00:00:04  
*Speaker 1:* So could you please introduce yourself briefly?

00:00:10  
*Speaker 2:* Yeah, I'm Rosario Justice and I'm lecturer at university. And I work on cyber security.

00:00:22  
*Speaker 1:* Great. So. How can cryptographic protocols ensure both security and trust in decision systems?

00:00:38  
*Speaker 2:* Uh, how?

00:00:40  
*Speaker 1:* I don't know how, uh. It's an open ended question. Uh. Then elaborate a bit. The question. What you want to know.

00:00:54  
*Speaker 2:* So how does, uh, for example, the GDPR protocols can protect data from the cyber security from the cyber attack.

00:01:05  
*Speaker 1:* Are GDPR?

00:01:10  
*Speaker 2:* Well, if. If they implement GDPR accordingly to the prescriptions, then they should not have to store the information. That means that actually if the company has a leaking attack, then they don't leak such information because they should not erase or not have this. So this is what comes to my mind.

00:01:45  
*Speaker 1:* So what are the most significant cyber warfare threats facing Denmark today, and how do they compare to global trends?

00:01:56  
*Speaker 2:* Um, well, I think, uh, I think, uh, um. While both state sponsored attacks and, uh, uh, um. And also. How they called, um. Yeah, this this, um, groups that are paid by, uh, like, competing companies or so on. So. Yeah. These two categories, I think, uh, poses the main threats to today, Denmark, uh, companies. You know.

00:02:45  
*Speaker 1:* You mentioned the state sponsored cyber attacks. So how does the state sponsored cyber attacks typically target the critical infrastructures? And what can Denmark do to defend against them?

00:03:00  
*Speaker 2:* Uh, well, how they they. Yes, they they they pay criminals. Yeah. The categories was criminals, so they pay criminal groups. That's, uh, the that that is, uh, this kind of, uh, attacks and, um, to disrupt, uh, so there are different, different way, right, to disrupt, um, the companies so they do this, um, uh, yeah. Attacks on infrastructure. As I said, they do attacks on this information. Uh, it's it's quite vast, I would say the the part and the way to defend. Well. Um, I think the first thing is to do is to invest more in cyber security. So invest more on, uh, on, uh, um, on people knowing, uh, and, uh. And teaching more cyber security aspects in companies. It's one way. So having awareness of these attacks. Uh. Yeah. This is what comes to my mind at first points, you know.

00:04:21  
*Speaker 1:* So currently the Denmark is more focused on, uh, sponsoring the development on the research areas such as quantum computers. Would you consider that spending more money on developing the cyber security and the cyber infrastructure will benefit Denmark?

00:04:46  
*Speaker 2:* Yeah, yeah, that's what they say. Yes.

00:04:51  
*Speaker 1:* So what role does intelligence gathering play in cyber warfare, and how can Denmark improve its cyber threat detection capabilities?

00:05:04  
*Speaker 2:* So I think it's key to in terms of intelligence gathering. Um. And yeah, how Denmark can well, uh. So I think invest on this technologies that. Yeah. That's helps to to contrast cyber warfare. Um, but invest in cyber security education and companies. So very important because I think the one key difference is that, um, when you, when it's kind of warfare, And the government protection is not, as they say, when you have like geopolitical and geographic protection. What do you say? So it's it's more on the companies that have to protect themselves. There's not much the government can do, uh, to, to prevent such attacks, I would say.

00:06:13  
*Speaker 1:* So what methodologies are most effective for conducting the risk assessment of national critical infrastructure, including hospitals and election systems?

00:06:27  
*Speaker 2:* Risk assessment? I think there is one from Mitra recently released. There are different. Yeah. Now I'm not going to address where might the military attack think uh, framework. Uh, there is something by next. Uh, I don't know if it is the same. And the trick? Um, yeah. My trick. My attack is one. And, uh. Yeah, there is this list framework. Uh, it's quite outdated. I think it's 20, 2012. So I think the minor attack is more recent.

00:07:28  
*Speaker 1:* What are the most damaging types of cyber attack?

00:07:34  
*Speaker 2:* Damage?

00:07:35  
*Speaker 1:* Yeah.

00:07:37  
*Speaker 2:* Uh. Well, it's hard to say what is the most, but, uh, I think the, uh, the one that, uh, targets, uh, the a critical infrastructure is one of the most damaging, I would say. So if you manage to attack the not the. Uh, electrical companies and, uh, and stuff like that would be quite, uh. Quite a problem. Um, yeah. So critical infrastructure, I think, is the one the main immediate, uh, uh, yeah. Attacks one can face.

00:08:32  
*Speaker 1:* So how do you assess the effectiveness of Denmark's current cyber security policies in mitigating the cyber warfare risks?

00:08:46  
*Speaker 2:* Policies are mitigating policies on mitigating. Um. Well, I have no idea how you can assess the policies. Uh, I think there is some center for the center for cyber Security was, uh, some sort of direct connection with the main companies that and and which are some direct connection. But I think it's not completely clear to me how this is happening, actually.

00:09:25  
*Speaker 1:* So what role does Denmark play in international cyber security research and collaboration against the cyber warfare?

00:09:34  
*Speaker 2:* So can you start by come again with the beginning. Because I think.

00:09:38  
*Speaker 1:* What role does Denmark play in international cyber security research and collaboration against cyber warfare.

00:09:49  
*Speaker 2:* Well, the research part, I will say, is not much. I don't know any, any, uh, specific, uh, funding, uh, partnership in the international context with Denmark. Uh, uh, what was the other part questions. You said the other point was the.

00:10:14  
*Speaker 1:* The collaboration against the cyber warfare.

00:10:17  
*Speaker 2:* Collaboration against the cyber warfare aspect. This is done and the within NATO probably. And, uh. And some. Yeah. But it's it's again, it's not completely clear to me, uh, I mean, because NATO is not so transparent to, to assess. So. I expect NATO has some. Collaboration there.

00:10:51  
*Speaker 1:* Which hacker groups or nation states pose the biggest cyber warfare threats to Denmark, and how can these threats be mitigated right now?

00:11:02  
*Speaker 2:* So right now I think is Russia, um, which poses the main threats. Uh, I mean, there is Iran, South Korea, uh, Russia and uh, okay, a fourth, I forgot the fourth stage, which is normally known, but yeah, these are um. And okay, how to mitigate these? Uh, well, I think I think that there is no direct fix on this. I mean, there is need for more education cybersecurity skills. The solution is not as quick as possible as the attack happens, right? Uh, because I think that normally this kind of attack bootstrap, uh, uh, from yeah, from policy is not following it and so on. And then if you want to fix this, there is not easy fix, not quick fix.

00:12:09  
*Speaker 1:* So last year there was a cyber attack on the I don't know what's called precisely but the water reservoir in Denmark. What is your opinion about this kind of cyber threats. Is it a cyber crime or is it a cyber terrorism?

00:12:32  
*Speaker 2:* Water. Somebody say?

00:12:36  
*Speaker 1:* Yeah.

00:12:38  
*Speaker 2:* Okay, let me see what it's about. It's, uh. Uh.

00:12:42  
*Speaker 1:* I'm not sure how it's called properly, but I think it was a cyber attack on the water station that they couldn't supply water to the citizens for a couple of hours.

00:12:59  
*Speaker 2:* Mhm. Uh, yeah. Okay. What? The plants? Uh, yeah. And, um. So, uh, I don't expect this to be. Uh, so. Okay. You see, uh, crime and, and, um, and and cyber terrorism's the, the main difference is that in cyberterrorism, Uh, your are not driven from economical, financial or just specific. Um, uh. Incentives while, uh, so terrorism is just to break stuff for the sake of breaking some kind of vandalism, I will say, but more, more, more, more oriented with some either ideology. So I will not say this terrorism is if we define this way, that terrorism, I will say more crime because it's more, um, I would expect this to be to be a signal that, yeah, they can attack, uh, uh, they can attack, uh, critical infrastructure.

00:14:27  
*Speaker 1:* So what is the biggest consequence can be from the cyber attack on the critical infrastructure, in your opinion?

00:14:38  
*Speaker 2:* The consequence?

00:14:39  
*Speaker 1:* Yeah.

00:14:43  
*Speaker 2:* Uh, well, you have, um. You have, um. The consequence is that, uh, the you have to care about that, right? You have to to focus on this. So. I don't think this is on the purpose of, uh, for, uh, it's kind of. Yeah. Testing attacks, the specifics. So in the big picture, when this happens, uh, at more, uh, yeah. Strong level, that will be because, uh, you are, uh, yeah. You are involved in a bigger things than just, uh, just the attack itself. So I think this kind of attacks are just mainly for, um. Yeah, testing the infrastructure of the targets.

00:15:53  
*Speaker 1:* What are the reasons can be to cyber like to target the hospitals and the healthcare institutions, in your opinion, for cyber attack?

00:16:06  
*Speaker 2:* The reasons to test the infrastructures. So it depends I mean, who is attacking this, right. So if you are saying that this is a state sponsored attacks, I would say is to test the promptness of the critical infrastructure. If there are criminals, uh, which are driven by so for instance, ransomware, Somewhere. Then there are clear, uh, um, economical benefits that are looking for because if they attack uh uh uh, hospital, they know that, uh, they have to pay in order to not, uh, to avoid the serious consequences. Right? So if there is that attack, uh, I don't know, I'd you probably is less inclined to pay. So it depends which kind of cyber activist group we are targeting as if they are state sponsored or they are, uh, yeah, criminals.

00:17:20  
*Speaker 1:* So how do you see the future of Denmark's digital infrastructure evolving, and what cyber security measures should be prioritized to mitigate emerging threats.

00:17:34  
*Speaker 2:* Uh, well, being. Well, um. I, I expect that this the kind of attacks would be increasing so more and more and, um, as I say, the thing that, uh, cybersecurity education among companies should be, should be, uh, yeah. One of the first things that that that should be done in order to on the long, the long term, avoid these, uh, attacks, be successful.

00:18:16  
*Speaker 1:* Do you consider that the population of Denmark is, like, well aware of the cyber threats and cyber warfare?

00:18:28  
*Speaker 2:* The population of Denmark. Um. Uh, well, I would say yes, probably. They are aware to some extent. Um. They are not completely blank on that, I will say, because the news are coming, but yeah, not probably as much as they could.

00:19:01  
*Speaker 1:* So Denmark evolved during the last three years in the digitalization of the documents. So previously they were using the name ID and right now they're using the method to identify the person. Do you see any risks in this kind of digitalization move.

00:19:28  
*Speaker 2:* From it made it to meet the, um. Where there are always risks when you change technologies. Uh. Uh, but in the specific, uh. I will say that, uh, overall risk is more or less the same as the previous one. So it's not a big change on assessment, the risk. So there is not a kind of increasing on the risk. So more or less the same risks that you had in mind are possible in the idea as well.

00:20:12  
*Speaker 1:* Can you name some of the measures to prevent the identity theft.

00:20:21  
*Speaker 2:* And prevent identity theft? Um. And then identity theft. Okay. So long run again. Um, I'm a bit boring on that, but cybersecurity education. So, um, specifically, uh, normally when, since we were talking about MIT idea, I think this is a way to which you can identify. So, uh, immediately, what is key is being probably the phone. So. Using, uh, uh. Not weak Pin, for instance. So if you just go on to go to specific to, that would be, uh, a way to avoid, uh, ID theft. Um. Yeah. But in general, I would say that the long run, again, is cybersecurity education. So just to have a principles that, you know, for instance, uh, using uh, uh, password managers and, and so on.

00:21:49  
*Speaker 1:* So what are the security and privacy implications of increasing the digitalization?

00:21:59  
*Speaker 2:* Of what we do? We have we have a lot of threats on privacy now and security and cyber security. The more we go towards digitalization, the higher the risks that this to, um, cyber security and privacy are central in, in that, you know.

00:22:22  
*Speaker 1:* So what are what future trends do you foresee in, for example, hospital cybersecurity and how should IT infrastructure evolve to address emerging threats?

00:22:38  
*Speaker 2:* Well, the first sorry, I forgot, I missed your starting of your question.

00:22:43  
*Speaker 1:* What future trends do you foresee in hospital cybersecurity and how should IT infrastructure evolve to address emerging threats?

00:22:55  
*Speaker 2:* So I I'm not 100% sure what is happening on the healthcare. The question is about healthcare. No. Hospitals, healthcare. Um, but what is in general a problem is, uh, a legacy, I think legacy software and so on. So not updating all the systems, uh, Because, um, most effective attacks normally are a combination of finding vulnerability on all systems in legacy systems, plus, uh, finding a bootstrap or among employer and employee. So in one side, I mean, again, cybersecurity helps you to, uh. Um, avoid. And so the people are completely unaware of the risks and companies as well. And hospital as well. And one of the things is always update your system to the state of the art, because they will continuously patch it systems, uh, against against security issues.

00:24:17  
*Speaker 1:* Is it important to patch the system regularly?

00:24:22  
*Speaker 2:* Yeah.

00:24:25  
*Speaker 1:* So which comments would you make about the cyber attack on the mask?

00:24:35  
*Speaker 2:* When the mask thing I think was was a problem of, um. If I recall correctly, the ransomware attacks. What kind of a combination on finding, uh, uh, a vulnerable entry point, which was, uh, some employee. I think that that that has access to some type of access. So, um, I would expect that this is always the common story now. So actually, yeah, you have the. have a employee or who. Who doesn't care who is not located in cyber security. So it gets the entry point for the series to then go through the systems because the employee has more privileges than an outsider. So this is always the story. Uh. So yeah, it's a combination of, uh, of of, uh, yeah. Of this.

00:25:54  
*Speaker 1:* So how is the ransomware threats are evolving and what preventive strategies are most effective?

00:26:07  
*Speaker 2:* Um. Well. The point of ransomware is that in order to succeed, they need higher privilege, you know, to access the data systems. So if you have kind of comparative compartmentalization in which you avoid that, uh, that, uh, you have multiple level of access and, um, yeah, one way to fix this is that you give, uh, uh, access to the critical infrastructure or the companies only to people who have been going through a security education. Uh, that could be a way to. Yeah, to fix stuff. So.

00:27:09  
*Speaker 1:* Yeah. I don't have any more questions.

00:27:12  
*Speaker 2:* Okay. Super.