Interviewer: Can you describe how you discovered the vulnerabilities in election systems and how these vulnerabilities can be applicable for Danish election systems?

Researcher: You have to distinguish what kind of technology you use in your elections. With paper elections, there is physical evidence that you can check and recount if necessary, but it must be securely stored. Vulnerabilities are usually detected when you count the results a second time, but only under the assumption that this evidence is securely stored.

With electronic elections, it's much more difficult because how do you recount an electronic vote? You can run the counting program again, but if somebody changed the database, you'll get the same incorrect result. This is why the concept of "verifiability" has been developed over the last ten years.

Verifiability means you can actually verify that the result of the computation is what it's supposed to be. In election systems, you always have to balance the privacy of the vote versus integrity. There's always a tension between secrecy and verifiability. If you want to verify everything, you'd need to know how people voted, but that compromises privacy. Conversely, if you want complete confidentiality, you'd need to encrypt everything, but then nobody can verify the election results.

Paper ballots solve this elegantly because you shuffle the ballot box—providing privacy first—and then gain integrity through many people counting. With electronic systems, it's extremely difficult, and impossible without making concessions. You can't have 100% privacy and 100% integrity simultaneously.

Finding attacks in verifiable systems is possible because the verification mechanisms will trigger alerts when something is wrong. Of course, the problem then becomes how to recover from it, which is much more complicated than simply running the election again.

If the system is verifiable, you can detect problems. If it's not verifiable, you can't figure it out. It's as simple as that.

Interviewer: Which main security flaws did you figure out?

Researcher: The primary flaw is that most systems are not truly verifiable. When analyzing election security, it's critical to examine the trust assumptions and adversary model. You need to know the capabilities of your adversary and who you're defending against. In elections, we're potentially facing nation-states and powerful intelligence services as adversaries.

At the same time, many people are involved in running elections, and you have to decide whom to trust. Ideally, you don't trust anyone, because trust is a liability—if you trust someone and they disappoint you, you're compromised. You want to minimize this trust as much as possible.

Election technologies need to satisfy certain security properties that go back to the UN Declaration of Human Rights, Article 21, which states that everyone has the right to government

constituted by genuine elections with secret ballots. So elections must have integrity and preserve privacy, plus have verifiability to make the whole process trustworthy.

Different systems have different flaws. In the Swiss system from 2019, researchers managed to exchange the ballot box with a different one, and all checks still worked—nobody would have known the result was compromised. That was an attack against election integrity.

In Norway in 2012, all votes were encrypted with the same randomness, meaning the ciphertexts were identical. So if you encrypted votes for Party X and saw the resulting ciphertext, you knew exactly how people voted. That was an attack against privacy.

I've also observed African elections where they use results transmission systems. They vote on paper and count on paper, but nobody trusts that the paper leaving the polling station is the same paper that arrives at the counting center. They've implemented a lot of technology in the electoral process, but the digital transmission systems always had flaws. Sometimes what was legally binding was what people typed into the computer—but if they made a typing mistake, that became the official result. In Kenya, the Supreme Court in 2017 invalidated an entire election because of such issues.

An election is not merely a technical system—technology is used to run it, but it's fundamentally a social computation. That's why there are laws, Supreme Court decisions, and high-level definitions involved, which makes this an extremely interesting field to study. It's different from, say, a company whose milk-selling system gets hacked. They might lose income for a day, but it doesn't destabilize an entire nation. Elections are absolutely critical to society.

Interviewer: How did the findings on election system vulnerabilities influence broader discussions on national cybersecurity? For example, if an election is happening in Denmark, how would it be affected?

Researcher: In my experience, elections are operations based heavily on national pride. Every country believes their way of running elections is the best. The paper elections we use in Denmark have evolved over the past hundred years or so, and the processes have been refined over time, as in many Western countries.

When you look at Danish elections, it's fascinating because all steps are verifiable. When polling stations report numbers to Statistics Denmark on election night, the information is transferred in three different ways: once to a computer system built in the 1980s, once through a telephone call, and once by handwriting in a book that's physically transported to Statistics Denmark. Because of these redundancies and checks, Denmark is largely unaffected by issues that occur in other countries.

That said, Denmark has moved to digital electoral rolls. When you arrive at the polling station, you show your card with a barcode, they scan it, and you're digitally crossed off the list. The question then becomes: what happens if the system goes down? This happened in Scotland around 2019, and it creates significant problems. Typically, there are paper backup books to fall back on.

Denmark's election system is very verifiable. In fact, Denmark is often ranked number one in measures of democratic quality. However, the people managing digital voter rolls are becoming concerned about cyber attacks. A few years ago, we worked with Copenhagen to provide training materials to prepare for potential attacks during Election Day—identifying weaknesses and developing defenses.

It's important to understand that a vulnerability in a technical system doesn't necessarily mean the overall process is vulnerable, because there might be operational mitigations in place. Denmark handles this well—for instance, there are always two people managing the digital voter rolls, so if one person is unavailable, the system remains secure.

Nevertheless, if power goes out and digital election lists fail, forcing a return to paper lists, it will be inconvenient and time-consuming, potentially damaging the reputation of the electoral process. There's always a trade-off between convenience and security, but Denmark has the whole spectrum covered and can recover if something goes wrong. The risks have been calculated, and they're deemed acceptable.

The digital voter rolls run on laptops with their own local network, not connected to the internet. So even if external power or internet fails, they should continue to function throughout Election Day. They would only fail in extreme circumstances like an electromagnetic pulse that disables all technology.

Interviewer: What parallels exist between election system vulnerabilities and risks to other crucial digital infrastructure, such as healthcare systems and energy grids?

Researcher: Elections are the quintessential challenge—if you understand election security, you understand all other domains. What makes elections unique is that integrity is easy to verify because votes are public, but you cannot check your individual vote since that would enable vote-selling. The tension between maintaining integrity, privacy, and verifiability is much more pronounced in elections than in other contexts.

That said, elections only happen periodically, while other critical systems must operate continuously. With elections, everything must work perfectly on Election Day—there's no option to say, "This function doesn't work yet, but it will be fixed next week." After the election is over, the system can be taken offline until the next election.

Another difference is the infrastructure structure. Elections are very hierarchical—polling stations communicate data upward to a central point where few people have access. Healthcare systems are much more decentralized, with many people having access at any time, which presents different challenges. Additionally, in a highly digital country like Denmark, you can't always have paper backups for healthcare systems.

I think countries are slowly recognizing that contingency planning should be considered when making cybersecurity infrastructure decisions. We've seen examples like telecommunications outages that weren't even caused by attacks but by software updates gone wrong. These incidents

reveal how dependent we've become on digital systems. Water, energy, food, and other critical infrastructure sectors face challenges similar to healthcare in this regard.

Interviewer: What role does Denmark play in international cybersecurity research and collaboration against cyber warfare?

Researcher: The non-political answer would be "not much." The more diplomatic answer is that Denmark has really understood the importance of cybersecurity over the last ten years and has invested significantly in building institutions like the Centre for Cyber Security (CFCS).

I understand that Denmark has been active in implementing European Union cybersecurity directives. Member states are required to deliver laws that implement these directives, and Denmark has been proactive in this regard.

However, Denmark's commitments to NATO and European defense don't heavily emphasize cybersecurity. Denmark has instead promised to focus on biotechnology and quantum computing. That's why much of the available funding in Denmark right now is directed toward quantum computing rather than cybersecurity—for some reason, the top political priority is quantum technology. This might be because NATO countries agreed that Denmark, the home of Niels Bohr, should focus on quantum research.

Many other countries like Germany and Italy have active cyber defense on their agendas, and I think Denmark would allocate more money to cybersecurity research if it were a priority at the EU or NATO level. Essentially, Denmark seems to be saying, "We don't prioritize cybersecurity, but we'll contribute in other areas instead."

Interviewer: How do you assess the effectiveness of Denmark's current cybersecurity policies in mitigating cyber warfare risks?

Researcher: I think there's a shame that they have to catch up. Denmark is way behind other countries in the sense that some of their laws require you to be quiet when you find security vulnerabilities—you're not allowed to talk to anyone about it, otherwise you risk going to prison. For example, look at the law number paragraph 14, which essentially says "don't talk about it or you go to prison for half a year."

This approach doesn't encourage your own people to find holes in the infrastructure so they can be fixed. It's based on outdated 20th-century thinking: "If we forbid it and penalize it, you won't do it." But this model doesn't work anymore in cybersecurity, especially against nation-states with excellent intelligence services that might plan to attack you. These foreign actors already know all the vulnerabilities but don't talk about them publicly, so they're not really covered by these laws. They're also not afraid of Danish laws—no hacker from a foreign country would say, "Oh my God, I shouldn't do this."

That said, Denmark is in the process of updating these laws right now. My students did research on this as part of an ethical hacking course. One team identified all the laws currently being discussed, which actually do address techniques for responsible disclosure. I haven't studied the

proposed legislation in detail, so I don't know if I agree with how it's being implemented, but at least these issues are being addressed.

Denmark is trying to catch up. There was a study by the ITU (International Telecommunication Union), a UN organization based in Geneva, which publishes a cybersecurity preparedness report. In 2022, Denmark was ranked around 38th or 40th, somewhere between Kazakhstan and China. That didn't look very good, though we should consider how they measure these things. When it comes to digitalization, Denmark is number one, but when it comes to protecting public and private assets, they could be doing better. I believe a new report has come out, but I don't know the latest ranking.

Interviewer: You mentioned that your students did research regarding vulnerabilities in Danish digital systems?

Researcher: Yes, we've looked at several systems. I have a former student who reverse-engineered the MitID app [Denmark's digital ID system]. He downloaded the code on the phone, examined how it was implemented, and found he could actually rebuild it. He could have created his own App Store app for MitID, which is not good.

Another issue, which isn't exactly a vulnerability but could be considered one, involves how MitID works with QR codes. The QR code is basically linked to your phone. But with the student's work, you could write your own app that works without the barcode.

As I mentioned earlier, security is defined in terms of trust assumptions and security policies. The trust assumption is that the QR code works securely and is bound to your location. But what the student showed is that this trust assumption can be violated. This reinforces my point that trust is a liability.

The student didn't do this work while studying here—he had already graduated a few years ago—but he contacted me about his findings. I helped him navigate the disclosure process so he wouldn't make a mistake by publishing things he shouldn't, although he hadn't signed any non-disclosure agreements. We managed to communicate with Digital Denmark, and I believe they pushed an update in fall of last year where the head of Digital Denmark thanked people anonymously.

In Denmark, there are no bug bounty programs. I think the student deserved some financial reward for finding this vulnerability, but he didn't receive any. He'll be giving a talk in my ethical hacking class in a few weeks to explain this process to our current students.

Interviewer: My thesis is regarding cybersecurity in the Region Hovedstaden [Capital Region of Denmark]. Specifically, it studies the emergency response to cyber attacks in regional healthcare.

Researcher: I see, so you're focusing on hospital cybersecurity and how they defend against cyber attacks. Your thesis concentrates on healthcare systems.

Researcher: You'll notice that in Denmark, there's a certain reluctance to talk about cybersecurity because people interpret any cyber attack as a weakness in their preparation. Nobody likes to talk about their weaknesses. This attitude is fundamentally what needs to change in Denmark.

We need to understand that if you're attacked, it's not necessarily because you have poor defenses. You're attacked because of factors beyond your control. The systems we're using have security vulnerabilities—they're like Swiss cheese with many holes. Instead of saying "we don't talk to each other," we need transparency and information exchange.

Most importantly, for critical infrastructure sectors, we need something like ISACs (Information Sharing and Analysis Centers). In the US, these bring together public and private organizations. It's not a full-time center, but these entities work together, know each other, and prepare for worst-case scenarios. If a cyber attack happens on the Danish train system and trains stop running, everyone should know what to do and whom to contact.

In the US, they conduct tabletop exercises to simulate these events and determine exactly who needs to be contacted. They can react within minutes. In Denmark, I have the feeling the response would be more like, "We got attacked. Who should we call? The Center for Cybersecurity? Oh, sorry, you're not responsible for this."

The only way forward is to anticipate and prepare for these events. It's not a question of if an attack will happen, but when it will happen and how you'll respond. This proprietary, secretive approach of "we don't want to talk about this, we don't share" won't get Denmark any further—it's a hindrance.

In the election security domain, you see that some countries are very open, like Denmark. In other countries, they meet behind closed doors, minutes aren't public, and there's no willingness to share information. This creates immediate frustration among political parties: "What are they doing?" This lack of transparency isn't good. In cybersecurity, you need openness and transparency, which is difficult to cultivate in Denmark.

The Danish levels of trust are so high that when you tell them "trust is a liability," they don't understand. How can you maintain a society where you trust everyone, and then a German professor comes along saying, "Trust is a liability; you shouldn't trust anyone"? It's not compatible with how Danish society is organized.

In some sense, I'm seen as the bearer of bad news, but I don't know how to reconcile these perspectives. There should be a way to combine cyber preparedness while maintaining high levels of trust in society. This is the challenge for Denmark over the next ten years—figuring out how to achieve this balance. I haven't seen many people talking about this issue, but I think it's essential.

The prevailing attitude is often "Nobody would do this; they're all nice people." But what about hackers from the other side of the planet? The response tends to be, "That's not going to happen; there are also nice people on the other side of the planet." This naiveté is concerning.

Interviewer: How would you describe how the politics of the outer world affect Danish cyber policy and cyber warfare? For example, conflicts between Asian countries and the US attempting to buy Greenland - how does this affect Denmark's approach?

Carsten: It affects us tremendously. Ten years ago, universities were encouraged to be more international and global. We were directed to work with Chinese companies, and money was actually given to strengthen Danish companies' interactions with Chinese partners.

Now the landscape has completely changed. When we work with somebody of Chinese heritage, we have to undergo security assessments at the university to determine if our work is covered by certain laws. In ten years, the entire landscape has shifted from open to closed. Denmark takes these security concerns very seriously.

Ten years ago, people like me who cautioned about geopolitical instability weren't listened to. Looking around now, the situation doesn't seem to be going well globally, which highlights the importance of self-sufficiency.

Carsten: Denmark is essentially a Microsoft country. All data is stored on American-owned servers, possibly based in Denmark, but it's fundamentally a Microsoft infrastructure. This includes extremely sensitive health data and potentially even national security data living on Microsoft servers.

I expect the country will eventually revise its position of dependence on American companies. The government hasn't had a chance to fully digest and react to these implications yet, but changes are likely coming.

Danish law requires that Danish data is stored on Danish territory, so Microsoft has a data center here that stores all the data. In emergencies, Danish authorities can go to the data center and require access to records, but the center itself is owned by Microsoft.

Other countries take different approaches. Estonia, for example, has data centers that are publicly owned and protected by the public. They have excellent cybersecurity professionals educated in their own country to manage these facilities. I've visited the Estonian cyber defense center in Tallinn and seen their infrastructure firsthand.

Carsten: Denmark's infrastructure is splintered and scattered. Every company and region hosts its own data systems stored in different places that aren't connected to each other. For instance, much of the medical data is stored on computers in the old nuclear research facility.

I recently gave a talk about how this facility has a huge high-performance computing cluster to work with genetic data. They have access to all of Denmark's genetic data - all children are genetically registered at birth, and that data goes to research projects. This began about ten years ago when project partnerships with foreign entities, including Chinese and US companies, were encouraged. Who knows where this data might have ended up?

It's difficult to advocate for centralizing all data now that it's already distributed. Denmark is highly digitized - everything is digital. This data exists somewhere, and access to it is currently granted based on trust in the government to handle it properly. But this relies on a very strong trust assumption.

If someone with resources like Elon Musk decided to target Denmark and gained access to all this data, they could link different datasets and identify patterns that would be deeply concerning from a privacy perspective.

Carsten: Years ago, someone from a digital organization mentioned they were actively linking dental records of children with social data about where they lived and who their parents were. The goal was to identify children with bad teeth who might be neglected by their parents.

In Germany, you could never find this kind of linked data - it simply isn't stored systematically. But in Denmark, all this data exists and is accessible, which can be concerning.

The protection we've seen in public infrastructure is inadequate because systems were built quickly without security as a priority. We've seen real consequences of this:

There was an incident with MitID (Denmark's digital identity system) where the first 50 people who logged in saw other people's data. A couple of weeks ago on a non-IT investment portal, a man logged in and suddenly had an account balance of half a million crowns that wasn't his.

These problems happen because the foundational structures and systems were built 10-15 years ago during Denmark's push for digitalization, but nobody thought seriously about security at the time. Security wasn't built into the systems.

To fix this properly requires significant investment - you need proper data management, cryptographic keys, encryption - and implementing these retroactively for systems built 15 years ago is almost impossible. Denmark, especially because of its leading position in digitalization, faces a gigantic challenge in securing its data infrastructure.

Interviewer: How vulnerable are the CPR numbers since they consist of our birth date and a few digits?

Carsten: The digits aren't even randomly created. The last digit reveals your sex - mine is odd, which indicates I'm male. You can distinguish the sex of a person by the CPR number, which probably already constitutes a leakage of personal information.

I would be very surprised if CPR numbers aren't actually illegal under some EU directive for data protection. Under GDPR, nobody has ever asked you if it's okay for a particular organization to know your sex - you didn't give consent to it. So in some sense, I think the CPR system may be at odds with GDPR requirements.

The same applies to health data - you didn't explicitly give consent to its storage in Denmark, but there are laws that say you've automatically given consent, though you have the right to withdraw it if you want.

I once gave an interview to a Japanese TV station that came here to understand how the CPR system works because such a system isn't possible in Japan.

CPR used to be really well protected as your secret identity. When I first moved here, if a CPR number leaked on a public document on Google, Google would be asked to remove it from the webpage. This has changed.

CPR numbers aren't as protected now. The real problem isn't that someone knows your number, but that it's used as a linking identifier across different datasets. It's this consistent use across different systems that creates the privacy risk with CPR numbers.

The system has served Denmark well compared to countries like Germany where such a number doesn't exist. It hasn't been seriously misused yet, but it's not protected in a way that would prevent someone with resources from linking your records and leaking significant information about you, potentially including your genetic code.

Interviewer: How would you advise securing the CPR number better, since we don't have any identification tied to it? You can just go to a hospital, give a CPR number, and no one will actually verify if you're the real person.

Carsten: There's substantial theory on identity systems. One approach involves using different numbers for different situations - linkable identities. You might have one identity for the library and a different one for the hospital, but these can be linked when appropriate. You can choose to reveal connections between identities or withdraw them. These are sometimes called revocable identities.

Another approach is to avoid using numbers entirely and instead use a chip on an ID card. When you log in, the chip verifies your identity through a signature checking process or similar mechanism. Estonia uses this system - they don't rely on identity numbers, and all laptops in Estonia have smartcard readers. When you want to vote, you insert your smartcard.

The disadvantage is that you must have the physical card, but it eliminates the need for remembering numbers. The Baltic countries are moving to something called Smart ID, which is somewhat similar to MitID. You could use something like that in Denmark too, but there are also issues with digital-only solutions, as not everyone has access to digital tools.

Interviewer: I should ask you about cybersecurity in Ukraine as well.

Carsten: I was part of the cybersecurity assessment for Ukraine in 2018, before the 2019 election. I've been to Kyiv a couple of times, though not since the war started. I've tried to keep a low profile regarding this work.

I work in many countries, including Greenland - I might be going there next week for their election on March 11th. I even hosted the former head of cyber defense from Ukraine, Viktor Zohar, who is a good friend of mine. The entire Ukrainian election commission visited me in 2015. It was a different time then, though there was already conflict. The commission needed smart people to help them but didn't have the funding to pay for Researcherise.

Interviewer: How would you compare the cybersecurity systems in Ukraine versus Denmark?

Carsten: From my experience back in 2018, Ukrainians are highly educated in cybersecurity, including offensive techniques. In Ukraine, attacks can come from outside but also from inside the country, which makes it completely different from Denmark, where the attack vectors are different due to the different history.

There was a significant attack against the Ukrainian voter registry two days before an election where attackers wiped all the computers containing the data. The election officials had to scramble to restore it the day before the election - it was very tight, and the election almost didn't happen.

One issue was that the technical equipment for public offices was outdated at that time. Security isn't something you implement once - you have to keep investing in it continuously. If you don't, you become increasingly insecure over time.

I haven't looked at their computer systems in detail since then. Our work typically involves talking to stakeholders, summarizing what we've heard, and presenting reports to the relevant authorities.

Interviewer: How would you describe the cyber warfare situation since the war in Ukraine started? Have there been any differences since you visited Ukraine in 2018?

Carsten: I know Kyiv stopped being regularly hacked sometime last year, but the fundamental challenge remains: all our equipment has vulnerabilities, known as "zero days" - so called because vendors have zero days to fix them once they're discovered. We simply don't know what all these zero days are, because if we did, they would have been fixed already. And we don't know who has access to this knowledge.

The situation has changed in that these zero days have become the ammunition for cyber warfare. There are people who actively search for vulnerabilities in systems, then publish and sell them on the black market. I believe one zero day vulnerability might sell for around $2 million. Intelligence services purchase these vulnerabilities, but they can only use each one once - because once it's deployed, everyone learns what it was, fixes it, and protects against it. So agencies must be very careful about how they use zero days.

Carsten: The Stuxnet attack against Iran many years ago demonstrates this sophistication. It was an attack engineered against the centrifuges that enriched uranium. According to a documentary I watched, President Bush said around 2004 or 2008 that he needed a "third option" for handling Iran - not just choosing between war or no war.

Subsequently, this virus was developed. A security company, possibly in Estonia or Belarus, got the virus and reverse-engineered it. In the documentary, you can see these analysts examining it and concluding that it was extremely well-organized code containing five zero days. That's a piece of code that, when released, can't be stopped - it just installs itself, and you can't do anything against it.

The code was specifically tailored for particular scanner devices - controllers for those centrifuges. They were Siemens devices with specific model numbers embedded in the code. The researchers didn't initially know what the target was, so they reverse-engineered the code, Googled the device numbers, and discovered they were centrifuges.

Carsten: All computer equipment we have contains many zero days. Every system we install and every security update might close some vulnerabilities but opens new ones. You simply can't expect anything to be 100% secure.

In Ukraine since 2018, the trust assumptions have fundamentally changed. Many people and entities who were previously trusted are no longer trusted. This invalidates the entire security argument for why something was considered secure.

Now you have to approach security from the perspective of: "If I'm being attacked by the intelligence service of another nation-state, how can I defend against this?" In the past, it might have been acceptable to have outdated routers or systems that weren't regularly updated because the assumption was that nobody would be interested in targeting them. Then suddenly, from one day to the next, everyone became interested.

Carsten: In any security-relevant system, with finite resources, you have to make decisions about how to allocate them. When the war in Ukraine began in 2014, Ukraine wasn't the richest country in the world. The Americans probably had more money to continuously upgrade their systems.

I can imagine that old laptops were repurposed for critical functions because of resource constraints. When you have limited resources, that's how you handle upgrades - you might not have the appropriate workforce to perform security updates, or systems might reach end-of-life without replacement. Bad things can happen in these situations.

It costs substantial money to properly secure systems. Denmark could afford it but is somewhat late to the game and has too much data to manage effectively. However, with sufficient investment, they could improve. I'm sure large companies like Novo Nordisk, Lego, and Maersk have learned from their mistakes and are implementing better security, though they're doing it privately, so we don't know exactly what measures they're taking.

As for Ukraine now, I haven't been back since 2018, so my information is outdated. But I still believe Ukraine has many intelligent people who are highly educated in this field. Simcorp actually had a production lab in Kyiv because they employed Ukrainian programmers who were very skilled, from what I've heard.

Interviewer: If we have more questions in the future, can I contact you again?

Carsten: Yes, sure, feel free to do so.

Interviewer: You're a professor for ethical hacking, correct?

Carsten: I'm teaching the ethical hacking course this semester. Alessandro designed the course, but he's on sabbatical, so I've taken over for now. I'm responsible for it, but many of my colleagues also teach these classes.

Interviewer: I was thinking about taking it next year as an elective for my master's degree.

Carsten: Yes, you definitely can. My first lecture was good, but I didn't record it. When I record my lectures, I don't talk as freely as I might otherwise. Even with you recording me now, I'm being careful about what I say.

Interviewer: I will send you the part of my thesis that I write based on our conversation. I won't mention your name if you prefer.

Carsten: Yes, please send it to me for review. Some of these topics are very sensitive.

Interviewer: I won't try to create any conflicts. Everything will be presented neutrally.

Carsten: It was good talking to you. I think there are some follow-up topics that should be discussed in the press. We'll see if I get an opportunity to address them again.

Interviewer: Thank you so much.

Carsten: Thank you. Have a nice day.