Interviewer: So if it's not a problem, can you please introduce yourself a little bit?

Researcher: Sure. I'm a person in cybersecurity at Aalborg University.

Interviewer: As cyber threats become more sophisticated, how crucial do you think it is for educational institutions to integrate cybersecurity into their curriculums? And at what educational level should it begin?

Researcher: I think so far the discussion of cyber competencies has very much been about the need for more Researchers, which is truly a problem. But I think the bigger problem is the need for everyone working with IT, resilience, and management to have sufficient knowledge on cybersecurity as well. That's the more broadly distributed group who don't need to be Researchers but need to have good foundational knowledge. That is the big lift that we need to do. And I think it's education within IT education selection but also education within management and risk management.

Interviewer: There is a growing demand for cybersecurity professionals, but many industries are struggling with skills gaps. What strategies can be implemented to bridge this gap and ensure that Denmark has a strong pipeline of cybersecurity talent in the years to come?

Researcher: I think we need to differentiate between the need for talent and networks working specifically with cybersecurity and then the many who are not Researchers, where cybersecurity is not the primary job, but who need to have a good foundational knowledge in cybersecurity. We need to address both skill gaps, and the shortage is, of course, a bit different.

One important aspect of either strategy is to focus on both hiring talent. But there is a limited pool. So it's also very much about growing talent from the people you have - like continuing education, upskilling of people who are already in IT, but also upskilling of people who are not in IT.

Interviewer: I read online that you are the coach of the national cybersecurity team. Which advice would you give for people who have talent but don't have enough education in cybersecurity, how to implement their interest into the field?

Researcher: First of all, I think that we really need to do more in the educational system for those people who don't have the formal qualifications, but who have a lot of practical experience, who are self-taught, who actually have knowledge without the paper. We need to make much better pathways for them in education than we have today.

There is a large amount of people who may not have worked well in the traditional educational system, or have different interests, or preferred learning in different ways with computers. There is a large pool of talent that we don't usually utilize enough today.

For an individual today, I would recommend doing some of the better certifications, but also to search how you can get more formal documentation of your qualifications, for example, through continuing education, through master's degrees, to also get the papers.

Interviewer: How important are cybersecurity competitions like the Danish Cyber Championships in developing real-world skills among young people? And do you think they should be more widely promoted as part of formal education?

Researcher: I think the competitions are great. I don't think they can stand alone. They cater to one audience, and you have other audiences that need to be reached in different ways.

In the way that we do the Danish competitions, it's not only for the most competitive or for the very best, but we are also doing it with foundational courses, foundational online training sessions, and lots of beginner training sessions. We had one in ICU that was so sold out that we had to do another one in Copenhagen.

We have a lot of really good training for young people that's also applicable outside competitions. I think we make a good impact in making cybersecurity accessible and interesting. That's an important part as well. We create a community where young people who are interested in or becoming interested in cybersecurity can go and learn more together with others, rather than just sitting alone in the basement in front of their computers.

I think there is more potential in cybersecurity competitions than maybe we are using today. What we have been doing in Denmark over the last 3 or 4 years is a good example that other countries could learn from. Especially when you compare to the size of the population, we actually manage to involve a lot of young people.

We have just made surveys about how many students came to know about our initiatives with the championships, the national team, and the cyber perspective. Around two-thirds of the students in the actual cybersecurity education programs know about these initiatives. That's a really high number considering how much information people are exposed to and how many are studying security. So I think the visibility and the training are providing results.

Interviewer: With the increasing frequency of cyber attacks on a global scale, how do you believe government and institutions can raise awareness about the risks of cyber warfare and its implications for national security?

Researcher: I think there is not a single way to do it. You need to divide people into different target groups because you can reach people in different ways depending on their profession, age, and interests.

I also think you need to think of training for private digital security and safety, because the habits that you have at home and at work are connected. As we already started the conversation, it's important that you think about cybersecurity in the whole school and educational system, not only for specific cybersecurity training. You need to think about it already from primary school, maybe not as cybersecurity training specifically, but as digital competencies combined with security. But we also need to train and educate those who are not in the educational system.

Interviewer: What kind of training and resources are necessary for preparing both students and professionals to handle the complexities of cyber warfare? And how can Denmark enhance its preparedness against state-sponsored cyber attacks?

Researcher: Again, I think there is not a single answer to that question. It's really a mix of different training approaches and campaigns.

We talk a lot about role-specific training, and I think that also applies when educating the general population. You have some people who are highly skilled, and you have elderly people, many of whom are becoming victims of digital theft and fraud. You need to use different approaches to educate different groups.

It's really a mix of campaigns and having a range of training materials available. But protection is just one component of it. Of course you should prevent attacks from happening, but you also need to have the warning step. You need to help people when an attack is occurring. People need a place to go to where they can get help in a situation where a fraud is happening or where they're under attack, and that is for both individuals and businesses.

Interviewer: Is there an institution like this right now in Denmark? Is it CFCS?

Researcher: It is CFCS. And then I think the new ministry, MSP, is actually working in this direction as well. Before, responsibility was fragmented into different ministries, and now they're trying to consolidate it into a single ministry. But my understanding is that they're still shaping exactly what they're doing and how they're going to do it.

Interviewer: How can Denmark's cybersecurity education system be further supported by government policies to make it a national priority? And what role does the private sector have in this effort?

Researcher: This is a question that could take a lot of time to discuss fully. I think first of all, we need to integrate digital skills and cybersecurity in all education programs - especially cybersecurity in IT education and management education programs. That's one part of it.

We already talked about people who don't have the formal competencies but actually are really good. We need to have a more flexible educational system where you are not caught in dead ends, but you can always study further and have a place to go to become better, including in the formal educational system.

And then I think in general we need to invest more in IT education because we are lacking people in IT and we are lacking people in cybersecurity. So the current policy of cutting down on IT education is definitely the wrong direction to go.

Interviewer: As cyber warfare becomes a more prominent part of international conflicts, what ethical considerations should be included in cybersecurity education, especially in relation to the use of offensive cyber capabilities?

Researcher: I think the most important aspect is to discuss ethics as part of the education. But I think even more important is actually to build good communities for people interested in cybersecurity - good, healthy, positive communities. So people also get a good social network and stay on the good side of things, and don't use their skills in a bad way.

We actually changed our master's degree program recently to include a course specifically on ethics as part of our master's program in cybersecurity, because it is so important that people understand the dilemmas and are conscious about how they work with these dilemmas.

Interviewer: Does Auburn University educate their students in offensive cyber capabilities?

Researcher: Not really. But I think everyone who's interested in the more technical aspects of cybersecurity can of course learn about offensive capabilities. It's difficult to train defensive capabilities without also understanding how attackers think and work. So when you learn how to defend, you will also learn some things about how to attack.

But I would say you don't really learn how to attack in the way an actual attacker would do it, because there would be different tools and different methods than what we are training our students to use. For example, when you are doing network scanning for vulnerabilities, as an attacker, you would prioritize staying stealthy to avoid being discovered. If you're doing it defensively, that's less important.

We are not really building the skill set of those working on offensive security, even though of course, it's also useful knowledge if you are working in some parts of the government and private sector.

Interviewer: As cyber warfare continues to impact international relations, how important do you think it is for diplomats and policymakers to understand cybersecurity principles and the implications of cyber attacks on international diplomacy?

Researcher: I can only say that it's really important. I don't know so much about warfare in general, but I think cyber is different from many other kinds of warfare because with cyber threats, you don't want to show your capabilities. If you are threatening with guns, you want to show how big of a gun you have. But with cyber weapons, you want them to be unknown because they are only effective if people don't know what you're capable of doing.

Also, attribution is usually difficult in cybersecurity - it's difficult to identify where an attack is coming from. That also makes cyber warfare different from many other kinds of warfare. So to navigate diplomacy, it's important to understand how cyber attacks work, how cyber warfare works, and what the similarities and differences are to other kinds of warfare.

Interviewer: Since Denmark changed from NemID to MitID in 2022, can you name any difficulties that arose during this digitalization step?

Researcher: I think the main difficulty was on the user side, especially onboarding users to get used to a new ID system. The whole onboarding process seemed to be difficult for many people,

especially elderly people and those who didn't have modern mobile devices. But I think that today nobody is missing the paper codes, which I consider to be less secure than the current solution.

Interviewer: What are the biggest cybersecurity challenges facing Danish critical infrastructures, such as hospitals or water structures?

Researcher: I think there are many challenges. The biggest risk is the lack of competencies, because that is foundational for doing all the rest. If you don't have the right competencies, you cannot do the right risk assessment and you cannot implement the right technical measures and countermeasures. So I would point to the lack of skilled people as the first challenge. It also takes a lot of time to build those skills, so it's not something you can fix quickly.

The second major challenge is management understanding that cybersecurity is not just an IT risk, but it's actually a business risk and a risk for your whole operations.

Interviewer: What are the most pressing cybersecurity threats facing Denmark today?

Researcher: Looking at the threat landscape today, it's a more mixed picture than it was five to seven years ago. It's not only cybercriminals - it's also nation states and cyber activists with more political agendas. What makes it difficult to navigate is that you have so many different threat actors who are all active and who all constitute major threats.

You can basically divide it into two big categories: one is for financial gain and one is more for political gain or visibility. Different organizations would typically be targeted by different threat actors. But both types of threat actors are very important.

When you're talking about critical infrastructure and cyber warfare, definitely the category that has been growing the most in capabilities and motivations is what other states are willing to do, and their collaboration with cyber activists.

Interviewer: Have you noticed any specific trends in cyber attacks targeting Danish businesses and infrastructure?

Researcher: There's an overall increase in activity from the different threat actors. You see more ransomware, more theft, more digital fraud, more attempts of advanced cyber attacks, and more attempts of attacking critical infrastructure. It's increasing across all areas.

Interviewer: Given the increasing number of attacks on critical infrastructure, how can Denmark strengthen its defense in sectors like energy, healthcare, and transportation?

Researcher: Critical infrastructure is different from what many other companies need to protect because they are targets of not only opportunistic cybercriminals but also more advanced threats. These advanced attacks can be expensive to execute, and there's a willingness from certain actors to invest resources, skills, and time into these sophisticated attacks.

For critical infrastructure protection, you really need to work on comprehensive risk assessment to determine what's most critical in your processes. You need to integrate cyber risk with other types of risk, such as physical security risks. When conducting risk assessments, you must be much more rigorous in evaluating your suppliers and your entire supply chain.

The whole risk identification process is much more extensive and even more important than for other companies. You need to work through the entire security chain: implementing proper protection, establishing effective detection systems, and having the ability to respond and recover quickly. You need to excel in every aspect of this chain. And you must understand that this is not just a one-time exercise—it's an ongoing process.

Interviewer: Since we have many digitalized services in Denmark, such as metro trains, what dangers can it pose for society if, for example, the transportation chain were to experience a cyberattack?

Researcher: The greatest concern is when attacks target multiple sectors simultaneously. This is where attackers can create more damage and uncertainty. While it's relatively straightforward to predict what happens if the transport sector is compromised—no trains, no cars, people unable to move—it becomes more complex when multiple systems are affected.

For instance, what happens when you also hit the telecommunications sector? People cannot commute and cannot communicate with each other. You may be concerned about your loved ones without any way to get clarification about the situation. These attacks that hit multiple sectors simultaneously are particularly concerning, especially when cyber attacks are combined with other types of attacks.

Interviewer: Would you consider attacks on healthcare institutions to be cybercrime or cyberterrorism?

Researcher: The healthcare sector is an attractive target for both terrorists and criminals. For terrorists, it's attractive because healthcare is a matter of life and death—they can cause significant harm. For criminals, healthcare is appealing because when conducting ransomware attacks, they can demand substantial ransoms when people's lives are at stake. Additionally, with double extortion ransomware attacks, attackers can exploit valuable medical data. Overall, healthcare is a high-value target for multiple threat actors.

Interviewer: How can technologies like AI and blockchain be leveraged to improve cybersecurity in Denmark?

Researcher: We can use AI in many ways. It's important to leverage AI for early detection of attacks by analyzing network traffic or different kinds of system activities. By correlating activities across different systems, we can identify attacks at an earlier stage and respond more effectively.

However, responsible use of AI is equally important because AI itself opens up many new attack vectors. It's really a double-edged sword—it also provides high value for attackers.

Interviewer: Do you see any differences in cyber warfare trends being affected by the geopolitical situation?

Researcher: I don't have comprehensive data to make definitive claims, though some research has been done on the situation in Ukraine. But certainly, geopolitics makes a difference. For example, when the USA indicates they're stopping offensive operations against Russia, this undoubtedly creates new opportunities for Russian cyber operations.

Interviewer: What do you see as the biggest cybersecurity challenge Denmark will face in the next 5 to 10 years?

Researcher: In the current environment, it's extremely difficult to predict with the political situation changing so rapidly. The biggest challenge is being prepared for threats we don't yet know or understand. Organizations easily prepare for threats they can see directly in front of them, but not for what they don't anticipate.

For example, the current shift with the US working more closely with Russia raises questions about the dangers of sharing data with American companies and authorities. So beyond the ongoing challenges of insufficient competencies and lack of management awareness, I believe the biggest challenge is staying ready for a constantly evolving threat landscape.

Interviewer: What should be Denmark's top priorities to ensure a secure digital future?

Researcher: Developing competencies is crucial. We must also focus on securing small and medium-sized companies, as they struggle to attract the right talent and implement proper security measures. They risk becoming irrelevant as larger companies become more mindful of supply chain security. Beyond these two priorities, securing our critical infrastructure is essential—as a country, we are highly dependent on our critical infrastructure functioning properly.

Interviewer: What advice would you give to future specialists or people pursuing education in cybersecurity?

Researcher: We need people with both technical skills and more business-oriented abilities such as compliance Researcherise. The field requires a broad skill set in cybersecurity.

Interviewer: Do you think Denmark's cyber intelligence is developed well enough to defend against state-sponsored cyber attacks in the future?

Researcher: It's always difficult to be adequately prepared because you don't know exactly what you're preparing against. But I can say that we definitely don't currently have the level of security that we would like to have.