Improving Cyber Risk Communication: Mental Models of VPN in a professional services firm in the Netherlands

Veroniek Binkhorst, Delft University of Technology

Abstract

More effective and efficient risk communication in the cybersecurity field needs to be designed to improve risk awareness among people and to increase resiliency. The field of cyber risk communication is relatively new, which limits the current knowledge on how to design risk communication. In this study the risk perception of eleven laypeople and eight experts is researched using a mental model approach and semi-structured interviews combined with a three part scenario-based drawing task. The data is analyzed using the grounded theory method and a substantive theory is formed on the similarities and differences between the mental models of experts and laypeople of VPN in a professional services firm in the Netherlands. The accuracy of the perceptions in the theory are evaluated by a comparison with a real-world representation of VPN organization. Further research can use the results of this study to determine the completeness of the mental models described. Additionally, the study design can be repeated in other settings to determine the generalizability of the identified beliefs. Furthermore, the prevalence of the identified beliefs among similar or different populations can be researched. And finally, the mental models can already be used to design risk communication in a more effective and efficient manner by considering the identified beliefs.

1. Introduction

The field of cyber risk communication is relatively new and questions exist on how to effectively communicate risks in the cyber domain [1]. The goal of cyber risk communication is to help people to be resilient and able to act in a secure manner when interacting with IT systems. To design effective and efficient risk communication, it is necessary to determine the risk perception of the audience [2], [3]. A person's risk perception is that person's view on the risk [4].

This study focuses on the perception of how a Virtual Private Network (VPN) works and the changes that occur in the threat landscape when a VPN is used. To study this perception a mental models approach is used. The working definition of a mental model in this research is the representation in an individual's mind of how a system works.

One out of nine persons were victim of cybercrime in 2017, which underlines the need for research on the effectivity of cyber risk communication on a user's security behavior are essential in the current world [5]. Ensuring that people are aware of the cyber situation is one the three most important challenges to reach adequate cybersecurity levels [6]. Mental models have been useful to research risk perception in other fields, like environmental [7], [8], health [8], and drug risks [7], and are therefore thought to be also useful to design cyber risk communication [9].

Furthermore, mental models of VPN are an important topic to research, because this mechanism offers people the capability to cope with threats and increase their self-efficacy. Coping and self-efficacy has been found to be a reliable, moderately strong predictor for cybersecurity intention and behavior [1].

Additionally, cybercrime is becoming more mature and is shifting its focus to larger and more profitable targets [10]. This research is focused on employees in a professional services firm in the Netherlands. The professional services firm selected is representative for other multinational professional services firms. Therefore, it is expected that the results found in this research will be applicable to similar firms as well.

The main research question of this study is *"what are the similarities and differences between the mental models of experts and laypeople of VPN in a professional services firm in the Netherlands?"*

This study contributes by adding to the knowledge base in this research area. This is the first study of perceptions and practices regarding VPN. The professional services firm selected is representative for other multinational professional services firms. Therefore, it is expected that the results found in this research will be applicable to similar firms as well. By studying both expert and laypeople perceptions, it was possible to explicate perceptions of both groups and differences between the groups. Mistaken beliefs in these perceptions have been identified and the consequences of these mistaken beliefs on behavior and its possible implications are described.

2. Virtual Private Networks

In this sections is explained how a VPN works and what changes in the threat landscape can occur when using a VPN. This overview is not meant to be complete and is based on what choices are made in general by organizations. The information for this section is provided by Dr.-Ing. Tobias Fiebig. In figure 1 a visual representation of the information in this section is presented. In the text numbers are added that refer to a part of the figure.

In general a VPN is used in two different settings. The first setting is in an organization and is described in section 2.1. The second setting is in a personal setting, which is described in section 2.2.

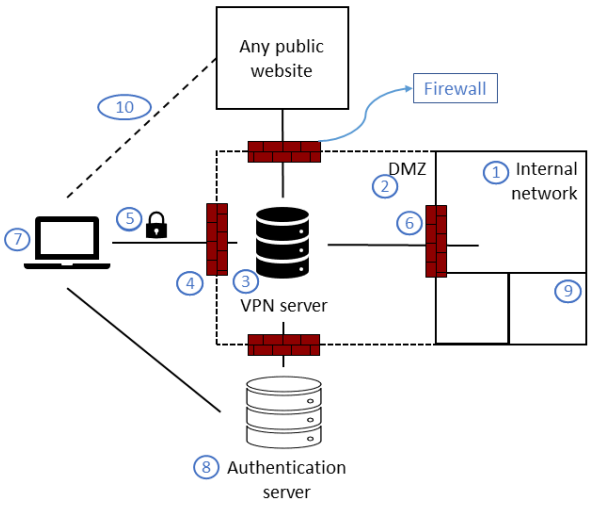

Figure 1: real-world model of a VPN

2.1. Corporate Virtual Private Network

A Virtual Private Network (VPN) is a means used by organizations to let employees access the corporate network via the Internet from a remote location. When the corporate network is accessed, resources become available to the employee as if directly connected to the corporate local area network. Network administrators can impose restrictions on what resources and services a remote access VPN client can use.

The corporate network consists of at least two segments. The first segment is the internal network (1) , which is not accessible from the public Internet and contains the resources and private webpages from the organization. The internal network is only accessible if connected directly to the local area network, or if connected via a VPN connection. The second segment is a demilitarized zone (DMZ)(2), which is a segment of the corporate network that is publicly accessible via the Internet. When a VPN connection is established, Internet traffic is routed via a VPN server in the DMZ to the internal network (3). To protect the corporate network, all webtraffic that enters the DMZ is filtered by a firewall (4).

The VPN connection is secured with encryption (5). By using encryption, the plaintext message is transformed into cyphertext. At the endpoint of the secured connection, the message is decrypted, which transforms the message back into plaintext. Encryption protects confidentiality by ensuring that no one other than the original sender and the receiver of the message know what is written in this message. Additionally, encryption protects integrity by ensuring that the message is not manipulated in transit.

When employees need to send confidential information over the Internet, encryption thus ensures that no third party can eavesdrop or manipulate the message. This is especially important when employees connect to a publicly available Internet connection in for example a café, hotel lobby, or random Wi-Fi hotspot. The encryption must be properly configured and using a proven protocol in order to be secure.

When encryption is used, traffic cannot be inspected on whether it complies with the firewall's filtering rules. Because of this reason, it is important to consider if the encryption is terminated before, at, or after a firewall. In most cases, the encryption is terminated at the VPN server inside the DMZ. This means that malicious webtraffic is able to pass through the firewall protecting the DMZ. In order to protect the internal network, another firewall is located between the DMZ and the internal network (6). This firewall is able to filter the decrypted webtraffic and protect the internal network from malicious traffic.

An employee can establish a VPN connection using a device with a local Internet link (7). In a corporate setting, this device can be company-issued and pre-configured. Employees are provided with a user account and will need to fill in their credentials in order to authenticate themselves. Authentication can be done directly by the VPN server itself, or it can be done by an external authentication server (8). If authentication is performed by an external authentication server, this server will send a ticket to the VPN server, so the employee can establish a VPN connection. When authentication is successful, a VPN connection is established and employees can access the internal network. However, the internal network consists of multiple segments and it depends on the authorization of the user which segments he or she may access (9).

Additionally, The VPN can be in own management or be provided by a third party. Because of price considerations, often a VPN service is provided by a third party. When a VPN service is provided by a third party, certain risks are introduced. For example, the VPN provider can make a mistake when implementing the solution and encryption protocols. Or, the employees from the VPN provider can misuse their access. These examples illustrate that certain arrangements need to be made when the VPN is provided by a third party.

Furthermore, a choice must be made by the organization on whether to allow Internet communication for VPN users. If this is the case, all webtraffic will be routed via the VPN server. Another option is to let employees visit any public website via their local Internet connection and not route this traffic via the VPN server (10). This is called a split tunnel. Using a split tunnel can pose a risk, where an Internet attack could breach the remote host and then use the VPN to access the corporate network.

Lastly, if the VPN uses tunnel mode encryption, the identity of the original sending device is confidential. In tunnel mode encryption, the original IP packet’s header and pay-

load are encrypted and this packet becomes the payload of a new IP packet, with a new IP header. Another option is transport mode encryption, which only encrypts the original IP packet's payload. Transport mode encryption helps VPNs link individual computers together and is in principle not used for remote access VPNs.

2.2. End-User Virtual Private Network

Aside from the use of a VPN in a corporate setting, a VPN can also be used in a personal setting. In a personal setting, the VPN is not provided by an organization to an employee, but is a service acquired by a person. The person can set up his or her own VPN, but in most cases the VPN service is acquired from a company.

When a VPN is used for personal use, the motivation to use a VPN and the technology behind the VPN is somewhat different. The motivation is different in the sense that the VPN would solely be used to access the Internet, and not a corporate network. Additionally, the personal VPN can be used to circumvent local restrictions or to protect someone's identity online.

Local restrictions can be circumvented when the VPN encrypts the IP packet's payload and header and the packet is send to a VPN server in a different location. When this happens, the message cannot be read and thus not filtered to check for local restrictions, and is sent unencrypted from the VPN server onwards. For example, when a local government blocks a certain website, a VPN can be used to visit this website as if a person were to be in a different country. Another example is to circumvent restrictions in place by streaming services. If someone would want to access content not available in their place of residence, this someone can make a VPN connection with a VPN server in a different place and circumvent this restriction. Many VPN service providers for personal use let the user choose with which VPN server they want to make a connection, where the VPN servers are located in different countries. This way, the VPN service provider lets the user choose from which location they want to access a website, for example the United States of America or Brazil.

The identity of a user is protected online if the original IP packet's header is encrypted. The packet will get a new IP header and it is impossible to trace the packet back to the original sending device.

There are some important notions to be made when a VPN service is acquired for personal use. First, it is important to consider whether the VPN provider monitors, collects, or sells data about the webtraffic. Second, a lot of configurations can be made when a VPN is set up, this is also true regarding whether encryption is used.

3. Methodology

In the following sections, we describe the research approach, data collection method, target group, data analysis method, and ethical considerations.

3.1. Study design and Procedure

To answer the research question, an inductive exploratory approach is used. A case study approach is used, focused on a representative multinational professional services firm in The Netherlands.

Data was collected via open-ended, semi-structured, one-on-one, and online interviews and a three part scenario-based drawing task. The interview consisted of three parts. The first part focused on how a VPN works. The second part focused on the current threat landscape. The third and final part focused on changes in the threat landscape that occur do to use of a VPN. The interview questions were developed based on the methodology book of [8], related work, and the elements of a theory [11]. The questions relating to the perception of the current threat landscape were developed based on the attributes of a cyber attack [12]. The interviewer tried remain as passive as possible and only keep the oral fluency of the interviewee. The interviewer tried to use neutral continuation prompts to stimulate the interviewee to continue talking and to clarify topics.

By including scenarios in the drawing task, the influence of a specific context on the mental model can be researched [13]. The scenarios were establishing a VPN connection from home, at a café, and the specific task of sending an e-mail. Participants were asked to think aloud while drawing and provide a concurrent verbal report [14]. All interviews were performed online, using an online conferencing platform. The platform used is based on the open source software BigBlueButton [15] and hosted by SURF, a joint initiative of Dutch education institutions [16]. Drawings were made using the whiteboard on the conferencing platform, allowing the interviewee and researcher to both see what is drawn simultaneously.

In order to make the participants as comfortable as possible, the choice was left to them whether the interview was held in Dutch or English and whether video was enabled or not. Both the Dutch and English interview protocols can be found in the appendix.

To validate the study design pilot interviews were performed. Validation focused on the understandability and unambiguous interpretation of the interview protocol. Additionally, the answers provided in the pilot interviews were analyzed to prevent bias due to wording of the protocol.

3.2. Target Group

The population was defined as employees in a professional services firm in The Netherlands. All employees interviewed handle confidential and/or personally identifiable

information. Experts are employees that work in an information technology department at the firm for a minimum of two years and/or employees that are in the possession of a relevant degree or certificate (e.g. EMITA, CISA, CISSP). Laypeople are employees that work in a department that is considered non-technical, for example the departments legal, finance, and HR.

Purposive sampling was used to draw a sample in a strategic way with the objective that the sample of employees consist of maximum variety on key characteristics. These key characteristics were educational qualifications, education area, role in the firm, and years active in the firm. Participants were recruited through a facilitating contact person for departments and via a department newsletter. The facilitating contact person was informed of the key characteristics. The recruitment texts did not include the topic of the study, to prevent self-selection bias and informing themselves before the interview.

3.3. Data Analysis

Interviews were transcribed with literal level of detail using the software Express Scribe [17]. All information relating to the identity of the company or employees was anonymized. The data used as input for the analysis consisted of the transcriptions of the interviews, the drawings made during the interviews, and hand-written notes of the interviewer.

Grounded theory was used to systematically analyze the data [11], [18], [19]. Coding was performed using the software Atlas.ti version 8.4 [20]. Open coding was executed in a line-by line manner. During open coding, the focus was on descriptive coding, process coding, and value coding [21]. Axial coding was used to group codes into categories and explore relationships between categories and between codes in categories. The theory generated was integrated and refined during selective coding. Both the Dutch and English interviews were coded using English codes.

Theoretical saturation has been reached in the combined groups, and the expert group separately, but not in the laypeople group separately. However, no new concepts emerged in the laypeople group when compared with the experts. Therefore, when looking at the complete sample, theoretical saturation has been reached.

To ensure that the data is interpreted in the same way by all users, partial double coding was performed to determine the reliability of the codebook. To infer reliability the Krippendorff c-alpha-binary was calculated. The c-alpha-binary coefficient indicates for each code whether the different coders have identified similar or the same areas in relation to a given code and takes chance agreements into account [22]. Three out of the eighteen interviews were used for double coding. At first, the overall c-alpha-binary was 0.724. As recommended by [23], disagreements were explored to develop more nuanced and useful codes. Disagreements consisted mainly of two issues. The first is a different application of the concept codes. The second is a difference is quotation length, where one researcher used one quotation, the other had divided it into two different quotations. After resolving these issues, the overall c-alpha binary was raised to 0,837, and equal to or above 0.74 for all semantic domains. The overall coefficient is above 0.8 and therefore the codebook is deemed reliable [24].

The results have been used to design a framework that illustrates the mental models of experts and laypeople of VPN in a professional services firm in the Netherlands. The concepts in the framework explain *when, where, why, how, or with what consequences* a VPN is used. The accuracy of this framework has been evaluated, by comparing it with the real-world model of a VPN as described in section 2.

To evaluate the accuracy of the perceptions of the current threat landscape, the answers were compared with the Cyber Security Assessment Netherlands [25].

3.4. Ethical considerations

This research was reviewed and approved by the Human Research Ethics Committee of Delft University of Technology (reference number: 55223). During recruitment and in other phases of the research possible participants were not in any way deceived.

Participants were recruited via an informative e-mail after their name was provided by a contact person. When a participant agreed to be interviewed, an informed consent form was sent to them two days before the interview to provide them with ample time to review the form. Participants were informed they could withdraw at any point without the need to provide a reason. Participants were not compensated for their participation.

Five types of data were gathered. The first type is the e-mail addresses of the participants. Second is a PDF file of the informed consent e-mail. Third is demographic information of the interviewees, consisting of the key characteristics. Fourth is the recording of the interviews, which included audio and included video if video was enabled during the interview. Fifth is the drawings made during the interview.

A possible risk for participants was identified, since their knowledge may be different than expected from experts and/or laypeople in a professional services firm. These concerns were addressed by taking five measures. First, all data stored in a secure manner. Second, transcriptions and drawings were anonymized, so they were not traceable to a person or the professional services firm. Third, demographic information is presented in a summarized manner. Fourth, the original e-mails were deleted from the e-mail inbox. Fifth, the e-mail addresses, original demographic information, interview recordings, and original drawings were deleted after the end of the study.

The online conferencing platform used to administer the interviews is developed in a privacy preserving manner. The servers used for this service are located in The Netherlands.

The participants were informed that the summarized demographic information, anonymized transcriptions, and anonymized drawings would be shared in products of the study and would be stored on the 4TU.Centre for Research Data for a minimum retention period of 10 years[1] after publication or public release of the work of the research.

The participants were informed that it was within their rights to request access to and rectification or erasure of personal data. Nobody except the project research team had access to the data during the study period.

4. Results

4.1. Participant statistics

In total eleven experts and seven laypeople were interviewed. The participants varied on key characteristics, presented in Table 1.

Table 1: Participant statistics

Characteristic	Sub-characteristic	Experts (n = 11)	Laypeople (n = 7)
Educational qualifications	Master	9 (82%)	6 (86%)
	Bachelor	2 (18%)	1 (14%)
Additional qualifications	IT-audit (EMITA or CISA)	7 (64%)	-
	Privacy (CIPP/E, CIPM, FIP, CIPT, DPO)	6 (55%)	-
	Cybersecurity (CISSP, CSX-P or ISO27001)	5 (45%)	-
Education area	Business administration	4 (36%)	3 (43%)
	Computer science	4 (36%)	1 (14%)
	Crisis and security management	1 (9%)	-
	Engineering, non-computer	3 (27%)	-
	Law	1 (9%)	2 (29%)
	Accountancy	-	1 (14%)
	Marketing	-	1 (14%)
	Sociology	-	2 (29%)
Role in the firm	Department director	0 (0%)	2 (29%)
	Department manager	3 (27%)	2 (29%)
	Staff	8 (73%)	3 (43%)
Years active in the firm	Median	4	6
	Minimum	1,5	1
	Maximum	6,5	34

4.2. Accuracy of the current threat landscape

The results on the perception of experts and laypeople in this sample of the current threat landscape is not completely correct when compared with the situation in reality. However, the perception is deemed acceptable and it can be concluded that a distorted view on the current threat landscape will not be the cause of a potentially distorted view on the changes in the threat landscape due to VPN usage.

4.3. Reason for use

Both experts and laypeople think the abbreviation VPN means a Virtual Private Network. Two reasons are described why a VPN is used. The first reason is to access the internal network and the second reason is for a security purpose.

The internal network is accessed to be able to access internal or private pages or other resources. When located outside of the corporate network, it is necessary to make a VPN connection to access these resources. It is not possible to access these resources if the employee is outside of the network and not connected to the VPN. However, one experts noted:

> *"I recently started using Edge or Chrome. And I believe, at least for Edge in the beginning, you sometimes didn't need a VPN connection to get to certain [the professional services firm] tools, so I found that interesting, how that works."* [Expert 6]

Additionally, confusion exists among experts on what resources are only accessible via a VPN connection. The most prominent example on which confusion seems to exist is e-mail:

> *"But e-mail, if I only have to use e-mail and [cloud software], then I leave the VPN off, because then it is not necessary."* [Expert 2]

> *"Within [the professional services firm] I use a VPN to set up a connection to [the professional services firm] network. People always say, so your traffic is safe. So I can safely check my e-mail."* [Expert 10]

> *"And I know, for example, that previously it was necessary for our mail traffic to connect to the [the professional services firm] network, and that is no longer the case nowadays."* [Expert 11]

The other reason why a VPN connection is used is because of a security purpose. A VPN connection is established when an unsecured network is used, in order to secure the connection. An unsecured network can be a Wi-Fi network in a café or train and can be protected with a password or not. According to experts and two laypeople, this would protect the confidentiality and integrity of communication:

> *"And that means that that connection basically forms a tunnel with the appropriate protocols and ensuring the encryption of the traffic. [...] to make sure the traffic is not readable to everyone around us, using the VPN to shield off and basically wrap-up the traffic in a format that they can't read it."* [Expert 3]

Not all laypeople who state to use a VPN when using an unsecured network indicate to know what makes the connection secure, it just does. On the other hand, some experts and laypeople think it would be unsafe to make a VPN connection when using an unsecured network:

[1] In accordance with the TU Delft Research Data Framework Policy. Available online: https://doi.org/10.5281/zenodo.2573160

"[...] I am a bit scared to use VPN from public places, like if I am sitting in a barista café [...] Well, in a way I am worried that someone tries to target my system, just because I have sensitive information and I am connected to a publicly accessible network, which may or may not be very secure. [...] I know there are a lot of hacks possible from a network which is not secure, especially when you're connecting VPN [...]

X: Why are you scared to use VPN in a public space?

Y: Because I am partially aware of the kind of attacks that are possible. I do not know if someone will try to listen or look at the traffic that is going through the channel, if the Internet that I am connecting to is not secure." [Expert 5]

Experts who are presented with this situation explain that they would either use the unsecured network if strictly necessary, but without a VPN connection, or that they would use their mobile network.

A mobile network is thought by experts to be more secure than an unsecured network because of two reasons. First, the mobile device is provided by the professional services firm, and therefore the firm has approved this mobile network. The second reason is that no entity is in the middle of the connection that could be listening in:

"So when I'm somewhere, like an airport or [example of restaurant], I just use my phone, that's a 4G network, that's my own network, so nobody can […] listen in on it, eavesdrop." [Expert 1]

One reason to use an unsecured network instead of a mobile network would be the costs of using the mobile network when outside of the European Union.

When using a mobile network, the choice to establish a VPN connection or not still remains. Reasons to make a connection could be because it is necessary to access the internal network or for security purposes. Some doubt exists on how secure the mobile network itself actually is:

"X: And what is the difference between your personal hotspot and the public network?

Y: Very good question. I don't dare to say and maybe that's why I always set up a VPN after all. [...] Better safe than sorry, let's just say." [Expert 10]

A simple reason not to establish a VPN connection would be because it is just not necessary to access the internal network.

4.4. Device on which the VPN is used

Experts and laypeople indicate using their personal computer, mobile phone or tablet to establish a VPN connection. Among both experts and laypeople confusion exists on whether their phone makes a VPN connection when internal applications are accessed:

"For work I only use my laptop. For my mobile device […] I don't know the name of the application, but [example of mobile application], and I suspect that's also somehow secured.

X: Do you also mean secured via a VPN connection or in some other way?

Y: I don't really know. It's a bit strange as a security expert that I don't know that, but you do expect that your place of work has made good arrangements. But [...] you do receive a message that it is encrypted. So I expect it to be, yes, I don't know if it's really a VPN, but I do expect it to be somehow, um, secure." [Expert 2]

4.5. User steps to establish a connection

To establish a VPN connection, users take the following actions. First, the user needs to connect to the Internet. Second, the user needs to launch the VPN software. Third, according to only experts, the user needs to enter his or her username. Fourth, the user needs to enter his or her password and access token code. As the final step, the user must click on a button to connect to the VPN. The code from the access token can be provided by a software or a hardware token. Layperson 7 describes these actions, states to make a connection with the corporate network, and also explicitly states he or she does not create a VPN connection, but this is done automatically.

4.6. Infrastructure

Laypeople and experts describe four possible configurations. Two of these configurations are only named by experts.

In the first configuration named by both experts and laypeople, a device simply makes a connection with the corporate network. This configuration is illustrated in figure 2. In a variation, layperson 5 explains a connection is made with a server or router of the professional services firm that is located in the corporate network. In this corporate network multiple servers can be found, described as a 'serverpark'. These servers reduce the risk of information loss, by being back-ups of each other.

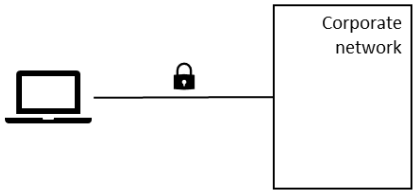

Figure 2: First infrastructure configuration

In the second configuration named by both experts and laypeople, the traffic is routed through a VPN server to the corporate network. This configuration is illustrated in figure 3. If a connection is made to a public website, this traffic is also routed through the VPN server. The location of the

VPN server is not specified or it is explicitly stated that the VPN server is located outside of the corporate network.

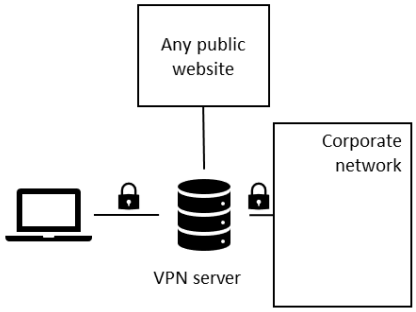

Figure 3: Second infrastructure configuration

Experts vary a bit in their description of what a server is, but essentially describe it as a computer that facilitates the connection. Laypeople are in contention what a server exactly is:

> *"A server is really just a computer."* [Layperson 2]
>
> *"I would describe that as an IT system where all data is stored."* [Layperson 5]
>
> *"[...] actually a folder on eh, so, yeah, just really a documents folder [...]"* [Layperson 1]

The third and fourth configuration are solely described by experts. In the third configuration, illustrated in figure 4, the VPN server is located inside the corporate network. If the user wants to access internal resources, this is where the connection ends. Or, if the user wants to visit any public website, traffic is routed through the VPN server in the corporate network to this public website. Contradictory, one expert stated that this architecture is not possible, that is just not exists.

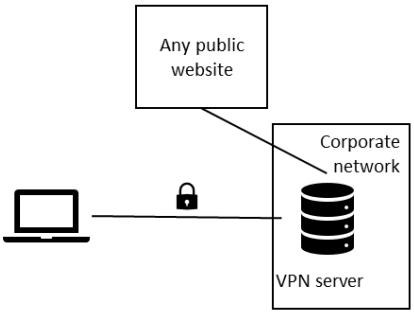

Figure 4: Third infrastructure configuration

The fourth configuration depicts two situations and is illustrated in figure 5. First, the server is located in a DMZ, or a demilitarized zone, which is described as a less secured, publicly available segment of the corporate network. The webtraffic is routed through the VPN server in the DMZ to the corporate network. The second variation of this architecture is the existence of a separate authentication server.

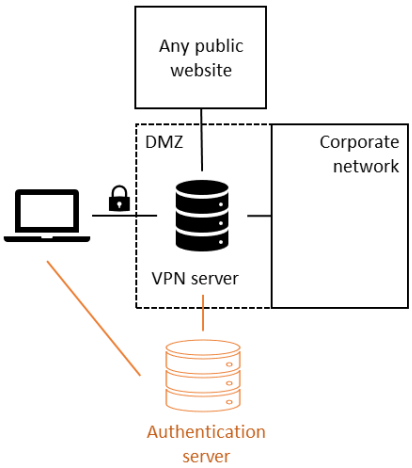

Figure 5: Fourth infrastructure configuration

When a connection is being made, this server is used for authentication. When it has authenticated the user, a signal is send to the VPN server, making it possible to rout the traffic to the VPN server and access the corporate network.

Next to these configurations, experts describe three additional specifications. The first specification, depicted in figure 6, is the existence of a split and complete VPN:

> *"[...] I call it complete and split tunnel. So you can route all the traffic through a VPN and what often happens, is you send all the traffic to the data center, which then redirects you back to the correct point. Either you have a shared or a split and then an organization determines which endpoints, or which IP addresses must go through a VPN tunnel and which not."* [Expert 1]

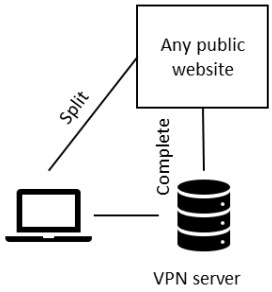

Figure 6: Split and complete VPN

The second specification, depicted in figure 7, is segmentation of the internal network:

> *"X: What do you mean by that, that it is segmented?*
>
> *Y: [...] so it's anyway its own virtual network within what belongs to [the professional services firm]. Of course the VPN receiver will never be able to open up free connections to the entire network that way, but only make sure that I can connect to the network or parts of the network. As will be the case with a normal connection."* [Expert 11]

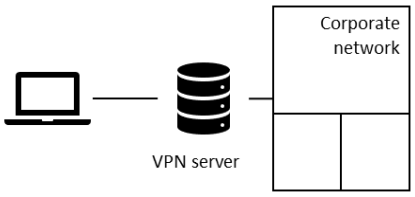

Figure 7: Segmentation of the corporate network

The third specification is the entity that is providing the VPN connection. It can be that the professional services firm is its own provider. Or it can be that a third party is the VPN provider. According to one expert, it is possible that one organization can have multiple providers.

4.7. What makes the connection secured

In section 3.2 was specified that one of the reasons to use a VPN connection is to make a secured connection. In this section is described what employees mean when they refer to a secured connection. In total seven different meanings are identified for a secured connection. Not all employees refer to all options and different options can be combined.

Two options are described by both experts and laypeople. The first option is encryption to ensure confidentiality of the information. Different conceptualizations of encryption exist. According to experts and a couple laypeople, encryptions is a way to code text, so others cannot read it, except for the entity the communication is intended for. Another description is provided by layperson 7:

> *"[...] but the message you make, is put in a kind of tube, as it were. And that tube, there is a key on it and on the other side that key goes off again. So should that message somewhere on the way, or should that tube somewhere along the way be opened, then you have to have that key to be able to read that message in it."* [Layperson 7]

Answers varied on which of the connections in the configurations are encrypted. All connections identified as encrypted by one or more experts and laypeople is depicted in the figures 2 until 5 by a lock. An interesting perception is that of layperson 7:

> *"Well, I think the encryption takes place from the VPN server. [...] Whether that also applies between the user and the VPN connection itself, which also runs over the Internet, I do not know."* [Layperson 7]

Another interesting perception is that of layperson 2, who at first describes the connection being encrypted until the server of the Internet Service Provider, and unencrypted afterwards. At a later moment, layperson 2 thinks the connection might be encrypted until it reaches the corporate network.

Layperson 6 describes another use case of encryption via VPN, where it is used to encrypt communication between two people. An example given is communication via e-mail or conferencing software. Layperson 6 however does point out that a VPN connection is not needed anymore for these applications, and infers this would mean that this communication is not encrypted anymore and anyone can listen in.

The second option described by both experts and laypeople is that the connection is secured because of the authentication measures used to verify the user's identity. The authentication measures exist of the combination of username, password, and access token code.

The third until the seventh option are solely described by experts. The third option is that the VPN connection is private, but not encrypted:

> *"X: Okay. And you describe it as a private network, what do you mean with private?*
>
> *Y: Um, as in not connected to the external Internet, I suppose. It is like a shell around your organization and inside the shell all the data traffic is of course not linked to the outside world [...]"* [Expert 9]

The fourth option is filtering of the connection. All webtraffic that goes through the VPN connection is filtered. This can be because the webtraffic goes through a firewall, IDS, IPS, antivirus, or just filters. One expert indicates that filters exist on the connection, but does not know exactly what these are, as illustrated in the drawing made by expert 9 in figure 8. Another expert indicates that the firewall and

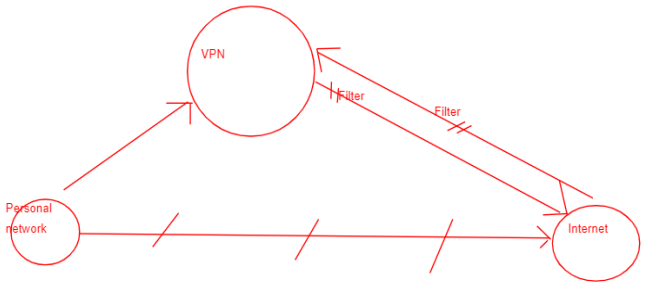

Figure 8: Drawing made by expert 9

antivirus are located in the VPN server. He or she explains that the own device has an antivirus, but the antivirus on the VPN server is of a higher level and offers better protection against malicious software coming through the webtraffic, because it has all latest updates. In this section we do not describe what experts understand a firewall or antivirus is, later on we explicate their perception of what this features can do.

The fifth option is the use of a private IP-address, that is only known between the VPN server and the corporate network:

> *"Normally I would connect to [the professional services firm] using my IP, which is my Internet name. [...] [the professional services firm] sees me as this and it will not allow me to enter their server to access their services. [...] So, I need to have a secure connection because this can be copied easily, this is a public IP, so anyone can*

use this public IP. [...] So, how can we make this secured connection is to have for example a number of secure IPs [...] it is a bit more complicated than this, but this is the concept that they have private IPs that are only known between the server and [the professional services firm].” [Expert 4]

The sixth option is related to the provider of the VPN connection. Different types can be distinguished and they vary on the risk of someone intervening in the middle and the strength of the antivirus protection:

“[...] you have multiple types of VPN. So, you have the commercial VPN, some company who bought a server, put it online and ask people to pay subscriptions to use this VPN server. So, this would be secure, but it would not be highly secure. Then you have another VPN server which is from a well-known corporate, so for example using secure [company] server. So, this [company] server, they have a name they need to maintain so they use a really state-of-the-art server. So, this is the second level. The third level, which is the highest level, is that a VPN that is provided from your corporate, for example from where I work at [the professional services firm], they have provided their own VPN, this is known, this is the highest level. [...] There is no way of anyone intervening in the middle. No third party.” [Expert 4]

The seventh and final option is masking of the IP-address. Because webtraffic is routed through the VPN server, the IP-address of the original sender is no longer visible to the receiving entity. Instead, it sees the IP-address of the VPN server. This allows for anonymous browsing. Or according to some experts, for partially anonymously browsing, because the IP-address can still be related back to the professional services firm.

4.8. Metaphors used

Both experts and laypeople use metaphors to illustrate their perceptions. These metaphors can be categorized into two groups. The first group of metaphors contains metaphors relating to authentication. In this group metaphors such as a safe, gate, door, shield, or secured zone are used. When the user does not have the right credentials, he or she is unable to open the safe, gate, or door, or unable to pass through the secured zone, and therefore are not able to establish the VPN connection. In figure 9 a drawing by layperson 5 is depicted, illustrating a shield protecting the corporate network.

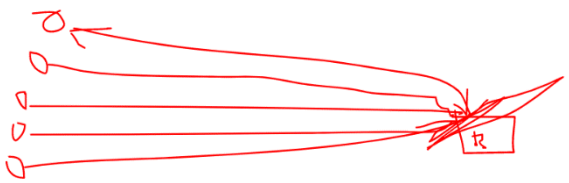

Figure 9: Drawing by layperson 5

The second group of metaphors describe how information is protected in the data transfer. The connection is described as a tunnel, a tube, or a shell, and information is this tunnel, tube, or shell is not readable to anyone trying to snoop in:

“X: You describe the connection as a tunnel, what do you mean by a tunnel?

Y: Yes. I see it a bit as a kind of protective cover that surrounds the data.

[...]

Y: Yes, as a kind of protective layer, so that you cannot see through it, say from the outside, and where that data then passes. Instead of just being open.” [Layperson 2]

4.9. Perception of threats mitigated due to VPN usage

According to experts and laypeople, establishing a VPN connection mitigates several threats. First, a VPN connection protects against threat actors snooping in on the connection and reading communication. This is because the data transfer is encrypted:

“I assume that the data is encrypted, which in that sense simply cannot be cracked, traced back by people who are watching the connection at that moment.” [Layperson 4]

According to experts, this is also a feature of the connection being private. Layperson 2 also thinks this is because of encryption, but are not entirely sure.

Second, using a VPN connection allows the user to browse the web anonymously, or according to some experts, more anonymously. Because webtraffic is routed through the VPN server, only the IP-address of the VPN server can be seen by the receiving entity:

“And if you use a VPN, I think that is like an extra wall in between, so my connection goes via the VPN to this external source. So, they cannot directly view what is my IP-address, among other data. I am not so sure what other data they can't get to, but pretty sure about the IP-address part.” [Expert 9]

Laypeople are not exactly sure how the IP-address is changed. But, according to experts, routing the traffic has an additional benefit. It creates a single point of attack from threats via webtraffic:

“X: What do you mean by restricting channels?

Y: Um, with your lines. So a line can be if I always let my data go through this server here, then I know that everything will enter here as well. So whether I go here to this point, go this way, go here, or go there, it always goes through this server instead of connecting directly from the client. Instead of having all those lines, thus have to catch all those threats, you now have that from a central point.” [Expert 7]

Third, when a threat actor is able to gain access to the device, either physically or digitally, he or she is unable to

access files, because the threat actor does not have the user's credentials.

The following threats mitigated are solely described by experts. Because the VPN connection employs filtering, multiple threats are mitigated. The first threat mitigated is someone accessing a malicious website, by blocking the user from entering it:

> *"I think, what I have in my mind is just a whitelisting and blacklisting feature. So, if I am connected to the VPN, they can regulate what sources I visit."* [Expert 9]

The second threat mitigated is the device getting infected with malicious software. The filters in the VPN, being a firewall, IDS, IPS, antivirus, or just filters, can stop malicious software at or before the VPN server, to ensure it doesn't reach the device:

> *"Because the VPN network of course has more security measures than I do at home, think of advanced firewall, think of analysis, the IDS and IPS, that adds to the security of my network traffic."* [Expert 11]

Additionally, the filters can deactivate the malicious part of the package, for example a malicious attachment from an e-mail, and only let the non-malicious part pass through. Furthermore, the filters can block the user from completing a download, to prevent the user from downloading malicious software.

Some disagreement exists among experts on the effect of a VPN on malicious software on a USB stick:

> *"And if I use a USB for example, a USB stick, in my device, this is a threat that the VPN is not covering. So, the VPN is only covering the risks from the Internet, as long as the VPN is activated."* [Expert 4]

> *"Well, of course, I can plug it in myself, but for example, what files can be run, like if it has an alter executable on the USB stick, I think a VPN can play a role in that, in preventing, or at least detecting what I am doing, with the data on the USB stick."* [Expert 9]

Filtering protects the user against two more threats. It protects against someone uploading a certain unwanted file to the cloud:

> *"It can also have alarming signals that someone who uploads something to [cloud software] that an IT team gets notified or something and then they can take appropriate action."* [Expert 9]

The final threat mitigated due to filtering is a user sending a certain file via an e-mail:

> *"If they do configure it and go very far, like even block my [e-mail] use, that I don't send some confidential data to my private e-mail or something, it can be very secure, but also very annoying for the users."* [Expert 9]

Because of these possibilities of filtering, according to expert 4, using a VPN is the most secure way to browse the web.

Apart from these threats that are mitigated, the VPN connection also ensures the software on the device is updated:

> *"X: Okay. And how would the automatic updates be sent?*
>
> *Y: That should be pushed to your laptop via the admin. Probably that goes through VPN too, because as long as you don't turn on a VPN […] no updates happen either." [Expert 2]*

According to both experts and laypeople, all these measures create extra hurdles and thereby make it more difficult for a threat actor to successfully execute an attack. Although, experts and laypeople do note that a VPN connection does not mitigate all computer security threats.

4.10. Perception of new threats due to VPN usage

Using a VPN connection also introduces new threats. The first threat is a threat actor gaining access to the device while the user is connected to a VPN. This can be physically, but also digitally. An example of digital access is explained by layperson 6:

> *"The moment I set up a VPN connection of course and I have software on my computer, malware, that can eventually read everything or record all my key combinations, yes, then a VPN of course only has limited effect. Because people can then just read what I do."* [Layperson 6]

The second threat is the current authentication measures. Multiple threats are identified by experts that can occur due to the current authentication measures. First, someone can use a user's credentials to establish a VPN connection. Acquiring credentials can happen when for example the password is stored unencrypted or apprehended when the user enters it, the access token is stolen, or if someone were to comprehend how the access token code is constructed and able to replicate the code. Second, the VPN connection is not coupled to the AD-user, which makes it possible to use credentials on different corporate devices. Third, the possibility exists to create multiple VPN connections at the same time using different devices and one person's credentials. The fourth and last problem identified related to the authentication measures is the use of a static password. The user only needs to set the password once and it is not necessary to change it at a point in time.

Layperson 5 also identifies two issues with the current authentication measures. The first point is that the combination of the password and the token might not result in enough possible combinations to be safe. As a solution, the user could be asked to fill in his or her credentials twice, where the access token code would be different the second time. The second point is:

> *"[…] part of the team works with a hardware token, if that goes down, then you have no connection to the software we use."* [Layperson 5]

Layperson 1 recommends using a fingerprint as credential to make the authentication measures more secure.

The third threat is solely named by laypeople and entails a threat actor listening in on the connection. Layperson 6 is not sure where the VPN connection starts and thinks it might be possible that someone can listen in on communication before the connection start, for example on the user's own Wi-Fi network.

The fourth threat is closely related to the third threat and arises when establishing a VPN when using an unsecured network:

> *"X: Why are you scared to use VPN in a public space?*
>
> *Y: Because I am partially aware of the kind of attacks that are possible. I do not know if someone will try to listen or look at the traffic that is going through the channel, if the Internet that I am connecting to is not secure. I do not know how, for example, the cookie and the communication logs are stored. Either way, I am not sure who the Internet Service Provider is for the café, how secure they are, what are their security measures, et cetera. So, all these things really make me worried a bit."* [Expert 5]

Layperson 1 contemplated if this threat can be ruled out by eliminating the need for Internet to make a VPN connection.

The fifth threat is the VPN provider itself. The user needs to trust the provider:

> *"[...] do you have confidence in your provider, where does the provider have his server, who has access to it, and that whole part of trust is very important in this. Who controls the business, who is the ultimate owner, how did they implement their internal security measures.*
>
> *[...]*
>
> *Well, I do trust the government itself, but I also know what they are capable of. And a VPN is not going to help with that. If they want your VPN connector or provider to give access to data, then I wonder if they would refuse. I don't even believe that."* [Expert 1]

If the professional services firm is its own provider, the employees who manage the VPN must still be trusted.

The sixth threat is when the VPN server is compromised, for example when someone is able to break into the server. Furthermore, experts also note that they do not know what data is monitored or even collected by the VPN server. Another threat identified by experts is the geographical location of the VPN server, since where the server is located also has implications for the security of the server.

The seventh threat identified is hacking. According to experts, vulnerabilities can exist in the VPN connection or a threat actor might be able to break the encryption of the connection. Experts note that protocols might be implemented incorrectly and layperson 6 points out that it is important to contemplate which protocols are used. Layperson 3 is wondering whether a VPN connection can be manipulated. Layperson 2 describes a threat actor can have special tools to get into to VPN tunnel and thinks it might be possible for a threat actor to redirect where the traffic send via the connection goes. The traffic could be redirected somewhere else, so the threat actor can read the communication.

Experts identify four more threats that are not mentioned by laypeople. The first threat is that malicious traffic can go through the security layers of the corporate network undetected, if the VPN server is located inside of the corporate network. Because no one other than the intended parties are able to read what data is transferred, malicious software can also pass through the security layers of the corporate network undetected.

The second threat identified solely by experts is a malfunction:

> *"I don't know how much um, powerful or how much big the servers are. So, there might be eh, if the powers goes off."* [Expert 8]

The third threat is that using a VPN connection makes the user more suspicious in the eyes of a state actor. Because it becomes more difficult for a state actor to monitor online actions, it might that they will surveil the user more intensively than usual. It is stated however that this is less of a threat when using a corporate VPN as opposed to a custom built VPN.

The fourth and final threat arises due to the limitations of masking the IP-address. While the user is able to browse the Internet a bit more anonymously, it is also possible to do a so-called 'ping trace':

> *"So it at least ensures that if you, for example, want to log in or just browsed or use the Internet, I don't know, and then they can't immediately see who you were. […] Look how it works technically, you have of course hops, so between you and me are I think at least four hops. [...] and suppose you would look into our connection, then you see that last step. But what you can also do yourself is ping trace. That's just you following as a package. So then you can see exactly which hops are in between [...]"* [Expert 1]

4.11. Change in human behavior to deal with new threats

When experts describe how their behavior changes to deal with new threats, they refer to threats that arise due to the authentication measures. They attempt to prevent access by other persons to their device and prevent other persons from being able to establish a VPN connection using their credentials:

> *"So basically, first, we do not share the same laptop. [partner] does not get to access the laptop [...] [partner] does not know the password to my system, [partner] cannot access it, [partner] doesn't have access to my phone, so [partner] cannot know the [access token pro-*

vider] token ID. All this information I mean, that is something that actively I try to do. I isolate the work environment away from the partner, so that the details are only limited to me." [Expert 5]

"Yes, well, I always keep my token in my pencil case, I don't let it- I actually always have my pencil case closed, because I only take out a pen and then I close it again, so I do pay attention to that." [Expert 6]

Laypeople and other experts state that their behavior does not change due to the new threats that arise because of the usage of a VPN connection. Their behavior does not change because they experience no control over how the VPN is set up and because they need to use the VPN connection in order to be able to work.

Layperson 7 does indicate that if he or she was aware that the connection is not protected with encryption, layperson 7 would not send sensitive data via this connection. But it is assumed that encryption is used and thus sensitive data can be send using the VPN connection.

However, some experts do describe measures they personally take in general. For example, expert 7 and 11 state to only use the VPN connection when necessary, mostly because of capacity issues. Another example is that activities such as online banking would not be performed when connected to Internet via the corporate network. This can be via a VPN, but this is not necessarily the case. When online banking via the corporate network, personal data is visible to the corporate network and this is unwanted. The last general behavior described is using separate devices for work and private use, as described by expert 1 and 11.

4.12 Framework illustrating the mental models

The results have been used to design a framework that illustrates the mental models of experts and laypeople of VPN in a professional services firm in the Netherlands. Indicated in framework are the theory elements known, which were determined at the outset of this research. At the center of the framework the selective code, or core category, is depicted. The framework has been divided into three core elements, namely the user element, the technology element, and the security element. The concepts in the framework explain *when, where, why, how, or with what consequences* a VPN is used. It is indicated whether a concept was mentioned by only experts or by both groups. The accuracy of this framework has been evaluated, by comparing it with the real-world model of a VPN, described in section 2.

5. Discussion

In this section the main question of this study is answered. The main question is "what are the similarities and differences between the mental models of experts and laypeople of VPN in a professional services firm in the Netherlands?"

5.1 Similarities and differences between the mental models

The framework shows that many similarities, but also important differences exist between the mental models of experts and laypeople. For example, in the user element many similarities can be identified. On the other hand, in the technology and security element many differences can also be identified. Since almost all concepts in the technology element that are only named by experts are also accurate, this indicates a less complete mental model for laypeople than experts on the technology element.

The framework also shows that the perceptions of both groups contain accurate and mistaken beliefs. Interesting to notice is that the inaccurate concepts in the security aspect group do not relate to additional inaccurate threats mitigated. The one inaccurate threat mitigated comes forth from an accurate concept, namely filtering. Another interesting fact to notice is that all inaccurate concepts in the groups security aspect and threats mitigated are named by only experts. On the other hand, experts do also name more accurate concepts than laypeople.

How the connection is secured in reality, and therefore what threats are mitigated, depends on the network configuration of the professional services firm and could be limited by the use of a split VPN. Mistaken beliefs and accurate perceptions that might not be in place in reality, depending on the network configuration, could result in an important consequence. This consequence can be that people think they are safer than they actually are, and therefore are either less watchful for threats or take more risks than they would otherwise. Since the mistaken belief in the concept group 'threats mitigated' is only mentioned by experts, and the other, more complicated, but accurate perceptions are only mentioned by experts as well, it can be expected that mainly experts in this target group overestimate the security of a VPN.

On the other hand, the inaccurate threats identified indicate a different result. Inaccurate threats, in the concept group 'new threats', could actually result in an underestimation of the security of a VPN and to more secure behavior than necessary. For example, because some experts and laypeople think a VPN does not protect against someone listening in on the communication, it was identified that they would sometimes choose to not establish a VPN connection when they use an unsecured network. Experts indicated they would use a mobile network instead as a precaution, which is a good solution, but laypeople did not mention this. The result of this inaccurate perceived threat could be that an unsecured network is used, but without creating a VPN connection. Since this would create a threat, this would ultimately result in an unnecessary risk due to a mistaken belief.

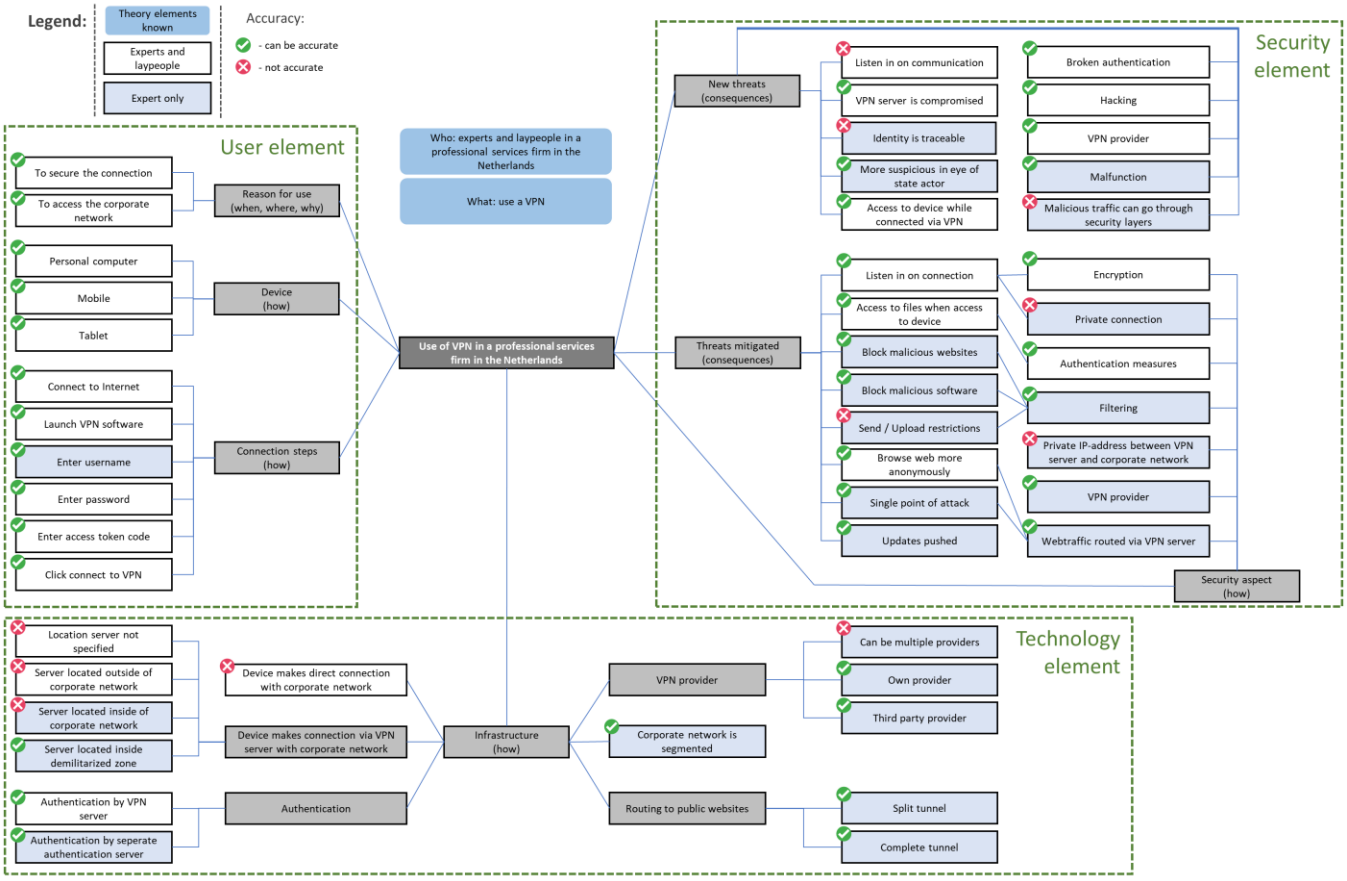

Figure 10: Framework illustrating the mental models of experts and laypeople

To conclude, many similarities, but also important differences exist between the mental models of experts and laypeople. The perceptions of both groups contain accurate and mistaken beliefs. The mistaken beliefs could result in more or less secure behavior than necessary in reality, and therefore create unnecessary precautions and risks.

5.2 Limitations of the study

While there is a general consensus on reliability, replicability, and validity as important quality criteria in quantitative research, there is no consensus on quality criteria in qualitative research [13], [23]. For this reason we will discuss the limitations of this research in general rather than based on quality criteria.

First, generalizability is limited due to the research approach used. A qualitative approach is used, therefore the frequency distribution of perceptions is not necessarily representative

for the population. This research focused which beliefs occur in the research population, but not how often these occur.

Generalizability is also limited because a case study is used. The beliefs among experts and laypeople in one professional services firm have been outlined. Factors such as company culture or national culture may influence the mental models of the population, resulting in different mental models in different firms or countries.

Second, the interviewing method and drawing can limit the quality of the results. The wording of the questions may introduce bias among interviewees. This has been minimized by using neutral formulations in the questions and by testing the interview protocol in pilot interviews. Additionally, most interviewees chose not to enable video during the interview. Therefore, the interviewer was unable to anticipate on the facial expressions or body language of the interviewee. But, the interviewee was also not influenced by the facial expressions or body language of the interviewer. Furthermore, because the drawings were made with limited tools online, this limits flexibility in the drawing.

Third, the participants were not familiar with the conferencing software used. Because of this reason, not all participants were able to participate in the interview using their personal computer and therefore two participants (laypeople 3 and 4) were not able to draw. Also, because participants were not familiar with the environment, they had to figure

out how to use the drawing tools. This was mainly an issue in the beginning of the drawing exercise, as participants became familiar with the available tools during the interview. Before the interview, participants were given the opportunity to enter an 'exploration room', in order to become familiar with the environment. Also, a short overview of the possibilities of the drawing tools was provided before each interview started.

Fourth, interviewees could have not described their complete mental model or could have on purpose rigged the results. Also, self-reported behavior does not always correlate with actual behavior [26]. Because of limited memory and recall, a lack of motivation, or participant fatigue, the interviewees could have report less than they actually know. To elicit as much information as possible and to try to prevent participant fatigue, a drawing exercise was used. Because participants volunteered to participate, they were motivated at least at the beginning of the interview. No indication exists that an interviewee deliberately told less than they know or something else than they actually thought.

Fifth, the interviewer is not an experienced interviewer or coder. With the use of the semi-structure interview protocol and neutral continuation prompts, is was attempted to prevent asking more than one question at a time or to ask leading questions. Furthermore, the manner of coding may influence the quality of the results. To ensure this quality, the theory was validated by revisiting the original data. To ensure the reliability of the codebook, partial double coding was performed by a second researcher and the inter coder agreement was reviewed.

6. Related work

Camp [7] proposed to use mental models to communicate cybersecurity risks. She suggested to use five metaphors as mental models, namely physical security, medical risks, crime, warfare, and markets. Camp did not describe the origin of these metaphors and they seem to be based on her own observations rather than literature or research.

Asgharpour et al. [27] researched to which group experts and non-experts relate certain cyber concepts. They conducted two closed card-sorting experiments with 33 experts and 76 non-experts and based their groups on the metaphors identified by [7]. The results show that experts and non-experts have significantly different mental models. A stricter definition of expert and non-expert led to even more dispersed mental models. However, the definition of experts and non-experts should not be confused with experts and laypeople. All participants in the study were faculty, staff, graduate or undergraduate students in informatics or computer science departments, where experts were longer active in the field than non-experts.

Mental models of experts have been studied in different settings [28]–[32]. For example Dietrich et al. [32] examined the perception of system operators on security misconfigurations. Six interviews were hold via internet relay chat and the results were used to design a survey with 221 participants. One third of the respondents described that a witnessed misconfiguration resulted in an actual security incident, but all misconfigurations had this potential. The results additionally indicated that institutional, organizational, and personal factors are a cause of human error in security operators.

Multiple papers focused on the perception of both experts and laypeople [33]–[36]. An example is the study of Kang et al. [33], which explored mental models of the Internet through interviews, a survey, and a drawing task. Laypeople did not mention Internet levels, organizations, and entities, whereas experts did. The results did not indicate a connection between a person's technical background and actions to protect their privacy and security.

Multiple studies have been done on laypeople's perception of malware. Wash [37] used interviews to elicit mental models from 33 laypeople on viruses, other malware, and hackers. This research served as input for an agent based study performed by Blythe & Camp [38], and a prevalence study of the beliefs identified among US internet users [39]. Another study was done by Spero et al. [40] on mental models of regular software and malware.

Several studies researched mental models of laypeople in response scenario's. Bravo-Lille et al. [41] studied the perception on security warning messages. Zou et al. [42] performed a case study of the Equifax breach to elicit perceptions of a data breach. And Deline et al. [43] suggested the existence of shared mental models in a cyber defense team in an incident response scenario.

Other research on laypeople mental models focused on a wide range of security topics [44], Microsoft Windows 7 updates [45], deleting a file in the cloud [46], secure communication tools [47], prevalence of end-to-end encryption mental models [48], security and privacy perceptions of smart home personal assistants [49], and children's password practices, perceptions and knowledge [50].

7. Conclusion

This study contributes by adding to the knowledge base in this research area. This study focused on mental models of VPN, which have not been researched before in literature. Furthermore, cybercrime is becoming more mature and is shifting its focus to larger and more profitable targets. This research was focused on a specific population, employees in a professional services firm in the Netherlands. The main research question was "*what are the similarities and differences between the mental models of experts and laypeople of VPN in a professional services firm in the Netherlands?"*

To answer this question, a qualitative and case study approach was used. Data was collected via semi-structured, online interviews and a three part scenario-based drawing task. The interviews consisted of three parts. The first part

focused on how a VPN works. The second part focused on the current threat landscape. The third and final part focused on changes in the threat landscape that occur do to use of a VPN.

Transcriptions of the interviews, the drawings, and notes of the interviews were analyzed according to the Grounded Theory method. Ethical considerations were taken into account for recruitment, data collection, data analysis, data publication, and data deletion.

The results describe who, what, when, where, why, how, and with what consequences a VPN is used by experts and laypeople in a professional services firm in the Netherlands. In specific, it is described what the reason for use is, on which devices a VPN connection is established, what the user actions are to establish a connection, what the perceptions are on the infrastructure, how and which threats are mitigated, which new threats arise, and changes in human behavior to cope with these new threats.

The results have been compared with a real-world representation of VPN organization, to determine the accuracy of the mental models. The findings have been combined in a framework that illustrates the mental models of laypeople and experts. Additionally, the results were interpreted and possible implications of the perspectives were considered.

Further research can be done to determine the completeness of the mental models explicated in this study.

Second, the generalizability of the identified beliefs can be researched by repeating this study design in another professional services firm, in another organization, or in yet another population, in order to determine if the results are generalizable to similar or other populations.

Third, the results of this study to determine the prevalence of the identified beliefs among similar or different populations. It is important to know this frequency distribution when risk communication is designed, to be able to focus the communication on frequently occurring beliefs, so the message has as much effect as possible.

And finally, the mental models can already be used to design risk communication in a more effective and efficient manner by considering the identified beliefs.

Acknowledgements

I want to thank the members of my graduation committee for their time, involvement, constructive feedback, and input. All this definitely had a valuable contribution to the quality of this research.

Availability

The data, consisting of the summarized demographic information, anonymized transcriptions, anonymized drawings, and coding files, are accessible in the 4TU.Centre for Research Data for a minimum period of 10 years.

References

[1] European Union Agency for Network and Information Security, “Cybersecurity Culture Guidelines: Behavioural Aspects of Cybersecurity,” 2018. doi: 10.2824/324042.

[2] International Organization for Standardization, “ISO 3100:2018,” 2018. https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-2:v1:en:term:3.1 (accessed Oct. 05, 2020).

[3] B. Rohrmann, “The evaluation of risk communication effectiveness,” *Acta Psychol. (Amst).*, vol. 81, no. 2, pp. 169–192, Nov. 1992, doi: 10.1016/0001-6918(92)90004-W.

[4] International Organization for Standardization, “ISO/Guide 73:2009,” 2009. https://www.iso.org/obp/ui/#iso:std:iso:guide:73:ed-1:v1:en (accessed Mar. 03, 2020).

[5] National Coordinator for Security and Counterterrorism, “Nederlandse Cybersecurity Agenda,” 2019. [Online]. Available: https://www.nctv.nl/onderwerpen/ncsa/documenten/publicaties/2018/04/21/nederlandse-cybersecurity-agenda.

[6] J. Van den Berg, “Grasping Cybersecurity: A set of Essential Mental Models,” in *Proceedings of the 18th European Conference on Cyber Warfare and Security*, 2019, pp. 534–543.

[7] L. J. Camp, “Mental Models of Privacy and Security,” *IEEE Technology and Society Magazine*, vol. 28, no. 3, pp. 37–46, 2009.

[8] M. G. Morgan, B. Fischhoff, A. Bostrom, and C. J. Atman, *Risk Communication: A Mental Models Approach*. Cambridge: Cambridge University Press, 2002.

[9] J. R. C. Nurse, S. Creese, M. Goldsmith, and K. Lamberts, “Trustworthy and effective communication of cybersecurity risks: A review,” in *Proceedings of the 1st Workshop on Socio-Technical Aspects in Security and Trust*, 2011, pp. 60–68, doi: 10.1109/STAST.2011.6059257.

[10] Europol & EC3, “Internet Organised Crime Threat Assessment 2019,” 2019. [Online]. Available: https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2019.

[11] A. Strauss and J. Corbin, *Basics of Qualitative Research: Techniques and Procedures for Developing Grounded Theory*, 2nd ed. Sage

Publications, Inc., 1998.

[12] J. Happa and G. Fairclough, “A Model to Facilitate Discussions About Cyber Attacks,” in *Ethics and Policies for Cyber Operations*, M. Taddeo and L. Glorioso, Eds. Springer International Publishing, 2017, pp. 169–185.

[13] A. Bryman, *Social Research Methods*, 4th ed. Oxford, New York: Oxford University Press Inc., 2012.

[14] M. E. Fonteyn, B. Kuipers, and S. J. Grobe, “A Description of Think Aloud Method and Protocol Analysis,” *Qual. Health Res.*, vol. 3, no. 4, pp. 430–441, Nov. 1993, doi: 10.1177/104973239300300403.

[15] BigBlueButton, “BigBlueButton.” https://bigbluebutton.org/ (accessed May 18, 2020).

[16] SURF, “SURF.” https://www.surf.nl/ (accessed May 18, 2020).

[17] NCH Software, “Express Scribe Transcription Software.” https://www.nch.com.au/scribe/index.html (accessed Apr. 22, 2020).

[18] J. Corbin and A. Strauss, “Grounded theory research: Procedures, canons, and evaluative criteria,” *Qual. Sociol.*, vol. 13, no. 1, 1990, doi: 10.1007/BF00988593.

[19] J. Corbin and A. Strauss, *Basics of Qualitative Research: Techniques and Procedures for Developing Grounded Theory*, 3rd ed. SAGE Publications, Inc., 2008.

[20] ATLAS.ti Scientific Software Development GmbH, “ATLAS.ti.” https://atlasti.com/ (accessed Apr. 22, 2020).

[21] J. Saldaña, *The Coding Manual for Qualitative Researchers*. SAGE Publications, Inc., 2016.

[22] K. Krippendorff, “ATLAS.ti manual appendix: Inter-Coder Agreement in ATLAS.ti.” [Online]. Available: https://downloads.atlasti.com/docs/ICA_Appendix.pdf?_ga=2.154971064.1688372037.1574613096-50067560.1570971353.

[23] R. S. Barbour, “Quality of Data Analysis,” in *The SAGE Handbook of Qualitative Data Analysis*, U. Flick, Ed. SAGE Publications, 2014, pp. 496–510.

[24] K. Krippendorff, *Content Analysis: An Introduction to Its Methodology*, 2nd ed. Sage Publications, Inc., 2004.

[25] National Cyber Security Centre, “Cyber Security Assessment Netherlands 2019,” 2019. [Online]. Available: https://english.ncsc.nl/topics/cybersecurity-assessment-netherlands/documents/publications/2019/09/13/cyber-secrurity-assessment-netherlands-2019.

[26] R. Wash, E. Rader, and C. Fennel, “Can People Self-Report Security Accurately?: Agreement Between Self-Report and Behavioral Measures,” in *Proceedings of the Conference on Human Factors in Computing Systems*, 2017, pp. 2228–2232, doi: 10.1145/3025453.3025911.

[27] F. Asgharpour, D. Liu, and L. J. Camp, “Mental Models of Security Risks,” in *Financial Cryptography and Data Security*, S. Dietrich and R. Dhamija, Eds. Springer Berlin Heidelberg, 2007, pp. 367–377.

[28] B. Al Sabbagh and S. Kowalski, “Developing Social Metrics for Security Modeling in the Security Culture of IT Workers Individuals (Case Study),” in *Proceedings of the 5th International Conference on Communications, Computers and Applications*, 2012, pp. 112–118, [Online]. Available: https://ieeexplore.ieee.org/abstract/document/6516793/.

[29] C. L. Paul and K. Whitley, “A Taxonomy of Cyber Awareness Questions for the User-Centered Design of Cyber Situation Awareness,” in *Human Aspects of Information Security, Privacy, and Trust*, L. Marinos and I. Askoxylakis, Eds. 2013, pp. 145–154.

[30] H. Märki, M. Maas, M. Kauer-Franz, and M. Oberle, “Increasing software security by using mental models,” in *Advances in Intelligent Systems and Computing*, D. Nicholson, Ed. Springer, Cham, 2016, pp. 347–359.

[31] J. Maier, A. Padmos, M. S. Bargh, and W. Wörndl, “Influence of mental models on the design of cyber security dashboards,” in *Proceedings of the 12th International Joint Conference on Computer Vision, Imaging and Computer Graphics Theory and Applications*, 2017, vol. 3, pp. 128–139, doi: 10.5220/0006170901280139.

[32] C. Dietrich, K. Krombholz, K. Borgolte, and T. Fiebig, “Investigating system operators’ perspective on security misconfigurations,” in *Proceedings of the ACM SIGSAC Conference on Computer and Communications Security*, 2018, vol. 18, pp. 1272–1289, doi: 10.1145/3243734.3243794.

[33] R. Kang, L. Dabbsih, N. Fruchter, and S. Kiesler, "'My Data Just Goes Everywhere:' User Mental Models of the Internet and Implications for Privacy and Security," in *Proceedings of the Eleventh Symposium On Usable Privacy and Security*, 2015, pp. 39–52, Accessed: Feb. 21, 2020. [Online]. Available: https://www.usenix.org/conference/soups2015/proceedings/presentation/kang.

[34] K. Gallagher, S. Patil, and N. Memon, "New Me: Understanding Expert and Non-Expert Perceptions and Usage of the Tor Anonymity Network," 2017, Accessed: Feb. 21, 2020. [Online]. Available: https://www.usenix.org/conference/soups2017/technical-sessions/presentation/gallagher.

[35] M. Oates *et al.*, "Turtles, Locks, and Bathrooms: Understanding Mental Models of Privacy Through Illustration," in *Proceedings on Privacy Enhancing Technologies*, 2018, vol. 2018, no. 4, pp. 5–32, doi: 10.1515/popets-2018-0029.

[36] K. Krombholz, K. Busse, K. Pfeffer, M. Smith, and E. von Zezschwitz, "'If HTTPS Were Secure, I Wouldn't Need 2FA' - End User and Administrator Mental Models of HTTPS," in *Proceedings of the IEEE Symposium on Security and Privacy*, 2019, pp. 1138–1155, doi: 10.1109/sp.2019.00060.

[37] R. Wash, "Folk models of home computer security," in *Proceedings of the 6th Symposium on Usable Privacy and Security*, 2010, pp. 1–16, doi: 10.1145/1837110.1837125.

[38] J. Blythe and L. J. Camp, "Implementing mental models," in *Proceedings of the IEEE Symposium on Security and Privacy Workshops*, 2012, pp. 86–90, doi: 10.1109/SPW.2012.31.

[39] R. Wash and E. Rader, "Too Much Knowledge? Security Beliefs and Protective Behaviors Among United States Internet Users," in *Proceedings of the 11th Symposium On Usable Privacy and Security*, 2015, pp. 309–325, [Online]. Available: https://www.usenix.org/conference/soups2015/proceedings/presentation/wash.

[40] E. Spero, M. Stojmenovic, Z. Hassanzadeh, S. Chiasson, and R. Biddle, "Mixed Pictures: Mental Models of Malware," 2019, doi: 10.1109/PST47121.2019.8949030.

[41] C. Bravo-Lillo, L. F. Cranor, J. Downs, and S. Komanduri, "Bridging the gap in computer security warnings: A mental model approach," *IEEE Secur. Priv.*, vol. 9, no. 2, pp. 18–26, 2011, doi: 10.1109/MSP.2010.198.

[42] Y. Zou, A. H. Mhaidli, A. Mccall, and F. Schaub, "'I've Got Nothing to Lose': Consumers' Risk Perceptions and Protective Actions after the Equifax Data Breach," in *Proceedings of the 14th Symposium on Usable Privacy and Security*, 2018, pp. 197–216, Accessed: Oct. 05, 2020. [Online]. Available: https://www.usenix.org/conference/soups2018/presentation/zou.

[43] S. Deline, L. Guillet, P. Rauffet, and C. Guérin, "Team cognition in a cyber defense context: focus on social support behaviors," *Cogn. Technol. Work*, 2019, doi: 10.1007/s10111-019-00614-y.

[44] S. Furman, M. F. Theofanos, Y.-Y. Choong, and B. Stanton, "Basing Cybersecurity Training on User Perceptions," *IEEE Secur. Priv. Mag.*, vol. 10, no. 2, pp. 40–49, Mar. 2012, doi: 10.1109/MSP.2011.180.

[45] K. Vaniea, E. Rader, and R. Wash, "Mental models of software updates," *Int. Commun. Assoc.*, pp. 1–39, 2014, [Online]. Available: http://scholar.google.com/scholar?hl=en&btnG=Search&q=intitle:No+Title#0.

[46] K. M. Ramokapane, A. Rashid, and J. M. Such, "'I feel stupid I can't delete...': A Study of Users' Cloud Deletion Practices and Coping Strategies," in *Proceedings of the 13th Symposium on Usable Privacy and Security*, 2017, pp. 241–256, Accessed: Oct. 05, 2020. [Online]. Available: www.usenix.org/conference/soups2017/technical-sessions/presentation/ramokapane.

[47] R. Abu-Salma, M. A. Sasse, J. Bonneau, A. Danilova, A. Naiakshina, and M. Smith, "Obstacles to the Adoption of Secure Communication Tools," in *Proceedings of the IEEE Symposium on Security and Privacy*, 2017, pp. 137–153, doi: 10.1109/SP.2017.65.

[48] R. Abu-Salma, E. M. Redmiles, B. Ur, and M. Wei, "Exploring User Mental Models of End-to-End Encrypted Communication Tools," 2018, Accessed: Feb. 21, 2020. [Online]. Available: https://www.usenix.org/conference/foci18/presentation/abu-salma.

[49] N. Abdi, J. M. Such, and K. M. Ramokapane, "More than Smart Speakers: Security and Privacy Perceptions of Smart Home Personal Assistants," in *Proceedings of the 15th Symposium on Usable Privacy and Security*, 2019, pp. 451–466, Accessed: Oct. 05, 2020. [Online]. Available: www.usenix.org/conference/soups2019/presentation

/abdi.

[50] Y.-Y. Choong, M. F. Theofanos, K. Renaud, and S. Prior, "'Passwords protect my stuff'—a study of children's password practices," *J. Cybersecurity*, vol. 5, no. 1, Jan. 2019, doi: 10.1093/cybsec/tyz015.

Appendix A: Interview protocol

Interview protocol English	**Interview Protocol Dutch**
A - Starting question 1. What is a VPN?	**A - Start vraag** 1. Wat is een VPN?
B - When drawing blank in block A (in order) 1. Have you ever heard the word VPN? Can you remember anything about it? 2. Let's see whether we can jog your memory. VPN is called <name of VPN in firm> within <name of firm>.	**B – Als geen idee bij vraag A (op volgorde)** 1. Heb je ooit gehoord van het woord VPN? Kan jij je er iets over herinneren? 2. Misschien kunnen we je geheugen helpen. VPN wordt <name of VPN in firm> genoemd binnen <name of firm>.
C - Questions how VPN works (not necessarily in this order) 1. Why do you use VPN? o When? o Where? 2. What actions do you take to create a VPN connection? 3. On what devices do you use a VPN? 4. How does a VPN work? / What happens when you make a VPN connection? 5. Drawing exercise a. Basis scenario: Make a VPN connection at home b. Second scenario (different location): Make a VPN connection at a coffee bar c. Third scenario (specific task): Send an e-mail with an active VPN connection	**C - Vragen voor how VPN works** (volgorde kan verschillen) 1. Waarom gebruik jij VPN? o Wanneer? o Waar? 2. Welke handelingen voer je uit om een VPN verbinding te maken? 3. Op welke apparaten gebruik je een VPN? 4. Hoe werkt een VPN? / Wat gebeurt er als je een VPN verbinding maakt? 5. Teken opdracht a. Basis scenario: Maak een VPN verbinding thuis b. Tweede scenario (andere locatie): Maak een VPN verbinding in een café c. Derde scenario (specifieke taak): Stuur een e-mail met een actieve VPN verbinding
D – Questions changes in threat landscape 1. What is the influence of a VPN connection on your computer security? o Why? o How? o <u>In drawing:</u> draw influence in previous drawing. 2. What kinds of digital threats do you deal with on a normal day? o How does the threat change because of the VPN connection? 3. What kinds of social threats do you deal with on a normal day? o How does the threat change because of the VPN connection? 4. Who or what could be an attacker behind a threat? o How does the kind of attacker change because of the VPN connection? o What would be an attacker's intention?	**D – Questions changes in threat landscape** 1. Wat is de invloed van een VPN verbinding op jouw computerbeveiliging? o Waarom? o Hoe? o <u>In tekening:</u> teken invloed in eerdere tekening. 2. Met wat voor digitale dreiging heb jij op een normale dag te maken? o Hoe verandert de soort dreiging door een VPN verbinding? 3. Met wat voor sociale dreiging heb jij op een normale dag te maken? o Hoe verandert de soort sociale dreiging door een VPN verbinding? 4. Wie of wat is de aanvaller die de dreiging veroorzaakt? o Hoe verandert de soort aanvaller door een VPN verbinding? o Wat is de motivatie van een aanvaller?

o What would be an attacker's capability? 5. What could be the impact of an attack? o Why? o How? <u>Vulnerabilities of VPN</u> 6. How secure is a VPN connection? 7. If not 100% secure: o Why? o <u>In drawing:</u> draw where it is not secure and the cause o How do your actions change because of this? o What are the consequences of these insecurities?	o Wat voor achtergrond heeft een aanvaller? 5. Wat zou de impact van een aanval kunnen zijn? o Waarom? o Hoe? <u>Kwetsbaarheden van VPN</u> 6. Hoe veilig is een VPN verbinding? 7. Als niet 100% veilig: o Waarom? o <u>In tekening:</u> teken waar het niet veilig is en waardoor o Hoe veranderen jouw handelingen hierdoor? o Wat zijn de consequenties van deze onveiligheden?
E - Example neutral continuation prompts • Could you elaborate on that? • Could you go into more detail about that? • Sorry, could you explain what you mean with …? • What do you mean with …? • Why do you say …? • What is …?	**E - Voorbeelden neutrale aanmoedigingen om meer te vertellen** • Kan je meer vertellen over …? • Zou je kunnen uitleggen wat je bedoelt met …? • Wat bedoel je met …? • Waarom zeg je …? • Wat is …?