrastructure like power plants. They might try to attack Danish waters and infrastructure in general.

We would be severely affected by such attacks—no power means no hospitals, no water, and other essential services disrupted. I wouldn't be as concerned about a direct attack on hospitals, as it would be more efficient to target infrastructure. If Putin wants to show the Danish people consequences for helping Ukraine, hospital attacks aren't as impactful as cutting power for three days. From a public ethics and opinion standpoint, infrastructure would be more strategic targets.

This scenario becomes more likely if Putin conquers Ukraine, either because Ukraine surrenders or if international support wanes. We recently saw a report indicating that if NATO doesn't increase military spending and Russia is allowed to rebuild over the next five years, Russia could start taking more countries. While Russia has lost many soldiers and rebuilding their population takes time, they could potentially receive manpower support from countries like China or North Korea.

Currently, we haven't been significantly targeted because Ukraine is Russia's primary focus. They don't need to move past Denmark, so they have little interest in doing more than sending signals or making small threats. They might briefly activate radar systems to demonstrate presence, but haven't done much else.

However, if multiple countries worldwide became involved in a war against Russia, the situation would change dramatically. Russian submarines would need to pass by Denmark, leading to sabotage, threats, and physical damage. During World War II, submarines were visible, but they're much harder to detect nowadays despite widespread monitoring systems. If such a conflict started, we would need sensors everywhere to detect incoming threats, and Russia would take countermeasures to prevent that detection, causing further escalation.

Regarding hybrid warfare, there's an interesting documentary about the Russian ship fleet. Data shows many ships in the Baltic Sea operating without tracking transponders. Russia owns numerous vessels, some registered under other countries. A few weeks ago, there was an incident involving two cables and a Russian-crewed ship owned by a foreign company.

These ships without transponders are virtually invisible unless physically spotted. We don't know what they're doing—possibly planting devices under cables or deploying buoys. They could be preparing for future attacks or setting up systems to disrupt communications or cause chaos. These activities aren't necessarily cyber attacks but components of hybrid warfare that would include cyber elements. If Russia needs to move ships or submarines past Denmark, we would likely see escalation of physical damage.

Interviewer: Are you knowledgeable about CrowdStrike? Would you advise using their materials in my bachelor thesis? I'm not sure if they're a reliable source.

Expert: Yes, CrowdStrike is a reliable source. They're a security company that can be trusted. Palo Alto's Unit 42 also produces good analysis. However, CrowdStrike lost some credibility recently due to a major incident where one of their updates crashed many machines worldwide, affecting numerous airports about half a year ago. It wasn't good—they lost approximately half their stock value in about a week and are still trying to rebuild their reputation. But I wouldn't say don't use CrowdStrike—they're generally reliable; they just had a particularly bad incident.

Interviewer: So you mentioned the attack on airports?

Expert: It wasn't an attack. It was CrowdStrike's enterprise software that caused the issue. They released a software update that triggered blue screens on almost every affected machine. The problem was that the only fix for over a week was to manually delete specific files from each machine.

If you have 3,000 servers, you would need to manually enter safe mode and delete files on each one. This is manageable for organizations with concentrated infrastructure and virtual machines, but if you have physical servers spread across large or difficult-to-access areas—like offshore wind parks where you need helicopters to reach platforms—you'd need to physically visit each location to implement the fix.

It wasn't a supply chain attack; it was just an unfortunate incident with a faulty update.

Interviewer: Thank you for your help today. I was really impressed by how political situations can affect even Denmark. I wasn't quite sure about that before.

Expert: We're a small country, but worldwide politics affects us significantly. Even something as simple as when Trump expressed interest in buying Greenland. In a normal situation, if someone threatened to invade your country, you'd firmly reject them. But since it's our biggest trading partner and ally, we need to be diplomatic. With the current U.S. administration, we're facing four interesting years of figuring out how these policies affect everything.

Decisions like withdrawing from the World Health Organization during an epidemic and preventing the healthcare system from reporting casualties affect everyone. No matter what we do, we're all impacted by these global political dynamics.

Interviewer: Thank you so much. Have a nice day.