00:00:02  
*Speaker 1:* So can you describe how you discovered the vulnerabilities in the election systems and how these vulnerabilities can be applicable for Danish election system?

00:00:14  
*Speaker 2:* Okay. So you have to distinguish what kind of technology you use in your elections. Um, so if you're doing a paper election and then there is um, then there are always that there's evidence that you have that you can check and recount if you want, but it has to be securely stored. So there are some, some, uh, if you ask where are the vulnerabilities and how do you detect them. So you usually detect them if you count the results for the second time. And uh, but only under the assumption that, um, the this evidence is securely stored. But the boxes resolve the ballots and you have an electronic election, and, uh, it's much more difficult, um, because how do you make how do you count again an electronic thing? When you write a program, you can count it again. But if somebody changed the database, then you get the same wrong result. So it's much, much more difficult. This is why there is in the last couple of years, ten years or so, the idea of verifiability has been defined. And verifiability is that when you compute something that you can actually verify that the result of the computation is what it's supposed to be. And in in election systems, it's always the case that you have to balance the privacy of the vote versus the integrity. And so when you have verifiability. Yes. Or it's basically it's just kind of saying like there's secrecy and there's verifiability. So if you want to verify okay, then you need to know all of the stuff, uh, how people voted because then who voted. Otherwise you, you can't figure out, um, you know, if the result is okay or not. Um, and vice versa. If you want to have, uh, confidentiality, then, you know, you have to encrypt everyone, and but nobody can actually figure out what the result of the election is. Um, that's how secure it is. Nobody knows at the end. Um, and you see that there is always a compromise in between these two things. And paper ballots solve this very easily because you shuffle the ballot box and then you have like, privacy first, and then comes integrity by many people counting. And you have an electronic system. It's really, really difficult. And it's, it's it's impossible to do it without concessions. So you always have to, uh, find something, you know, you say like, okay, I have this a compromise. I'm not. I don't require a 100% privacy. Um, I don't require 100% integrity, but most of the time, people require 100% of the integrity. So, um, finding, uh, finding, uh, Finding a tax in verifiable systems is possible because, uh, the, the, the mechanisms you have built in in order to verify that everything is okay, they will trigger and then there will be like a red light going off and saying, like, here's something that can check and then you can investigate and then you'll figure it out. Of course, the problem only then begins because now you have to recover from it somehow. Um, which is much more complicated than running an election because you just can't run it again just because there was a small mistake and going on. Let me just take this one second. My daughter got a driver's license, and then suddenly they send me pictures from the beach in the car. It just took the car and took off. So, okay, now I'm really irrelevant in the family. Okay. So, um. Yeah. So if the system is verifiable, you can figure it out. If it's not verifiable, if you can't figure it out. It's as easy as that.

00:04:48  
*Speaker 1:* So which the main security flaws. Did you figure out?

00:04:55  
*Speaker 2:* That the system is not very viable? Most of the systems are not very verifiable. So, um, so that means, you know, okay, so to kind of give it maybe a bit of a bigger explanation. Whenever you look at election security, it's really critical to look at the trust assumptions and the adversary model. You have to know what are the capabilities of your adversary. Whom do you want to defend against? And in elections, it's, uh, it's really it's, uh, it's nation states is very powerful secret services that are the potential adversary. So you have to potentially protect a very, very, very, very strong adversary. And at the same time, there are lots of people running the election. And you have to understand whom you should trust, that whom you shouldn't trust. And essentially you don't trust anyone Because trust is a liability. If you trust somebody and the person disappoints you and you're screwed. Um, so you want to kind of remove as much of this trust as you can and, uh. Um, and, uh, so, uh, you know, these election technologies and they have certain security properties. The security properties are usually, you know, there's actually they go all the way back to the declaration, the UN Declaration of Human Rights. Paragraph 21, it actually talks about, you know, that, um, everyone has the right to be governed. Um, the government should constitute by periodic genuine elections since the secrecy of the vote. So so you see, it's genuine. It's like it is. The election has to have integrity. It has to be privacy preserving. Um, so it has to kind of these are the, the properties. And um, then, you know, there's of course the verifiability aspect to it in order to make the whole thing trustworthy. And so when you look at it, you know, many different systems have different floors. So the Swiss system from 2019, there were some researchers, Vanessa Tech from uh, from Australia, they looked at it and they actually managed to exchange the ballot box by a different one. And all of the checks still worked out. Nobody would have ever known that this is actually not the right result. So there was an attack against the integrity of the election. Um, in, in, in Norway in 2012, um, all of the votes were encrypted was the same randomness. So the ciphertext are the same. So, you know, they were essentially encrypted votes in the ballot box, but all of the votes for the same party were encrypted with the same ciphertext. So if you encrypt, uh, party X and you see the ciphertext, then you know exactly how the people voted. So that was an attack against the privacy. Um, so all of these things have been have been broken, especially in internet voting systems. Um, and um, and then there are also other uh, systems like, uh, you know, I've been to African elections where there was like, um, uh, results transmission system. So, you know, they vote on paper, they count on paper. But the problem is that nobody trusts when paper leaves the polling station that this is the same paper that actually arrives. So they have put a lot of technology in the in the electoral process. And, you know, people tend to kill each other after elections. And then some of the African countries, which is not very, very friendly. Uh, I think it's got much, much better now since 2007. Um, and yes, they have the results transmission system, the digital transmission system always had flaws, um, of one way or the other. So one time, um, you could just, um, you know, what was legally binding was what people typed into the into the computer. But if they make a typing mistake. Then it was legally binding. Um, so, uh, so a result of this, the Supreme Court in 2017, actually a multi election, they had to rerun the entire election. So there's a lot of a lot of things that, uh, um, you know, lots of things that can go wrong. And uh, but it always immediately it's not a technical an election is not a technical system per se. It is a technology is used to run them. But, um, it's always a social, a social, uh, it's a social computation. And, um, as such, you know, there's immediately the laws, the Supreme Court. Um, this was high level things, high level definitions and decisions that have to be made, which makes them extremely interesting, uh, field to study. It's different, you know, like, if you just look at a company that, let's say, sells Cells look okay. Their systems were hacked. Okay, so they didn't sell any milk that day, and then they rebooted it on the next day. That was selling milk again. Okay, it's tragic for them. Maybe they lost their income for a day or two, but, uh, it's it hasn't destabilised the entire nation. So this is what makes these elections actually really absolutely critical to society.

00:10:08  
*Speaker 1:* So touching the top again, how did the findings on the election system vulnerabilities influence broader discussion on national cybersecurity? So you mentioned a little bit that it's very important for the people. So how do you comment on the national cyber security. So for example, if an election is going on in Denmark, how will it be affected.

00:10:36  
*Speaker 2:* Um, from other or from other uh, events in other countries, you mean? Or if, uh, um, there's a is. Okay. So elections are, um, it's a, um, in my experience, it's an operation based on has a lot to do with national pride. And every country believes that the way how they run elections, the best way to run them. Um, so, uh, in, uh, in the elections, I think the paper elections that we use in Denmark, they have evolved over the last hundred years, plus or minus, um, and they have basically been debunked over, over the years. And also in many other Western countries, they have been they have been running and they have, uh, their processes. And, you know, when when you actually look at the elections that are run in Denmark, it is absolutely fascinating because all of the steps are always verifiable. You know, when polling stations to call in the numbers to Denmark statistic on election night. The information has been transferred in three different ways. One times to a computer system which was built in the 80s, one time through a telephone call. And then the third one is by handwriting in a book that is then transported to Denmark. Statistic. So because of these, these operations of uh, um, yeah, these these, these, these this double checks and, uh, and everything in Denmark is very unaffected by all of this stuff that goes in other countries. But having said this, there's a, um. Denmark has moved now to digital electoral roll. The digital borderless. When you go in and you, you show your card, which you get by the mail, it's a barcode on it. And they scan the barcode. They know who you are, you're being digitally crossed of the list. And so, um, um, what actually happens then is what happens if the system goes down. And it happened like I think six years ago, 2019 or something in Scotland, which was at a high school or to a school in noble. Um, but these things just didn't start. Um, and then then you are getting into a lot of issues because then when the system worked for a little while and then it doesn't work anymore, then usually have backup books, then they use the paper backup books. So even they're right. You know, there's a backup. So so there's always everywhere is the backup solution. So Denmark is uh, is rather rather secure in that regard. So I don't I don't believe that, uh, you know, you will. The Danish election is very verifiable. Um, so there's, uh, so actually, Denmark is the election. Don't touch world champion agenda. And there are measures of democracy, you know, the the quality of democracy in countries. Denmark is always number one. Um, that's how well it works here. But I think that, uh, the people running, uh, digital voter disks, they actually are starting to get concerned about, um, cyber attacks. And they actually have provided, um, for Copenhagen computers a few years ago with the Masters students. We actually provided training materials for people to train all of the potential events that could happen in the electoral, uh, during Election day, you know, like, what kind of attacks could they be, where the weaknesses, how do you defend against it? And so the other thing to add is that, um, uh, you know, when there's a, um, vulnerability in a technical system, that does not mean that the process is vulnerable because there might be operational, operational, um, uh, mitigations that were put in place in order to, to make sure that you're still okay. And again, they are. Denmark is actually doing it very well because there are for example, there are always um, when you have these digital borderless, there's always two people have to sit there. Okay. So internet one falls over, um, because of, you know, it has to go to the bathroom. Um, there will be still it will still be guarded, so to speak. Um, and this, this system and these these processes are designed precisely with this in mind, but, uh, nevertheless, when, when the, when the power goes out and all of the digital election lists will go out and everyone will fall back on paper lists, that will be, um, people have grown, uh, you know, reliant on the, the comfort of just going there and then it never goes fast. But then when people have to go through big books and find you, they will take a lot. A lot of time will be inconvenient, and it will actually have a negative effect on the reputation. Um, the there's a reputational loss of the quality of the, the thing. So people I think people are aware of, but, um, um, yeah, nobody has uh, the, there's this trade off between convenience and, um, and security and the so Denmark has the whole spectrum covered and, uh, if there's something goes wrong, it will be able to recover and the risks are computed into it. So the risks were too high to use digital election and voter lists. They would I'm pretty sure they wouldn't use them, but, uh, they, they deemed the risk something was wrong is very small. I also believe that, uh, I don't remember, but I don't think that these now they're laptops. So even if the power goes out right, the digital and they're running their own little network, so they're like, uh, there's a PCA instead of the main laptop, which has the borderless. And then there's all of the terminals that are in it on a local network. So they only talk to each other. They're not connected to the internet. And so the power goes out except the router in the middle. I don't know if they have a battery for this, but you should be able to actually run the digital voter list throughout the day. Even if the internet goes out, the power goes out. It still should still work. It will not work anymore when there's an electromagnetic impulse. Um, and then, you know, all of the technology goes down, but that's a different thing. I hope I'm answering your questions, but yeah.

00:17:01  
*Speaker 1:* So what parallels exist between election system vulnerabilities and the risk to other crucial digital infrastructure, such as health care system and energy?

00:17:12  
*Speaker 2:* I think that the elections is the quintessential. It's if you if you understand the elections, you understand all of the others. Um, the, the other's, uh, health data, their integrity is easy to verify because everyone can always check it's public. It's a vote. You cannot check your vote because there's a danger that you can sell it. So the election question of maintaining the integrity and privacy of the verifiability and integrity of the confidentiality and the verifiability of data is much, much more pronounced than in all of the other things. And so, um, having said this, um, elections only happen once every so many years. And so, um, there are you know, they don't they have to work on the day and there's an election. So you can't say like, uh, sorry, uh, uh, this function doesn't work yet, but, uh, we'll be it'll be done in a week from now. This is not possible. So this is an absolute no no. Okay. So being able to deliver the service in time is something that is also common to others. Okay, but the others have to continuously deliver the service. And with an election, it stops after a day of or so after the result has been determined. So, uh, so, uh, the, the other, um, infrastructures that I think, uh, or the infrastructural, uh, component to this question is that in an election it's very hierarchical. Okay. So yeah, like all of those, those little polling stations, but then they communicate the data up to a point. And in that point there are very few people who have access to it. In a health system, it's much more decentralized, um, that many people have access to all of it at any time. Um, it's, uh, brings a different, uh, a different set of, uh, set of problems. And you can also not have paper backups, uh, in a digital country as digital as Denmark. And I think this is only something that the country starts slowly start seeing that this is actually something that should be taken into consideration for decision making. When it comes to, you know, cybersecurity infrastructure. It's like, okay, so if this doesn't work out then we are in deep shit. Um, and you see some of the examples like the, uh, G5, whatever the telecommunication was, they went out, nobody attacked them. They take themselves by installing and bring update. Okay. Okay. So they shot in their own foot. Um, uh, but. Yeah. Um, then the other. Yeah. Okay. So there are many of those examples, right? Where the stuff actually doesn't work for a time, and then you actually realize how dependent you have become on it. And uh, um, so yeah, I think that is the big the differences and, you know, water, um, energy, food, all of the other critical infrastructure sectors are very similar, I think, to health.

00:20:25  
*Speaker 1:* So what role does Denmark play in international cybersecurity research and collaboration against the cyber warfare are?

00:20:37  
*Speaker 2:* The nonpolitical answer will be, uh, not much. Um, the more diplomatic answer is that, um, Denmark is is I think in the last ten years has really understood that cyber security is important. And they have, um, added a lot of money into building institutions like CFCs nowadays. Um, thanks to my students. I understand also that Denmark has been very actively has a lot proposed, a lot actually, to implement this tool for Denmark. So what is this to all of the member states supposed to deliver, Um, laws that actually implement these things. Okay. And, um, so that, uh, that is, um, that's that's what is going on on the nature level. I believe that, uh, um, and I think you can look it up. Um, uh, Denmark has actually made promises to NATO, uh, to NATO and to European defense. And I think that these, uh, uh, and these things do not include cyber security. So what Denmark promises is, uh, biotechnology and, uh, quantum computer, quantum quantum computing. And, uh, I also think that, uh, because of that, you see that a lot of the funding that is available in Denmark right now is not for cyber security, but it's for quantum computing, um, for for Denmark, somehow, for some bizarre reason, to remove this bizarre. But for some reason, uh, the, uh, um, that the top priority politically is, is quantum. And it could be that this is just like because the NATO countries have agreed that in the home of Niels Bohr, that should look at quantum, but many other countries like Germany and Italy and so on, they have uh, active, uh, cyber defense on their, on their schedule. And I think there would also be more money in Denmark given to these, to these, these subjects and the research area, if that was a priority. Um, on the, on the, on the EU or the NATO level. Um, so I think, yeah, basically Denmark says like we don't do cyber security, you can do it, but give you something else instead.

00:23:01  
*Speaker 1:* So how do you assess the effectiveness of Denmark's current cyber security policies in in mitigating the cyber warfare risks?

00:23:12  
*Speaker 2:* Um, I think there are there's a shame that they have to catch up. I think they're way behind other countries in the sense that, uh, some of their laws, um, require you to be quiet when you find something and you're not allowed to talk to anyone about it. Uh, otherwise, you go to prison. See, for example, the log in law number. You know, uh, paragraph 14, I think it is called Townhill split. Don't talk about it. Otherwise you go to prison for half a year. Um, this is not a that's not an a good encouragement for your own people to find holes in the infrastructure for them to fix. It is more based on this, uh, on this old, uh, you know, 1900 and the 20th century kind of thinking of like, uh. Okay. So, uh, you, uh, if we forbid you and we give you a penalty for it, you won't do it. But, uh, this this model just doesn't work anymore in cyber security, especially if you have a firm for states. Um, that might um, we can always excellent secret services that might actually plan to attack you. They know all of the vulnerabilities. Um, but they don't have they don't have, uh, you know, they don't talk about it, so they're not really covered by by this law. They're also not afraid of the Danish law. I don't think so. There's no, uh, no hacker from a foreign country would say like, oh, my God, I shouldn't do this. Um, so, um. Yeah. So the last I think you have to be updated. But as I said, they are in progress of doing it right now. Um, and, uh, my students have figured this out. It's very good. I teach ethical hacking, and it was the homework assignment. I said, like, you know, guys, uh, what is the status? Was one of the problems. So what is the status of Denmark in implementing these two? And there was actually one team that found all of the, uh, the laws that are being discussed right now. So. And I haven't studied it in detail, but it actually actually touches also on techniques for responsible disclosure and it touches on them. I do not know if I agree with the way how it is implemented, but I know it is addressed. Um, but yeah, so things that the Denmark is moving ahead and is trying to catch up and there was a um, um, a study by the ITU, um, not our ITU, but the IT union, the information uh Telecommunication Union and say you un, uh organization which is based in Geneva and they bring a cyber security preparedness report out. And in 2022, Denmark was on place number 38 or 40 or something between Kazakhstan and China. So it did not look very good on that thing. But the question is also how do they measure this? Of course. Well, you know, like but um, it's definitely when it comes to digitalization, Denmark is number one. But when it is about protecting public and private assets. Um, yeah, okay. Could be doing better, but I think there's a new report has come out. Um, but I have not. I have I don't know what the number is that you would have to check it. But this is, like, always like, uh, especially journalists like this kind of things, like. Oh my God.

00:26:34  
*Speaker 1:* You mentioned that your students did a research regarding the vulnerabilities.

00:26:41  
*Speaker 2:* It's about, uh. Is it about what? I have many students, too many vulnerabilities about many things.

00:26:47  
*Speaker 1:* If I was.

00:26:47  
*Speaker 2:* If.

00:26:48  
*Speaker 1:* It was a Danish digital system, as far as I understood.

00:26:52  
*Speaker 2:* Um, which one? I would be hacked to evaluate clearing system. We hacked. Uh, uh, we had done different things. Yes.

00:27:03  
*Speaker 1:* I did, I did, I did Did.

00:27:07  
*Speaker 2:* Did you research? Maybe they might add.

00:27:09  
*Speaker 1:* Oh yeah yeah yeah yeah yeah yeah. So there's a I have a former student. Reverse engineer the app of BDD. Um, so, you know, you download the code on the phone and then you just look at what you find and how it is implemented. And, um, so what, he found out he could actually rebuild it. Okay. So he could have his own App Store app for, uh, for BDD. That was, um, not so good. The other vulnerability in this is not really a vulnerability, but in some sense it's a valid vulnerability because you can say, uh, you know, the media works with this QR code, right? Yeah. And so the QR code, uh, um, is basically linked to your telephone. But, you know, with the students work, you could actually, you know, write your app without the barcode is like so, so. And as I said earlier. Right. You know, security is obviously defined in terms of trust assumptions and security policies. Okay. So the trust assumption, um, is that, uh, the QR code works for it to be secure and, uh, be bound to your own, to your location, so to speak. But what the student has actually shown that this trust assumption is violated. So trust us and you can't trust it. Trust is a liability. And so, uh, so this was basically the, the, the, the example of uh, of that, that, that thing. Yes. But uh, the in response to this, uh, the, uh, the student did not do it while he was a student here. He already graduated a few years ago, but he contacted me about his findings, and, uh, I, I helped him to navigate the disclosure of orders, um, in such a way that he didn't make a mistake. Of, uh. Uh, yeah. Uh, publishing things that you shouldn't publish, although he hasn't signed anything. Um, so. And I and we, we managed to talk to digital settings too soon to actually update it. So I think in the fall of last year, there was an update was pushed where the head of digital is saying thank the people for meitu anonymously. And, uh, so this is like, uh, what you can imagine. But in Denmark, there's no bug bounty programs there. I think, you know, uh, the student, uh, deserved some bounty, some, some money for actually finding this vulnerability. But, um. Yes, um, he he hasn't. He's, by the way, giving a talk in the ethical hacking class in a few weeks. So it tactics explains to our students on how to do this.

00:30:04  
*Speaker 2:* Is it possible to contact him? Do you think he will agree to talk with me?

00:30:09  
*Speaker 1:* Sure. There's a student at ITU and? And this is your specialist thesis, right? Yeah, I just ask him. It's just he's someone. What's your season?

00:30:58  
*Speaker 2:* Uh. My thesis. Is regarding cyber security in a region hostile.

00:31:08  
*Speaker 1:* What about cybersecurity? Let me just.

00:31:13  
*Speaker 2:* Yeah.

00:31:13  
*Speaker 1:* So I can make it up. Yeah.

00:31:15  
*Speaker 2:* So the study of the emergency response of the, uh, for the cybersecurity, for the cyber attack in the region. Host. Hold still.

00:31:25  
*Speaker 1:* Okay. Let's say an emergency.

00:31:28  
*Speaker 2:* The emergency response on cyber attack.

00:31:34  
*Speaker 1:* On cyber attack.

00:31:36  
*Speaker 2:* In the region hosted, if I'm pronouncing correctly.

00:31:41  
*Speaker 1:* Yeah. Where are you from?

00:31:43  
*Speaker 2:* I'm from Ukraine.

00:31:47  
*Speaker 1:* It's also cyber in the. In the region hosted. Okay. Yeah, I forget about the region, which then seems to be unnecessarily limiting. Um. Let's see.

00:32:40  
*Speaker 2:* Yeah, because I work as a hospital. So therefore my study was mainly focused on the hospital cybersecurity. And how do they fend from the cyber attacks? So therefore my thesis is also focused on the healthcare systems. So therefore I'm also asking not only about the election and the general cybersecurity, but also how it affects the health care system.

00:33:07  
*Speaker 1:* Okay, okay I see. And you work in the IT department. Yeah. One on one second. I just, uh I said yes, I'm just going to send you your, his contact information. But. I know. You can copy this. Just click on it. Okay. No. God, it's too advanced. These systems. Okay. His name is Lucas.

00:34:12  
*Speaker 2:* And he was a student of Ai2.

00:34:15  
*Speaker 1:* He was my two year student. It's the seasons. He reverse engineered remedy. And then here one evening, he was bored, and then he reverse engineered midday with surprising results. And I still don't know if it's fixed or not. Really satisfactorily fixed. Okay, but you can ask him.

00:34:40  
*Speaker 2:* Yeah. Thank you so much for the contact. If you have any people who you can recommend, who I can also interview for my bachelor thesis, please do so.

00:34:53  
*Speaker 1:* Yes, sir. I think you could, uh, reach out to, uh, KFC's center for Cyber Security. Um, the leadership just changed. I don't know the new guy. I don't know personally yet. Um, I have not met him. Um, you can also ask the digitally, thanks to them, but I don't think they want to talk to you. Um, but you can still try. Um. Let's see. These are the circumstances. Thickest.

00:35:32  
*Speaker 2:* No. Um. Iggy Dali.

00:35:46  
*Speaker 1:* Stuff. You can also reach out to, you know. At least your seasonal skill.

00:36:13  
*Speaker 2:* Yeah.

00:36:13  
*Speaker 1:* Because you want to ask. Yeah. You want to ask another, um, scientist as somebody who has very, very active uh, is him here? He said he's not always. You just copy this thing or what? So difficult. This question.

00:36:47  
*Speaker 2:* So I think he is, um.

00:36:49  
*Speaker 1:* He's a computer scientist, but he has a lot of experience, and he has a lot of experience with the, um, there's the laws and the contracts and then these two and so on, and zero trust and so on. And so he's a good person to talk to.

00:37:06  
*Speaker 2:* Yeah. Because I haven't found really like a lot of people who can help me with my research.

00:37:13  
*Speaker 1:* Yes. So there's like you will notice that in Denmark there's a certain.

00:37:17  
*Speaker 2:* It's.

00:37:18  
*Speaker 1:* People not, uh, willing to talk about it because any cyber tech, they, they interpret this as a weakness in their preparation. And nobody likes to talk about their weaknesses. Um, and I think this is fundamentally what needs to change in Denmark. Is this, um, this understanding that if you're attacked, it's not because you have poor defense. It is like the attack because of things that are beyond your control. And by using the systems that we're using, there are security Swiss cheese. They have a lot of holes in them. And so instead of saying, like, we don't talk to each other, we need to have transparency, we need to exchange information. And most importantly for critical infrastructure sectors, we have to have something like Isaac's. Isaac's is the US. Uh, I think they also come in obviously to this, uh, information sharing and analysis centers, basically public and private organizations. They they work together. It's a it's a it's it's not a full time center or anything, but they are they are working together. They know each other and they are preparing for the worst case. So should some, you know, in the Danish uh, train station system, some, some cyber attacks should happen and the trains don't go. Everyone knows what to do. Okay. Everyone knows whom to contact. They have their day in the US. They do. I don't know how often they do that to tabletop exercises. They actually simulate those those things and know exactly who do I have to talk to? They can react within minutes. Uh, in Denmark, I have the feeling they were like, okay, we got a tag now. Um, whom are we going to call? Ghostbusters or CFCs? Uh, no, sorry. You're not responsible for this. So this is this is the only way forward is to to anticipate and to prepare for these events. It's not a question of if this event is happening. The question is when is happening and how are you able to react to it? And this this is this proprietary. We don't want to talk about this. We don't share nonsense. They're not going to get any further. Um, that's a hindrance. And uh, and so from the thing in the election domain. You will see that in some countries people are very open, like in Denmark. In other countries they are not okay. So they are actually like meeting someone behind closed doors. The minutes are not public. There's also no willingness to share. And then there's a frustration by political parties immediately of like, you know, what are they doing? And and so on. So this is not good. You know, in cybersecurity you have to have openness and transparency that is very difficult to, uh, to teach, um, to Denmark. And I think those are the Danish levels of trust are so high that, uh, you know, when you tell them that trust is a liability, they don't understand that. How can how can you trust everyone and live in a very nice society? And then that comes as German clown and says, like, you know, trust is a liability. You shouldn't trust anyone. It's not compatible with the way how society is organized. And, um, and in some sense, you know, I'm said to be the bad bringer of news, but I do not know how to do this today. There should be a way where you can combine this, you know, cyber preparedness and maintain the high levels of trust in the society. And I think that this is like this is the job for the next ten years for the country to figure out how this actually goes. Have I seen many people talk about this now? Not really, but I think that's essential. Because you can't, you know, until that day, you know, the trust. Like nobody would do this. Yeah. Nobody would do this. But course, nobody would do it because they're all nice people, right? But maybe some hacker from the other side of the planet, you might want to do it. And what are you going to do then? Oh, that's not going to happen. It's also nice people on the other side of the planet. We don't know.

00:41:37  
*Speaker 2:* But anyway, like how would you describe how does the politics of the outer world affect the Danish cyber cyber policy, cyber warfare? So basically, the result of conflicts between the Asian countries and right now is the US is trying to buy Greenland. So how does it affect it?

00:41:58  
*Speaker 1:* I think it affects us tremendously actually. Um, you know in but you know, so, uh, ten years ago the universities had to be more international, more global. Okay. And, uh, we had to work with Chinese companies and everything because that was really, like, encouraged. Um, they actually money was given to strengthening Danish companies, interactions with Chinese companies and so on. Now it's like, uh, when you work with somebody of Chinese heritage, you have to, uh, We have to you. We have to go. So, um, uh, security assessment at the university. If our work is covered by by laws and so on. So this in ten years, the entire landscape has changed from open to closed. So, uh, Denmark takes it very seriously. Um, but, uh, ten years ago, people like me who kind of said, like, we don't know how stable the geopolitical situation is. You know, we didn't have any. Nobody listens to us. It's like, what's this guy talking about? It's going so well when you look around now. Um, yeah. It doesn't seem to be going so well. No, you really should be self-sufficient. The other thing is also that, um, uh. And you see it and I haven't seen any, uh, any movements to the opposite, but, uh, Denmark is a Microsoft country. All data. It's an American owned servers possibly in, you know, based in Denmark, but it's a Microsoft country. And, uh, so, uh, the security of the data and this is not just like a health data. This is, you know, that, of course, is extremely sensitive. But as I think it's also other national security data that actually lives on Microsoft servers. So, uh, you know, in what I expect to see is that, uh, the country is, uh, going to revise its position of dependence on American companies and, uh, um, things might change. But, you know, this this changes, I think I know. Well, the reason so government hasn't had to get a chance to digest and to react to it. But I would expect, um, that this, um. Yeah, I'm actually invited to give a talk. I should accept that. Not since I talk to you, I think. Makes sense. So again, I don't want to be like the one again, bringing the bad news, but, um, this dependence can can backfire. Um, you know, uh, who knows what the future brings? So, uh, it's a very it's it's a somewhat sad development in the world, um, that, uh, we'll have to do it like this. I know that, uh, Danish law requires that Danish data is stored on the Danish continent, but, uh, so as Microsoft has a data center someplace here that stores all of the data. So in the case of emergency, the Danish authorities can go to the data center and, uh, require access to records. But the, uh, the the the center itself is owned by Microsoft. So, uh, other countries, uh, in Estonia, for example, that these data centers that are Actually owned by the public. And, uh, um, they are protected by the public and they have, uh, excellent cyber security people educated in their own country, uh, to actually take over the roles I've been I've been to the asserted, uh, cyber defense Center in Tallinn. So, um, you know, it is a I've been also to the, uh, I've seen the server in the data center where the internet votes are collected, um, which is just one out of many, many, many servers. Um, it's actually just a small little thing. It says like it was it posted on other stuff like internet, more internet connection. That's it. But, um, Denmark has chosen a different way. The entire infrastructure is so splintered and splattered. Every company, every, uh, region hosted and probably has its own data system, their own computer systems that are stored someplace which are not connected to the one from all those, um, lots of the medical data is stored on and on. On computers. In research. In the old nuclear research facility. I just gave a talk about, uh. I was interviewed by Dr. on, um, you know, the, uh, always has a huge HPC cluster, the high performance computer. Um, to actually do genetic, uh, to work with genetic data. They have access to all of the data of dates, the genetic data. All of the kids are being, uh, genetically registered when they're born. That data is going to do this research project. What could go wrong? And it was started in a year and ten years ago. So where the project partners, you had to work with project partners from abroad? The Chinese companies, US companies. Who knows where this data is? Okay. So, uh, there's a certain it's difficult, you know, to come and say, like, you should have one data center and the data is already out there. And also Denmark has like a lot of data. It's highly digitized. All of the data is digital. Everything. So this data is someplace. Access to this data is a given. At the moment. We trust the government, um, to actually handle it. Right. But this is also a very strong trust assumption. And there are very, very little if you just think about like an Elon Musk is taking on Denmark and, uh, gets access to all of the data, I think they can they will have they will have the opportunity to to link data and see patterns. There was many years ago that somebody from digital is sharing students and gave a talk here and he said like, um, you know, we have um, the dental data of, you know, when the kids have bad teeth and uh, and social data of the kids live and who the parents are and so on. And so they actually they're working actively. Maybe they don't anymore. Who knows? But I'm actually linking these two data sets to figure out, like kids with bad teeth and possibly neglected by their parents. Um, as, like, uh, this data is like in Germany. You could never find this data. It's not stored. I mean, maybe in some fun, some faxes and some folder in some shelf someplace, right? But here in Denmark, it's all the data is all there. And the access to this data, the way how it is organized. Uh, this is actually also something talking to a journalist about, uh, Monday. It's it's it's it's actually, uh, slightly scary. Yeah. It is, it can it can be scary. And, uh, you know, the, the protection we have seen, you know, like, uh, the way the public, um, infrastructure is built, I think because it is built fast and quick, it's not built with security in mind. Um, and you can see it, uh, that there was a midday midpoint, um, because you can read your ebooks, data validation, and then the first 50 people. When they logged in, they saw other people's data. Okay. Last week or two weeks ago, non-it investors, you know, for investment I don't I didn't know about the investment portal. Okay. Keep the same thing, people. There was a guy logging in, and he suddenly had a account balance of half, half a million, half a million crowns. And he didn't know what to do with this because was not there was not his account. So how can how can this happen? This is this can only happen because the the foundational structures and the programs and the systems that are built. They were built to ten, 15 years ago during the attempt to Denmark try to be more, um, you know, more digital. But nobody thought about security at the time. And it's not built into the systems. So to make it, to build it properly, you actually have to invest. It's really expensive. Uh, you know that you need data. You need maybe cryptographic keys. You have to encrypt stuff. You know, it's like, how do you actually get the honor? I have to do this all retroactively from, like, 15 years ago. What are you doing? How do you do it? It's almost impossible. So Denmark, especially because of its leading position in digitalization, I think is a gigantic challenge in securing their data infrastructure. And, you know, if they are like if they're ready or not, I do not know. Sometimes I get a little excluded here from public, uh, public conversations. So everything I say is not my personal opinion. It doesn't reflect anything anyone really has told me. But, uh, this is just my my my observations over the years. Yeah.

00:51:10  
*Speaker 2:* How vulnerable are the CPR numbers since they consist of our birth date? And I guess it's for randomly created digits.

00:51:22  
*Speaker 1:* And not randomly created. You know, the last digit is. This is even I can tell you this already. Yeah. Um. Mine is. Mine is odd. Okay, men, you can distinguish the sex of a person by the CPI number. That probably already constitutes a leakage of personal information. I actually, I would be very surprised if CPI numbers are not illegal under some EU EU directive for the protection. They probably not GDPR. Nobody has ever asked you if it is okay for a particular organisation to know your sex. You did not give consent to it. So in some sense I think the CPI, by the way, definitions are actually okay. And this is me talking as a computer scientist, not a lawyer. There might be some clause that protects this, but I would be very I think it is actually, uh, at odds with the requirements of GDPR. On the other hand, there's also some other data like health data. And you also didn't give consent to its storage in Denmark. But there are laws that say that you have automatically given consent, but you have the right to withdraw consent when you if you want. I think I gave once an interview to a Japanese station TV station. They came here and they wanted to know how the CPR system works because in Japan you can't have it. Okay. Um, yes. And so, uh, it used to be that CPR was a really, really well protected display, like your secret identity. And it was actually a time when I moved here. And there's a CPR number leaked on the public document on Google. Google was asked to please remove it from the webpage wherever it was and the search register. Okay. This is changed. um, no, uh, CPI numbers are not that, you know, because of midday, you have to have midday in order to identify and authenticate. It used to be that they called the tax office said the CPR number, and then they could change your taxes or somebody else's taxes on that for that matter. The only thing which is problematic is the CPR numbers that that allows you to link data because, you know, the databases we just talked about, they're all stored. So it's the linking identifier. It's not the fact that you know it, but it's the fact that it is used in different data sets consistently, which is the problem with the CPR number right now. Um, so, uh, you know, yeah. That's it. Um, it's uh, it's it's old. It's, um, it has served Denmark very well. I think, uh, compared to Germany. But there's such a number does not exist. Um, it has not been, uh, misused to what we see for. But we will People not know it's not protected. I don't think the number is protected in a way that would prevent from somebody with the same of ambitions as Elon Musk to link to your business, and would actually leak a lot of information about you all the way to your genetic code.

00:54:32  
*Speaker 2:* How would you advise to secure the car number? Better, since basically we don't have any identification on it. So you can just come to the hospital and say like, this is my CPR number and no one will actually know if you're like the real deal. So like.

00:54:49  
*Speaker 1:* Okay, there's a lot of theory on, um, on these identities. Okay. So, um, one of the, uh, there are linkable identities, I think I forgot not exactly what they are really copied. So basically you have different numbers for different situations, and you can, um, you can reveal Information about who you are. But then this number can't be misused. But you know, when you go to a library, this you have one identity. But when you go to a hospital, you're going to have a different identity. But this identity then can be linked to your health records identity, and you can choose to reveal it, but you can also choose to withdraw, um, these, these identities. So, um, so there are more complicated ways of, you know, they're they're really there there are people in this world, computer scientists, who are thinking about those things and how to how to revocable. I think they're called revocable identities. Well, I don't know. Um, and, um, today there are different ways on how you could actually do it. Um, another thing is you don't actually have a number, but you just have a chip on the CPR on the card, you know, and you use this, uh, this, this chip to, uh, Uh, share information. You know, when you when you log in. So then the chip will actually, uh, it will check that, uh, it's really you by by a process of, like, signature checking or something else. But it could be that there's the secret key is, like, embedded in this chip, and they have it in Estonia like this. I don't think in Estonia they have any numbers. And all of the laptops in Estonia have a little smartcard reader. You just when you want to vote, you just insert your smartcard into the thing. So that has the the advantages and disadvantages, the disadvantages that you have to have that card. And so it is somewhat better in terms of this. And then you don't need your CPR number but identify yourself okay. Hold on to my other daughter my second. They are driving to pick me up. Okay. Yeah. Identities or something or. Yeah. Oh, but how do we do this better? Yes. So, um. Yeah. Yeah, there are ways how to do this better. Okay. And then in Estonia you have to have this card. And so Estonia is actually moving to all of these. The Baltic countries are moving to something called smart ID. But they actually it's a little bit like midday. But you know, maybe you have smart ideas in uh, in Ukraine, I don't know. There you go. There you have the dot, right? Yeah, yeah. So the, the you know, you could also use something like Dia, but there's also something problematic about Dia. I understand this correctly. And there was something about the voting for the. I mean but the big problem is Dia of course, is that, uh, you, um, um, not everyone has it. It's not that many people who don't have the D. Probably also many people who don't have a telephone.

00:58:54  
*Speaker 2:* Yeah. And, uh, if you know that, uh, in December last year, the president was giving, like, some sort of, like, a financial aid to the citizens, and by agreeing to receive it, they agreed to share all of their like, bank records and personal information to the government. So yes, it was very smart move from the government to kind of like track the citizens.

00:59:22  
*Speaker 1:* Yes. Yeah. Because at the moment, yeah. In the UK it's difficult to track people. Right. But there's no central register. I know I've been working with the, uh, Election Commission of the Ukraine, so.

00:59:39  
*Speaker 2:* I should ask you more questions about the cyber security in Ukrainian as well.

00:59:44  
*Speaker 1:* I was actually part of the cyber security assessment for I was in 2018 before the 2019 election. In Kiev. I was there. Yeah. Yeah. That's been I've been to Kiev a couple of times, but I have not been since the war started. I leave it to Oksana. Gary.

01:00:04  
*Speaker 2:* I'm very impressed.

01:00:08  
*Speaker 1:* About what?

01:00:10  
*Speaker 2:* About the fact that you know so much about the Ukraine, the cyber security in Ukraine. Because I. I honestly haven't found any information about you, like in the articles regarding the Ukraine.

01:00:21  
*Speaker 1:* Yes, I've tried to keep a low profile. I, you know, I work with a lot of and I work in many countries. I even work in Greenland. I might be going next week to Greenland for the election.

01:00:34  
*Speaker 2:* Oh, wow.

01:00:37  
*Speaker 1:* So March 11th or March 11th? Yes. Okay. That's that's what's missing in my calendar. I knew that there's a problem. Okay. Yeah. No, no, I know I've I've I've been to many places. I've been also. Yeah, I even hosted, you know, the former head of cyber defense is a good friend of mine in the Ukraine, Viktor Zohar. Because he was actually here, I invited him here, and he came here and said the entire election commission, they came to visit me in 2015. There was a time where there was a different time because, uh, the, um, um, yeah, the preparedness and the money was different. I mean, there was a, there was already a conflict. Um, but, uh, but the, the, um, so I always had the feeling that, like, the commission is missing smart people to help them. Uh, they just didn't have the funding to pay for people to just, like, you know. Yeah, I don't know. I know many, I know many.

01:01:45  
*Speaker 2:* How would you comment about the cyber security system in Ukraine versus Denmark?

01:01:51  
*Speaker 1:* I, um, so okay, so from my experience, this is all back to 2018, And that was very clear that there's um. So the number one is Ukrainians are highly educated in cybersecurity, offensive techniques. And so, you know, in Ukraine you can have attacks coming from the outside, but you can also have a tax coming from the inside. Um, and um, that makes it makes it completely different from, from here because, you know, the, uh, because of the history of, of of Denmark, it's much this is a the the, the the attack vectors are different. They're here. Um, other than that, the Ukraine and, um, and and then there was a, you know, I b there were uh, there was this it was this attack against the voter registry. So two days before the election, uh, they removed that. They, they, they cleaned all of the computers that had, uh, all the data on it. So that meant actually on Election Day, basically, they had to scramble and they managed to kind of restore it again. Uh, the day before the election, it was really, really tight. There was almost no election after after after this, this attack. And the question is really why was that and how could have this been prevented better? But, you know, there are at least in 2018, I don't I hope I don't say anything wrong, but, um, it seemed to be that, uh, in the technical equipment for public offices was outdated. If I remember correctly. And, um. Yes. So this is something that, um, better stays between us. Yes. Um, this goes nowhere. No report. Um, but, uh, um, the, uh. Um. Yeah. And and I think it was just, you know, we have to have security. Do you not secure your secure for a second before becoming insecure? And then you have to keep on investing in it? And if you don't do that, then, um, you know, and it takes a lot of resources, but if you don't do it, then you become insecure and more and more insecure over time. And so I have not looked at any computer system in detail. Right. The way what we do is always we talk to interlocutors, um, and uh, and then, you know, summarize the feelings and, uh, what we've heard and to report essentially, um, and then this report is presented to whomever. And so what I, what I tell you, here's all my personal opinions, and it's nothing to do with any official mission. I was on one too many missions, but, uh, yeah, I should tell you this. Yeah, yeah, I've been. Yeah, I've been, I've been I've been seeing a lot of interest in the Georgian election also last year.

01:04:56  
*Speaker 2:* So how would you I would say like describe the cyber warfare since the war in Ukraine started. So was there any differences since you've been in Ukraine in 2018 and probably you heard about the situation now there.

01:05:12  
*Speaker 1:* So how do so I know about Kiev. Kiev stopped being hacked in was last year or something. But um, you know, all all of our equipments have vulnerabilities. Um, they are called zero days. So because that's the vendors had zero days to fix them. We just don't know what the zero days are because otherwise they would have fixed them. And we do not know who's access to this knowledge. You know, like, um, I think the, uh, um, the, the, the situation has changed in the sense that, uh, these zero days have become the ammunition for cyber war. Um, and, uh, you know, there are people who are actually looking at vulnerabilities in systems, and then they publish them and sell them on the black market. I mean, you know, like, I think one zero day goes like for $2 million or something like that. So if you want to, but then, you know, a Secret Service buys it. Um, and then I have it and this is like, you can do one shot with this thing because once you've used it, everyone knows what it was. And then they fix and protect against it and then you can't use it anymore. So you have to be very careful about how they use the zero days. And, uh. Um, there was the Stuxnet attack against Iran. And then like many, many years ago, um, and there was a I was like an attack that was, uh, engineered against, uh, the centrifuges that enriched uranium. Um, and so basically there was a documentary. I watched this and I got this. I was never in Iran. I have no idea. But there's really but I've seen the documentary. And so there was then President Bush said, uh, you know, 2004 or 8, whatever. He said, like, I need a man handling with Iran. I need a third option. Okay. I can't just decide between war or not. War. I need a third option. And so, uh, then somehow that's at least what was written was explained in this documentary. And this, this this virus was developed and there was a company, I think, in the, I think in Estonia or in, I don't know where, uh, and then maybe even Belarus, I have no idea. But there was a security company that actually got the virus and reverse engineered it. And in this documentary actually see these people, that's how it starts. And then they kind of look at it and said, this is extremely well organized code and it contained five zero days. So it is like it's a piece of code that when you let it out in the, in the it doesn't stop, but, you know, it just installs itself on a computer. You don't if you can't do it, Can't do anything against it. Right. And it had five of those things in it. It could use five different ways to access a system. And it was only only it was a piece of code that actually, um, it was really tailored to particular, um, scanner devices like these, these, these, these, um, these controllers for those centrifuges. And they were like Siemens whatever. They had some number in the, in the code and they didn't even know what it was. And the reverse engineered the code and they looked at it and said, what is this thing? And then they googled it and they said, okay, these are centrifuges are okay. So what is this thing actually for? So, uh, so, you see, um, what I want to say is like all of our computer equipment that we have had some many zeros on it, and there's every system that we installed, every security date update might close some, but it opens new ones. Um, so you can't you just you can't expect this to be 100% secure. And so I think in, uh, in, in, in the Ukraine over the, uh, the 2018, the trust assumption just changed, um, in the sense that many people were trusted, many entities were trusted, and suddenly they were no longer trusted. And so that meant that, uh, the entire security argument for why something is secure or not is probably, uh, is invalid. Right? So you have to basically look at it. So what is if I, if I'm being attacked by like a the Secret Service from a different nation state, how can I defend against this. And so, uh, yeah. So this is um, and this, this I think what is what what has changed and and maybe in the good old times, it was okay to have old routers or old systems that weren't updated because the trust assumptions were like, okay, nobody's going to look, nobody's going to be interested in this anyway. And then suddenly from one day to the other, everyone was interested in them. So and, you know, in any security, um, source relevant system, you have to make a decision when you have finite resources, how do you spend these resources? And, uh, you know, there was a lot of, uh, when Ukrainian Ukraine was not, uh, in 2000, you know, when the when the real war began. I mean, was it the richest country in the world? Probably not. Um, the American that probably had more money to always upgrade their systems. Could imagine that, like, old laptops were reused and in critical things, like somebody and I, you know, this thing I don't need fast enough. We'll use it to control this and this. Right. Um, and, uh, and but I don't know if that's for sure. I don't know if that's for sure, but I, I can imagine that if you have, like, uh, resource constraints, this is how you, uh, how you handle, uh, handle upgrades, and you don't, uh, don't have maybe not the right, uh, power manpower to, to do security the updates. Maybe they are. The systems are end of life. You know, bad things can happen in these situations. So it costs a lot of money to kind of secure something. I think Denmark could afford it but is a little late to the game. Um has too much data to do it effectively, but maybe when they put a lot of money into it, then they do it. And I'm sure the big companies like Nuvo and Lego and Maersk, they have learned from their mistakes. And I think they're doing it, but they're doing it in a very private way. We don't know what they're doing. Um, and in the Ukraine. Yeah, I don't know. I haven't been I haven't been back since 2000, 2007. 2018 was the last time I was there, I think. Uh, yeah, that was one time before, but, uh. Yeah. Yeah, this is interesting. I get a lot of, uh, views on more top, you know, not just academic views, but also real life views. I just don't know what to do with this. And I don't know if it's like all of this is a little bit of hearsay, but is what I said about the Ukraine is my personal impressions that I took away from talking to people, I hope precise they are. They're definitely outdated and that there are certain years outdated. Um, but, uh, yeah, but I still think that, uh, Ukraine has a lot of clever people in it. They're highly educated and they are even. You know, Simcoe actually has a production lab in Kiev. I had a production life in Kiev. Um, because, you know, they just employ Ukrainian programmers and they're very, very good, as far as I've heard. Um, but have. Any other questions?

01:12:29  
*Speaker 2:* No. Not really.

01:12:31  
*Speaker 1:* Not really.

01:12:33  
*Speaker 2:* If in the future we have questions, can I contact you again?

01:12:36  
*Speaker 1:* Yeah, sure. Do it. Yeah.

01:12:40  
*Speaker 2:* And I would like to ask you. So your professor for the ethical hacking.

01:12:47  
*Speaker 1:* Yeah. I'm teaching. Okay. I'm. Alessandro has designed this course. Ethical hacking. But I'm, uh, he's on sabbatical, so I've taken over his course for this this semester, and I. Yeah. And, uh, so it's called ethical hacking. And, uh. Yeah. That's me. But, yeah, it's it's it's actually all of us. I'm responsible for it. But, uh, lots of my colleagues are teaching these classes. Okay. So.

01:13:17  
*Speaker 2:* Yeah, because. Yeah, I was thinking taking it next year as an elective for my master's degree.

01:13:25  
*Speaker 1:* Yes, yes.

01:13:26  
*Speaker 2:* Oh, you definitely can. Um, yeah. I saw my first lecture. Was really good, by the way. It's too late. I didn't record it. And you know, when I. When I record my lectures, then I don't talk as freely as for example, via you also recording me. But I'm also careful what I'm saying. Um, but, uh. Yeah.

01:13:49  
*Speaker 1:* Yeah, but I will send you the I will say the part of my thesis that I will write about talking to you. So like, I will not I will not mention your name if you didn't want it.

01:14:03  
*Speaker 2:* Yeah.

01:14:04  
*Speaker 1:* Yeah, yeah. Just just send it to me and we can see. So in some of these things is, as you know, very touchy. Um.

01:14:12  
*Speaker 2:* Yeah.

01:14:14  
*Speaker 1:* Yeah. No worries. I will not, uh, I will not try to create any conflicts. So everything will be neutral.

01:14:22  
*Speaker 2:* Yeah.

01:14:23  
*Speaker 1:* Just, uh. Yeah, a little bit. It was good talking to you. So I think there's some, uh, some follow up things that, uh, one should be discussing in the press. Let's see if I ever get an opportunity again.

01:14:35  
*Speaker 2:* Yeah. All right.

01:14:38  
*Speaker 1:* Yes. Thank you so much. Yeah. Thank you so much. Yeah. Have a nice.

01:14:42  
*Speaker 2:* Day. Yeah. It will. Bye bye.