**Interviewer**: Could you please introduce yourself briefly?

**Researcher**: I'm Researcher Justice and I'm a lecturer at the university. I work on cyber security.

**Interviewer**: How can cryptographic protocols ensure both security and trust in decision systems?

**Researcher**: If we consider GDPR protocols for example, when implemented according to their prescriptions, organizations should not store unnecessary information. This means that if a company experiences a data breach, sensitive information isn't leaked because they shouldn't have it stored in the first place.

**Interviewer**: What are the most significant cyber warfare threats facing Denmark today, and how do they compare to global trends?

**Researcher**: I think the main threats to Danish companies today come from two categories: state-sponsored attacks and groups that are paid by competing companies.

**Interviewer**: You mentioned state-sponsored cyber attacks. How do they typically target critical infrastructures? And what can Denmark do to defend against them?

**Researcher**: These states pay criminal groups to conduct various types of attacks. They disrupt companies through attacks on infrastructure and disinformation campaigns. The threats are quite diverse.

As for defense, the first thing is to invest more in cyber security—invest in people with knowledge and teach more cyber security aspects in companies. Creating awareness of these attacks is one important approach.

**Interviewer**: Currently, Denmark is focused on sponsoring research in areas such as quantum computers. Would you consider that spending more money on developing cyber security and cyber infrastructure would benefit Denmark?

**Researcher**: Yes, definitely.

**Interviewer**: What role does intelligence gathering play in cyber warfare, and how can Denmark improve its cyber threat detection capabilities?

**Researcher**: Intelligence gathering is key in cyber warfare. Denmark can improve by investing in technologies that help counter cyber warfare and by investing in cyber security education for companies.

One key difference with cyber warfare, compared to traditional warfare, is that there's no geographic protection. Companies largely have to protect themselves, as there's not much the government can do to prevent such attacks directly.

**Interviewer**: What methodologies are most effective for conducting risk assessment of national critical infrastructure, including hospitals and election systems?

**Researcher**: There are several frameworks available. MITRE has recently released one. There's also the MITRE ATT&CK framework. The NIST framework exists as well, though it's quite outdated from around 2012. I think the MITRE ATT&CK is more recent and relevant.

**Interviewer**: What are the most damaging types of cyber attack?

**Researcher**: It's hard to say which is the most damaging, but attacks targeting critical infrastructure are among the most serious. If attackers manage to compromise electrical companies and similar utilities, that would cause significant problems. Critical infrastructure attacks present the most immediate threat.

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

**Researcher**: I'm not entirely clear on how to assess these policies. There is the Center for Cyber Security which has direct connections with major companies, but I'm not completely clear on how this collaboration functions in practice.

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

**Researcher**: Regarding research, I don't know of any specific funding partnerships in the international context involving Denmark. For collaboration against cyber warfare, this likely happens within NATO, though NATO isn't very transparent about these matters.

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

**Researcher**: Right now, I think Russia poses the main threat. There's also Iran, North Korea, and another major state actor that I'm forgetting. As for mitigation, there's no quick fix. We need more education and cyber security skills. These attacks often exploit policy gaps, and fixing those isn't a simple or quick process.

**Interviewer**: Last year there was a cyber attack on a water facility in Denmark where they couldn't supply water to citizens for a couple of hours. Is this cyber crime or cyber terrorism?

**Researcher**: The main difference between cyber crime and cyber terrorism is that cyber terrorism isn't driven by economic or financial incentives. Terrorism is breaking things for ideological reasons—a form of vandalism with ideological motivation.

I would classify this water facility attack as cyber crime rather than terrorism. It was likely a signal that they can attack critical infrastructure, possibly testing the vulnerability of these systems.

**Interviewer**: What could be the biggest consequence of a cyber attack on critical infrastructure?

**Researcher**: The immediate consequence is that you have to address the vulnerability. These types of attacks are often tests—probing attacks to understand the infrastructure of the targets. When these happen at a larger scale, it's usually because there are bigger geopolitical factors at play.

**Interviewer**: What reasons might there be to target hospitals and healthcare institutions for cyber attacks?

**Researcher**: If it's state-sponsored attacks, the reason is to test the readiness of critical infrastructure. If it's criminals driven by profit, such as with ransomware, there are clear economic benefits. Hospitals often have to pay ransoms to avoid serious consequences that could affect patient care. Different threat actors have different motivations.

**Interviewer**: How do you see the future of Denmark's digital infrastructure evolving, and what cyber security measures should be prioritized to mitigate emerging threats?

**Researcher**: I expect these kinds of attacks will increase. Cyber security education among companies should be one of the first priorities to avoid successful attacks in the long term.

**Interviewer**: Do you consider that the population of Denmark is well aware of cyber threats and cyber warfare?

**Researcher**: I would say yes, to some extent. They're not completely uninformed because news about these threats is available, but probably not as aware as they could be.

**Interviewer**: Denmark has evolved during the last three years in the digitalization of documents. Previously they were using NemID and now they're using MitID to identify people. Do you see any risks in this kind of digitalization move?

**Researcher**: There are always risks when you change technologies. However, in this specific case, I would say the overall risk is more or less the same as with the previous system. There isn't a significant increase in risk—the same types of risks apply to MitID as to NemID.

**Interviewer**: Can you name some measures to prevent identity theft?

**Researcher**: Regarding MitID specifically, the phone is the key authentication factor, so using strong PINs is important to avoid ID theft. More generally, following basic security principles like using password managers is crucial. In the long run, cyber security education remains the key factor.

**Interviewer**: What are the security and privacy implications of increasing digitalization?

**Researcher**: We already face many threats to privacy and security. The more we move toward digitalization, the higher the risks become. Cyber security and privacy are central concerns in this process.

**Interviewer**: What future trends do you foresee in hospital cybersecurity, and how should IT infrastructure evolve to address emerging threats?

**Researcher**: A general problem in healthcare is legacy software and systems. Most effective attacks typically combine exploiting vulnerabilities in legacy systems with finding entry points through employees. Organizations should regularly update their systems to the state of the art, as vendors continuously patch security issues.

**Interviewer**: Is it important to patch systems regularly?

**Researcher**: Yes.

**Interviewer**: What comments would you make about the cyber attack on Maersk?

**Researcher**: The Maersk incident was a ransomware attack. If I recall correctly, it was a combination of finding a vulnerable entry point through an employee who had certain access privileges. This is a common pattern: an employee who isn't well-versed in cyber security becomes the entry point for attackers to penetrate systems, as employees have more privileges than outsiders.

**Interviewer**: How are ransomware threats evolving, and what preventive strategies are most effective?

**Researcher**: For ransomware to succeed, attackers need higher privileges to access data systems. Compartmentalization is important—having multiple levels of access control. One way to address this is to only give access to critical infrastructure or company systems to people who have undergone security education.