Qualitative Data Analysis

May 11, 2025

1 Participant Codes

Table 1: Table of interview participants

ID	Industrial Classification	Participant Role
P11	Private Sector Specialist	Security Consultant
P6	Healthcare	Antivirus Administrator and Operational Security Specialist
P5	Healthcare	Security Specialist
P10	Healthcare	Operational Security Specialist
P14	Healthcare	Security Specialist
P1	Healthcare	Security Specialist
P2	Academia	Professor
P8	Private Sector Specialist	Infrastructure Specialist
P3	Academia	Professor
P4	Academia	Professor
P7	Academia	Professor
P9	Academia	Professor
P12	Academia	Professor
P13	Academia	Professor
P15	Academia	Professor

2 Interview Labeling

Research Question Subsection	Quote	Participant	Pattern Label
Digitization in Denmark	"I anticipate that working with and countering artificial intelligence will dominate our focus in the coming years."	P5	AI Threat Anticipation
Digitization in Denmark	"MitID and NemID are critical pieces of infrastructure, and security should always be the top priority when handling issues."	P8	Digital Identity Infrastructure
Digitization in Denmark	"With NemID, the biggest problem was social engineering. Someone could send you a photo of the key card, or if they knew when you were logging in, they could send you a request that you might approve."	P8	Social Engineering Vulnerability
Digitization in Denmark	"The biggest issue I encountered was when we discovered you could find people's usernames in MitID by simply enumerating them."	P8	Authentication System Weakness
Digitization in Denmark	"The main challenge for hospitals is legacy software. While we've closed the last Windows 2000 systems last year, we still maintain Windows XP, Windows 7, and other outdated systems."	P6	Legacy System Dependence
Digitization in Denmark	"One of the biggest challenges is budget constraints. We have a lot of old medical equipment running on outdated systems like Windows 7. Purchasing new equipment is very expensive."	P10	Resource Limitation Impact
Digitization in Denmark	"Yes, there was a ransomware incident where one of our doctors was using network drives. The ransomware not only encrypted local files but also mapped network drives, including a connection to two Azure servers containing blood analysis results. The recent blood test data was encrypted."	P6	Healthcare Data Breach

Research Question Subsection	Quote	Participant	Pattern Label
Digitization in Denmark	"We were able to restore it, but the server was unavailable during recovery. The biggest impact was on blood analysis—we couldn't access previous results temporarily and had to slow down processing new samples. Staff had to record results manually rather than uploading to the server while systems were being restored. If there were critical blood tests needed immediately, we still had the physical samples and could repeat the analysis. So no patient care was compromised—we just had to spend extra time redoing some tests. Nothing was permanently lost."	P6	Incident Recovery Process
Strategic Targeting of Danish Infrastructure	"Denmark is a highly digitalized country, so most public services use information systems that demand protection."	P2	Digital Ecosystem Vulnerability
Strategic Targeting of Danish Infrastructure	"The healthcare sector is an attractive target for both terrorists and criminals. For terrorists, it's attractive because healthcare is a matter of life and death."	P7	Healthcare Targeting Risk
Strategic Targeting of Danish Infrastructure	"Last year there was a cyberattack on a water facility in Denmark where they couldn't supply water to citizens for a couple of hours."	P12	Utility Infrastructure Disruption
Strategic Targeting of Danish Infrastructure	"Denmark has moved to digital electoral rolls... The question becomes: what happens if the system goes down?"	P3	Democratic Process Vulnerability
Strategic Targeting of Danish Infrastructure	"Imagine a hospital gets hacked and equipment stops working entirely... the moral effect would be much greater because it strongly affects society."	P15	Societal Impact Concern
Multi-Vector Attacks	"The greatest concern is when attacks target multiple sectors simultaneously."	P7	Coordinated Attack Concern
Multi-Vector Attacks	"DDoS attacks are unlikely to be effective on their own. There was one case when hackers targeted an energy company, complementing their operation by flooding their hotline with calls."	P15	Combined Disruption Strategy
Multi-Vector Attacks	"Russia hacked Okhmatdyt Children's Hospital's network before a missile strike."	P15	Cyber-Physical Attack Coordination

Research Question Subsection	Quote	Participant	Pattern Label
Multi-Vector Attacks	"Hackers often employ persistence techniques based on the MITRE ATT&CK framework. They create child processes and backdoors that are difficult to detect."	P11	Advanced Persistence Techniques
Multi-Vector Attacks	"95% of malware comes through emails. That's been our main risk since I started doing these presentations in 2017."	P6	Email-Based Threat Dominance
Multi-Vector Attacks	"With generative AI, it's now easier for adversaries to craft better-looking phishing emails by gathering information from places like LinkedIn to personalize attacks."	P1	AI-Enhanced Phishing Evolution
The Human Factor in Hybrid Defense	"The Danish levels of trust are so high that when you tell them 'trust is a liability,' they don't understand."	P3	Cultural Trust Exploitation
The Human Factor in Hybrid Defense	"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?"	P3	Naive Security Mindset
The Human Factor in Hybrid Defense	"The younger generation seems to have a better understanding and sensitivity to these issues, while the older generation might be more reluctant to invest in cybersecurity."	P13	Generational Security Divide
The Human Factor in Hybrid Defense	"Studies show that 85-90% of cyber attacks result from human error. Attackers target users as the entry point."	P11	Human Security Weakness
The Human Factor in Hybrid Defense	"I would like to see the government implement a bug bounty program."	P8	Vulnerability Reporting Incentive
The Human Factor in Hybrid Defense	"At minimum, they need proper contact points for security issues and people who know how to handle them—people who don't panic when presented with security issues and understand you're trying to help. They should understand you didn't have to report the issue and appreciate that you did."	P8	Security Response Professionalism

Research Question Subsection	Quote	Participant	Pattern Label
The Human Factor in Hybrid Defense	"The ideal outcome might be a centralized portal serving all Danish agencies where you can submit security issues and specify which agencies are affected. The government is in a unique position to have a single portal for all government systems, which could ensure reports are handled correctly. Regarding bounties, this is standard practice in companies. Especially with ongoing international conflicts, it's more important than ever to ensure there's not only profit to be made by those with malicious intent. Right now, the ability to compromise MitID might be valuable to certain adversaries, but the Danish government doesn't place any monetary value on that information."	P8	Centralized Vulnerability Management
The Human Factor in Hybrid Defense	"Our biggest problem is users because they will click on anything without thinking about it."	P6	User Behavior Risk
The Human Factor in Hybrid Defense	"Currently, we're allowed 40 minutes per year for security awareness training. With 50,000 employees, if we asked for one hour, that would be 50,000 person-hours annually."	P6	Training Resource Constraint
The Human Factor in Hybrid Defense	"The biggest risk is the lack of competencies, because that is foundational for doing all the rest."	P7	Expertise Shortage Impact
The Human Factor in Hybrid Defense	"Security is as much about human behavior as technology."	P10	Socio-Technical Security Approach
Incident Response and National Resilience	"When an incident occurs, we gather in a designated room with all relevant personnel: communications staff to handle press inquiries, administrative directors, my department, and representatives from clinical departments."	P6	Incident Response Coordination
Incident Response and National Resilience	"We work on two tracks simultaneously: a technical track focused on containing damage, investigating the cause, and restoring systems; and a communications track focused on keeping the press, users, and patients informed."	P6	Parallel Response Methodology
Incident Response and National Resilience	"We also prepare for scenarios where attacks might disable power, mobile phones, or telecommunications by practicing old-fashioned communication methods."	P14	Low-Tech Contingency Planning
Incident Response and National Resilience	"I can't recall seeing any public information campaigns about what to do if mobile phones go down or during an electricity outage."	P13	Public Preparedness Gap

Research Question Subsection	Quote	Participant	Pattern Label
Incident Response and National Resilience	"If we imagine that a provider stops supporting us, we wouldn't be able to get updates for antivirus or security solutions."	P13	Vendor Dependency Risk
Incident Response and National Resilience	"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."	P12	Human Capital Investment Need
Governance Fragmentation in Danish Infrastructure	"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?'"	P3	Response Protocol Deficiency
Governance Fragmentation in Danish Infrastructure	"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."	P3	Decentralized System Vulnerability
Governance Fragmentation in Danish Infrastructure	"For years, security was neglected. There was no dedicated security department whatsoever."	P6	Historical Security Negligence
Governance Fragmentation in Danish Infrastructure	"Previously, departments would purchase and install whatever they wanted without consulting IT."	P6	Uncontrolled Technology Acquisition
Governance Fragmentation in Danish Infrastructure	"Before, responsibility was fragmented into different ministries, and now they're trying to consolidate it into a single ministry."	P7	Governance Centralization Effort
Governance Fragmentation in Danish Infrastructure	"Four years ago, we finally established a proper security department, starting with me and my colleague. Today, we've grown to 26 people."	P6	Security Function Evolution
Governance Fragmentation in Danish Infrastructure	"All our information is governed by GDPR. Everything you do needs to consider what happens with the data and how it's used."	P4	Regulatory Compliance Emphasis
Governance Fragmentation in Danish Infrastructure	"The biggest problem, though, is that many of the methods claiming to protect privacy don't actually work... What people think is secure is often not secure at all."	P4	False Security Perception
Governance Fragmentation in Danish Infrastructure	"Regulatory frameworks like GDPR have a positive impact from a security perspective. But there's a price to pay - everything you do has to go through extra checks and processes."	P9	Compliance-Efficiency Tradeoff
Foreign Technology Dependencies	"Denmark is essentially a Microsoft country. All data is stored on American-owned servers."	P3	Foreign Technology Reliance

Research Question Subsection	Quote	Participant	Pattern Label
Foreign Technology Dependencies	"We're relying too much on tools from other countries, which makes us vulnerable. We need to become more independent in our cybersecurity infrastructure."	P13	Technology Sovereignty Need
Foreign Technology Dependencies	"We had a massive problem with Chinese cameras because they might have backdoors. Most government functions in Denmark are not allowing official Chinese cameras."	P6	Foreign Hardware Distrust
Foreign Technology Dependencies	"We've also banned some AI applications from China."	P10	Foreign AI Restriction
Foreign Technology Dependencies	"The current shift with the US working more closely with Russia raises questions about the dangers of sharing data with American companies."	P7	Geopolitical Trust Shift
Foreign Technology Dependencies	"We're closely monitoring statements from the US and what Trump is saying, especially regarding Greenland, where he hasn't excluded the use of military power."	P1	Alliance Relationship Uncertainty
Foreign Technology Dependencies	"When there are only one or two suppliers worldwide, our leverage is limited."	P6	Market Monopoly Vulnerability
Asia's Advanced Persistent Threats	"In terms of activity, China would be the most active, followed by Russia, North Korea, and Iran."	P15	Threat Actor Hierarchy
Asia's Advanced Persistent Threats	"For China, it's about intellectual property - they want to copy whatever they can get their hands on."	P6	Intellectual Property Targeting
Asia's Advanced Persistent Threats	"Someone, most likely Chinese, targeted a specific sub-program for Linux that was maintained by just one developer on GitHub. The attackers created 3-4 accounts that all contributed useful software on GitHub to build their credibility. They spent over three years infiltrating this developer's trust, with their accounts saying things like, 'Why don't you update more often?' and 'I have some free time, I can help.'"	P6	Long-Term Trust Infiltration
Asia's Advanced Persistent Threats	"We can see examples with Ukraine and Russia - whenever a political figure says something that upsets Russia, there can be consequences."	P14	Political Statement Retaliation
Asia's Advanced Persistent Threats	"As international cooperation becomes more destabilized, countries like Russia have greater incentives to target nations like Denmark."	P5	Geopolitical Instability Exploitation
Asia's Advanced Persistent Threats	"If an attack were conducted by a state actor like the Russian government, it would be considered cyber warfare -essentially a declaration of war."	P5	Cyber Warfare Definition

Research Question Subsection	Quote	Participant	Pattern Label
Asia's Advanced Persistent Threats	"If they can take down hospitals, power supply, or water supply, then people stop caring about the war because they care about their own welfare."	P6	Civilian Infrastructure Targeting
Asia's Advanced Persistent Threats	"North Korea, due to all the embargoes against them, basically only gets outside money from cyber warfare, and they have many skilled people doing it."	P6	Economic Motivation Strategy
Asia's Advanced Persistent Threats	"The main threats come from rogue states that don't hide their efforts and those who make money from it, like North Korea with the Lazarus Group."	P15	State-Sponsored Threat Actors
Asia's Advanced Persistent Threats	"I think we need a good way to block new Chinese AI systems like Deepsea Eagle, DeepMind, and a few others because the second someone starts putting data into them, it all goes to the Chinese."	P6	Foreign AI Data Extraction
Asia's Advanced Persistent Threats	"We do block Chinese AI tools and other less trusted systems."	P14	Foreign Technology Restriction
Asia's Advanced Persistent Threats	"When I joined 'University A' in 2009, we were 'best friends' with China and had many exchange programs. Now, this is completely forbidden."	P9	International Relationship Deterioration
Asia's Advanced Persistent Threats	"Currently, you cannot work with Russians or Chinese, full stop."	P9	International Collaboration Ban
International Cooperation and Threat Intelligence	"In Denmark, we have the Center for Cybersecurity that works with all regions across Denmark. Their job is to coordinate information about attacks, intrusions, or any potential dangers to the regions."	P14	National Security Coordination
International Cooperation and Threat Intelligence	"We also participate in a threat-sharing platform with different regions in Denmark. If one region experiences a threat, they submit their findings to this platform so everyone is aware."	P1	Threat Intelligence Sharing
International Cooperation and Threat Intelligence	"We collaborate extensively with other regions, the European Union, the Danish Ministry of Defense, and various entities to ensure we maintain multiple perspectives on cybersecurity."	P5	Multi-Level Security Collaboration
International Cooperation and Threat Intelligence	"We could form consortiums with other Nordic countries like Sweden and Norway to develop common solutions for these challenges."	P13	Regional Defense Coalition

Research Question Subsection	Quote	Participant	Pattern Label
International Cooperation and Threat Intelligence	"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."	P3	Public-Private Security Partnership
Russia's Hybrid Warfare in Ukraine: Anticipating Advanced Tactics	"Right now, I think Russia poses the main threat."	P12	Russian Threat Primacy
Russia's Hybrid Warfare in Ukraine: Anticipating Advanced Tactics	"Obviously, the number of cyberattacks has increased because it became a priority for Russia. But Russia has been actively attacking us for years."	P15	Persistent State Aggression
Russia's Hybrid Warfare in Ukraine: Anticipating Advanced Tactics	"Russia is a big worry right now due to the Ukrainian-Russian war... Right now, if Russia can change public opinion, that's perfect for them."	P6	Public Opinion Manipulation
Russia's Hybrid Warfare in Ukraine: Anticipating Advanced Tactics	"About a month ago, a Russian propaganda agency had almost all their internal documentation leaked. Russia has been involved in propaganda and election manipulation for years, but has denied it."	P6	Disinformation Campaign Evidence
Russia's Hybrid Warfare in Ukraine: Anticipating Advanced Tactics	"Russia excel at social engineering and developing viruses."	P15	Russian Cyber Capabilities
Russia's Hybrid Warfare in Ukraine: Anticipating Advanced Tactics	"Through multiple annual threat intelligence reports, social engineering remains the predominant technique used by external threat actors."	P1	Social Engineering Prevalence
Russia's Hybrid Warfare in Ukraine: Anticipating Advanced Tactics	"We've blocked a lot of the world - Ukraine, Russia, China, India, and around 17 or 18 other countries. We open access if people need it for specific sites."	P6	Geographic Access Restriction
Russia's Hybrid Warfare in Ukraine: Anticipating Advanced Tactics	"If there's international exchange of intelligence about attacks, this information is instantly distributed to all other countries, and threat hunting begins."	P15	Cross-Border Intelligence Sharing
Evolution of Threat Landscape	"Quantum computers, if we are able to construct one that is large and stable enough, would be able to run algorithms that solve some of the computationally hard problems that underpin our most widely used cryptographic algorithms."	P2	Quantum Cryptography Threat
Evolution of Threat Landscape	"The biggest challenge is not actually designing them - they already exist. The key challenge is transitioning to those algorithms, standardizing them, and deploying them."	P2	Post-Quantum Transition Challenge

Research Question Subsection	Quote	Participant	Pattern Label
Evolution of Threat Landscape	"Currently, technology exists that combines real-time deepfakes with AI like ChatGPT, which can speak Danish."	P6	Advanced Deepfake Capability
Evolution of Threat Landscape	"Most authentication systems use additional parameters like detecting heat around the face. A screen generating a pattern won't generate the right heat signature."	P4	Biometric Defense Mechanism
Evolution of Threat Landscape	"Systems also check if eye movements appear natural."	P4	Behavioral Biometric Authentication
Evolution of Threat Landscape	"You can spoof iris recognition patterns - that's been demonstrated."	P4	Biometric Spoofing Vulnerability
Evolution of Threat Landscape	"The eye is controlled by muscles and is essentially the only visible part of the brain -it's directly connected to your brain. Emotions are also reflected in eye movements, so you have some certainty about who the individual is."	P4	Neurobiological Identity Marker
Evolution of Threat Landscape	"Nothing is perfect. With good generative models, you can model anything, including heat signatures and other factors. If you can do that, you can potentially fool any system."	P4	AI Circumvention Potential
Evolution of Threat Landscape	"If you combine fingerprints, eye tracking, facial recognition, hair growth patterns, and other biometrics—yes, certainly."	P4	Multi-Factor Biometric Security

3 Survey Labeling

Quote	Subsection	Pattern Label
"The importance of medical data access to medical histories, diagnoses, laboratory tests can be under threat or theft"	Digitization in Denmark	Medical Data Vulnerability
"As an example, we can cite the recent attack on the HELSI medical information system, the essence of which was to use the vulnerabilities of the database systems, as a result of which a lot of patient data was sold on the DarkNet."	Digitization in Denmark	Medical System Breach Example
"Some private medical institutions are even ready to cooperate with cybercriminals (pay a ransom to quickly restore work and prevent the leakage of patients' personal data)."	Digitization in Denmark	Ransomware Response Strategy
"Energy infrastructure facilities were among the main targets of cyberattacks from Russian cyber groups"	Strategic Targeting of Danish Infrastructure	Critical Infrastructure Targeting

Quote	Subsection	Pattern Label
"In the medical field, such attacks pose a serious threat as they can block access to electronic medical records, stop the operation of vital equipment, and lead to the leakage of confidential data"	Strategic Targeting of Danish Infrastructure	Healthcare Impact Assessment
"Russia uses combined attacks on critical infrastructure, such as attacks can serve as missile strikes in combination with a cyberattack on infrastructure"	Multi-Vector Attacks	Combined Attack Strategy
"Since the beginning of the full-scale invasion, 'cyberwar' has expanded the range of tactics and tools used in cyberattacks"	Multi-Vector Attacks	Tactics Evolution
"80% of breaches start with phishing, a simple and effective way to penetrate a hospital's network, insufficient awareness of hospital staff about cyber hygiene"	The Human Factor in Hybrid Defense	Attack Vector Statistics
"If each medical institution follows Ukraine's cybersecurity strategy, then in general, one can achieve the best level of cybersecurity and minimize 75% of cyberattacks"	The Human Factor in Hybrid Defense	Best Practice Recommendation
"Lack of qualified personnel (personnel shortage), as hostilities make their adjustments"	The Human Factor in Hybrid Defense	Workforce Challenge
"presence of an incompetent head of an organization or institution, which in turn can lead to the 'decline' of cybersecurity issues in general"	The Human Factor in Hybrid Defense	Leadership Impact
"Backup and cloud technologies have proven their effectiveness – Ukraine transferred critical data to secure clouds, which allowed quick recovery of systems after attacks"	Incident Response and National Resilience	Data Recovery Strategy
"Centralization of cybersecurity, use of technology for data preservation, rapid response to attacks"	Governance Fragmentation in Danish Infrastructure	Governance Recommendation
"Proactive monitoring and response to threats to quickly detect and neutralize attacks"	Governance Fragmentation in Danish Infrastructure	Defense Strategy
"Legal limitations and complexities in international law regarding cybercrimes"	International Cooperation and Threat Intelligence	Legal Framework Challenges

Quote	Subsection	Pattern Label
"Cooperation with international partners helps Ukraine receive material and technical assistance, free staff training, and exchange of indicators and information about cyber threats"	Foreign Technology Dependencies	International Assistance Value
"Ukraine's cybersecurity cooperation with Western countries has strengthened its hybrid defense, increased resilience to cyberattacks, and contributed to rapprochement with the EU and NATO"	International Cooperation and Threat Intelligence	Alliance Strengthening

Quote	Subsection	Pattern Label
"Ukraine actively cooperates with international partners, receiving data on new cyberattacks in real time"	International Cooperation and Threat Intelligence	Real-time Intelligence Sharing
"Ukraine accepts citizens in medical institutions from other countries, and this is the security not only of Ukraine but also of international partners in general"	International Cooperation and Threat Intelligence	Cross-border Healthcare Security
"Russia uses combined attacks on critical infrastructure, such attacks can serve as missile strikes in combination with a cyberattack on infrastructure."	Russia's Hybrid Warfare in Ukraine	Combined Attack Approach
"Energy infrastructure facilities were among the main targets of cyberattacks from Russian cyber groups."	Russia's Hybrid Warfare in Ukraine	Energy Sector Targeting
"low entry threshold, quick effect, and maximum destructive impact"	Russia's Hybrid Warfare in Ukraine	Attack Efficiency Characteristics
"phishing campaigns, ransomware, DDoS attacks."	Russia's Hybrid Warfare in Ukraine	Common Attack Methods
"influence elections, manipulate public opinion, and conduct economic warfare."	Russia's Hybrid Warfare in Ukraine	Information Warfare Objectives
"If each medical institution follows Ukraine's cybersecurity strategy, then in general, one can achieve the best level of cybersecurity and minimize 75% of cyberattacks."	Russia's Hybrid Warfare in Ukraine	Security Strategy Effectiveness
"Backup and cloud technologies have proven their effectiveness – Ukraine transferred critical data to secure clouds, which allowed quick recovery of systems after attacks."	Russia's Hybrid Warfare in Ukraine	Resilience Mechanism
"limiting and localizing a resource that has been attacked to prevent spread by attackers"	Russia's Hybrid Warfare in Ukraine	Containment Strategy
"If there's international exchange of intelligence about attacks, this information is instantly distributed to all other countries, and threat hunting begins"	Russia's Hybrid Warfare in Ukraine	Collaborative Defense
"Today, government agencies, organizations, and institutions can be aware of certain cyber threats that have already occurred in the national resilience system and predict (prevent) similar cases in their own infrastructures"	Russia's Hybrid Warfare in Ukraine	Threat Intelligence Application

4 Distinct Labels from Interview

Pattern Label	Source	Cluster
Healthcare Data Breach	Interview	Healthcare Security Vulnerabilities
Healthcare Targeting Risk	Interview	Healthcare Security Vulnerabilities
Digital Identity Infrastructure	Interview	Digital Infrastructure Challenges
Authentication System Weakness	Interview	Digital Infrastructure Challenges
Legacy System Dependence	Interview	Digital Infrastructure Challenges
Resource Limitation Impact	Interview	Digital Infrastructure Challenges
Digital Ecosystem Vulnerability	Interview	Digital Infrastructure Challenges
Utility Infrastructure Disruption	Interview	Critical Infrastructure Protection
Democratic Process Vulnerability	Interview	Critical Infrastructure Protection
Civilian Infrastructure Targeting	Interview	Critical Infrastructure Protection

Pattern Label	Source	Cluster
Combined Disruption Strategy	Interview	Advanced Attack Strategies
Cyber-Physical Attack Coordination	Interview	Advanced Attack Strategies
Advanced Persistence Techniques	Interview	Advanced Attack Strategies
Social Engineering Vulnerability	Interview	Social Engineering and Human Vulnerabilities
Email-Based Threat Dominance	Interview	Social Engineering and Human Vulnerabilities
AI-Enhanced Phishing Evolution	Interview	Social Engineering and Human Vulnerabilities
Cultural Trust Exploitation	Interview	Social Engineering and Human Vulnerabilities
Naive Security Mindset	Interview	Social Engineering and Human Vulnerabilities
Human Security Weakness	Interview	Social Engineering and Human Vulnerabilities
User Behavior Risk	Interview	Social Engineering and Human Vulnerabilities
Social Engineering Prevalence	Interview	Social Engineering and Human Vulnerabilities
Generational Security Divide	Interview	Workforce and Expertise Challenges
Training Resource Constraint	Interview	Workforce and Expertise Challenges
Expertise Shortage Impact	Interview	Workforce and Expertise Challenges
Human Capital Investment Need	Interview	Workforce and Expertise Challenges
Incident Recovery Process	Interview	Incident Response and Recovery
Incident Response Coordination	Interview	Incident Response and Recovery
Parallel Response Methodology	Interview	Incident Response and Recovery
Low-Tech Contingency Planning	Interview	Incident Response and Recovery
Response Protocol Deficiency	Interview	Governance and Strategic Planning
Decentralized System Vulnerability	Interview	Governance and Strategic Planning
Historical Security Negligence	Interview	Governance and Strategic Planning
Uncontrolled Technology Acquisition	Interview	Governance and Strategic Planning
Governance Centralization Effort	Interview	Governance and Strategic Planning
Security Function Evolution	Interview	Governance and Strategic Planning
Regulatory Compliance Emphasis	Interview	Regulatory and Compliance Matters
False Security Perception	Interview	Regulatory and Compliance Matters
Compliance-Efficiency Tradeoff	Interview	Regulatory and Compliance Matters
National Security Coordination	Interview	International Collaboration
Threat Intelligence Sharing	Interview	International Collaboration
Multi-Level Security Collaboration	Interview	International Collaboration
Regional Defense Coalition	Interview	International Collaboration
Public-Private Security Partnership	Interview	International Collaboration
Cross-Border Intelligence Sharing	Interview	International Collaboration
Foreign Technology Reliance	Interview	Foreign Technology Considerations
Technology Sovereignty Need	Interview	Foreign Technology Considerations
Foreign Hardware Distrust	Interview	Foreign Technology Considerations
Foreign AI Restriction	Interview	Foreign Technology Considerations
Market Monopoly Vulnerability	Interview	Foreign Technology Considerations
Foreign Technology Restriction	Interview	Foreign Technology Considerations
Foreign AI Data Extraction	Interview	Foreign Technology Considerations
Geopolitical Trust Shift	Interview	Geopolitical Security Dimensions
Alliance Relationship Uncertainty	Interview	Geopolitical Security Dimensions
International Relationship Deterioration	Interview	Geopolitical Security Dimensions
International Collaboration Ban	Interview	Geopolitical Security Dimensions
Geopolitical Instability Exploitation	Interview	Geopolitical Security Dimensions
Cyber Warfare Definition	Interview	Geopolitical Security Dimensions

Pattern Label	Source	Cluster
Threat Actor Hierarchy	Interview	State-Sponsored Threat Actors
Intellectual Property Targeting	Interview	State-Sponsored Threat Actors
Long-Term Trust Infiltration	Interview	State-Sponsored Threat Actors
Political Statement Retaliation	Interview	State-Sponsored Threat Actors
Economic Motivation Strategy	Interview	State-Sponsored Threat Actors
State-Sponsored Threat Actors	Interview	State-Sponsored Threat Actors
Russian Threat Primacy	Interview	State-Sponsored Threat Actors
Persistent State Aggression	Interview	State-Sponsored Threat Actors
Russian Cyber Capabilities	Interview	State-Sponsored Threat Actors
Public Opinion Manipulation	Interview	Information Operations
Disinformation Campaign Evidence	Interview	Information Operations
Geographic Access Restriction	Interview	Information Operations
Societal Impact Concern	Interview	Information Operations
AI Threat Anticipation	Interview	Emerging Technology Threats
Quantum Cryptography Threat	Interview	Emerging Technology Threats
Post-Quantum Transition Challenge	Interview	Emerging Technology Threats
Advanced Deepfake Capability	Interview	Emerging Technology Threats
AI Circumvention Potential	Interview	Emerging Technology Threats
Biometric Defense Mechanism	Interview	Biometric Security Considerations
Behavioral Biometric Authentication	Interview	Biometric Security Considerations
Biometric Spoofing Vulnerability	Interview	Biometric Security Considerations
Neurobiological Identity Marker	Interview	Biometric Security Considerations
Multi-Factor Biometric Security	Interview	Biometric Security Considerations

5 Distinct Labels from Survey

Pattern Label	Source	Cluster
Medical Data Vulnerability	Survey	Healthcare Security Vulnerabilities
Medical System Breach Example	Survey	Healthcare Security Vulnerabilities
Ransomware Response Strategy	Survey	Healthcare Security Vulnerabilities
Healthcare Impact Assessment	Survey	Healthcare Security Vulnerabilities
Critical Infrastructure Targeting	Survey	Critical Infrastructure Protection
Energy Sector Targeting	Survey	Critical Infrastructure Protection
Combined Attack Strategy	Survey	Advanced Attack Strategies
Tactics Evolution	Survey	Advanced Attack Strategies
Combined Attack Approach	Survey	Advanced Attack Strategies
Attack Efficiency Characteristics	Survey	Advanced Attack Strategies
Common Attack Methods	Survey	Advanced Attack Strategies
Attack Vector Statistics	Survey	Social Engineering and Human Vulnerabilities
Workforce Challenge	Survey	Workforce and Expertise Challenges
Leadership Impact	Survey	Workforce and Expertise Challenges
Data Recovery Strategy	Survey	Incident Response and Recovery
Containment Strategy	Survey	Incident Response and Recovery
Resilience Mechanism	Survey	Incident Response and Recovery
Governance Recommendation	Survey	Governance and Strategic Planning
Defense Strategy	Survey	Governance and Strategic Planning
Best Practice Recommendation	Survey	Governance and Strategic Planning
Security Strategy Effectiveness	Survey	Governance and Strategic Planning
Legal Framework Challenges	Survey	Regulatory and Compliance Matters
International Assistance Value	Survey	International Collaboration
Alliance Strengthening	Survey	International Collaboration
Real-time Intelligence Sharing	Survey	International Collaboration

Pattern Label	Source	Cluster
Cross-border Healthcare Security	Survey	International Collaboration
Collaborative Defense	Survey	International Collaboration
Threat Intelligence Application	Survey	International Collaboration
Information Warfare Objectives	Survey	Information Operations

6 Data for Affinity Diagram

Pattern Label	Quote	Participant
Medical Data Vulnerability	"The importance of medical data access to medical histories, diagnoses, laboratory tests can be under threat or theft"	Anonymous
Medical System Breach Example	"As an example, we can cite the recent attack on the HELSI medical information system, the essence of which was to use the vulnerabilities of the database systems, as a result of which a lot of patient data was sold on the DarkNet."	Anonymous
Ransomware Response Strategy	"Some private medical institutions are even ready to cooperate with cybercriminals (pay a ransom to quickly restore work and prevent the leakage of patients' personal data)."	Anonymous
Healthcare Data Breach	"Yes, there was a ransomware incident where one of our doctors was using network drives. The ransomware not only encrypted local files but also mapped network drives, including a connection to two Azure servers containing blood analysis results. The recent blood test data was encrypted."	P6
Healthcare Targeting Risk	"The healthcare sector is an attractive target for both terrorists and criminals. For terrorists, it's attractive because healthcare is a matter of life and death."	P7
Healthcare Impact Assessment	"In the medical field, such attacks pose a serious threat as they can block access to electronic medical records, stop the operation of vital equipment, and lead to the leakage of confidential data"	Anonymous
Digital Identity Infrastructure	"MitID and NemID are critical pieces of infrastructure, and security should always be the top priority when handling issues."	P8
Authentication System Weakness	"The biggest issue I encountered was when we discovered you could find people's usernames in MitID by simply enumerating them."	P8
Legacy System Dependence	"The main challenge for hospitals is legacy software. While we've closed the last Windows 2000 systems last year, we still maintain Windows XP, Windows 7, and other outdated systems."	P6
Resource Limitation Impact	"One of the biggest challenges is budget constraints. We have a lot of old medical equipment running on outdated systems like Windows 7. Purchasing new equipment is very expensive."	P10
Digital Ecosystem Vulnerability	"Denmark is a highly digitalized country, so most public services use information systems that demand protection."	P2

Continued on next page

Table 7 – *Continued from previous page*

Pattern Label	**Quote**	**Participant**
Critical Infrastructure Targeting	"Energy infrastructure facilities were among the main targets of cyberattacks from Russian cyber groups"	Anonymous
Utility Infrastructure Disruption	"Last year there was a cyberattack on a water facility in Denmark where they couldn't supply water to citizens for a couple of hours."	P12
Democratic Process Vulnerability	"Denmark has moved to digital electoral rolls... The question becomes: what happens if the system goes down?"	P3
Energy Sector Targeting	"Energy infrastructure facilities were among the main targets of cyberattacks from Russian cyber groups."	Anonymous
Civilian Infrastructure Targeting	"If they can take down hospitals, power supply, or water supply, then people stop caring about the war because they care about their own welfare."	P6
Combined Attack Strategy	"Russia uses combined attacks on critical infrastructure, such as attacks can serve as missile strikes in combination with a cyberattack on infrastructure"	Anonymous
Tactics Evolution	"Since the beginning of the full-scale invasion, 'cyberwar' has expanded the range of tactics and tools used in cyberattacks"	Anonymous
Combined Disruption Strategy	"DDoS attacks are unlikely to be effective on their own. There was one case when hackers targeted an energy company, complementing their operation by flooding their hotline with calls."	P15
Cyber-Physical Attack Coordination	"Russia hacked Okhmatdyt Children's Hospital's network before a missile strike."	P15
Advanced Persistence Techniques	"Hackers often employ persistence techniques based on the MITRE ATT&CK framework. They create child processes and backdoors that are difficult to detect."	P11
Combined Attack Approach	"Russia uses combined attacks on critical infrastructure, such attacks can serve as missile strikes in combination with a cyberattack on infrastructure."	Anonymous
Attack Efficiency Characteristics	"low entry threshold, quick effect, and maximum destructive impact"	Anonymous
Common Attack Methods	"phishing campaigns, ransomware, DDoS attacks."	Anonymous
Social Engineering Vulnerability	"With NemID, the biggest problem was social engineering. Someone could send you a photo of the key card, or if they knew when you were logging in, they could send you a request that you might approve."	P8
Email-Based Threat Dominance	"95% of malware comes through emails. That's been our main risk since I started doing these presentations in 2017."	P6
AI-Enhanced Phishing Evolution	"With generative AI, it's now easier for adversaries to craft better-looking phishing emails by gathering information from places like LinkedIn to personalize attacks."	P1
Cultural Trust Exploitation	"The Danish levels of trust are so high that when you tell them 'trust is a liability,' they don't understand."	P3
Naive Security Mindset	"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?"	P3

Continued on next page

Table 7 – *Continued from previous page*

Pattern Label	**Quote**	**Participant**
Human Security Weakness	"Studies show that 85-90% of cyber attacks result from human error. Attackers target users as the entry point."	P11
User Behavior Risk	"Our biggest problem is users because they will click on anything without thinking about it."	P6
Attack Vector Statistics	"80% of breaches start with phishing, a simple and effective way to penetrate a hospital's network, insufficient awareness of hospital staff about cyber hygiene"	Anonymous
Social Engineering Prevalence	"Through multiple annual threat intelligence reports, social engineering remains the predominant technique used by external threat actors."	P1
Generational Security Divide	"The younger generation seems to have a better understanding and sensitivity to these issues, while the older generation might be more reluctant to invest in cybersecurity."	P13
Training Resource Constraint	"Currently, we're allowed 40 minutes per year for security awareness training. With 50,000 employees, if we asked for one hour, that would be 50,000 person-hours annually."	P6
Expertise Shortage Impact	"The biggest risk is the lack of competencies, because that is foundational for doing all the rest."	P7
Human Capital Investment Need	"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."	P12
Workforce Challenge	"Lack of qualified personnel (personnel shortage), as hostilities make their adjustments"	Anonymous
Leadership Impact	"presence of an incompetent head of an organization or institution, which in turn can lead to the 'decline' of cybersecurity issues in general"	Anonymous
Incident Recovery Process	"We were able to restore it, but the server was unavailable during recovery. The biggest impact was on blood analysis—we couldn't access previous results temporarily and had to slow down processing new samples. Staff had to record results manually rather than uploading to the server while systems were being restored. If there were critical blood tests needed immediately, we still had the physical samples and could repeat the analysis. So no patient care was compromised—we just had to spend extra time redoing some tests. Nothing was permanently lost."	P6
Incident Response Coordination	"When an incident occurs, we gather in a designated room with all relevant personnel: communications staff to handle press inquiries, administrative directors, my department, and representatives from clinical departments."	P6
Parallel Response Methodology	"We work on two tracks simultaneously: a technical track focused on containing damage, investigating the cause, and restoring systems; and a communications track focused on keeping the press, users, and patients informed."	P6

Continued on next page

Table 7 – *Continued from previous page*

Pattern Label	**Quote**	**Participant**
Low-Tech Contingency Planning	"We also prepare for scenarios where attacks might disable power, mobile phones, or telecommunications by practicing old-fashioned communication methods."	P14
Data Recovery Strategy	"Backup and cloud technologies have proven their effectiveness – Ukraine transferred critical data to secure clouds, which allowed quick recovery of systems after attacks."	Anonymous
Containment Strategy	"limiting and localizing a resource that has been attacked to prevent spread by attackers"	Anonymous
Resilience Mechanism	"Backup and cloud technologies have proven their effectiveness – Ukraine transferred critical data to secure clouds, which allowed quick recovery of systems after attacks."	Anonymous
Response Protocol Deficiency	"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?'"	P3
Decentralized System Vulnerability	"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."	P3
Historical Security Negligence	"For years, security was neglected. There was no dedicated security department whatsoever."	P6
Uncontrolled Technology Acquisition	"Previously, departments would purchase and install whatever they wanted without consulting IT."	P6
Governance Centralization Effort	"Before, responsibility was fragmented into different ministries, and now they're trying to consolidate it into a single ministry."	P7
Security Function Evolution	"Four years ago, we finally established a proper security department, starting with me and my colleague. Today, we've grown to 26 people."	P6
Governance Recommendation	"Centralization of cybersecurity, use of technology for data preservation, rapid response to attacks"	Anonymous
Defense Strategy	"Proactive monitoring and response to threats to quickly detect and neutralize attacks"	Anonymous
Best Practice Recommendation	"If each medical institution follows Ukraine's cybersecurity strategy, then in general, one can achieve the best level of cybersecurity and minimize 75% of cyberattacks."	Anonymous
Security Strategy Effectiveness	"If each medical institution follows Ukraine's cybersecurity strategy, then in general, one can achieve the best level of cybersecurity and minimize 75% of cyberattacks."	Anonymous
Regulatory Compliance Emphasis	"All our information is governed by GDPR. Everything you do needs to consider what happens with the data and how it's used."	P4
False Security Perception	"The biggest problem, though, is that many of the methods claiming to protect privacy don't actually work... What people think is secure is often not secure at all."	P4

Continued on next page

Table 7 – *Continued from previous page*

Pattern Label	**Quote**	**Participant**
Compliance-Efficiency Tradeoff	"Regulatory frameworks like GDPR have a positive impact from a security perspective. But there's a price to pay - everything you do has to go through extra checks and processes."	P9
Legal Framework Challenges	"Legal limitations and complexities in international law regarding cybercrimes"	Anonymous
National Security Coordination	"In Denmark, we have the Center for Cybersecurity that works with all regions across Denmark. Their job is to coordinate information about attacks, intrusions, or any potential dangers to the regions."	P14
Threat Intelligence Sharing	"We also participate in a threat-sharing platform with different regions in Denmark. If one region experiences a threat, they submit their findings to this platform so everyone is aware."	P1
Multi-Level Security Collaboration	"We collaborate extensively with other regions, the European Union, the Danish Ministry of Defense, and various entities to ensure we maintain multiple perspectives on cybersecurity."	P5
Regional Defense Coalition	"We could form consortiums with other Nordic countries like Sweden and Norway to develop common solutions for these challenges."	P13
Public-Private Security Partnership	"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."	P3
Cross-Border Intelligence Sharing	"If there's international exchange of intelligence about attacks, this information is instantly distributed to all other countries, and threat hunting begins."	P15
International Assistance Value	"Cooperation with international partners helps Ukraine receive material and technical assistance, free staff training, and exchange of indicators and information about cyber threats"	Anonymous
Alliance Strengthening	"Ukraine's cybersecurity cooperation with Western countries has strengthened its hybrid defense, increased resilience to cyberattacks, and contributed to rapprochement with the EU and NATO"	Anonymous
Real-time Intelligence Sharing	"Ukraine actively cooperates with international partners, receiving data on new cyberattacks in real time"	Anonymous
Cross-border Healthcare Security	"Ukraine accepts citizens in medical institutions from other countries, and this is the security not only of Ukraine but also of international partners in general"	Anonymous
Collaborative Defense	"If there's international exchange of intelligence about attacks, this information is instantly distributed to all other countries, and threat hunting begins"	Anonymous
Threat Intelligence Application	"Today, government agencies, organizations, and institutions can be aware of certain cyber threats that have already occurred in the national resilience system and predict (prevent) similar cases in their own infrastructures"	Anonymous

Continued on next page

Table 7 – *Continued from previous page*

Pattern Label	**Quote**	**Participant**
Foreign Technology Reliance	"Denmark is essentially a Microsoft country. All data is stored on American-owned servers."	P3
Technology Sovereignty Need	"We're relying too much on tools from other countries, which makes us vulnerable. We need to become more independent in our cybersecurity infrastructure."	P13
Foreign Hardware Distrust	"We had a massive problem with Chinese cameras because they might have backdoors. Most government functions in Denmark are not allowing official Chinese cameras."	P6
Foreign AI Restriction	"We've also banned some AI applications from China."	P10
Market Monopoly Vulnerability	"When there are only one or two suppliers worldwide, our leverage is limited."	P6
Foreign Technology Restriction	"We do block Chinese AI tools and other less trusted systems."	P14
Foreign AI Data Extraction	"I think we need a good way to block new Chinese AI systems like Deepsea Eagle, DeepMind, and a few others because the second someone starts putting data into them, it all goes to the Chinese."	P6
Geopolitical Trust Shift	"The current shift with the US working more closely with Russia raises questions about the dangers of sharing data with American companies."	P7
Alliance Relationship Uncertainty	"We're closely monitoring statements from the US and what Trump is saying, especially regarding Greenland, where he hasn't excluded the use of military power."	P1
International Relationship Deterioration	"When I joined 'University A' in 2009, we were 'best friends' with China and had many exchange programs. Now, this is completely forbidden."	P9
International Collaboration Ban	"Currently, you cannot work with Russians or Chinese, full stop."	P9
Geopolitical Instability Exploitation	"As international cooperation becomes more destabilized, countries like Russia have greater incentives to target nations like Denmark."	P5
Cyber Warfare Definition	"If an attack were conducted by a state actor like the Russian government, it would be considered cyber warfare -essentially a declaration of war."	P5
Threat Actor Hierarchy	"In terms of activity, China would be the most active, followed by Russia, North Korea, and Iran."	P15
Intellectual Property Targeting	"For China, it's about intellectual property - they want to copy whatever they can get their hands on."	P6
Long-Term Trust Infiltration	"Someone, most likely Chinese, targeted a specific sub-program for Linux that was maintained by just one developer on GitHub. The attackers created 3-4 accounts that all contributed useful software on GitHub to build their credibility. They spent over three years infiltrating this developer's trust, with their accounts saying things like, 'Why don't you update more often?' and 'I have some free time, I can help.'"	P6
Political Statement Retaliation	"We can see examples with Ukraine and Russia - whenever a political figure says something that upsets Russia, there can be consequences."	P14

Continued on next page

Table 7 – *Continued from previous page*

Pattern Label	**Quote**	**Participant**
Economic Motivation Strategy	"North Korea, due to all the embargoes against them, basically only gets outside money from cyber warfare, and they have many skilled people doing it."	P6
State-Sponsored Threat Actors	"The main threats come from rogue states that don't hide their efforts and those who make money from it, like North Korea with the Lazarus Group."	P15
Russian Threat Primacy	"Right now, I think Russia poses the main threat."	P12
Persistent State Aggression	"Obviously, the number of cyberattacks has increased because it became a priority for Russia. But Russia has been actively attacking us for years."	P15
Russian Cyber Capabilities	"Russia excel at social engineering and developing viruses."	P15
Public Opinion Manipulation	"Russia is a big worry right now due to the Ukrainian-Russian war... Right now, if Russia can change public opinion, that's perfect for them."	P6
Disinformation Campaign Evidence	"About a month ago, a Russian propaganda agency had almost all their internal documentation leaked. Russia has been involved in propaganda and election manipulation for years, but has denied it."	P6
Geographic Access Restriction	"We've blocked a lot of the world - Ukraine, Russia, China, India, and around 17 or 18 other countries. We open access if people need it for specific sites."	P6
Information Warfare Objectives	"influence elections, manipulate public opinion, and conduct economic warfare."	Anonymous
Societal Impact Concern	"Imagine a hospital gets hacked and equipment stops working entirely... the moral effect would be much greater because it strongly affects society."	P15
AI Threat Anticipation	"I anticipate that working with and countering artificial intelligence will dominate our focus in the coming years."	P5
Quantum Cryptography Threat	"Quantum computers, if we are able to construct one that is large and stable enough, would be able to run algorithms that solve some of the computationally hard problems that underpin our most widely used cryptographic algorithms."	P2
Post-Quantum Transition Challenge	"The biggest challenge is not actually designing them - they already exist. The key challenge is transitioning to those algorithms, standardizing them, and deploying them."	P2
Advanced Deepfake Capability	"Currently, technology exists that combines real-time deepfakes with AI like ChatGPT, which can speak Danish."	P6
AI Circumvention Potential	"Nothing is perfect. With good generative models, you can model anything, including heat signatures and other factors. If you can do that, you can potentially fool any system."	P4
Biometric Defense Mechanism	"Most authentication systems use additional parameters like detecting heat around the face. A screen generating a pattern won't generate the right heat signature."	P4
Behavioral Biometric Authentication	"Systems also check if eye movements appear natural."	P4

Continued on next page

Table 7 – *Continued from previous page*

Pattern Label	Quote	Participant
Biometric Spoofing Vulnerability	"You can spoof iris recognition patterns - that's been demonstrated."	P4
Neurobiological Identity Marker	"The eye is controlled by muscles and is essentially the only visible part of the brain -it's directly connected to your brain. Emotions are also reflected in eye movements, so you have some certainty about who the individual is."	P4
Multi-Factor Biometric Security	"If you combine fingerprints, eye tracking, facial recognition, hair growth patterns, and other biometrics—yes, certainly."	P4

7 All Labels and Source

Pattern Label	Source
Medical Data Vulnerability	Survey
Medical System Breach Example	Survey
Ransomware Response Strategy	Survey
Healthcare Impact Assessment	Survey
Critical Infrastructure Targeting	Survey
Energy Sector Targeting	Survey
Combined Attack Strategy	Survey
Tactics Evolution	Survey
Combined Attack Approach	Survey
Attack Efficiency Characteristics	Survey
Common Attack Methods	Survey
Attack Vector Statistics	Survey
Workforce Challenge	Survey
Leadership Impact	Survey
Data Recovery Strategy	Survey
Containment Strategy	Survey
Resilience Mechanism	Survey
Governance Recommendation	Survey
Defense Strategy	Survey
Best Practice Recommendation	Survey
Security Strategy Effectiveness	Survey
Legal Framework Challenges	Survey
International Assistance Value	Survey
Alliance Strengthening	Survey
Real-time Intelligence Sharing	Survey
Cross-border Healthcare Security	Survey
Collaborative Defense	Survey
Threat Intelligence Application	Survey
Information Warfare Objectives	Survey
Healthcare Data Breach	Interview
Healthcare Targeting Risk	Interview
Digital Identity Infrastructure	Interview
Authentication System Weakness	Interview
Legacy System Dependence	Interview
Resource Limitation Impact	Interview
Digital Ecosystem Vulnerability	Interview
Utility Infrastructure Disruption	Interview
Democratic Process Vulnerability	Interview
Civilian Infrastructure Targeting	Interview

Pattern Label	Source
Combined Disruption Strategy	Interview
Cyber-Physical Attack Coordination	Interview
Advanced Persistence Techniques	Interview
Social Engineering Vulnerability	Interview
Email-Based Threat Dominance	Interview
AI-Enhanced Phishing Evolution	Interview
Cultural Trust Exploitation	Interview
Naive Security Mindset	Interview
Human Security Weakness	Interview
User Behavior Risk	Interview
Social Engineering Prevalence	Interview
Generational Security Divide	Interview
Training Resource Constraint	Interview
Expertise Shortage Impact	Interview
Human Capital Investment Need	Interview
Incident Recovery Process	Interview
Incident Response Coordination	Interview
Parallel Response Methodology	Interview
Low-Tech Contingency Planning	Interview
Response Protocol Deficiency	Interview
Decentralized System Vulnerability	Interview
Historical Security Negligence	Interview
Uncontrolled Technology Acquisition	Interview
Governance Centralization Effort	Interview
Security Function Evolution	Interview
Regulatory Compliance Emphasis	Interview
False Security Perception	Interview
Compliance-Efficiency Tradeoff	Interview
National Security Coordination	Interview
Threat Intelligence Sharing	Interview
Multi-Level Security Collaboration	Interview
Regional Defense Coalition	Interview
Public-Private Security Partnership	Interview
Cross-Border Intelligence Sharing	Interview
Foreign Technology Reliance	Interview
Technology Sovereignty Need	Interview
Foreign Hardware Distrust	Interview
Foreign AI Restriction	Interview
Market Monopoly Vulnerability	Interview
Foreign Technology Restriction	Interview
Foreign AI Data Extraction	Interview
Geopolitical Trust Shift	Interview
Alliance Relationship Uncertainty	Interview
International Relationship Deterioration	Interview
International Collaboration Ban	Interview
Geopolitical Instability Exploitation	Interview
Cyber Warfare Definition	Interview
Threat Actor Hierarchy	Interview
Intellectual Property Targeting	Interview
Long-Term Trust Infiltration	Interview
Political Statement Retaliation	Interview
Economic Motivation Strategy	Interview
State-Sponsored Threat Actors	Interview
Russian Threat Primacy	Interview
Persistent State Aggression	Interview

Pattern Label	Source
Russian Cyber Capabilities	Interview
Public Opinion Manipulation	Interview
Disinformation Campaign Evidence	Interview
Geographic Access Restriction	Interview
Societal Impact Concern	Interview
AI Threat Anticipation	Interview
Quantum Cryptography Threat	Interview
Post-Quantum Transition Challenge	Interview
Advanced Deepfake Capability	Interview
AI Circumvention Potential	Interview
Biometric Defense Mechanism	Interview
Behavioral Biometric Authentication	Interview
Biometric Spoofing Vulnerability	Interview
Neurobiological Identity Marker	Interview
Multi-Factor Biometric Security	Interview

8 Affinity Diagram Clustering

Cluster	Distinct Labels
Healthcare Security Vulnerabilities	Medical Data Vulnerability, Medical System Breach Example, Ransomware Response Strategy, Healthcare Data Breach, Healthcare Targeting Risk, Healthcare Impact Assessment
Digital Infrastructure Challenges	Digital Identity Infrastructure, Authentication System Weakness, Legacy System Dependence, Resource Limitation Impact, Digital Ecosystem Vulnerability
Critical Infrastructure Protection	Critical Infrastructure Targeting, Utility Infrastructure Disruption, Democratic Process Vulnerability, Energy Sector Targeting, Civilian Infrastructure Targeting
Advanced Attack Strategies	Combined Attack Strategy, Tactics Evolution, Combined Disruption Strategy, Cyber-Physical Attack Coordination, Advanced Persistence Techniques, Combined Attack Approach, Attack Efficiency Characteristics, Common Attack Methods
Social Engineering and Human Vulnerabilities	Social Engineering Vulnerability, Email-Based Threat Dominance, AI-Enhanced Phishing Evolution, Cultural Trust Exploitation, Naive Security Mindset, Human Security Weakness, User Behavior Risk, Attack Vector Statistics, Social Engineering Prevalence
Workforce and Expertise Challenges	Generational Security Divide, Training Resource Constraint, Expertise Shortage Impact, Human Capital Investment Need, Workforce Challenge, Leadership Impact
Incident Response and Recovery	Incident Recovery Process, Incident Response Coordination, Parallel Response Methodology, Low-Tech Contingency Planning, Data Recovery Strategy, Containment Strategy, Resilience Mechanism
Governance and Strategic Planning	Response Protocol Deficiency, Decentralized System Vulnerability, Historical Security Negligence, Uncontrolled Technology Acquisition, Governance Centralization Effort, Security Function Evolution, Governance Recommendation, Defense Strategy, Best Practice Recommendation, Security Strategy Effectiveness
Regulatory and Compliance Matters	Regulatory Compliance Emphasis, False Security Perception, Compliance-Efficiency Tradeoff, Legal Framework Challenges

Continued on next page

Table 9 – *Continued from previous page*

Cluster	Distinct Labels
International Collaboration	National Security Coordination, Threat Intelligence Sharing, Multi-Level Security Collaboration, Regional Defense Coalition, Public-Private Security Partnership, Cross-Border Intelligence Sharing, International Assistance Value, Alliance Strengthening, Real-time Intelligence Sharing, Cross-border Healthcare Security, Collaborative Defense, Threat Intelligence Application
Foreign Technology Considerations	Foreign Technology Reliance, Technology Sovereignty Need, Foreign Hardware Distrust, Foreign AI Restriction, Market Monopoly Vulnerability, Foreign Technology Restriction, Foreign AI Data Extraction
Geopolitical Security Dimensions	Geopolitical Trust Shift, Alliance Relationship Uncertainty, International Relationship Deterioration, International Collaboration Ban, Geopolitical Instability Exploitation, Cyber Warfare Definition
State-Sponsored Threat Actors	Threat Actor Hierarchy, Intellectual Property Targeting, Long-Term Trust Infiltration, Political Statement Retaliation, Economic Motivation Strategy, State-Sponsored Threat Actors, Russian Threat Primacy, Persistent State Aggression, Russian Cyber Capabilities
Information Operations	Public Opinion Manipulation, Disinformation Campaign Evidence, Geographic Access Restriction, Information Warfare Objectives, Societal Impact Concern
Emerging Technology Threats	AI Threat Anticipation, Quantum Cryptography Threat, Post-Quantum Transition Challenge, Advanced Deepfake Capability, AI Circumvention Potential
Biometric Security Considerations	Biometric Defense Mechanism, Behavioral Biometric Authentication, Biometric Spoofing Vulnerability, Neurobiological Identity Marker, Multi-Factor Biometric Security

9 Clusters after Affinity Diagram for Interviews

Table 10: Interview Patterns by Cluster

Pattern Label	Source	Cluster
Healthcare Data Breach	Interview	Healthcare Security Vulnerabilities
Healthcare Targeting Risk	Interview	Healthcare Security Vulnerabilities
Digital Identity Infrastructure	Interview	Digital Infrastructure Challenges
Authentication System Weakness	Interview	Digital Infrastructure Challenges
Legacy System Dependence	Interview	Digital Infrastructure Challenges
Resource Limitation Impact	Interview	Digital Infrastructure Challenges
Digital Ecosystem Vulnerability	Interview	Digital Infrastructure Challenges
Utility Infrastructure Disruption	Interview	Critical Infrastructure Protection
Democratic Process Vulnerability	Interview	Critical Infrastructure Protection
Civilian Infrastructure Targeting	Interview	Critical Infrastructure Protection
Combined Disruption Strategy	Interview	Advanced Attack Strategies
Cyber-Physical Attack Coordination	Interview	Advanced Attack Strategies
Advanced Persistence Techniques	Interview	Advanced Attack Strategies
Social Engineering Vulnerability	Interview	Social Engineering and Human Vulnerabilities
Email-Based Threat Dominance	Interview	Social Engineering and Human Vulnerabilities
AI-Enhanced Phishing Evolution	Interview	Social Engineering and Human Vulnerabilities
Cultural Trust Exploitation	Interview	Social Engineering and Human Vulnerabilities
Naive Security Mindset	Interview	Social Engineering and Human Vulnerabilities

Pattern Label	Source	Cluster
Human Security Weakness	Interview	Social Engineering and Human Vulnerabilities
User Behavior Risk	Interview	Social Engineering and Human Vulnerabilities
Social Engineering Prevalence	Interview	Social Engineering and Human Vulnerabilities
Generational Security Divide	Interview	Workforce and Expertise Challenges
Training Resource Constraint	Interview	Workforce and Expertise Challenges
Expertise Shortage Impact	Interview	Workforce and Expertise Challenges
Human Capital Investment Need	Interview	Workforce and Expertise Challenges
Incident Recovery Process	Interview	Incident Response and Recovery
Incident Response Coordination	Interview	Incident Response and Recovery
Parallel Response Methodology	Interview	Incident Response and Recovery
Low-Tech Contingency Planning	Interview	Incident Response and Recovery
Response Protocol Deficiency	Interview	Governance and Strategic Planning
Decentralized System Vulnerability	Interview	Governance and Strategic Planning
Historical Security Negligence	Interview	Governance and Strategic Planning
Uncontrolled Technology Acquisition	Interview	Governance and Strategic Planning
Governance Centralization Effort	Interview	Governance and Strategic Planning
Security Function Evolution	Interview	Governance and Strategic Planning
Regulatory Compliance Emphasis	Interview	Regulatory and Compliance Matters
False Security Perception	Interview	Regulatory and Compliance Matters
Compliance-Efficiency Tradeoff	Interview	Regulatory and Compliance Matters
National Security Coordination	Interview	International Collaboration
Threat Intelligence Sharing	Interview	International Collaboration
Multi-Level Security Collaboration	Interview	International Collaboration
Regional Defense Coalition	Interview	International Collaboration
Public-Private Security Partnership	Interview	International Collaboration
Cross-Border Intelligence Sharing	Interview	International Collaboration
Foreign Technology Reliance	Interview	Foreign Technology Considerations
Technology Sovereignty Need	Interview	Foreign Technology Considerations
Foreign Hardware Distrust	Interview	Foreign Technology Considerations
Foreign AI Restriction	Interview	Foreign Technology Considerations
Market Monopoly Vulnerability	Interview	Foreign Technology Considerations
Foreign Technology Restriction	Interview	Foreign Technology Considerations
Foreign AI Data Extraction	Interview	Foreign Technology Considerations
Geopolitical Trust Shift	Interview	Geopolitical Security Dimensions
Alliance Relationship Uncertainty	Interview	Geopolitical Security Dimensions
International Relationship Deterioration	Interview	Geopolitical Security Dimensions
International Collaboration Ban	Interview	Geopolitical Security Dimensions
Geopolitical Instability Exploitation	Interview	Geopolitical Security Dimensions
Cyber Warfare Definition	Interview	Geopolitical Security Dimensions
Threat Actor Hierarchy	Interview	State-Sponsored Threat Actors
Intellectual Property Targeting	Interview	State-Sponsored Threat Actors
Long-Term Trust Infiltration	Interview	State-Sponsored Threat Actors
Political Statement Retaliation	Interview	State-Sponsored Threat Actors
Economic Motivation Strategy	Interview	State-Sponsored Threat Actors
State-Sponsored Threat Actors	Interview	State-Sponsored Threat Actors
Russian Threat Primacy	Interview	State-Sponsored Threat Actors
Persistent State Aggression	Interview	State-Sponsored Threat Actors
Russian Cyber Capabilities	Interview	State-Sponsored Threat Actors
Public Opinion Manipulation	Interview	Information Operations
Disinformation Campaign Evidence	Interview	Information Operations
Geographic Access Restriction	Interview	Information Operations
Societal Impact Concern	Interview	Information Operations
AI Threat Anticipation	Interview	Emerging Technology Threats
Quantum Cryptography Threat	Interview	Emerging Technology Threats

Pattern Label	Source	Cluster
Post-Quantum Transition Challenge	Interview	Emerging Technology Threats
Advanced Deepfake Capability	Interview	Emerging Technology Threats
AI Circumvention Potential	Interview	Emerging Technology Threats
Biometric Defense Mechanism	Interview	Biometric Security Considerations
Behavioral Biometric Authentication	Interview	Biometric Security Considerations
Biometric Spoofing Vulnerability	Interview	Biometric Security Considerations
Neurobiological Identity Marker	Interview	Biometric Security Considerations
Multi-Factor Biometric Security	Interview	Biometric Security Considerations

10 Clusters after Affinity Diagram for Survey

Table 11: Survey Patterns by Cluster

Pattern Label	Source	Cluster
Medical Data Vulnerability	Survey	Healthcare Security Vulnerabilities
Medical System Breach Example	Survey	Healthcare Security Vulnerabilities
Ransomware Response Strategy	Survey	Healthcare Security Vulnerabilities
Healthcare Impact Assessment	Survey	Healthcare Security Vulnerabilities
Critical Infrastructure Targeting	Survey	Critical Infrastructure Protection
Energy Sector Targeting	Survey	Critical Infrastructure Protection
Combined Attack Strategy	Survey	Advanced Attack Strategies
Tactics Evolution	Survey	Advanced Attack Strategies
Combined Attack Approach	Survey	Advanced Attack Strategies
Attack Efficiency Characteristics	Survey	Advanced Attack Strategies
Common Attack Methods	Survey	Advanced Attack Strategies
Attack Vector Statistics	Survey	Social Engineering and Human Vulnerabilities
Workforce Challenge	Survey	Workforce and Expertise Challenges
Leadership Impact	Survey	Workforce and Expertise Challenges
Data Recovery Strategy	Survey	Incident Response and Recovery
Containment Strategy	Survey	Incident Response and Recovery
Resilience Mechanism	Survey	Incident Response and Recovery
Governance Recommendation	Survey	Governance and Strategic Planning
Defense Strategy	Survey	Governance and Strategic Planning
Best Practice Recommendation	Survey	Governance and Strategic Planning
Security Strategy Effectiveness	Survey	Governance and Strategic Planning
Legal Framework Challenges	Survey	Regulatory and Compliance Matters
International Assistance Value	Survey	International Collaboration
Alliance Strengthening	Survey	International Collaboration
Real-time Intelligence Sharing	Survey	International Collaboration
Cross-border Healthcare Security	Survey	International Collaboration
Collaborative Defense	Survey	International Collaboration
Threat Intelligence Application	Survey	International Collaboration
Information Warfare Objectives	Survey	Information Operations

11 Clustered Codes after Affinity Diagram

Pattern Label	Source	Cluster
Medical Data Vulnerability	Survey	Healthcare Security Vulnerabilities
Medical System Breach Example	Survey	Healthcare Security Vulnerabilities
Ransomware Response Strategy	Survey	Healthcare Security Vulnerabilities
Healthcare Data Breach	Interview	Healthcare Security Vulnerabilities
Healthcare Targeting Risk	Interview	Healthcare Security Vulnerabilities

Pattern Label	Source	Cluster
Healthcare Impact Assessment	Survey	Healthcare Security Vulnerabilities
Digital Identity Infrastructure	Interview	Digital Infrastructure Challenges
Authentication System Weakness	Interview	Digital Infrastructure Challenges
Legacy System Dependence	Interview	Digital Infrastructure Challenges
Resource Limitation Impact	Interview	Digital Infrastructure Challenges
Digital Ecosystem Vulnerability	Interview	Digital Infrastructure Challenges
Critical Infrastructure Targeting	Survey	Critical Infrastructure Protection
Utility Infrastructure Disruption	Interview	Critical Infrastructure Protection
Democratic Process Vulnerability	Interview	Critical Infrastructure Protection
Energy Sector Targeting	Survey	Critical Infrastructure Protection
Civilian Infrastructure Targeting	Interview	Critical Infrastructure Protection
Combined Attack Strategy	Survey	Advanced Attack Strategies
Tactics Evolution	Survey	Advanced Attack Strategies
Combined Disruption Strategy	Interview	Advanced Attack Strategies
Cyber-Physical Attack Coordination	Interview	Advanced Attack Strategies
Advanced Persistence Techniques	Interview	Advanced Attack Strategies
Combined Attack Approach	Survey	Advanced Attack Strategies
Attack Efficiency Characteristics	Survey	Advanced Attack Strategies
Common Attack Methods	Survey	Advanced Attack Strategies
Social Engineering Vulnerability	Interview	Social Engineering and Human Vulnerabilities
Email-Based Threat Dominance	Interview	Social Engineering and Human Vulnerabilities
AI-Enhanced Phishing Evolution	Interview	Social Engineering and Human Vulnerabilities
Cultural Trust Exploitation	Interview	Social Engineering and Human Vulnerabilities
Naive Security Mindset	Interview	Social Engineering and Human Vulnerabilities
Human Security Weakness	Interview	Social Engineering and Human Vulnerabilities
User Behavior Risk	Interview	Social Engineering and Human Vulnerabilities
Attack Vector Statistics	Survey	Social Engineering and Human Vulnerabilities
Social Engineering Prevalence	Interview	Social Engineering and Human Vulnerabilities
Generational Security Divide	Interview	Workforce and Expertise Challenges
Training Resource Constraint	Interview	Workforce and Expertise Challenges
Expertise Shortage Impact	Interview	Workforce and Expertise Challenges
Human Capital Investment Need	Interview	Workforce and Expertise Challenges
Workforce Challenge	Survey	Workforce and Expertise Challenges
Leadership Impact	Survey	Workforce and Expertise Challenges
Incident Recovery Process	Interview	Incident Response and Recovery
Incident Response Coordination	Interview	Incident Response and Recovery
Parallel Response Methodology	Interview	Incident Response and Recovery
Low-Tech Contingency Planning	Interview	Incident Response and Recovery
Data Recovery Strategy	Survey	Incident Response and Recovery
Containment Strategy	Survey	Incident Response and Recovery
Resilience Mechanism	Survey	Incident Response and Recovery
Response Protocol Deficiency	Interview	Governance and Strategic Planning
Decentralized System Vulnerability	Interview	Governance and Strategic Planning
Historical Security Negligence	Interview	Governance and Strategic Planning
Uncontrolled Technology Acquisition	Interview	Governance and Strategic Planning
Governance Centralization Effort	Interview	Governance and Strategic Planning

Pattern Label	Source	Cluster
Security Function Evolution	Interview	Governance and Strategic Planning
Governance Recommendation	Survey	Governance and Strategic Planning
Defense Strategy	Survey	Governance and Strategic Planning
Best Practice Recommendation	Survey	Governance and Strategic Planning
Security Strategy Effectiveness	Survey	Governance and Strategic Planning
Regulatory Compliance Emphasis	Interview	Regulatory and Compliance Matters
False Security Perception	Interview	Regulatory and Compliance Matters
Compliance-Efficiency Tradeoff	Interview	Regulatory and Compliance Matters
Legal Framework Challenges	Survey	Regulatory and Compliance Matters
National Security Coordination	Interview	International Collaboration
Threat Intelligence Sharing	Interview	International Collaboration
Multi-Level Security Collaboration	Interview	International Collaboration
Regional Defense Coalition	Interview	International Collaboration
Public-Private Security Partnership	Interview	International Collaboration
Cross-Border Intelligence Sharing	Interview	International Collaboration
International Assistance Value	Survey	International Collaboration
Alliance Strengthening	Survey	International Collaboration
Real-time Intelligence Sharing	Survey	International Collaboration
Cross-border Healthcare Security	Survey	International Collaboration
Collaborative Defense	Survey	International Collaboration
Threat Intelligence Application	Survey	International Collaboration
Foreign Technology Reliance	Interview	Foreign Technology Considerations
Technology Sovereignty Need	Interview	Foreign Technology Considerations
Foreign Hardware Distrust	Interview	Foreign Technology Considerations
Foreign AI Restriction	Interview	Foreign Technology Considerations
Market Monopoly Vulnerability	Interview	Foreign Technology Considerations
Foreign Technology Restriction	Interview	Foreign Technology Considerations
Foreign AI Data Extraction	Interview	Foreign Technology Considerations
Geopolitical Trust Shift	Interview	Geopolitical Security Dimensions
Alliance Relationship Uncertainty	Interview	Geopolitical Security Dimensions
International Relationship Deterioration	Interview	Geopolitical Security Dimensions
International Collaboration Ban	Interview	Geopolitical Security Dimensions
Geopolitical Instability Exploitation	Interview	Geopolitical Security Dimensions
Cyber Warfare Definition	Interview	Geopolitical Security Dimensions
Threat Actor Hierarchy	Interview	State-Sponsored Threat Actors
Intellectual Property Targeting	Interview	State-Sponsored Threat Actors
Long-Term Trust Infiltration	Interview	State-Sponsored Threat Actors
Political Statement Retaliation	Interview	State-Sponsored Threat Actors
Economic Motivation Strategy	Interview	State-Sponsored Threat Actors
State-Sponsored Threat Actors	Interview	State-Sponsored Threat Actors
Russian Threat Primacy	Interview	State-Sponsored Threat Actors
Persistent State Aggression	Interview	State-Sponsored Threat Actors
Russian Cyber Capabilities	Interview	State-Sponsored Threat Actors
Public Opinion Manipulation	Interview	Information Operations
Disinformation Campaign Evidence	Interview	Information Operations
Geographic Access Restriction	Interview	Information Operations
Information Warfare Objectives	Survey	Information Operations
Societal Impact Concern	Interview	Information Operations
AI Threat Anticipation	Interview	Emerging Technology Threats
Quantum Cryptography Threat	Interview	Emerging Technology Threats
Post-Quantum Transition Challenge	Interview	Emerging Technology Threats
Advanced Deepfake Capability	Interview	Emerging Technology Threats
AI Circumvention Potential	Interview	Emerging Technology Threats
Biometric Defense Mechanism	Interview	Biometric Security Considerations
Behavioral Biometric Authentication	Interview	Biometric Security Considerations

Pattern Label	Source	Cluster
Biometric Spoofing Vulnerability	Interview	Biometric Security Considerations
Neurobiological Identity Marker	Interview	Biometric Security Considerations
Multi-Factor Biometric Security	Interview	Biometric Security Considerations

12 All clusters

Table 13: Cluster Presence by Source (Interview vs Survey)

Cluster	Interview	Survey
Healthcare Security Vulnerabilities	+	+
Digital Infrastructure Challenges	+	x
Critical Infrastructure Protection	+	+
Advanced Attack Strategies	+	+
Social Engineering and Human Vulnerabilities	+	+
Workforce and Expertise Challenges	+	+
Incident Response and Recovery	+	+
Governance and Strategic Planning	+	+
Regulatory and Compliance Matters	+	+
International Collaboration	+	+
Foreign Technology Considerations	+	x
Geopolitical Security Dimensions	+	x
State-Sponsored Threat Actors	+	x
Information Operations	+	+
Emerging Technology Threats	+	x
Biometric Security Considerations	+	x

13 Full List of Clusters

1. Healthcare Security Vulnerabilities
2. Digital Infrastructure Challenges
3. Critical Infrastructure Protection
4. Advanced Attack Strategies
5. Social Engineering and Human Vulnerabilities
6. Workforce and Expertise Challenges
7. Incident Response and Recovery
8. Governance and Strategic Planning
9. Regulatory and Compliance Matters
10. International Collaboration
11. Foreign Technology Considerations
12. Geopolitical Security Dimensions
13. State-Sponsored Threat Actors
14. Information Operations
15. Emerging Technology Threats
16. Biometric Security Considerations

14 Affinity Diagram with Quotes

Cluster	Quotes from Participants
Healthcare Security Vulnerabilities	"The importance of medical data access to medical histories, diagnoses, laboratory tests can be under threat or theft"; "As an example, we can cite the recent attack on the HELSI medical information system, the essence of which was to use the vulnerabilities of the database systems, as a result of which a lot of patient data was sold on the DarkNet."; "Some private medical institutions are even ready to cooperate with cybercriminals (pay a ransom to quickly restore work and prevent the leakage of patients' personal data)."; "Yes, there was a ransomware incident where one of our doctors was using network drives. The ransomware not only encrypted local files but also mapped network drives, including a connection to two Azure servers containing blood analysis results. The recent blood test data was encrypted." (P6); "In the medical field, such attacks pose a serious threat as they can block access to electronic medical records, stop the operation of vital equipment, and lead to the leakage of confidential data"; "The healthcare sector is an attractive target for both terrorists and criminals. For terrorists, it's attractive because healthcare is a matter of life and death." (P7)
Digital Infrastructure Challenges	"MitID and NemID are critical pieces of infrastructure, and security should always be the top priority when handling issues." (P8); "The biggest issue I encountered was when we discovered you could find people's usernames in MitID by simply enumerating them." (P8); "The main challenge for hospitals is legacy software. While we've closed the last Windows 2000 systems last year, we still maintain Windows XP, Windows 7, and other outdated systems." (P6); "One of the biggest challenges is budget constraints. We have a lot of old medical equipment running on outdated systems like Windows 7. Purchasing new equipment is very expensive." (P10); "Denmark is a highly digitalized country, so most public services use information systems that demand protection." (P2)
Critical Infrastructure Protection	"Energy infrastructure facilities were among the main targets of cyberattacks from Russian cyber groups"; "Energy infrastructure facilities were among the main targets of cyberattacks from Russian cyber groups."; "Last year there was a cyberattack on a water facility in Denmark where they couldn't supply water to citizens for a couple of hours." (P12); "Denmark has moved to digital electoral rolls... The question becomes: what happens if the system goes down?" (P3); "If they can take down hospitals, power supply, or water supply, then people stop caring about the war because they care about their own welfare." (P6)
Advanced Attack Strategies	"Russia uses combined attacks on critical infrastructure, such as attacks can serve as missile strikes in combination with a cyberattack on infrastructure"; "Since the beginning of the full-scale invasion, 'cyberwar' has expanded the range of tactics and tools used in cyberattacks"; "DDoS attacks are unlikely to be effective on their own. There was one case when hackers targeted an energy company, complementing their operation by flooding their hotline with calls." (P15); "Russia hacked Okhmatdyt Children's Hospital's network before a missile strike." (P15); "Hackers often employ persistence techniques based on the MITRE ATT&CK framework. They create child processes and backdoors that are difficult to detect." (P11); "Russia uses combined attacks on critical infrastructure, such attacks can serve as missile strikes in combination with a cyberattack on infrastructure."; "low entry threshold, quick effect, and maximum destructive impact"; "phishing campaigns, ransomware, DDoS attacks."

Continued on next page

Table 14 – *Continued from previous page*

Cluster	**Quotes from Participants**
Social Engineering and Human Vulnerabilities	"With NemID, the biggest problem was social engineering. Someone could send you a photo of the key card, or if they knew when you were logging in, they could send you a request that you might approve." (P8); "95% of malware comes through emails. That's been our main risk since I started doing these presentations in 2017." (P6); "With generative AI, it's now easier for adversaries to craft better-looking phishing emails by gathering information from places like LinkedIn to personalize attacks." (P1); "The Danish levels of trust are so high that when you tell them 'trust is a liability,' they don't understand." (P3); "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?" (P3); "Studies show that 85-90% of cyber attacks result from human error. Attackers target users as the entry point." (P11); "Our biggest problem is users because they will click on anything without thinking about it." (P6); "80% of breaches start with phishing, a simple and effective way to penetrate a hospital's network, insufficient awareness of hospital staff about cyber hygiene"; "Through multiple annual threat intelligence reports, social engineering remains the predominant technique used by external threat actors." (P1)
Workforce and Expertise Challenges	"The younger generation seems to have a better understanding and sensitivity to these issues, while the older generation might be more reluctant to invest in cybersecurity." (P13); "Currently, we're allowed 40 minutes per year for security awareness training. With 50,000 employees, if we asked for one hour, that would be 50,000 person-hours annually." (P6); "The biggest risk is the lack of competencies, because that is foundational for doing all the rest." (P7); "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." (P12); "Lack of qualified personnel (personnel shortage), as hostilities make their adjustments"; "presence of an incompetent head of an organization or institution, which in turn can lead to the 'decline' of cybersecurity issues in general"
Incident Response and Recovery	"We were able to restore it, but the server was unavailable during recovery. The biggest impact was on blood analysis—we couldn't access previous results temporarily and had to slow down processing new samples. Staff had to record results manually rather than uploading to the server while systems were being restored. If there were critical blood tests needed immediately, we still had the physical samples and could repeat the analysis. So no patient care was compromised—we just had to spend extra time redoing some tests. Nothing was permanently lost." (P6); "When an incident occurs, we gather in a designated room with all relevant personnel: communications staff to handle press inquiries, administrative directors, my department, and representatives from clinical departments." (P6); "We work on two tracks simultaneously: a technical track focused on containing damage, investigating the cause, and restoring systems; and a communications track focused on keeping the press, users, and patients informed." (P6); "We also prepare for scenarios where attacks might disable power, mobile phones, or telecommunications by practicing old-fashioned communication methods." (P14); "Backup and cloud technologies have proven their effectiveness – Ukraine transferred critical data to secure clouds, which allowed quick recovery of systems after attacks."; "limiting and localizing a resource that has been attacked to prevent spread by attackers"; "Backup and cloud technologies have proven their effectiveness – Ukraine transferred critical data to secure clouds, which allowed quick recovery of systems after attacks."

Continued on next page

Table 14 – *Continued from previous page*

Cluster	**Quotes from Participants**
Governance and Strategic Planning	"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?'" (P3); "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." (P3); "For years, security was neglected. There was no dedicated security department whatsoever." (P6); "Previously, departments would purchase and install whatever they wanted without consulting IT." (P6); "Before, responsibility was fragmented into different ministries, and now they're trying to consolidate it into a single ministry." (P7); "Four years ago, we finally established a proper security department, starting with me and my colleague. Today, we've grown to 26 people." (P6); "If each medical institution follows Ukraine's cybersecurity strategy, then in general, one can achieve the best level of cybersecurity and minimize 75% of cyberattacks."; "Centralization of cybersecurity, use of technology for data preservation, rapid response to attacks"; "Proactive monitoring and response to threats to quickly detect and neutralize attacks"; "If each medical institution follows Ukraine's cybersecurity strategy, then in general, one can achieve the best level of cybersecurity and minimize 75% of cyberattacks."
Regulatory and Compliance Matters	"All our information is governed by GDPR. Everything you do needs to consider what happens with the data and how it's used." (P4); "The biggest problem, though, is that many of the methods claiming to protect privacy don't actually work... What people think is secure is often not secure at all." (P4); "Regulatory frameworks like GDPR have a positive impact from a security perspective. But there's a price to pay - everything you do has to go through extra checks and processes." (P9); "Legal limitations and complexities in international law regarding cybercrimes"

Continued on next page

Table 14 – *Continued from previous page*

Cluster	**Quotes from Participants**
International Collaboration	"In Denmark, we have the Center for Cybersecurity that works with all regions across Denmark. Their job is to coordinate information about attacks, intrusions, or any potential dangers to the regions." (P14); "We also participate in a threat-sharing platform with different regions in Denmark. If one region experiences a threat, they submit their findings to this platform so everyone is aware." (P1); "We collaborate extensively with other regions, the European Union, the Danish Ministry of Defense, and various entities to ensure we maintain multiple perspectives on cybersecurity." (P5); "We could form consortiums with other Nordic countries like Sweden and Norway to develop common solutions for these challenges." (P13); "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." (P3); "If there's international exchange of intelligence about attacks, this information is instantly distributed to all other countries, and threat hunting begins." (P15); "Cooperation with international partners helps Ukraine receive material and technical assistance, free staff training, and exchange of indicators and information about cyber threats"; "Ukraine's cybersecurity cooperation with Western countries has strengthened its hybrid defense, increased resilience to cyberattacks, and contributed to rapprochement with the EU and NATO"; "Ukraine actively cooperates with international partners, receiving data on new cyberattacks in real time"; "Ukraine accepts citizens in medical institutions from other countries, and this is the security not only of Ukraine but also of international partners in general"; "If there's international exchange of intelligence about attacks, this information is instantly distributed to all other countries, and threat hunting begins"; "Today, government agencies, organizations, and institutions can be aware of certain cyber threats that have already occurred in the national resilience system and predict (prevent) similar cases in their own infrastructures"
Foreign Technology Considerations	"Denmark is essentially a Microsoft country. All data is stored on American-owned servers." (P3); "We're relying too much on tools from other countries, which makes us vulnerable. We need to become more independent in our cybersecurity infrastructure." (P13); "We had a massive problem with Chinese cameras because they might have backdoors. Most government functions in Denmark are not allowing official Chinese cameras." (P6); "We've also banned some AI applications from China." (P10); "When there are only one or two suppliers worldwide, our leverage is limited." (P6); "We do block Chinese AI tools and other less trusted systems." (P14); "I think we need a good way to block new Chinese AI systems like Deepsea Eagle, DeepMind, and a few others because the second someone starts putting data into them, it all goes to the Chinese." (P6)
Geopolitical Security Dimensions	"The current shift with the US working more closely with Russia raises questions about the dangers of sharing data with American companies." (P7); "We're closely monitoring statements from the US and what Trump is saying, especially regarding Greenland, where he hasn't excluded the use of military power." (P1); "As international cooperation becomes more destabilized, countries like Russia have greater incentives to target nations like Denmark." (P5); "If an attack were conducted by a state actor like the Russian government, it would be considered cyber warfare -essentially a declaration of war." (P5); "When I joined 'University A' in 2009, we were 'best friends' with China and had many exchange programs. Now, this is completely forbidden." (P9); "Currently, you cannot work with Russians or Chinese, full stop." (P9)

Continued on next page

Table 14 – *Continued from previous page*

Cluster	Quotes from Participants
State-Sponsored Threat Actors	"In terms of activity, China would be the most active, followed by Russia, North Korea, and Iran." (P15); "For China, it's about intellectual property - they want to copy whatever they can get their hands on." (P6); "Someone, most likely Chinese, targeted a specific sub-program for Linux that was maintained by just one developer on GitHub. The attackers created 3-4 accounts that all contributed useful software on GitHub to build their credibility. They spent over three years infiltrating this developer's trust, with their accounts saying things like, 'Why don't you update more often?' and 'I have some free time, I can help.'" (P6); "We can see examples with Ukraine and Russia - whenever a political figure says something that upsets Russia, there can be consequences." (P14); "North Korea, due to all the embargoes against them, basically only gets outside money from cyber warfare, and they have many skilled people doing it." (P6); "The main threats come from rogue states that don't hide their efforts and those who make money from it, like North Korea with the Lazarus Group." (P15); "Right now, I think Russia poses the main threat." (P12); "Obviously, the number of cyberattacks has increased because it became a priority for Russia. But Russia has been actively attacking us for years." (P15); "Russia excel at social engineering and developing viruses." (P15)
Information Operations	"Russia is a big worry right now due to the Ukrainian-Russian war... Right now, if Russia can change public opinion, that's perfect for them." (P6); "About a month ago, a Russian propaganda agency had almost all their internal documentation leaked. Russia has been involved in propaganda and election manipulation for years, but has denied it." (P6); "We've blocked a lot of the world - Ukraine, Russia, China, India, and around 17 or 18 other countries. We open access if people need it for specific sites." (P6); "influence elections, manipulate public opinion, and conduct economic warfare."; "Imagine a hospital gets hacked and equipment stops working entirely... the moral effect would be much greater because it strongly affects society." (P15)
Emerging Technology Threats	"I anticipate that working with and countering artificial intelligence will dominate our focus in the coming years." (P5); "Quantum computers, if we are able to construct one that is large and stable enough, would be able to run algorithms that solve some of the computationally hard problems that underpin our most widely used cryptographic algorithms." (P2); "The biggest challenge is not actually designing them - they already exist. The key challenge is transitioning to those algorithms, standardizing them, and deploying them." (P2); "Currently, technology exists that combines real-time deepfakes with AI like ChatGPT, which can speak Danish." (P6); "Nothing is perfect. With good generative models, you can model anything, including heat signatures and other factors. If you can do that, you can potentially fool any system." (P4)
Biometric Security Considerations	"Most authentication systems use additional parameters like detecting heat around the face. A screen generating a pattern won't generate the right heat signature." (P4); "Systems also check if eye movements appear natural." (P4); "You can spoof iris recognition patterns - that's been demonstrated." (P4); "The eye is controlled by muscles and is essentially the only visible part of the brain -it's directly connected to your brain. Emotions are also reflected in eye movements, so you have some certainty about who the individual is." (P4); "If you combine fingerprints, eye tracking, facial recognition, hair growth patterns, and other biometrics—yes, certainly." (P4)

15 Research Question and Cluster connection

Table 15: RQ1 and RQ2 Sections and Their Matching Clusters

Section	**Matches Cluster(s)**
5.1 RQ1: How does digitization aid in hybrid warfare campaigns, and how does this challenge Denmark's cybersecurity governance frameworks?	
Digitization in Denmark	Digital Infrastructure Challenges / Governance and Strategic Planning
Strategic Targeting of Danish Infrastructure	Critical Infrastructure Protection / Advanced Attack Strategies
Multi-Vector Attacks	Advanced Attack Strategies / State-Sponsored Threat Actors
The Human Factor in Hybrid Defense	Social Engineering and Human Vulnerabilities / Workforce and Expertise Challenges
Incident Response and National Resilience	Incident Response and Recovery / Governance and Strategic Planning
Governance Fragmentation in Danish Infrastructure	Governance and Strategic Planning / Regulatory and Compliance Matters
5.2 RQ2: How do geopolitical tensions influence evolution of cyberwarfare against Denmark?	
Foreign Technology Dependencies	Foreign Technology Considerations
Asia's Advanced Persistent Threats	State-Sponsored Threat Actors / Geopolitical Security Dimensions
International Cooperation and Threat Intelligence	International Collaboration / Information Operations
Russia's Hybrid Warfare in Ukraine	State-Sponsored Threat Actors / Advanced Attack Strategies / Information Operations
Evolution of Threat Landscape	Emerging Technology Threats / Geopolitical Security Dimensions / Information Operations