Qualitative Data Analysis for Validation

1 Participant Codes

Table 1: Table of interview participants for Validation

ID	Industrial Classification	Participant Role
PV1	Public Sector/Academia	Senior Software Developer
PV2	Private Sector	Expert in Modern and Future Warfare
PV3	Private Sector	Information Security Consultant

2 Interview Quotes

Research Question Subsection	Quote
PV3	"Being a trust-based society is actually positive, and being one of the most digitalized countries is good too. But when you combine these two factors in the context of cybercrime, it creates significant vulnerabilities."
PV3	"As you noted in your thesis, we are vulnerable as a country. Most people appreciate our high level of digitalization and our trustworthy, polite culture, but they don't connect these characteristics to cybersecurity implications - and that's the issue."
PV1	"After reading what I read, I feel that we are on thin ice. The feeling that we are on much thinner ice than I realized. We have a lot of complexity built into our society that is very vulnerable."
PV1	"Could it be that the amount of measures you have to take grows much faster than proportional? Every addition to our already complex system might exacerbate the security problem much more."
PV2	"Information technology is changing warfare on many levels. It's the technology driving drones, enabling battlefield management systems like Delta in Ukraine, and allowing ordinary citizens to contribute to warfighting efforts."

Research Question Subsection	Quote
PV2	"Smartphones function as multipurpose tools in modern warfare—they're computers for running military applications, cameras for intelligence gathering, communication devices, and news sources."
PV3	"Denmark is one of the wealthiest countries in the world despite having limited natural resources. This prosperity is largely due to high efficiency achieved through digitalization."
PV3	"What might require multiple forms, stamps, and visits to offices in France can be done with five clicks on a mobile phone in Denmark. That's one of the reasons Denmark is so wealthy - because of the high level of technology adoption."
PV3	"We are considered critical infrastructure because we're involved with trains."
PV3	"Our ownership structure is 50% state-owned, 25% owned by Copenhagen Municipality, and 25% by Frederiksberg Municipality. These owners are part of critical infrastructure."
PV2	"The obvious targets include electricity and telecommunications. However, attackers often focus on wherever they find vulnerabilities. If that's the water supply, that's what they'll target. I think target selection is largely vulnerability-driven."
PV2	"When discussing hybrid warfare beyond just cyber aspects, it's important to note that the number of vulnerabilities is so high that it's impossible to defend against everything."
PV1	"What I was often thinking about was the centralization of IT competencies at the university. You get more and more a single point of attack, in my view."
PV1	"If everybody had their own security system, it would be harder for an enemy to have a widespread attack. But all those small systems are not well developed and must have lots of errors, so they are weak."
PV1	"Somehow you have to find a balance, and I'm not sure what the right balance is."
PV3	"The level of threats and attacks has increased approximately 300% since the Ukraine war began. That's a direct quote from global cybersecurity sources."
PV3	"It's not a question of if you're going to be going to be attacked, it's about when."

Research Question Subsection	**Quote**
PV2	"It's often discussed that in modern warfare, the first wave of attack will be in cyberspace. It makes sense as an easy way to create chaos before exploiting that opportunity with physical forces."
PV2	"They attacked Ukraine's digital systems first and then physically invaded a few hours later."
PV1	"I think it was unwise for postal services to stop bringing letters around because you need something to fall back on. If our digital systems fail, we need letters again. We need this parallel system."
PV1	"The breakdown of lower technology things is concerning. Earlier there was talk about abolishing FM radio, and even earlier we had medium wave... You could always fall back on long wave and medium wave, but now it's impossible because those systems don't exist anymore."
PV3	"My perspective on awareness is that employees are both the greatest strength and the greatest weakness of any organization - the difference between those two states comes down to awareness."
PV3	"Approximately 40% of employees don't lock their computer screens when leaving their workstations - it's equivalent to leaving your home with the front door wide open."
PV3	"Unfortunately, the general level of awareness is low, which is why we're working on it."
PV2	"In the early days of the Ukraine conflict, civilians could take pictures of Russian tanks and send them through telegram bots. This technology involves all of society in warfare, raising questions about who's a combatant versus a civilian."
PV2	"Ukraine seemed quite prepared for this approach, so I don't think it had the effect Russia hoped for. This is likely due to Ukraine's eight years of prior conflict with Russia, during which they experienced severe cyber attacks."
PV1	"There is an interesting point about our trust-based society. The trust doesn't go so far that we get informed by everybody because they trust us."

Research Question Subsection	Quote
PV1	"We do not get information from our IT department about the threats they have seen, which I think would be very interesting for us lower in the pyramid to know."
PV1	"We are clearly in a kind of COVID-like period where people tend to support the government more than they did just a few months ago. We more or less agree about what the government is doing. We trust the government."
PV3	"We have an incident response plan that outlines who does what and when if an incident occurs. The existing plan wasn't very good, so I've rewritten it."
PV3	"We're planning to conduct a tabletop exercise where we'll run through different scenarios to test the plan and then refine it based on what we learn."
PV3	"Just this morning, we had a meeting about creating a 'war room' for handling incidents. This includes having standalone computers, backup batteries, and specific software ready for emergency situations."
PV2	"Resilience becomes crucial—the ability to quickly restore systems after an attack or have redundant alternatives in place. For example, if the electricity grid is compromised, having alternative power sources is essential."
PV2	"If Russia wanted to launch a major attack at a specific point, it might be advantageous for them to temporarily disable Ukraine's Delta system for 30 minutes. While Ukraine would likely restore the system quickly, that window might be sufficient for Russia to achieve tactical objectives."
PV1	"What I was thinking about is parallel systems or backup systems. To keep things online, you could have parallel systems doing exactly the same thing but developed by completely different unrelated groups."
PV1	"That's very expensive - everything is twice as expensive - but it could tremendously improve security. In spacecraft, it's normal to have redundant systems."
PV1	"I think I could continue working without internet because I have lots of materials on my computer itself. If the university's system breaks down, I still have source code on GitHub."

Research Question Subsection	Quote
PV3	"Looking at security standards, at the top of the pyramid you have policies - the 'why' of cybersecurity. The next level is ISO 27001, which addresses who's going to implement security measures. Then there's AT-18 compliance, which details how to implement security at a concrete, technical level."
PV3	"Nobody in this company was knowledgeable about these frameworks, so we're bringing in external experts to assess our current level and develop a roadmap for improvement. This will take 1-2 years."
PV2	"Kilcullen's model for 'liminal warfare' is useful here, describing different thresholds in hybrid space: 1. Detection threshold - Recognizing that something is happening; 2. Attribution threshold - Gathering enough information to identify who is responsible; 3. Response threshold - Having sufficient information for politicians to make decisions."
PV2	"We need both technical solutions and organizational readiness, with regular exercises to practice these responses."
PV1	"We have nice websites that pose everyday practical questions... Websites like that could also address security problems, but you don't see it anywhere. Perhaps they exist, but they're not advertised as places you go to for security information."
PV1	"That would be very nice, yes." [Regarding bug bounty programs]
PV3	"As you noted in your thesis, approximately 90% of global data is stored in the US, which is problematic."
PV3	"We're talking about Amazon with all their data centers, and Microsoft Office, which is used by over 90% of both private and public offices. If these systems were somehow blocked or compromised by US actions, it would create major problems for our email systems, productivity software, and more."
PV3	"There's a growing level of concern about how to proceed, as US-based software companies aren't perceived as reliable as they once were."

Research Question Subsection	Quote
PV2	"In Danish society, my greater concern is the dependency on American technology. These discussions about digital sovereignty are important, as we saw with the recent Microsoft outage that affected systems nationwide. When an entire country essentially runs on Windows, that creates significant vulnerabilities."
PV2	"We'll likely see a new European security structure emerge where Europeans take responsibility without depending on the United States. This should include greater focus on digital sovereignty and bringing technology under European control."
PV1	"We've been thinking about moving away from software packages from Microsoft, for example. I think that's something we have to do at the university, where we are Microsoft and Oracle dependent, along with other foreign providers."
PV1	"The political situation has changed my perspective. Before, I trusted Google, Dropbox, and a few other American companies. I know they make good products."
PV1	"But now I'm thinking perhaps we should use a European cloud system like NextCloud instead of Microsoft OneDrive... because of the political situation."
PV1	"That's hard. There are countries that use European office-based solutions. I use LibreOffice, and it has a long history already, but it's still not stable. I've had crashes with it lots of times, so there are hiccups in the software."
PV2	"North Korea is actively fighting in Ukraine now, so they're clearly a concerning actor. Much depends on how relations develop with the United States. If American support wanes, European countries might look elsewhere for security arrangements, potentially opening up new discussions with China."
PV2	"For Europe, I don't see China as the primary threat—it's quite clearly Russia. How we respond will depend on how the situation develops."
PV1	"I think Russia is the worst threat, not the US and not China. China is interested in theft of information and technology, which is criminal."

Research Question Subsection	**Quote**
PV1	"Russia is trying to influence elections secretly, while America does it more openly. I think Russia is the biggest threat."
PV3	"Russia, no doubt, and China [are the greatest dangers]."
PV3	"It's similar to what's happening on the military front - Denmark is now sending military personnel to Ukraine to learn about drone technology, where Ukraine has developed world-leading capabilities through necessity."
PV3	"The rest of Europe and the world can learn from what Ukraine has built. When I read your thesis, I saw the parallel with Danish soldiers going to Ukraine to learn about drone technology - it follows the same pattern of knowledge transfer."
PV2	"Hopefully we'll see a new European security structure emerge where Europeans take responsibility without depending on the United States... Europe isn't fully ready for this transition yet, but I hope we'll develop this new security structure, which should include Ukraine."
PV2	"If American support wanes, European countries might look elsewhere for security arrangements."
PV1	"I think Denmark must keep this tradition of trust, but must also be more wary about becoming independent of other countries. Even Ukraine could turn on us."
PV1	"We like what Ukraine can do, but we should not become too dependent on them. The political situation in Ukraine is not stable. There's still a lot of corruption as far as I know."
PV1	"As a small country, we have to be dependent on other countries; we have to cooperate, perhaps with countries of about the same size as Denmark, because they probably face similar situations."
PV2	"One of the interesting challenges is the problem of attribution in cyberspace. It's not always clear who is behind an attack, even when it appears to come from Russia. Is it state-sponsored or a criminal group? There's a blurring of lines with private actor involvement in warfare, which is very clear in cyber warfare."

Research Question Subsection	**Quote**
PV2	"I suspect some attacks on Denmark already come from Russia, but authorities may not publicize this. When transportation systems experience 'malfunctions,' there's a likelihood that some are actually cyber incidents."
PV2	"Ukraine has managed these threats quite well, showing that proper preparation can mitigate cyber threats. It's been interesting to see Ukraine also engage in offensive activities, with private actors and groups being encouraged to participate. We've witnessed quite a battle playing out in the cyber domain."
PV3	"The general consensus across these forums is that a large part of the attacks can be traced back to Russia. There's no doubt about that."
PV3	"I found your angle on Ukraine particularly interesting - how Ukraine has been targeted most heavily by Russian cyberattacks, and the lessons that can be learned from their experience and applied to the rest of Europe."
PV1	"Yes, we know that Ukraine has made a tiger jump in knowledge about hybrid warfare and that we have to learn from Ukraine. You pointed that out clearly."
PV2	"The war in Ukraine has revolutionized and permanently changed Europe's security landscape. The previous security order no longer exists. NATO is in its deepest crisis in 75 years, with some arguing that the alliance is becoming worthless."
PV2	"It's a very dangerous time overall. The risk that current tensions could develop into a wider war involving Denmark is higher than it has been for many years."
PV2	"The next decade is particularly dangerous, especially while Putin remains in power. How the Ukraine conflict ends could either embolden or restrain Russia's future actions toward NATO."
PV2	"Hybrid attacks happen continuously, not as discrete events."
PV3	"The technology is constantly evolving, laws are changing all the time, and hacker techniques are continuously advancing."
PV3	"Our job in cybersecurity is trying to stay just a little ahead of the hackers. We don't always succeed, but that's what we strive for."

Research Question Subsection	Quote
PV3	"It's always a trade-off between efficiency and security. That balance is constantly being evaluated."
PV3	"The political developments in the US have served as a wake-up call for many who weren't previously concerned about these dependencies."
PV3	"The political situation in the US has definitely raised awareness about how dependent we are on American companies."

3 Interview Labeling

Participant	Quote	Thematic Code
PV3	"Being a trust-based society is actually positive, and being one of the most digitalized countries is good too. But when you combine these two factors in the context of cybercrime, it creates significant vulnerabilities."	Digital Vulnerability
PV3	"As you noted in your thesis, we are vulnerable as a country. Most people appreciate our high level of digitalization and our trustworthy, polite culture, but they don't connect these characteristics to cybersecurity implications - and that's the issue."	Security Awareness Gap
PV1	"After reading what I read, I feel that we are on thin ice. The feeling that we are on much thinner ice than I realized. We have a lot of complexity built into our society that is very vulnerable."	Systemic Fragility
PV1	"Could it be that the amount of measures you have to take grows much faster than proportional? Every addition to our already complex system might exacerbate the security problem much more."	Security Complexity
PV2	"Information technology is changing warfare on many levels. It's the technology driving drones, enabling battlefield management systems like Delta in Ukraine, and allowing ordinary citizens to contribute to warfighting efforts."	Evolving Warfare
PV2	"Smartphones function as multipurpose tools in modern warfare—they're computers for running military applications, cameras for intelligence gathering, communication devices, and news sources."	Technology in Warfare
PV3	"Denmark is one of the wealthiest countries in the world despite having limited natural resources. This prosperity is largely due to high efficiency achieved through digitalization."	Digital Economy
PV3	"What might require multiple forms, stamps, and visits to offices in France can be done with five clicks on a mobile phone in Denmark. That's one of the reasons Denmark is so wealthy - because of the high level of technology adoption."	Digital Efficiency
PV3	"We are considered critical infrastructure because we're involved with trains."	Critical Infrastructure
PV3	"Our ownership structure is 50% state-owned, 25% owned by Copenhagen Municipality, and 25% by Frederiksberg Municipality. These owners are part of critical infrastructure."	Infrastructure Governance
PV2	"The obvious targets include electricity and telecommunications. However, attackers often focus on wherever they find vulnerabilities. If that's the water supply, that's what they'll target. I think target selection is largely vulnerability-driven."	Target Selection
PV2	"When discussing hybrid warfare beyond just cyber aspects, it's important to note that the number of vulnerabilities is so high that it's impossible to defend against everything."	Defense Limitations
PV1	"What I was often thinking about was the centralization of IT competencies at the university. You get more and more a single point of attack, in my view."	Centralization Risk

Participant	Quote	Thematic Code
PV1	"If everybody had their own security system, it would be harder for an enemy to have a widespread attack. But all those small systems are not well developed and must have lots of errors, so they are weak."	Centralization Dilemma
PV1	"Somehow you have to find a balance, and I'm not sure what the right balance is."	Security Trade-offs
PV3	"The level of threats and attacks has increased approximately 300% since the Ukraine war began. That's a direct quote from global cybersecurity sources."	Threat Escalation
PV3	"It's not a question of if you're going to be going to be attacked, it's about when."	Attack Inevitability
PV2	"It's often discussed that in modern warfare, the first wave of attack will be in cyberspace. It makes sense as an easy way to create chaos before exploiting that opportunity with physical forces."	Cyber-First Strategy
PV2	"They attacked Ukraine's digital systems first and then physically invaded a few hours later."	Hybrid Warfare Sequence
PV1	"I think it was unwise for postal services to stop bringing letters around because you need something to fall back on. If our digital systems fail, we need letters again. We need this parallel system."	System Redundancy
PV1	"The breakdown of lower technology things is concerning. Earlier there was talk about abolishing FM radio, and even earlier we had medium wave... You could always fall back on long wave and medium wave, but now it's impossible because those systems don't exist anymore."	Legacy System Loss
PV3	"My perspective on awareness is that employees are both the greatest strength and the greatest weakness of any organization - the difference between those two states comes down to awareness."	Human Factor
PV3	"Approximately 40% of employees don't lock their computer screens when leaving their workstations - it's equivalent to leaving your home with the front door wide open."	Security Behavior
PV3	"Unfortunately, the general level of awareness is low, which is why we're working on it."	Awareness Deficit
PV2	"In the early days of the Ukraine conflict, civilians could take pictures of Russian tanks and send them through telegram bots. This technology involves all of society in warfare, raising questions about who's a combatant versus a civilian."	Civilian Involvement
PV2	"Ukraine seemed quite prepared for this approach, so I don't think it had the effect Russia hoped for. This is likely due to Ukraine's eight years of prior conflict with Russia, during which they experienced severe cyber attacks."	Preparedness Effect
PV1	"There is an interesting point about our trust-based society. The trust doesn't go so far that we get informed by everybody because they trust us."	Trust Limitations
PV1	"We do not get information from our IT department about the threats they have seen, which I think would be very interesting for us lower in the pyramid to know."	Information Silos
PV1	"We are clearly in a kind of COVID-like period where people tend to support the government more than they did just a few months ago. We more or less agree about what the government is doing. We trust the government."	Crisis Trust
PV3	"We have an incident response plan that outlines who does what and when if an incident occurs. The existing plan wasn't very good, so I've rewritten it."	Incident Planning
PV3	"We're planning to conduct a tabletop exercise where we'll run through different scenarios to test the plan and then refine it based on what we learn."	Scenario Testing
PV3	"Just this morning, we had a meeting about creating a 'war room' for handling incidents. This includes having standalone computers, backup batteries, and specific software ready for emergency situations."	Emergency Preparation
PV2	"Resilience becomes crucial—the ability to quickly restore systems after an attack or have redundant alternatives in place. For example, if the electricity grid is compromised, having alternative power sources is essential."	System Resilience
PV2	"If Russia wanted to launch a major attack at a specific point, it might be advantageous for them to temporarily disable Ukraine's Delta system for 30 minutes. While Ukraine would likely restore the system quickly, that window might be sufficient for Russia to achieve tactical objectives."	Tactical Vulnerability

Participant	Quote	Thematic Code
PV1	"What I was thinking about is parallel systems or backup systems. To keep things online, you could have parallel systems doing exactly the same thing but developed by completely different unrelated groups."	System Redundancy
PV1	"That's very expensive - everything is twice as expensive - but it could tremendously improve security. In spacecraft, it's normal to have redundant systems."	Cost of Security
PV1	"I think I could continue working without internet because I have lots of materials on my computer itself. If the university's system breaks down, I still have source code on GitHub."	Personal Resilience
PV3	"Looking at security standards, at the top of the pyramid you have policies - the 'why' of cybersecurity. The next level is ISO 27001, which addresses who's going to implement security measures. Then there's AT-18 compliance, which details how to implement security at a concrete, technical level."	Security Framework
PV3	"Nobody in this company was knowledgeable about these frameworks, so we're bringing in external experts to assess our current level and develop a roadmap for improvement. This will take 1-2 years."	Expertise Gap
PV2	"Kilcullen's model for 'liminal warfare' is useful here, describing different thresholds in hybrid space: 1. Detection threshold - Recognizing that something is happening; 2. Attribution threshold - Gathering enough information to identify who is responsible; 3. Response threshold - Having sufficient information for politicians to make decisions."	Response Framework
PV2	"We need both technical solutions and organizational readiness, with regular exercises to practice these responses."	Holistic Preparedness
PV1	"We have nice websites that pose everyday practical questions... Websites like that could also address security problems, but you don't see it anywhere. Perhaps they exist, but they're not advertised as places you go to for security information."	Information Access
PV1	"That would be very nice, yes." [Regarding bug bounty programs]	Security Innovation
PV3	"As you noted in your thesis, approximately 90% of global data is stored in the US, which is problematic."	Data Sovereignty
PV3	"We're talking about Amazon with all their data centers, and Microsoft Office, which is used by over 90% of both private and public offices. If these systems were somehow blocked or compromised by US actions, it would create major problems for our email systems, productivity software, and more."	Foreign Dependency
PV3	"There's a growing level of concern about how to proceed, as US-based software companies aren't perceived as reliable as they once were."	Trust Erosion
PV2	"In Danish society, my greater concern is the dependency on American technology. These discussions about digital sovereignty are important, as we saw with the recent Microsoft outage that affected systems nationwide. When an entire country essentially runs on Windows, that creates significant vulnerabilities."	Technological Dependency
PV2	"We'll likely see a new European security structure emerge where Europeans take responsibility without depending on the United States. This should include greater focus on digital sovereignty and bringing technology under European control."	European Autonomy
PV1	"We've been thinking about moving away from software packages from Microsoft, for example. I think that's something we have to do at the university, where we are Microsoft and Oracle dependent, along with other foreign providers."	Technology Transition
PV1	"The political situation has changed my perspective. Before, I trusted Google, Dropbox, and a few other American companies. I know they make good products."	Shifting Trust
PV1	"But now I'm thinking perhaps we should use a European cloud system like NextCloud instead of Microsoft OneDrive... because of the political situation."	Digital Sovereignty
PV1	"That's hard. There are countries that use European office-based solutions. I use LibreOffice, and it has a long history already, but it's still not stable. I've had crashes with it lots of times, so there are hiccups in the software."	Transition Challenges

Participant	Quote	Thematic Code
PV2	"North Korea is actively fighting in Ukraine now, so they're clearly a concerning actor. Much depends on how relations develop with the United States. If American support wanes, European countries might look elsewhere for security arrangements, potentially opening up new discussions with China."	Threat Actors
PV2	"For Europe, I don't see China as the primary threat—it's quite clearly Russia. How we respond will depend on how the situation develops."	Threat Prioritization
PV1	"I think Russia is the worst threat, not the US and not China. China is interested in theft of information and technology, which is criminal."	Threat Assessment
PV1	"Russia is trying to influence elections secretly, while America does it more openly. I think Russia is the biggest threat."	Russian Threat
PV3	"Russia, no doubt, and China [are the greatest dangers]."	Primary Threats
PV3	"It's similar to what's happening on the military front - Denmark is now sending military personnel to Ukraine to learn about drone technology, where Ukraine has developed world-leading capabilities through necessity."	Knowledge Transfer
PV3	"The rest of Europe and the world can learn from what Ukraine has built. When I read your thesis, I saw the parallel with Danish soldiers going to Ukraine to learn about drone technology - it follows the same pattern of knowledge transfer."	Ukrainian Expertise
PV2	"Hopefully we'll see a new European security structure emerge where Europeans take responsibility without depending on the United States... Europe isn't fully ready for this transition yet, but I hope we'll develop this new security structure, which should include Ukraine."	European Security
PV2	"If American support wanes, European countries might look elsewhere for security arrangements."	Security Realignment
PV1	"I think Denmark must keep this tradition of trust, but must also be more wary about becoming independent of other countries. Even Ukraine could turn on us."	Cautious Cooperation
PV1	"We like what Ukraine can do, but we should not become too dependent on them. The political situation in Ukraine is not stable. There's still a lot of corruption as far as I know."	Dependency Concerns
PV1	"As a small country, we have to be dependent on other countries; we have to cooperate, perhaps with countries of about the same size as Denmark, because they probably face similar situations."	Small Nation Strategy
PV2	"One of the interesting challenges is the problem of attribution in cyberspace. It's not always clear who is behind an attack, even when it appears to come from Russia. Is it state-sponsored or a criminal group? There's a blurring of lines with private actor involvement in warfare, which is very clear in cyber warfare."	Attribution Challenge
PV2	"I suspect some attacks on Denmark already come from Russia, but authorities may not publicize this. When transportation systems experience 'malfunctions,' there's a likelihood that some are actually cyber incidents."	Undisclosed Attacks
PV2	"Ukraine has managed these threats quite well, showing that proper preparation can mitigate cyber threats. It's been interesting to see Ukraine also engage in offensive activities, with private actors and groups being encouraged to participate. We've witnessed quite a battle playing out in the cyber domain."	Cyber Countermeasures
PV3	"The general consensus across these forums is that a large part of the attacks can be traced back to Russia. There's no doubt about that."	Russian Attribution
PV3	"I found your angle on Ukraine particularly interesting - how Ukraine has been targeted most heavily by Russian cyberattacks, and the lessons that can be learned from their experience and applied to the rest of Europe."	Knowledge Transfer
PV1	"Yes, we know that Ukraine has made a tiger jump in knowledge about hybrid warfare and that we have to learn from Ukraine. You pointed that out clearly."	Ukrainian Expertise
PV2	"The war in Ukraine has revolutionized and permanently changed Europe's security landscape. The previous security order no longer exists. NATO is in its deepest crisis in 75 years, with some arguing that the alliance is becoming worthless."	Security Paradigm Shift
PV2	"It's a very dangerous time overall. The risk that current tensions could develop into a wider war involving Denmark is higher than it has been for many years."	Heightened Risk

Participant	Quote	Thematic Code
PV2	"The next decade is particularly dangerous, especially while Putin remains in power. How the Ukraine conflict ends could either embolden or restrain Russia's future actions toward NATO."	Future Uncertainty
PV2	"Hybrid attacks happen continuously, not as discrete events."	Continuous Threat
PV3	"The technology is constantly evolving, laws are changing all the time, and hacker techniques are continuously advancing."	Dynamic Landscape
PV3	"Our job in cybersecurity is trying to stay just a little ahead of the hackers. We don't always succeed, but that's what we strive for."	Security Arms Race
PV3	"It's always a trade-off between efficiency and security. That balance is constantly being evaluated."	Security Trade-offs
PV3	"The political developments in the US have served as a wake-up call for many who weren't previously concerned about these dependencies."	Geopolitical Awareness
PV3	"The political situation in the US has definitely raised awareness about how dependent we are on American companies."	Dependency Recognition

4 Distinct Labels from Interview

Thematic Code	Participants
Digital Vulnerability	PV3
Security Awareness Gap	PV3
Systemic Fragility	PV1
Security Complexity	PV1
Evolving Warfare	PV2
Technology in Warfare	PV2
Digital Economy	PV3
Digital Efficiency	PV3
Critical Infrastructure	PV3
Infrastructure Governance	PV3
Target Selection	PV2
Defense Limitations	PV2
Centralization Risk	PV1
Centralization Dilemma	PV1
Security Trade-offs	PV1, PV3
Threat Escalation	PV3
Attack Inevitability	PV3
Cyber-First Strategy	PV2
Hybrid Warfare Sequence	PV2
System Redundancy	PV1
Legacy System Loss	PV1
Human Factor	PV3
Security Behavior	PV3
Awareness Deficit	PV3
Civilian Involvement	PV2
Preparedness Effect	PV2
Trust Limitations	PV1
Information Silos	PV1
Crisis Trust	PV1
Incident Planning	PV3
Scenario Testing	PV3
Emergency Preparation	PV3
System Resilience	PV2
Tactical Vulnerability	PV2

Thematic Code	Participants
System Redundancy	PV1
Cost of Security	PV1
Personal Resilience	PV1
Security Framework	PV3
Expertise Gap	PV3
Response Framework	PV2
Holistic Preparedness	PV2
Information Access	PV1
Security Innovation	PV1
Data Sovereignty	PV3
Foreign Dependency	PV3
Trust Erosion	PV3
Technological Dependency	PV2
European Autonomy	PV2
Technology Transition	PV1
Shifting Trust	PV1
Digital Sovereignty	PV1
Transition Challenges	PV1
Threat Actors	PV2
Threat Prioritization	PV2
Threat Assessment	PV1
Russian Threat	PV1
Primary Threats	PV3
Knowledge Transfer	PV3
Ukrainian Expertise	PV3, PV1
European Security	PV2
Security Realignment	PV2
Cautious Cooperation	PV1
Dependency Concerns	PV1
Small Nation Strategy	PV1
Attribution Challenge	PV2
Undisclosed Attacks	PV2
Cyber Countermeasures	PV2
Russian Attribution	PV3
Security Paradigm Shift	PV2
Heightened Risk	PV2
Future Uncertainty	PV2
Continuous Threat	PV2
Dynamic Landscape	PV3
Security Arms Race	PV3
Geopolitical Awareness	PV3
Dependency Recognition	PV3

5 Affinity Diagram Clustering

Code	Participants	Theme
Digital Vulnerability	PV3	Digital Security Challenges
Security Awareness Gap	PV3	Human Factor in Security
Systemic Fragility	PV1	System Vulnerabilities
Security Complexity	PV1	Digital Security Challenges
Evolving Warfare	PV2	Hybrid Warfare Dynamics
Technology in Warfare	PV2	Hybrid Warfare Dynamics

Code	Participants	Theme
Digital Economy	PV3	Critical Infrastructure
Digital Efficiency	PV3	Critical Infrastructure
Critical Infrastructure	PV3	Critical Infrastructure
Infrastructure Governance	PV3	Critical Infrastructure
Target Selection	PV2	Hybrid Warfare Tactics
Defense Limitations	PV2	Defensive Capabilities
Centralization Risk	PV1	System Vulnerabilities
Centralization Dilemma	PV1	System Vulnerabilities
Security Trade-offs	PV1, PV3	Security Implementation
Threat Escalation	PV3	Threat Evolution
Attack Inevitability	PV3	Threat Evolution
Cyber-First Strategy	PV2	Hybrid Warfare Tactics
Hybrid Warfare Sequence	PV2	Hybrid Warfare Dynamics
System Redundancy	PV1	Resilience Strategies
Legacy System Loss	PV1	System Vulnerabilities
Human Factor	PV3	Human Factor in Security
Security Behavior	PV3	Human Factor in Security
Awareness Deficit	PV3	Human Factor in Security
Civilian Involvement	PV2	Societal Resilience
Preparedness Effect	PV2	Societal Resilience
Trust Limitations	PV1	Trust and Information Sharing
Information Silos	PV1	Trust and Information Sharing
Crisis Trust	PV1	Trust and Information Sharing
Incident Planning	PV3	Preparedness and Response
Scenario Testing	PV3	Preparedness and Response
Emergency Preparation	PV3	Preparedness and Response
System Resilience	PV2	Resilience Strategies
Tactical Vulnerability	PV2	Defensive Capabilities
System Redundancy	PV1	Resilience Strategies
Cost of Security	PV1	Security Implementation
Personal Resilience	PV1	Societal Resilience
Security Framework	PV3	Security Implementation
Expertise Gap	PV3	Knowledge and Expertise
Response Framework	PV2	Preparedness and Response
Holistic Preparedness	PV2	Preparedness and Response
Information Access	PV1	Trust and Information Sharing
Security Innovation	PV1	Security Implementation
Data Sovereignty	PV3	Digital Sovereignty
Foreign Dependency	PV3	Digital Sovereignty
Trust Erosion	PV3	Trust and Information Sharing
Technological Dependency	PV2	Digital Sovereignty
European Autonomy	PV2	Digital Sovereignty
Technology Transition	PV1	Digital Sovereignty
Shifting Trust	PV1	Trust and Information Sharing
Digital Sovereignty	PV1	Digital Sovereignty
Transition Challenges	PV1	Digital Sovereignty
Threat Actors	PV2	Threat Landscape
Threat Prioritization	PV2	Threat Landscape
Threat Assessment	PV1	Threat Landscape
Russian Threat	PV1	Threat Landscape
Primary Threats	PV3	Threat Landscape
Knowledge Transfer	PV3	Knowledge and Expertise
Ukrainian Expertise	PV3, PV1	Knowledge and Expertise

Code	Participants	Theme
European Security	PV2	International Cooperation
Security Realignment	PV2	International Cooperation
Cautious Cooperation	PV1	International Cooperation
Dependency Concerns	PV1	International Cooperation
Small Nation Strategy	PV1	International Cooperation
Attribution Challenge	PV2	Attribution and Response
Undisclosed Attacks	PV2	Attribution and Response
Cyber Countermeasures	PV2	Attribution and Response
Russian Attribution	PV3	Attribution and Response
Security Paradigm Shift	PV2	Future Security Landscape
Heightened Risk	PV2	Future Security Landscape
Future Uncertainty	PV2	Future Security Landscape
Continuous Threat	PV2	Future Security Landscape
Dynamic Landscape	PV3	Future Security Landscape
Security Arms Race	PV3	Future Security Landscape
Geopolitical Awareness	PV3	International Cooperation
Dependency Recognition	PV3	Digital Sovereignty

6 All Clusters

Themes
Digital Security Challenges
Human Factor in Security
System Vulnerabilities
Hybrid Warfare Dynamics
Critical Infrastructure
Hybrid Warfare Tactics
Defensive Capabilities
Security Implementation
Threat Evolution
Resilience Strategies
Societal Resilience
Trust and Information Sharing
Preparedness and Response
Knowledge and Expertise
Digital Sovereignty
Threat Landscape
International Cooperation
Attribution and Response
Future Security Landscape

Table 6: Identified Themes from Qualitative Analysis

7 Validation Clusters correlated with Main Clusters

Code	Participant	Theme	Main Theme
Digital Vulnerability	PV3	Digital Security Challenges	Digitization in Denmark
Security Awareness Gap	PV3	Human Factor in Security	Digitization in Denmark
Systemic Fragility	PV1	System Vulnerabilities	Digitization in Denmark
Security Complexity	PV1	Digital Security Challenges	Digitization in Denmark

Code	Participant	Theme	Main Theme
Evolving Warfare	PV2	Hybrid Warfare Dynamics	Digitization in Denmark
Technology in Warfare	PV2	Hybrid Warfare Dynamics	Digitization in Denmark
Digital Economy	PV3	Critical Infrastructure	Digitization in Denmark
Digital Efficiency	PV3	Critical Infrastructure	Digitization in Denmark
Critical Infrastructure	PV3	Critical Infrastructure	Strategic Targeting of Danish Infrastructure
Infrastructure Governance	PV3	Critical Infrastructure	Strategic Targeting of Danish Infrastructure
Target Selection	PV2	Hybrid Warfare Tactics	Strategic Targeting of Danish Infrastructure
Defense Limitations	PV2	Defensive Capabilities	Strategic Targeting of Danish Infrastructure
Centralization Risk	PV1	System Vulnerabilities	Strategic Targeting of Danish Infrastructure
Centralization Dilemma	PV1	System Vulnerabilities	Strategic Targeting of Danish Infrastructure
Security Trade-offs	PV1, PV3	Security Implementation	Strategic Targeting of Danish Infrastructure
Threat Escalation	PV3	Threat Evolution	Multi-Vector Attacks
Attack Inevitability	PV3	Threat Evolution	Multi-Vector Attacks
Cyber-First Strategy	PV2	Hybrid Warfare Tactics	Multi-Vector Attacks
Hybrid Warfare Sequence	PV2	Hybrid Warfare Dynamics	Multi-Vector Attacks
System Redundancy	PV1	Resilience Strategies	Multi-Vector Attacks
Legacy System Loss	PV1	System Vulnerabilities	Multi-Vector Attacks
Human Factor	PV3	Human Factor in Security	The Human Factor in Hybrid Defense
Security Behavior	PV3	Human Factor in Security	The Human Factor in Hybrid Defense
Awareness Deficit	PV3	Human Factor in Security	The Human Factor in Hybrid Defense
Civilian Involvement	PV2	Societal Resilience	The Human Factor in Hybrid Defense
Preparedness Effect	PV2	Societal Resilience	The Human Factor in Hybrid Defense
Trust Limitations	PV1	Trust and Information Sharing	The Human Factor in Hybrid Defense
Information Silos	PV1	Trust and Information Sharing	The Human Factor in Hybrid Defense
Crisis Trust	PV1	Trust and Information Sharing	The Human Factor in Hybrid Defense
Incident Planning	PV3	Preparedness and Response	Incident Response and National Resilience
Scenario Testing	PV3	Preparedness and Response	Incident Response and National Resilience
Emergency Preparation	PV3	Preparedness and Response	Incident Response and National Resilience
System Resilience	PV2	Resilience Strategies	Incident Response and National Resilience
Tactical Vulnerability	PV2	Defensive Capabilities	Incident Response and National Resilience
System Redundancy	PV1	Resilience Strategies	Incident Response and National Resilience
Cost of Security	PV1	Security Implementation	Incident Response and National Resilience
Personal Resilience	PV1	Societal Resilience	Incident Response and National Resilience
Security Framework	PV3	Security Implementation	Governance Fragmentation in Danish Infrastructure

Code	Participant	Theme	Main Theme
Expertise Gap	PV3	Knowledge and Expertise	Governance Fragmentation in Danish Infrastructure
Response Framework	PV2	Preparedness and Response	Governance Fragmentation in Danish Infrastructure
Holistic Preparedness	PV2	Preparedness and Response	Governance Fragmentation in Danish Infrastructure
Information Access	PV1	Trust and Information Sharing	Governance Fragmentation in Danish Infrastructure
Security Innovation	PV1	Security Implementation	Governance Fragmentation in Danish Infrastructure
Data Sovereignty	PV3	Digital Sovereignty	Foreign Technology Dependencies
Foreign Dependency	PV3	Digital Sovereignty	Foreign Technology Dependencies
Trust Erosion	PV3	Trust and Information Sharing	Foreign Technology Dependencies
Technological Dependency	PV2	Digital Sovereignty	Foreign Technology Dependencies
European Autonomy	PV2	Digital Sovereignty	Foreign Technology Dependencies
Technology Transition	PV1	Digital Sovereignty	Foreign Technology Dependencies
Shifting Trust	PV1	Trust and Information Sharing	Foreign Technology Dependencies
Digital Sovereignty	PV1	Digital Sovereignty	Foreign Technology Dependencies
Transition Challenges	PV1	Digital Sovereignty	Foreign Technology Dependencies
Threat Actors	PV2	Threat Landscape	Asia's Advanced Persistent Threats
Threat Prioritization	PV2	Threat Landscape	Asia's Advanced Persistent Threats
Threat Assessment	PV1	Threat Landscape	Asia's Advanced Persistent Threats
Russian Threat	PV1	Threat Landscape	Asia's Advanced Persistent Threats
Primary Threats	PV3	Threat Landscape	Asia's Advanced Persistent Threats
Knowledge Transfer	PV3	Knowledge and Expertise	International Cooperation and Threat Intelligence
Ukrainian Expertise	PV3, PV1	Knowledge and Expertise	International Cooperation and Threat Intelligence
European Security	PV2	International Cooperation	International Cooperation and Threat Intelligence
Security Realignment	PV2	International Cooperation	International Cooperation and Threat Intelligence
Cautious Cooperation	PV1	International Cooperation	International Cooperation and Threat Intelligence
Dependency Concerns	PV1	International Cooperation	International Cooperation and Threat Intelligence
Small Nation Strategy	PV1	International Cooperation	International Cooperation and Threat Intelligence
Attribution Challenge	PV2	Attribution and Response	Russia's Hybrid Warfare in Ukraine
Undisclosed Attacks	PV2	Attribution and Response	Russia's Hybrid Warfare in Ukraine
Cyber Countermeasures	PV2	Attribution and Response	Russia's Hybrid Warfare in Ukraine
Russian Attribution	PV3	Attribution and Response	Russia's Hybrid Warfare in Ukraine
Security Paradigm Shift	PV2	Future Security Landscape	Evolution of Threat Landscape
Heightened Risk	PV2	Future Security Landscape	Evolution of Threat Landscape
Future Uncertainty	PV2	Future Security Landscape	Evolution of Threat Landscape
Continuous Threat	PV2	Future Security Landscape	Evolution of Threat Landscape
Dynamic Landscape	PV3	Future Security Landscape	Evolution of Threat Landscape
Security Arms Race	PV3	Future Security Landscape	Evolution of Threat Landscape
Geopolitical Awareness	PV3	International Cooperation	Evolution of Threat Landscape
Dependency Recognition	PV3	Digital Sovereignty	Evolution of Threat Landscape

8 Validation Themes correlated with Main Clusters

Main Theme	Related Themes
Digitization in Denmark	Digital Security Challenges, Human Factor in Security, System Vulnerabilities, Hybrid Warfare Dynamics, Critical Infrastructure
Strategic Targeting of Danish Infrastructure	Critical Infrastructure, Hybrid Warfare Tactics, Defensive Capabilities, System Vulnerabilities, Security Implementation
Multi-Vector Attacks	Threat Evolution, Hybrid Warfare Tactics, Hybrid Warfare Dynamics, Resilience Strategies, System Vulnerabilities
The Human Factor in Hybrid Defense	Human Factor in Security, Societal Resilience, Trust and Information Sharing
Incident Response and National Resilience	Preparedness and Response, Resilience Strategies, Defensive Capabilities, Security Implementation, Societal Resilience
Governance Fragmentation in Danish Infrastructure	Security Implementation, Knowledge and Expertise, Preparedness and Response, Trust and Information Sharing
Foreign Technology Dependencies	Digital Sovereignty, Trust and Information Sharing
Asia's Advanced Persistent Threats	Threat Landscape
International Cooperation and Threat Intelligence	Knowledge and Expertise, International Cooperation
Russia's Hybrid Warfare in Ukraine	Attribution and Response
Evolution of Threat Landscape	Future Security Landscape, International Cooperation, Digital Sovereignty

9 Validation Codes correlated with Main Clusters

Quote Label	Participant	Main Theme
Digital Vulnerability	PV3	Digitization in Denmark
Security Awareness Gap	PV3	Digitization in Denmark
Systemic Fragility	PV1	Digitization in Denmark
Security Complexity	PV1	Digitization in Denmark
Evolving Warfare	PV2	Digitization in Denmark
Technology in Warfare	PV2	Digitization in Denmark
Digital Economy	PV3	Digitization in Denmark
Digital Efficiency	PV3	Digitization in Denmark
Critical Infrastructure	PV3	Strategic Targeting of Danish Infrastructure
Infrastructure Governance	PV3	Strategic Targeting of Danish Infrastructure
Target Selection	PV2	Strategic Targeting of Danish Infrastructure
Defense Limitations	PV2	Strategic Targeting of Danish Infrastructure
Centralization Risk	PV1	Strategic Targeting of Danish Infrastructure
Centralization Dilemma	PV1	Strategic Targeting of Danish Infrastructure
Security Trade-offs	PV1	Strategic Targeting of Danish Infrastructure
Threat Escalation	PV3	Multi-Vector Attacks
Attack Inevitability	PV3	Multi-Vector Attacks
Cyber-First Strategy	PV2	Multi-Vector Attacks
Hybrid Warfare Sequence	PV2	Multi-Vector Attacks
System Redundancy	PV1	Multi-Vector Attacks

Quote Label	Participant	Main Theme
Legacy System Loss	PV1	Multi-Vector Attacks
Human Factor	PV3	The Human Factor in Hybrid Defense
Security Behavior	PV3	The Human Factor in Hybrid Defense
Awareness Deficit	PV3	The Human Factor in Hybrid Defense
Civilian Involvement	PV2	The Human Factor in Hybrid Defense
Preparedness Effect	PV2	The Human Factor in Hybrid Defense
Trust Limitations	PV1	The Human Factor in Hybrid Defense
Information Silos	PV1	The Human Factor in Hybrid Defense
Crisis Trust	PV1	The Human Factor in Hybrid Defense
Incident Planning	PV3	Incident Response and National Resilience
Scenario Testing	PV3	Incident Response and National Resilience
Emergency Preparation	PV3	Incident Response and National Resilience
System Resilience	PV2	Incident Response and National Resilience
Tactical Vulnerability	PV2	Incident Response and National Resilience
System Redundancy	PV1	Incident Response and National Resilience
Cost of Security	PV1	Incident Response and National Resilience
Personal Resilience	PV1	Incident Response and National Resilience
Security Framework	PV3	Governance Fragmentation in Danish Infrastructure
Expertise Gap	PV3	Governance Fragmentation in Danish Infrastructure
Response Framework	PV2	Governance Fragmentation in Danish Infrastructure
Holistic Preparedness	PV2	Governance Fragmentation in Danish Infrastructure
Information Access	PV1	Governance Fragmentation in Danish Infrastructure
Security Innovation	PV1	Governance Fragmentation in Danish Infrastructure
Data Sovereignty	PV3	Foreign Technology Dependencies
Foreign Dependency	PV3	Foreign Technology Dependencies
Trust Erosion	PV3	Foreign Technology Dependencies
Technological Dependency	PV2	Foreign Technology Dependencies
European Autonomy	PV2	Foreign Technology Dependencies
Technology Transition	PV1	Foreign Technology Dependencies
Shifting Trust	PV1	Foreign Technology Dependencies
Digital Sovereignty	PV1	Foreign Technology Dependencies
Transition Challenges	PV1	Foreign Technology Dependencies
Threat Actors	PV2	Asia's Advanced Persistent Threats
Threat Prioritization	PV2	Asia's Advanced Persistent Threats
Threat Assessment	PV1	Asia's Advanced Persistent Threats
Russian Threat	PV1	Asia's Advanced Persistent Threats
Primary Threats	PV3	Asia's Advanced Persistent Threats
Knowledge Transfer	PV3	International Cooperation and Threat Intelligence

Quote Label	Participant	Main Theme
Ukrainian Expertise	PV3	International Cooperation and Threat Intelligence
European Security	PV2	International Cooperation and Threat Intelligence
Security Realignment	PV2	International Cooperation and Threat Intelligence
Cautious Cooperation	PV1	International Cooperation and Threat Intelligence
Dependency Concerns	PV1	International Cooperation and Threat Intelligence
Small Nation Strategy	PV1	International Cooperation and Threat Intelligence
Attribution Challenge	PV2	Russia's Hybrid Warfare in Ukraine
Undisclosed Attacks	PV2	Russia's Hybrid Warfare in Ukraine
Cyber Countermeasures	PV2	Russia's Hybrid Warfare in Ukraine
Russian Attribution	PV3	Russia's Hybrid Warfare in Ukraine
Knowledge Transfer	PV3	Russia's Hybrid Warfare in Ukraine
Ukrainian Expertise	PV1	Russia's Hybrid Warfare in Ukraine
Security Paradigm Shift	PV2	Evolution of Threat Landscape
Heightened Risk	PV2	Evolution of Threat Landscape
Future Uncertainty	PV2	Evolution of Threat Landscape
Continuous Threat	PV2	Evolution of Threat Landscape
Dynamic Landscape	PV3	Evolution of Threat Landscape
Security Arms Race	PV3	Evolution of Threat Landscape
Security Trade-offs	PV3	Evolution of Threat Landscape
Geopolitical Awareness	PV3	Evolution of Threat Landscape
Dependency Recognition	PV3	Evolution of Threat Landscape

10 Clusters and Research Question Relation

Research Question	Theme	Main Theme
RQ1: How does digitization aid in hybrid warfare campaigns, and how does this challenge Denmark's cybersecurity governance	Digital Security Challenges	Digitization in Denmark
	Human Factor in Security	Digitization in Denmark
	System Vulnerabilities	Digitization in Denmark
	Hybrid Warfare Dynamics	Digitization in Denmark
	Critical Infrastructure	Strategic Targeting of Danish Infrastructure
	Hybrid Warfare Tactics	Strategic Targeting of Danish Infrastructure
	Defensive Capabilities	Strategic Targeting of Danish Infrastructure
	System Vulnerabilities	Strategic Targeting of Danish Infrastructure
	Security Implementation	Strategic Targeting of Danish Infrastructure
	Threat Evolution	Multi-Vector Attacks
	Hybrid Warfare Tactics	Multi-Vector Attacks
	Hybrid Warfare Dynamics	Multi-Vector Attacks
	Resilience Strategies	Multi-Vector Attacks
	Human Factor in Security	The Human Factor in Hybrid Defense
	Societal Resilience	The Human Factor in Hybrid Defense
	Trust and Information Sharing	The Human Factor in Hybrid Defense

Research Question	Theme	Main Theme
	Preparedness and Response	Incident Response and National Resilience
	Resilience Strategies	Incident Response and National Resilience
	Defensive Capabilities	Incident Response and National Resilience
	Security Implementation	Incident Response and National Resilience
	Societal Resilience	Incident Response and National Resilience
	Security Implementation	Governance Fragmentation in Danish Infrastructure
	Knowledge and Expertise	Governance Fragmentation in Danish Infrastructure
	Preparedness and Response	Governance Fragmentation in Danish Infrastructure
	Trust and Information Sharing	Governance Fragmentation in Danish Infrastructure
RQ2: How do geopolitical tensions influence evolution of cyber warfare against Denmark?	Digital Sovereignty	Foreign Technology Dependencies
	Trust and Information Sharing	Foreign Technology Dependencies
	Threat Landscape	Asia's Advanced Persistent Threats
	Knowledge and Expertise	International Cooperation and Threat Intelligence
	International Cooperation	International Cooperation and Threat Intelligence
	Attribution and Response	Russia's Hybrid Warfare in Ukraine
	Knowledge and Expertise	Russia's Hybrid Warfare in Ukraine
	Future Security Landscape	Evolution of Threat Landscape
	International Cooperation	Evolution of Threat Landscape
	Digital Sovereignty	Evolution of Threat Landscape

11 Affinity Diagram with Quotes

Theme	Quote	Participant
Digitization in Denmark	"Being a trust-based society is actually positive, and being one of the most digitalized countries is good too. But when you combine these two factors in the context of cybercrime, it creates significant vulnerabilities."	PV3
Digitization in Denmark	"As you noted in your thesis, we are vulnerable as a country. Most people appreciate our high level of digitalization and our trustworthy, polite culture, but they don't connect these characteristics to cybersecurity implications - and that's the issue."	PV3
Digitization in Denmark	"After reading what I read, I feel that we are on thin ice. The feeling that we are on much thinner ice than I realized. We have a lot of complexity built into our society that is very vulnerable."	PV1
Digitization in Denmark	"Could it be that the amount of measures you have to take grows much faster than proportional? Every addition to our already complex system might exacerbate the security problem much more."	PV1

Theme	Quote	Participant
Digitization in Denmark	"Information technology is changing warfare on many levels. It's the technology driving drones, enabling battlefield management systems like Delta in Ukraine, and allowing ordinary citizens to contribute to warfighting efforts."	PV2
Digitization in Denmark	"Smartphones function as multipurpose tools in modern warfare—they're computers for running military applications, cameras for intelligence gathering, communication devices, and news sources."	PV2
Digitization in Denmark	"Denmark is one of the wealthiest countries in the world despite having limited natural resources. This prosperity is largely due to high efficiency achieved through digitalization."	PV3
Digitization in Denmark	"What might require multiple forms, stamps, and visits to offices in France can be done with five clicks on a mobile phone in Denmark. That's one of the reasons Denmark is so wealthy - because of the high level of technology adoption."	PV3
Strategic Targeting of Danish Infrastructure	"We are considered critical infrastructure because we're involved with trains."	PV3
Strategic Targeting of Danish Infrastructure	"Our ownership structure is 50% state-owned, 25% owned by Copenhagen Municipality, and 25% by Frederiksberg Municipality. These owners are part of critical infrastructure."	PV3
Strategic Targeting of Danish Infrastructure	"The obvious targets include electricity and telecommunications. However, attackers often focus on wherever they find vulnerabilities. If that's the water supply, that's what they'll target. I think target selection is largely vulnerability-driven."	PV2
Strategic Targeting of Danish Infrastructure	"When discussing hybrid warfare beyond just cyber aspects, it's important to note that the number of vulnerabilities is so high that it's impossible to defend against everything."	PV2
Strategic Targeting of Danish Infrastructure	"What I was often thinking about was the centralization of IT competencies at the university. You get more and more a single point of attack, in my view."	PV1
Strategic Targeting of Danish Infrastructure	"If everybody had their own security system, it would be harder for an enemy to have a widespread attack. But all those small systems are not well developed and must have lots of errors, so they are weak."	PV1
Strategic Targeting of Danish Infrastructure	"Somehow you have to find a balance, and I'm not sure what the right balance is."	PV1
Multi-Vector Attacks	"The level of threats and attacks has increased approximately 300% since the Ukraine war began. That's a direct quote from global cybersecurity sources."	PV3
Multi-Vector Attacks	"It's not a question of if you're going to be going to be attacked, it's about when."	PV3
Multi-Vector Attacks	"It's often discussed that in modern warfare, the first wave of attack will be in cyberspace. It makes sense as an easy way to create chaos before exploiting that opportunity with physical forces."	PV2
Multi-Vector Attacks	"They attacked Ukraine's digital systems first and then physically invaded a few hours later."	PV2
Multi-Vector Attacks	"I think it was unwise for postal services to stop bringing letters around because you need something to fall back on. If our digital systems fail, we need letters again. We need this parallel system."	PV1

Theme	Quote	Participant
Multi-Vector Attacks	"The breakdown of lower technology things is concerning. Earlier there was talk about abolishing FM radio, and even earlier we had medium wave... You could always fall back on long wave and medium wave, but now it's impossible because those systems don't exist anymore."	PV1
The Human Factor in Hybrid Defense	"My perspective on awareness is that employees are both the greatest strength and the greatest weakness of any organization - the difference between those two states comes down to awareness."	PV3
The Human Factor in Hybrid Defense	"Approximately 40% of employees don't lock their computer screens when leaving their workstations - it's equivalent to leaving your home with the front door wide open."	PV3
The Human Factor in Hybrid Defense	"Unfortunately, the general level of awareness is low, which is why we're working on it."	PV3
The Human Factor in Hybrid Defense	"In the early days of the Ukraine conflict, civilians could take pictures of Russian tanks and send them through telegram bots. This technology involves all of society in warfare, raising questions about who's a combatant versus a civilian."	PV2
The Human Factor in Hybrid Defense	"Ukraine seemed quite prepared for this approach, so I don't think it had the effect Russia hoped for. This is likely due to Ukraine's eight years of prior conflict with Russia, during which they experienced severe cyber attacks."	PV2
The Human Factor in Hybrid Defense	"There is an interesting point about our trust-based society. The trust doesn't go so far that we get informed by everybody because they trust us."	PV1
The Human Factor in Hybrid Defense	"We do not get information from our IT department about the threats they have seen, which I think would be very interesting for us lower in the pyramid to know."	PV1
The Human Factor in Hybrid Defense	"We are clearly in a kind of COVID-like period where people tend to support the government more than they did just a few months ago. We more or less agree about what the government is doing. We trust the government."	PV1
Incident Response and National Resilience	"We have an incident response plan that outlines who does what and when if an incident occurs. The existing plan wasn't very good, so I've rewritten it."	PV3
Incident Response and National Resilience	"We're planning to conduct a tabletop exercise where we'll run through different scenarios to test the plan and then refine it based on what we learn."	PV3
Incident Response and National Resilience	"Just this morning, we had a meeting about creating a 'war room' for handling incidents. This includes having standalone computers, backup batteries, and specific software ready for emergency situations."	PV3
Incident Response and National Resilience	"Resilience becomes crucial—the ability to quickly restore systems after an attack or have redundant alternatives in place. For example, if the electricity grid is compromised, having alternative power sources is essential."	PV2
Incident Response and National Resilience	"If Russia wanted to launch a major attack at a specific point, it might be advantageous for them to temporarily disable Ukraine's Delta system for 30 minutes. While Ukraine would likely restore the system quickly, that window might be sufficient for Russia to achieve tactical objectives."	PV2

Theme	Quote	Participant
Incident Response and National Resilience	"What I was thinking about is parallel systems or backup systems. To keep things online, you could have parallel systems doing exactly the same thing but developed by completely different unrelated groups."	PV1
Incident Response and National Resilience	"That's very expensive - everything is twice as expensive - but it could tremendously improve security. In spacecraft, it's normal to have redundant systems."	PV1
Incident Response and National Resilience	"I think I could continue working without internet because I have lots of materials on my computer itself. If the university's system breaks down, I still have source code on GitHub."	PV1
Governance Fragmentation in Danish Infrastructure	"Looking at security standards, at the top of the pyramid you have policies - the 'why' of cybersecurity. The next level is ISO 27001, which addresses who's going to implement security measures. Then there's AT-18 compliance, which details how to implement security at a concrete, technical level."	PV3
Governance Fragmentation in Danish Infrastructure	"Nobody in this company was knowledgeable about these frameworks, so we're bringing in external experts to assess our current level and develop a roadmap for improvement. This will take 1-2 years."	PV3
Governance Fragmentation in Danish Infrastructure	"Kilcullen's model for 'liminal warfare' is useful here, describing different thresholds in hybrid space: 1. Detection threshold - Recognizing that something is happening; 2. Attribution threshold - Gathering enough information to identify who is responsible; 3. Response threshold - Having sufficient information for politicians to make decisions."	PV2
Governance Fragmentation in Danish Infrastructure	"We need both technical solutions and organizational readiness, with regular exercises to practice these responses."	PV2
Governance Fragmentation in Danish Infrastructure	"We have nice websites that pose everyday practical questions... Websites like that could also address security problems, but you don't see it anywhere. Perhaps they exist, but they're not advertised as places you go to for security information."	PV1
Governance Fragmentation in Danish Infrastructure	"That would be very nice, yes." [Regarding bug bounty programs]	PV1
Foreign Technology Dependencies	"As you noted in your thesis, approximately 90% of global data is stored in the US, which is problematic."	PV3
Foreign Technology Dependencies	"We're talking about Amazon with all their data centers, and Microsoft Office, which is used by over 90% of both private and public offices. If these systems were somehow blocked or compromised by US actions, it would create major problems for our email systems, productivity software, and more."	PV3
Foreign Technology Dependencies	"There's a growing level of concern about how to proceed, as US-based software companies aren't perceived as reliable as they once were."	PV3
Foreign Technology Dependencies	"In Danish society, my greater concern is the dependency on American technology. These discussions about digital sovereignty are important, as we saw with the recent Microsoft outage that affected systems nationwide. When an entire country essentially runs on Windows, that creates significant vulnerabilities."	PV2

Theme	Quote	Participant
Foreign Technology Dependencies	"We'll likely see a new European security structure emerge where Europeans take responsibility without depending on the United States. This should include greater focus on digital sovereignty and bringing technology under European control."	PV2
Foreign Technology Dependencies	"We've been thinking about moving away from software packages from Microsoft, for example. I think that's something we have to do at the university, where we are Microsoft and Oracle dependent, along with other foreign providers."	PV1
Foreign Technology Dependencies	"The political situation has changed my perspective. Before, I trusted Google, Dropbox, and a few other American companies. I know they make good products."	PV1
Foreign Technology Dependencies	"But now I'm thinking perhaps we should use a European cloud system like NextCloud instead of Microsoft OneDrive... because of the political situation."	PV1
Foreign Technology Dependencies	"That's hard. There are countries that use European office-based solutions. I use LibreOffice, and it has a long history already, but it's still not stable. I've had crashes with it lots of times, so there are hiccups in the software."	PV1
Asia's Advanced Persistent Threats	"North Korea is actively fighting in Ukraine now, so they're clearly a concerning actor. Much depends on how relations develop with the United States. If American support wanes, European countries might look elsewhere for security arrangements, potentially opening up new discussions with China."	PV2
Asia's Advanced Persistent Threats	"For Europe, I don't see China as the primary threat—it's quite clearly Russia. How we respond will depend on how the situation develops."	PV2
Asia's Advanced Persistent Threats	"I think Russia is the worst threat, not the US and not China. China is interested in theft of information and technology, which is criminal."	PV1
Asia's Advanced Persistent Threats	"Russia is trying to influence elections secretly, while America does it more openly. I think Russia is the biggest threat."	PV1
Asia's Advanced Persistent Threats	"Russia, no doubt, and China [are the greatest dangers]."	PV3
International Cooperation and Threat Intelligence	"It's similar to what's happening on the military front - Denmark is now sending military personnel to Ukraine to learn about drone technology, where Ukraine has developed world-leading capabilities through necessity."	PV3
International Cooperation and Threat Intelligence	"The rest of Europe and the world can learn from what Ukraine has built. When I read your thesis, I saw the parallel with Danish soldiers going to Ukraine to learn about drone technology - it follows the same pattern of knowledge transfer."	PV3
International Cooperation and Threat Intelligence	"Hopefully we'll see a new European security structure emerge where Europeans take responsibility without depending on the United States... Europe isn't fully ready for this transition yet, but I hope we'll develop this new security structure, which should include Ukraine."	PV2
International Cooperation and Threat Intelligence	"If American support wanes, European countries might look elsewhere for security arrangements."	PV2
International Cooperation and Threat Intelligence	"I think Denmark must keep this tradition of trust, but must also be more wary about becoming independent of other countries. Even Ukraine could turn on us."	PV1

Theme	Quote	Participant
International Cooperation and Threat Intelligence	"We like what Ukraine can do, but we should not become too dependent on them. The political situation in Ukraine is not stable. There's still a lot of corruption as far as I know."	PV1
International Cooperation and Threat Intelligence	"As a small country, we have to be dependent on other countries; we have to cooperate, perhaps with countries of about the same size as Denmark, because they probably face similar situations."	PV1
Russia's Hybrid Warfare in Ukraine	"One of the interesting challenges is the problem of attribution in cyberspace. It's not always clear who is behind an attack, even when it appears to come from Russia. Is it state-sponsored or a criminal group? There's a blurring of lines with private actor involvement in warfare, which is very clear in cyber warfare."	PV2
Russia's Hybrid Warfare in Ukraine	"I suspect some attacks on Denmark already come from Russia, but authorities may not publicize this. When transportation systems experience 'malfunctions,' there's a likelihood that some are actually cyber incidents."	PV2
Russia's Hybrid Warfare in Ukraine	"Ukraine has managed these threats quite well, showing that proper preparation can mitigate cyber threats. It's been interesting to see Ukraine also engage in offensive activities, with private actors and groups being encouraged to participate. We've witnessed quite a battle playing out in the cyber domain."	PV2
Russia's Hybrid Warfare in Ukraine	"The general consensus across these forums is that a large part of the attacks can be traced back to Russia. There's no doubt about that."	PV3
Russia's Hybrid Warfare in Ukraine	"I found your angle on Ukraine particularly interesting - how Ukraine has been targeted most heavily by Russian cyberattacks, and the lessons that can be learned from their experience and applied to the rest of Europe."	PV3
Russia's Hybrid Warfare in Ukraine	"Yes, we know that Ukraine has made a tiger jump in knowledge about hybrid warfare and that we have to learn from Ukraine. You pointed that out clearly."	PV1
Evolution of Threat Landscape	"The war in Ukraine has revolutionized and permanently changed Europe's security landscape. The previous security order no longer exists. NATO is in its deepest crisis in 75 years, with some arguing that the alliance is becoming worthless."	PV2
Evolution of Threat Landscape	"It's a very dangerous time overall. The risk that current tensions could develop into a wider war involving Denmark is higher than it has been for many years."	PV2
Evolution of Threat Landscape	"The next decade is particularly dangerous, especially while Putin remains in power. How the Ukraine conflict ends could either embolden or restrain Russia's future actions toward NATO."	PV2
Evolution of Threat Landscape	"Hybrid attacks happen continuously, not as discrete events."	PV2
Evolution of Threat Landscape	"The technology is constantly evolving, laws are changing all the time, and hacker techniques are continuously advancing."	PV3
Evolution of Threat Landscape	"Our job in cybersecurity is trying to stay just a little ahead of the hackers. We don't always succeed, but that's what we strive for."	PV3

Theme	Quote	Participant
Evolution of Threat Landscape	"It's always a trade-off between efficiency and security. That balance is constantly being evaluated."	PV3
Evolution of Threat Landscape	"The political developments in the US have served as a wake-up call for many who weren't previously concerned about these dependencies."	PV3
Evolution of Threat Landscape	"The political situation in the US has definitely raised awareness about how dependent we are on American companies."	PV3

12 Research Question and Cluster Connection

Research Question	Thematic Cluster	Supporting Evidence (Participant)
RQ1	Digitization in Denmark	"Being a trust-based society is actually positive, and being one of the most digitalized countries is good too. But when you combine these two factors in the context of cybercrime, it creates significant vulnerabilities." (PV3)
RQ1	Digitization in Denmark	"After reading what I read, I feel that we are on thin ice. The feeling that we are on much thinner ice than I realized. We have a lot of complexity built into our society that is very vulnerable." (PV1)
RQ1	Digitization in Denmark	"Information technology is changing warfare on many levels. It's the technology driving drones, enabling battlefield management systems like Delta in Ukraine, and allowing ordinary citizens to contribute to warfighting efforts." (PV2)
RQ1	Strategic Targeting of Danish Infrastructure	"We are considered critical infrastructure because we're involved with trains." (PV3)
RQ1	Strategic Targeting of Danish Infrastructure	"The obvious targets include electricity and telecommunications. However, attackers often focus on wherever they find vulnerabilities. If that's the water supply, that's what they'll target." (PV2)
RQ1	Strategic Targeting of Danish Infrastructure	"What I was often thinking about was the centralization of IT competencies at the university. You get more and more a single point of attack, in my view." (PV1)
RQ1	Multi-Vector Attacks	"The level of threats and attacks has increased approximately 300% since the Ukraine war began." (PV3)
RQ1	Multi-Vector Attacks	"It's often discussed that in modern warfare, the first wave of attack will be in cyberspace. It makes sense as an easy way to create chaos before exploiting that opportunity with physical forces." (PV2)
RQ1	Multi-Vector Attacks	"I think it was unwise for postal services to stop bringing letters around because you need something to fall back on. If our digital systems fail, we need letters again." (PV1)
RQ1	The Human Factor in Hybrid Defense	"My perspective on awareness is that employees are both the greatest strength and the greatest weakness of any organization - the difference between those two states comes down to awareness." (PV3)
RQ1	The Human Factor in Hybrid Defense	"In the early days of the Ukraine conflict, civilians could take pictures of Russian tanks and send them through telegram bots. This technology involves all of society in warfare." (PV2)
RQ1	The Human Factor in Hybrid Defense	"There is an interesting point about our trust-based society. The trust doesn't go so far that we get informed by everybody because they trust us." (PV1)
RQ1	Incident Response and National Resilience	"We have an incident response plan that outlines who does what and when if an incident occurs. The existing plan wasn't very good, so I've rewritten it." (PV3)

Research Question	Thematic Cluster	Supporting Evidence (Participant)
RQ1	Incident Response and National Resilience	"Resilience becomes crucial—the ability to quickly restore systems after an attack or have redundant alternatives in place." (PV2)
RQ1	Incident Response and National Resilience	"What I was thinking about is parallel systems or backup systems. To keep things online, you could have parallel systems doing exactly the same thing but developed by completely different unrelated groups." (PV1)
RQ1	Governance Fragmentation in Danish Infrastructure	"Looking at security standards, at the top of the pyramid you have policies - the 'why' of cybersecurity. The next level is ISO 27001, which addresses who's going to implement security measures." (PV3)
RQ1	Governance Fragmentation in Danish Infrastructure	"Kilcullen's model for 'liminal warfare' is useful here, describing different thresholds in hybrid space: 1. Detection threshold - Recognizing that something is happening..." (PV2)
RQ1	Governance Fragmentation in Danish Infrastructure	"We have nice websites that pose everyday practical questions... Websites like that could also address security problems, but you don't see it anywhere." (PV1)
RQ2	Foreign Technology Dependencies	"As you noted in your thesis, approximately 90% of global data is stored in the US, which is problematic." (PV3)
RQ2	Foreign Technology Dependencies	"In Danish society, my greater concern is the dependency on American technology. These discussions about digital sovereignty are important." (PV2)
RQ2	Foreign Technology Dependencies	"We've been thinking about moving away from software packages from Microsoft, for example. I think that's something we have to do at the university." (PV1)
RQ2	Asia's Advanced Persistent Threats	"North Korea is actively fighting in Ukraine now, so they're clearly a concerning actor." (PV2)
RQ2	Asia's Advanced Persistent Threats	"I think Russia is the worst threat, not the US and not China. China is interested in theft of information and technology, which is criminal." (PV1)
RQ2	Asia's Advanced Persistent Threats	"Russia, no doubt, and China [are the greatest dangers]." (PV3)
RQ2	International Cooperation and Threat Intelligence	"The rest of Europe and the world can learn from what Ukraine has built." (PV3)
RQ2	International Cooperation and Threat Intelligence	"Hopefully we'll see a new European security structure emerge where Europeans take responsibility without depending on the United States." (PV2)
RQ2	International Cooperation and Threat Intelligence	"I think Denmark must keep this tradition of trust, but must also be more wary about becoming independent of other countries. Even Ukraine could turn on us." (PV1)
RQ2	Russia's Hybrid Warfare in Ukraine	"One of the interesting challenges is the problem of attribution in cyberspace. It's not always clear who is behind an attack, even when it appears to come from Russia." (PV2)
RQ2	Russia's Hybrid Warfare in Ukraine	"The general consensus across these forums is that a large part of the attacks can be traced back to Russia. There's no doubt about that." (PV3)
RQ2	Russia's Hybrid Warfare in Ukraine	"Yes, we know that Ukraine has made a tiger jump in knowledge about hybrid warfare and that we have to learn from Ukraine." (PV1)
RQ2	Evolution of Threat Landscape	"The war in Ukraine has revolutionized and permanently changed Europe's security landscape. The previous security order no longer exists." (PV2)
RQ2	Evolution of Threat Landscape	"The technology is constantly evolving, laws are changing all the time, and hacker techniques are continuously advancing." (PV3)