00:00:00  
*Speaker 1:* So if it's not a problem, can you please introduce yourself a little bit?

00:00:05  
*Speaker 2:* Sure. I'm a person in cybersecurity at Auburn University.

00:00:14  
*Speaker 1:* So 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?

00:00:33  
*Speaker 2:* I think so far the discussion of cyber competencies was very much been about the need for more experts, which is also a really a true problem. But I think maybe a little bit more. The problem is the need for more. Um, yeah. For everyone working with IEC and resilience and management to have some sufficient knowledge on cyber security as well. So that is the more broadly all those who don't need to be experts but need to have good foundational knowledge. That is the big lift that we that we need to do. And I think it's it's education within i.t. Education selection but also education within. Management and risk management.

00:01:19  
*Speaker 1:* So there is a growing demand for cybersecurity professionals. But many industries are struggling with skills that 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.

00:01:40  
*Speaker 2:* But I think we need to differentiate between the need for, you can say, talent and networks working specifically with cybersecurity and then the many who are not experts, and where cyber security is not the primary job, but who needs to have a good foundational knowledge in cyber security. And I need I think we need to address both the skill gaps. Um, and the shortage is, of course, a bit different. But one important aspect of, 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. Um, like continuing education, a upskilling first upskilling of people who are already in I.T, but also upskilling of people who are not in.

00:02:35  
*Speaker 1:* Gens who disappeared.

00:02:52  
*Speaker 2:* And like how much to do good.

00:03:00  
*Speaker 1:* Yeah. So, uh, I read in line that you are the coach of the cyber security team, the national cyber security team.

00:03:08  
*Speaker 2:* True.

00:03:09  
*Speaker 1:* So which advice would you give for the people who have talent but don't have enough education in cybersecurity, how to implement their interest into the field?

00:03:24  
*Speaker 2:* So first of all, I think that we really need to do more in the educational system to do more for those people who don't have the formal qualifications, but who have a lot of practical experience, who are self-taught, uh, who actually have knowledge without the paper. And I think we need to make much better pathways for them in education, in the criminal system than we have today, because there is a there is a large amount of people, maybe the model how to say this, um, people who did not. Work. Well, maybe in the educational system, or have different interests, or preferred and preferred learning in different ways with computers. And so there is a large pool of talent that we don't usually utilize enough today. Um, but what to do as an individual today, I would, I would recommend to do some of the better certifications, but also to search how you can actually get more and more formal paper on your qualifications, for example, through a continuing education, through master's degree, through. I don't know the word English competency, but um, to also get to get the papers.

00:04:40  
*Speaker 1:* How important are the cyber security competitions like the Danish Cyber Championships in developing the real world skills among young people? And do you think they should be more widely promoted as part of formal education?

00:04:56  
*Speaker 2:* I think the competitions are great. I don't think they can stand alone. I think they to cater to one audience and you have all the audiences and on Twitter in different ways. Um, but I think we manage in the way that we do the tennis competition. That is not only for the most competitive, it's not only for the very best actors, but we are doing it also with foundational courses, foundational online training sessions, uh, lots of beginner training sessions. We had one, I think one in ICU, uh, that was so sold out that we had to keep doing one in Copenhagen. Um, so I think that that we have a lot of really good training for the young people that's also applicable outside. And I also think we do a great I think we make a good impact in making substitutes usable. So we learned young people that subsequences are interesting. And um, that's an important part as well. And then we create a community where young people who are interested in becoming interested in cyber security, where they can go and learn more together with other young people in a in a community where just sitting alone in the basement in front of their computers. So I think we're doing an important job, and I think there is more potential in cybersecurity competitions then than maybe we are we are using today. But I think actually what we have been doing in Denmark over the last 3 or 4 years is a good example that other countries could learn from involving, especially when if you compare to the size of the population, we actually manage to involve a lot of young people. And I'm just it's not official yet, but but you can be welcome to run it that we have just made surveys about how many actually came to know about our bodies with the championships, with the national team, with the cyber perspective. And it's there on to a third of the students on the actual occasions. And I think it's really it's a really a high number considering how much information you are exposed to and how how many people are studying security. So I think that the visibility and the training providers.

00:07:14  
*Speaker 1:* So with the increasing frequency of cyber attacks on the global scale. How do you believe government and institutions can raise awareness about the risks of cyber warfare and its implications for national security?

00:07:34  
*Speaker 2:* I think there is not a single way to do it, but I think it's about. This could be a really long interview, because I think you need to, um, to divide people into different target groups because you can reach people in different ways depending on their profession, depending on the age, depending on the Interest.

00:08:04  
*Speaker 1:* I think.

00:08:06  
*Speaker 2:* I also think you need to think of training and work skills training for private digital security and safety, because the habits that you have at home and at work is also the ones that you take to develop them. But but I think that we need to come in, of course, as we already started the conversation. It's important that you think about cyber security in the, um, in the whole school and educational system, not only for specific cyber security training. You need to think it in already from primary school, maybe not in cyber security training, but but digital competencies combined with security. But it also needs to train and educate those who are not in the educational system.

00:08:58  
*Speaker 1:* So what kind of training and resources are necessary unnecessary for preparing both students and professionals to handle the complexities of cyber warfare. And how can Denmark enhance the preparedness against state sponsored cyber attacks?

00:09:18  
*Speaker 2:* Again, I think there is not a single answer to that question. I really think it's a mix of the trainings and the campaigns. Just a moment. I just got my bike by bike here. Sorry. I will come back in two minutes.

00:09:36  
*Speaker 1:* Yeah.

00:09:38  
*Speaker 2:* Um, I also got a bit more, a bit more chance to think about your question, because I think there is so much you need to do. Um, also from the government side, um, in cybersecurity, which we talk a lot about role specific training, and I think that also comes when it's about educating the general population, because you have some, some people who are highly skilled.

00:10:01  
*Speaker 1:* In What would I see? You have the people and. You have the elderly people.

00:10:11  
*Speaker 2:* Many of which are becoming victims also of what's called digital theft and fraud. And I think you need to use different ways to educate the different people. So it's really a mix of, again, of campaigns have a bunch of training materials being available. But also I think protection is just one component of it. Like you should of course prevent theft from prevented theft. You should prevent attacks from happening. But you also need to have what is the warning step? Um. You need to be you need to help people when an attack is occurring. So you have a place to go to where you can get help in a situation where a fraud is happening or where you're under an attack, and that is for both people and for businesses.

00:11:11  
*Speaker 1:* Is there an institution like this right now in Denmark? Is it CFCs?

00:11:17  
*Speaker 2:* It is CFCs. And then I think that the new ministry, um, MSP, I think it's actually working in this direction as well, because before it was fragmented into different ministries, and now they're trying to put it in in one single ministry. But my understanding is that they're still shaping exactly what they're doing and how they're going to do it.

00:11:41  
*Speaker 1:* So 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?

00:11:58  
*Speaker 2:* Um, again, this is a question that you could actually spend a lot of time on just discussing this one question. Um, I think I think we need first of all, we need to integrate, uh, digital skills and cyber security in all indications. Of course, especially cyber security in IT, education and and management educations. That's that's one part of it. I think we need we started we already talked a bit about the people who don't have the formal competencies but actually actually are really good. So we need to also have a more flexible educational system where you are not caught in cul de sacs, but you can always study further, and you can always have a place to go to become better and also become better in the in the formal educational system. And then we need, I think, in general to invest more in it recreation because we are lacking people in IT and we are lacking people in cyber security. So the cover of the current policy, which is about cutting down on equivocation, is definitely the wrong direction to go.

00:13:15  
*Speaker 1:* As cyber warfare becomes a more prominent part of international conflicts. What ethical considerations should be included in cyber security education, especially in relation to the use of offensive cyber capabilities?

00:13:32  
*Speaker 2:* I actually think that the most important aspect, of course, is to discuss ethics as part of the education. That's one aspect, but I think the most important is actually to build good communities for people interested in cyber security. So good, healthy, positive communities. So you are so you also get a good social network and stay on the good side of things. And don't use your skills in a bad way. So what we actually actually we actually changed our master's degree program recently to include a course specifically on on ethics as part of our master's program in cyber security, because it is so important that people understand that they can they can, they can be in and that they are um, yeah, aware about those dilemmas and then and conscious about what.

00:14:36  
*Speaker 1:* Does all work.

00:14:37  
*Speaker 2:* Conscious about how they work with the dilemmas is maybe the right way to put it.

00:14:42  
*Speaker 1:* Does all work University educate their students in offensive cyber capabilities?

00:14:50  
*Speaker 2:* Not really. But I think everyone who's interested in cyber security and with the more technical aspects, uh, can of course learn about the more offensive Calculators. Uh, and it's, it's difficult to train defensive capabilities without also understanding how attackers are thinking and working. So when you learn how to defend, you will also learn some things about how to attack, but you don't. I would say you don't really learn how to attack in the way that an evil 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 using it because of its technical, but when you are doing a network scanning, so you are scanning for vulnerabilities and finding vulnerabilities. As an evil attacker, you would prioritize to stay stealthy, to not be discovered. If you're doing it on the good side, that is less important. Um, and then we are not really killing the skill set, 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 U.S. government and private sector.

00:16:11  
*Speaker 1:* As in, cyber warfare continues to impact the international relations. How important do you think it is for diplomats and policymakers to understand cyber security principles and the implications of cyber attacks on international diplomacy?

00:16:30  
*Speaker 2:* I can only say that it's really important for us, because I don't know so much about warfare in general. I want to know about cyber, but I think cyber is different from many other kinds of warfare because the threat is like, if you are threatening by shooting with guns, you want to show how big of a gun you have if you are threatening the type of weapon. We do want to be unknown because they are only efficient if the people don't know what you're capable of doing. And so cyber is different from many other kinds of water. And also attribution is usually difficult in cyber security. So it's difficult to see where an attack is coming from. And that also makes the difference between cyber warfare and many other kinds of warfare. So to to navigate in the diplomacy, it's an it's important to understand, um, how cyber attacks are working, how cyber warfare is working and what are the similarities and differences to all kinds of warfare.

00:17:43  
*Speaker 1:* Since Denmark changed the method to name it from. Since Denmark changed the name to timidity in 2022. Can you name any difficulties that arose during this digitalization step?

00:18:01  
*Speaker 2:* I think actually the main difficulty was on the user side, um, and especially on onboarding the users to first to get used to a new ID system, but also the whole onboarding, um, seemed to be difficult for many people, especially elderly people, and especially those who didn't have, uh, a modern home. But I think that today nobody is missing the the paper codes, which I also consider to be. I also consider that to be to be more secure, of course, than the solution.

00:18:43  
*Speaker 1:* What are the biggest cybersecurity challenges facing Danish emergency infrastructures, such as hospitals or water water structures?

00:18:58  
*Speaker 2:* I think I think there are many um, I actually think that that the biggest risk is the lack of competencies, because that is foundational for doing all the rest. So if you don't have the right competencies, you cannot do the right risk assessment and you cannot do the right technical measures and countermeasures. So I would point to the lack of skill people. That's the first one. It also takes a lot of time. So it's not something you can fix from day to day. And then I think that, uh, the management understanding that this is not just an I.T. risk, but it's actually a business risk, um, and it's a risk for not only i.t, but for your whole operations. I think that would be, uh, that would be a second major challenge.

00:19:57  
*Speaker 1:* So what are the most pressing cybersecurity security threats facing Denmark today.

00:20:05  
*Speaker 2:* I think looking at the threat picture today, um, it's a more it's a more mixed picture than it was five, seven years ago. So it's not only cybercriminals, it's cybercriminals, and it's also nation states. It's also cyber activists with a more political agenda. So I think actually what makes it all so difficult to navigate is that you have so many different state actors who are all active and who all constitute, uh, a major threat and a big threat.

00:20:39  
*Speaker 1:* How?

00:20:40  
*Speaker 2:* Well, and I think you can you can basically divide it in instead of the two big ones, which is one is for financial gain and one is more for for political gain or for visibility. And then different companies would be hit, usually by different threat actors. But both are very robust. Types of threat actors are I'm very important that when you're talking about critical infrastructure and cyberwarfare, uh, definitely the one that has been growing the most in capabilities and motivations is what? Other states are willing to do, other states and their collaboration with cyber activists.

00:21:23  
*Speaker 1:* Have you noticed any specific trends in cyber attacks targeting Danish businesses and infrastructure?

00:21:31  
*Speaker 2:* Um. Just an overall increase in what is coming from the different threat actors. So I wouldn't want to one in particular. So you see more ransomware, you see more theft, you see more, uh, digital fraud. You see more attempts of sort of advanced cyber attacks. You see more attempts of attacking critical infrastructure. So I think it's uh. Yeah. Oliver.

00:22:06  
*Speaker 1:* So, given the increasing number of attacks on critical infrastructure, how can Denmark strengthen its defence in sectors like energy, healthcare and transportation?

00:22:21  
*Speaker 2:* I think we're getting a little bit back to what we had before. Uh, but when we're talking critical infrastructure.

00:22:30  
*Speaker 1:* Oh. You disappeared.