Security at the End of the Tunnel: The Anatomy of VPN Mental Models Among Experts and Non-Experts in a Corporate Context

Binkhorst, V.F.; Fiebig, T.; Krombholz, Katharina; Pieters, Wolter; Labunets, K.

Publication date
2022

Document Version
Final published version

Published in
USENIX Security Symposium 2022

Security at the End of the Tunnel: The Anatomy of VPN Mental Models Among Experts and Non-Experts in a Corporate Context

Veroniek Binkhorst, *Technical University of Delft;* Tobias Fiebig, *Max-Planck-Institut für Informatik and Technical University of Delft;* Katharina Krombholz, *CISPA Helmholtz Center for Information Security;* Wolter Pieters, *Radboud University;* Katsiaryna Labunets, *Utrecht University*

https://www.usenix.org/conference/usenixsecurity22/presentation/binkhorst

This paper is included in the Proceedings of the 31st USENIX Security Symposium.

August 10–12, 2022 • Boston, MA, USA

978-1-939133-31-1

Open access to the Proceedings of the 31st USENIX Security Symposium is sponsored by USENIX.

Security at the End of the Tunnel: The Anatomy of VPN Mental Models Among Experts and Non-Experts in a Corporate Context

Veroniek Binkhorst[1], Tobias Fiebig[4,1], Katharina Krombholz[2], Wolter Pieters[5], and Katsiaryna Labunets[3]

[1]Technical University of Delft
[2]CISPA Helmholtz Center for Information Security
[3]Utrecht University
[4]Max-Planck-Institut für Informatik
[5]Radboud University

Abstract

With the worldwide COVID-19 pandemic in 2020 and 2021 necessitating working from home, corporate Virtual Private Networks (VPNs) have become an important item securing the continued operation of companies around the globe. However, due to their different use case, corporate VPNs and how users interact with them differ from public VPNs, which are now commonly used by end-users.

In this paper, we present a first explorative study of eleven experts' and seven non-experts' mental models in the context of corporate VPNs. We find a partial alignment of these models in the high-level technical understanding while diverging in important parameters of *how*, *when*, and *why* VPNs are being used. While, in general, experts have a deeper technical understanding of VPN technology, we also observe that even they sometimes hold false beliefs on security aspects of VPNs. In summary, we show that the mental models of corporate VPNs differ from those for related security technology, e.g., HTTPS.

Our findings allow us to draft recommendations for practitioners to encourage a secure use of VPN technology (through training interventions, better communication, and system design changes in terms of device management). Furthermore, we identify avenues for future research, e.g., into experts' knowledge and balancing privacy and security between system operators and users.

1 Introduction

Virtual Private Networks (VPNs) have become a cornerstone of security advice for Internet users. They are used to counter censorship [66], geographical content filters [41], state-level surveillance [47], corporate privacy invasions [43], and threats of insecure local Internet access [34]. Especially the rise of commercial VPN providers puts VPNs on the list of popular security tools employed by individual end-users on the Internet [34]. As such, VPN usage by end-users receives increasing attention in recent empirical studies [26, 34, 45, 61].

However, this perspective on private end users' use of VPN services neglects other—equally important and far older—use cases of VPNs, i.e., the use of VPNs in a corporate context to manage and connect remote workstations to internal corporate resources. Especially due to the COVID-19 pandemic in 2020 and 2021 and the associated work-from-home orders, the importance of these corporate VPNs has risen, as highlighted by the increased deployment of corporate VPNs during the first wave of COVID-19 related lockdowns [22]. Moreover, data handled via these VPNs used in a professional context may be highly sensitive and confidential.

Hence, it is important to understand *how*, *when*, and *why* corporate users—trained IT professionals and non-experts—do or do not use VPNs, how they see the impact of these tools on the threat landscape, and how they think VPNs work. By exploring the perception of VPNs by users in a corporate context, i.e., by eliciting their mental models, we can more accurately tailor training interventions to these populations [29, 57], identify use cases that have been so far overlooked to further improve the usability of these tools, and lay the foundation of further quantitative studies on the subject to get a globally representative picture. This is especially important if—as in our case—the mental models we find differ from those already found in the context of similar Internet security technology, e.g., HTTPS [25, 36].

In this paper, we conduct a qualitative study in a large consultancy firm's[1] regional office, located in the Netherlands, to describe the mental models of experts and non-experts in the context of corporate VPN usage. We recruit experts (participants holding additional IT and IT security-related qualifications) and non-experts (participants from non-IT related departments in non-technical roles, e.g., HR and finance) for semi-structured interviews. We find that the mental models of experts and non-experts actually *align* on an abstract level but diverge in the groups' perspectives on the threat landscape. Based on the data we collected, we make the following contributions:

[1]See the Big Four (PwC, Deloitte, E&Y, and KPMG) for comparable organizations in terms of services offered and size.

- We identify mental models for the use of VPNs in a corporate context for experts and non-experts, and find that these are fundamentally aligned but diverge in perspective on threat models and privacy.
- We identify issues limiting the use of VPNs (policy limitations, privacy concerns) among experts and non-experts, and connect them to the differences in mental models we identify.
- We document limitations in the technical understanding of VPNs, even among experts, and provide a discussion about potential causes.
- We provide concrete steps for security practitioners to improve the security-related efficacy of VPNs in their corporation.
- We provide the first step to future qualitative and quantitative studies in the context of VPNs, and share our interview transcripts and code-books with the community as open data.

Structure: We first present our methodology—including ethical considerations—in Section 2, where we also describe the specific VPN solution used in our participant population in Section 2.4. We then provide an overview of the results in Section 3 and derive the mental models in Section 4. Finally, we first discuss our results and provide recommendations rooted in our data in Section 5, before comparing our results with related work in Section 6, and concluding in Section 7.

2 Research Methodology

In this section, we present the design and procedure of our study, including how we recruit participants and how we collect and analyze our data.

2.1 Study Design

A mental model is a representation of a person's knowledge of a subject, see, e.g., Sanders & Stappers [59]. To elicit the mental models of VPN technology of our participants, we combine techniques previously used in the literature. Specifically, we combine semi-structured interviews with a drawing task, similar to Krombholz et al. [36] and Mayer et al. [39]. By combining these two methods, we obtain data on how our participants visualize their mental model [44], but also get information on how they reason about these concepts and which relationships they see between different parts of the model. Hence, our method aids us in structuring [13] and verifying [30] our participants' mental models, while also reducing participant fatigue [27]. Moreover, drawing is a technique that many people are familiar with, and it offers a lot of freedom of expression.

Based on related work [11, 28, 44] and a general grounded theory approach [63], we designed open-ended and semi-structured interview questions and additional drawing tasks that included three scenarios:

1. Using the corporate VPN from one's home-office
2. Using the corporate VPN while being at a coffee bar
3. Sending an e-mail while using the corporate VPN

Please see Appendix A for the full interview protocol. Furthermore, we asked participants to think aloud while drawing [24], to form a concurrent verbal report (instead of retrospection), as it captures more consistent information about participants mental processes than retrospection [24].

All interviews were conducted via an online video conferencing software with an integrated digital whiteboard. Recordings were created using the platform for later analysis, which also included the drawings made by the participants.

Interview Language: The language used for the interviews was either Dutch or English, and the informed consent form was available in the interviewees' language. Excerpts from Dutch interviews in this paper have been translated, but analysed in their original form. The interviews were analyzed in their corresponding language by Dutch native speakers.

Pilot Interviews: We validated the study design with pilot interviews. Validation focused on the understandability and unambiguous interpretation of the interview protocol. Additionally, we audited the answers from the pilot interviews to detect potential bias due to the wording of the questions.

We conducted four pilot interviews with participants not included in our final sample. Based on the outcomes of these initial interviews, we adjusted the protocol and evaluated it on two more experts and three non-experts. No further issues surfaced during this second round of pilot interviews.

2.2 Ethical Considerations

To mitigate any possible risk for participants and the associated company, we anonymized the interview transcripts and drawings, and only report aggregate demographics. The signed consent forms do not contain any links to the interview transcripts. PII (email addresses, recordings, drawings, non-aggregate demographics) was deleted after the study.

Participants were informed of the purpose of this study via the recruitment email and the informed consent form, see Appendix B. These documents made them aware that we collect aggregated demographic information and anonymized versions of the interview transcripts and produced drawings. We informed them that this data would be made public for a minimum retention period of 10 years via an open data repository. Furthermore, the participants were informed about their subject data access rights, i.e., that—before anonymization, see below—they could retract their consent to participate in the study at any time, and have the right to request access to and rectification or erasure of personal data. Nobody except the project research team had access to the unredacted data.

This research project was reviewed and approved by the Delft University of Technology Human Research Ethics Committee (reference number: 55223).

Table 1: Demographics
The interviewed experts reported the following certifications in IT-auditing: EMITA or CISA; in Privacy: CIPP/E, CIPM, FIP, CIPT, DPO; and in Cybersecurity: CISSP, CSX-P or ISO27001. Percentages do not add up to 100% as one participant may hold multiple qualifications.

Area	Variable/Scale	Experts (n = 11)	Non-Experts (n = 7)
Education	Master	9 (82%)	6 (86%)
	Bachelor	2 (18%)	1 (14%)
Additional certificates	IT-audit	7 (64%)	-
	Privacy	6 (55%)	-
	Cybersecurity	5 (45%)	-
Area of expertise	Business administration	4 (36%)	3 (43%)
	Computer science	4 (36%)	1 (14%)[2]
	Crisis/security management	1 (9%)	-
	Engineering, non-CS	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 in the firm	Median	4	6
	Min–Max	(1,5–6,5)	(1–34)

2.3 Participants and Recruitment

We recruited our participants from the employees of a professional consulting firm offering a wide range of services from financial auditing to IT security assessments. The participants were working in the Dutch office, and recruited via corporate channels, i.e., after management buy-in individual department chairs were contacted and asked to share our interview advertisement with employees in their department corresponding to our sampling criteria, see below. Nevertheless, participation in the study was voluntary, and informed consent was explicitly collected, see Sec. 2.2.

Following our objective of comparing experts' and non-experts' mental models, we sampled for 'experts' in terms of computer security and 'non-experts'. For our study, we considered participants as experts if they worked in an applied technical role in an information technology-related department of the company for at least two years or held a relevant technical certification or degree (e.g., EMITA, CISA, CISSP). Non-Experts are participants who work in a non-technical role in a non-technical department, such as legal, finance, and HR, and do not hold a degree or certification related to computer security. Nevertheless, we ensure that all participants work in roles that include handling and/or processing confidential or personally identifiable information. Furthermore, due to the company's ongoing work-from-home order, all participants had experience using the corporate VPN.

[2]The non-expert listed as a computer scientist does *not* have a background in applied computer science, i.e., computer security, computer networks, programming, or IT operations.

We iteratively analyzed interviews and recruited additional participants until we reached theoretical saturation [11, 63]. We considered theoretical saturation to be reached once three subsequent interviews did not contribute new concepts. In total, we performed 18 interviews, 11 with experts and 7 with non-experts before reaching theoretical saturation for the overall sample. See Table 1 for an overview of our participants.

2.4 VPN Used by Interviewee Population

Here, we describe the VPN technology used by the organization in which we conduct our study. Note that different VPN technologies exist. We discuss how the specific technology used here may influence users' mental models in Section 5.2.

VPN Product Overview: The organization in which we conduct our study uses a product ultimately supplied by a major network device vendor. However, they source it via a third party supplier that provides custom white-labeled client and integration services. This integration provides—instead of the generic client which would be provided by the vendor directly—a CI (Corporate Identity) compliant login interface. This login interface abstracts the technical configuration of the clients away, and instead only requires users to input their username, password, and two-factor authentication (2FA) token.

Technical Description: The specific VPN used in the company is encapsulation based. Practically, this means that, at the client, a virtual TUN(nel) interface is created. This interface appears to the local system like any other interface, and receives a local IP address as well as an IP address for the remote system to configure a point-to-point IP only configuration [56]. When an application sends to a socket on this interface, the resulting packet is handed off to the VPN application, which then encapsulates this packet in a packet that is part of the established TLS session with the VPN server. The resulting packet is then sent by the VPN application via the external interface of the client to the VPN server. Receiving packets then works analogously, with the VPN application decapsulating packets. The whole process is transparent for the application.

The company's VPN utilizes IPSec in tunneling mode for encapsulation. However, as IPSec relies on IKE messages to be exchanged via UDP/500, users may experience issues on public networks with a restrictive outbound firewalling policy [31]. To counteract this, the used VPN solution *additionally* encapsulates IPSec traffic in a TLS session with the VPN endpoint. Please note that this indeed leads to double encryption of traffic, as the vendor documentation notes [31]. While the application also supports tunneling over port TCP/443 without an additional TLS session, this approach makes the VPN more robust against application-level firewalls [31]. Note that, similarly to our organization, major VPN providers on the consumer market use TLS encapsulation for similar reasons [48].

Network and Routing Setup: Depending on the use-case, all network traffic, or only traffic for selected destinations, e.g., internal company resources, may be sent via a VPN. In the organization from which we recruit participants, all network traffic—apart from traffic directed towards the VPN endpoint itself—is redirected via the VPN connection.

2.5 Data Analysis

To analyze the collected qualitative data, we followed a process inspired by grounded theory [16, 17], with four steps: open coding, axial coding, selective coding, and theory generation (or in our case, model generation). This approach is commonly used in similar studies [36] to analyze qualitative data and build corresponding theoretical models.

For the open coding step, we include i) *descriptive coding* where the code represents the topic of the statement, ii) *process coding* where codes represent actions described in the data, and iii) *value coding* where codes represent values, attitudes and beliefs, following Saldana et al. [58].

Codebook Creation: At the beginning of the coding process, two authors developed an initial codebook based on independent coding of two interview transcripts and consequent discussion for reaching an agreement. After, the axial coding grouped the codes into categories and explored the relationships between categories and between codes in categories. Open coding and axial coding were performed iteratively. During the coding process, the researcher used memo writing to keep track of the thought process and theory development. This way, we could document which new codes were developed and why, which were difficult to differentiate, and what patterns and themes emerged. Via these steps and constant communication between the coders, we developed a final codebook after analyzing all interviews.

Reliability: The intermediary codebook was used for double coding on three interviews to ensure that the coders interpreted the data in the same way. We calculated the *Krippendorff c-alpha-binary* [35] using ATLAS.ti[3]. This process lead to a *c-alpha binary* of 0.724. As recommended by Barbour [6], we explored the disagreements to develop more nuanced and useful codes. The disagreements were mainly due to i) a different application of 'concept codes', and ii) differences in quotation length, i.e., differences in the length of annotated segments between the coders. After solving these disagreements and creating a final codebook, see Appendix C, the overall *c-alpha binary* reached 0.837, with all semantic domains being equal to or above 0.74 for the three interviews coded by both coders. This indicates a reliable codebook.

Additional Closed Coding: To analyze participants' perception of changes in the threat landscape, we coded the related part of the transcripts in a partially closed manner. We did it to align our observations with existing threat frameworks and evaluate the accuracy of the perception of the current threat landscape. We used the MITRE ATT&CK framework [42] to code threat types, the typology by de Bruijne et al. [10] for threat actors, the typology by Casey [14] for threat motivation, the Threat Agent Library [15] for threat capability, and the Cyber Security Assessment Netherlands 2019 report by the Dutch NCSC [46] for threat impact coding.

Accuracy of the Mental Models: To evaluate the technical accuracy of the mental models solicited from participants, we compare them to the technical information presented in Section 2.4. To evaluate the accuracy of the perception of the current threat landscape by participants, we compared the results for threats, threat actors, and threat impact with the threat matrix in the Cyber Security Assessment Netherlands 2019 report [46].

[3] To code qualitative data we used ATLAS.ti 8 for Windows http://www.atlasti.com/.

3 Results

We cluster our results with respect to three major themes: *i)* Our participants' perspective on *using* a VPN, i.e., why (in which use cases) they use VPNs, on which devices they use them, and how they interact with the software, *ii)* Our participants' concept of *how* VPNs *work* from a technical point of view, and, *iii)* Our participants' perspective on how VPNs change the threat landscape for them, i.e., which threats are mitigated by VPNs and which may be introduced by them. We provide a structured overview of our codebook and code-counts in Table 2 in Appendix C.

3.1 VPN Usage

In this subsection, we describe our findings on how and why experts and non-experts use VPNs, and in which situations they do so. We note that, although our interview script only references 'VPN', all participants were either able to expand this abbreviation explicitly to 'Virtual Private Network' (6 experts (E) and 2 non-experts (NE)), or could do so implicitly using general description or metaphors like "tunnel".

Devices Used and Connection Establishment: Experts and non-experts indicate using their personal computer (all participants), mobile phone (6 E / 4 NE), or tablet (2 E / 1 NE) to establish a VPN connection. For the process of connecting to (their specific) corporate VPN, participants in general described the same process (see C-codes in Table 2): *i)* connect to the Internet, *ii)* launch the VPN software, *iii)* enter credentials, *iv)* enter 2-factor token, and, *v)* click the connect button in the VPN software.

Interestingly, as one non-expert notes explicitly, we find that non-experts see the procedure as part of their routine, and not them explicitly starting a VPN:

> *"Well, I press an icon at the bottom of my taskbar, because I put it there. Then I enter my personal password plus the, what are they, five digits that appear on the [VPN of the company] app. And together they connect to the intranet*

of [the company]. I do not specifically start the VPN. But my presumption is that that is behind it. That the intranet applications all are accessible via a VPN connection and that you start it up automatically with [the VPN of the company]." [Non-Expert 7]

This is supported by the fact that only 3 experts and 3 non-experts mentioned that they *"click connect to VPN"* (see C.4. in Table 2). This also highlights the importance of integrating the VPN practice into the workflow to ensure its use.

Use cases: Our participants from both samples mirrored the use cases already outlined in Section 2.4. That is, they use the company's VPN for: *i)* Getting access to *internal* company resources not accessible via the Internet (mentioned by all participants), and, *ii)* Securing their network access against local eavesdropping (10 E / 6 NE).

With regard to the first use case, we found significant confusion, even among experts, of which resources are within the scope of the VPN, i.e., which resources require the VPN to be accessible. One expert noted:

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

Still, the same expert notes that certain resources are exempt from requiring the VPN, even though they are internal, for example, email:

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

Ultimately, we attribute this confusion to recent changes in the local security policy, and insufficient communication of the new policy:

"And I know, for example, that previously it was necessary for our mail traffic to go via the [company's] network and that is no longer the case nowadays." [Expert 11]

The second use case is usually invoked around the users' *perception* of the local network being insecure, for example, when using an open WiFi in an airport, train, or cafe. By contrast, a home network is often considered to be 'more secure'.

"[. . .] if I look at my home situation then [. . .] I only have one person who logs in, who has the password for the router. At a cafe connection or [airport] you have more people logging in on the same network. I don't know if that's [. . .] safe or not. I assume that the moment you use your VPN that it is safe." [Non-Expert 5]

Nevertheless, we also find doubt (especially among experts) on whether a VPN actually is sufficiently secure (see Section 3.2). One expert and one non-expert had similar doubts about whether it is secure to use a VPN if the local network seems insecure (see J.10. in Table 2).

"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 [. . .] " [Expert 5]

In that case, 5 experts recommended using other ways to connect to the Internet, e.g., using tethering with one's mobile phone instead of a public WiFi (see A.4. in Table 2).

"When I'm somewhere, like an airport or [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]

We found this recommendation to be connected with the general threat modelling around VPN use. Participants seemed to be highly concerned about *local* attackers, and VPNs protecting against them, namely 8 experts and 4 non-experts mentioned that VPN mitigates *"listening on communication"* issues (see H.3. in Table 2). The security of a network connection—as one of our experts mentioned—assumes that the portion *after* the local access network can generally be considered more trusted, especially if the provider is directly contracted by their company.

" [. . .] the hotspot is provided by a [telecom provider] network that is approved by [the company]. [. . .] I can imagine [the provider] is taking extensive measures to make sure their, the Internet that they are providing through the phone is secure and it is not easily crackable. " [Expert 5]

This highlights the importance of users' threat models in the decision to (not) use a VPN. Therefore, we will explore our participants' threat models in the next subsection.

3.2 VPN Threat Modeling

In this subsection, we take a closer look at which threats our participants consider mitigated by using a VPN, and which *new* threats they think VPNs introduce. Thereafter, we will also take a closer look at how these perceived mitigated and introduced threats impact their *behavior*.

Threats Mitigated by VPNs: Several participants noted that using a VPN mitigates the threat of an external party listening in to network communication from a client connected to the VPN (8 E / 4 NE, see H.3. in Table 2). Seven experts in our sample clearly attributed this to the encrypted connection provided by the software. In contrast, only two non-experts noted that this might have something to do something with encryption:

"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." [Non-Expert 4]

Furthermore, 7 experts and 2 non-experts noted that the VPN 'hides' one's IP address insofar that only an address related to the (company-operated) VPN server is visible to resources they access on the Internet (see H.4. in Table 2).

Especially experts also listed several mitigations a VPN enables that are not directly related to its basic functionality. Instead, these mitigations relate to the IT operations department's ability to apply security policies and mechanisms to users' machines and network traffic as if they were on-site and enable users to work on data remotely without having a copy on the client. For example, 5 experts note that using a VPN allows the IT department to inspect the client's network traffic (see F.11 in Table 2), and 3 experts also note that VPN enables applying corporate filter lists for malicious sites and preventing the downloading of malware (see H.8. in Table 2). Or, as put by Expert 7:

> *"[. . .] I always let my data go through this server here, then I know that everything will enter here as well. [. . .] it always goes through this server instead of connecting directly from the client. [. . .] thus to catch all those threats, you now have that on a central point."* [Expert 7]

Besides looking at external attacks, one of our experts also notes that inspecting traffic when using a VPN can prevent users from leaking internal data to, e.g., cloud services:

> *"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]

Interestingly, the same mechanism is attributed to email communication, even though threat inspection should take place independent of a VPN being used:

> *"[. . .] Now, within the VPN, they have the applications that should scan all coming packages, for example, anti-virus, anti-ware, firewall- [. . .] for example, you are receiving an email from an unknown source, you will get the email, but you will not be able to open the attachment. So, the attachment is deactivated, for example."* [Expert 4]

This observation again highlights the uncertainty, even of experts, on *what* parts of system usage are influenced by a VPN, as already documented in Section 3.1. This is not only limited to applying policies to clients' network traffic, but also to software and policy updates. As one of the experts notes:

> *"[automatic updates] should be pushed to your laptop by the admins. Probably that goes through a VPN too, because as long as you don't turn on a VPN [. . .] no updates happen either."* [Expert 2]

Similarly, as suggested by 3 experts, a VPN may enable an IT department to monitor and update other policies, such as not allowing users to plug in USB sticks.

> *"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]

This statement is likely related to services like Active Directory commonly used to update such policies only being reachable when the client is connected via the VPN. However, please note that the cited experts hold a misconception here, as an active connection is only necessary for *updating* and *installing new* policies. As soon as new policies have been rolled out, the system will enforce them even without an active connection to, e.g., Active Directory.

Finally, both experts (4 participants) and non-experts (2 participants) see an opportunity in using VPNs to keep confidential data from being stored on mobile clients, which may be stolen (see H.6. in Table 2):

> *"Even if someone is able to steal my laptop, they will not be able to connect to the [company's] systems without the [access token provider] token, which is on my phone. Or in the case where it is a physical token, the thief will have to steal both of them to be able to access [the company's] systems."* [Expert 5]

As confidential data is stored on remote file shares only reachable via the VPN and not on the client itself, an attacker stealing the notebook can not get access to it. Furthermore, due to the 2FA used for the VPN, an attacker stealing a notebook still does not gain access to confidential data.

Regarding user behavior, some of our experts shared the security practices that they use on top of VPN like *not sharing the same laptop with others* and *use separate devices for work and private matters*, *use VPN only when is necessary* and *do not use VPN for private matters* (see *I. Change in use behavior* in Table 2). Non-experts have not revealed any specific practices they follow in the light of using a VPN.

Lastly, almost half of the participants (6 E / 4 NE, see H.5. in Table 2) admit that using a VPN complicates attacks, but it does not solve all threats as stressed by one non-expert and eight experts (see H.2. in Table 2).

Threats Introduced by a VPN: Apart from mitigating existing threats, our participants report on new threats introduced by using a VPN which cluster broadly into three categories: *i)* Enabling unauthorized access, *ii)* Reduced reliability of the working environment, and, *iii)* Privacy issues.

While, as mentioned before, participants see benefits for *preventing* unauthorized access to corporate resources, they hold concerns in this regard, too. Specifically, 3 experts and 2 non-experts note that setting up a VPN connection may open the corporate network up to easier attacks from clients (see J.1. in Table 2):

> *"Eh, however, if you have a physical token, if you are like most of the people, who keep their physical token also in the laptop bag, which means if your laptop is stolen, your secure token is also stolen."* [Expert 5]

This point is strengthened by Expert 7, who notes that:

"[. . .] a VPN connection can be started from anyone who has a username and ultimately password plus key. But that also means that you can have multiple sessions per person." [Expert 7]

This relates to the impact of the VPN server itself being compromised as noted by 5 experts and one non-expert (see J.8. in Table 2), or as Expert 10 notes:

"Well, if your VPN server is compromised, it does not really make sense to setup the VPN, as it is just an illusion of a secure connection then. [Expert 10]

In terms of reliability, both groups show concerns about the resilience of the VPN system.

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

Given the experiences of the COVID-19 pandemic, which was underway when this study was conducted, and many companies struggling with scaling their remote work capabilities, doubting the reliability of the VPN infrastructure is a reasonable assumption. Similarly, non-experts showed concerns about the impact of, e.g., the 2FA mechanism becoming unavailable, preventing the use of the VPN:

"[. . .] part of the team works with a hardware token. If that goes down, then you have no connection to the software we use." [Non-Expert 5]

Note, however, that authentication is a crucial component in most IT systems, and it being unavailable leads to a loss of productivity.

In terms of privacy, our participants considered both organizational and personal perspectives. Several participants (3 E / 2 NE, see J.11. in Table 2) focus on the operational requirements of running the VPN service and consider aspects relevant in case the service is outsourced:

"[. . .] do you have confidence in your provider, where does the provider have his servers, who has access to it. 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." [Expert 1]

"[. . .] if employees within [the company] have those who manage those VPN servers and [they] make a deal with hackers then it stops of course. You always have that human factor. [Non-Expert 7]

On the personal side, only 2 experts consider issues of *private* information suddenly being routed via corporate infrastructure and, therefore, they do not use the VPN for private matters (see I.1. in Table 2). This point is highly relevant in the prolonged home-office situation we find ourselves in at the time of writing.

In addition to specific threats, both groups also discuss general threats not specific to VPNs. In this category, one of our experts was concerned about targeted attacks, e.g., by state level actors (see J.7. in Table 2).

"I think the NSA did that as well, that they actually were scanning for people using a VPN or you know, using their search terms to connect to a VPN and then put them on a list of people requiring more surveillance because they felt that was by default suspicious, that someone would try and keep their web traffic and those connections private." [Expert 3]

'Hacking' is another threat theme considered by 8 experts and 3 non-experts (see J.3. in Table 2). In particular, they were concerned about the VPN, after all, not being *secure enough*, as 'there is always a way to get in'. As one non-expert notes:

"Well, just as you can break into other systems, you can probably break into a VPN tunnel. I mean, there are weaknesses everywhere, so probably also in that shell that surrounds it." [Non-Expert 2]

We note that this may be rooted in a limited understanding of the underlying technology. In fact, another non-expert specifically remarks that their concerns are rooted in their uncertainty about *what* a VPN actually does.

"I do not know where the VPN starts, so it might be possible that someone can listen in on your WiFi network." [Non-Expert 6]

Hence, we will next explore non-experts' and experts' understanding of *how* a VPN works.

3.3 Technical Description

In this subsection, we describe our participants perspective on *how* a VPN actually works in general and how it is implemented within the company. We first look at the common items described by all participants and then discuss the additional aspects brought up only by experts.

General VPN Setup: In general, all participants were able to communicate the basic idea of a VPN: A client connects to a VPN server to establish a connection to another network, whereby the connection creates an overlay—the VPN—securing this process (see D.10.–D.11. in Table 2). For this connection step, experts would reflect on authentication, which was not mentioned in-depth by non-experts. We observed that codes D.1.–D.3. co-occurred with D.11. only in the statements made by experts (5 E). In comparison, only 3 non-experts made statements coded with more general codes D.1. and D.10 (see Table 2). Non-Experts tend to describe this connection as a *"tunnel"*, *"tube"*, or *"shell"*. When information is transmitted through this tunnel, tube, or shell, it is not readable to anyone trying to eavesdrop. For example, when asked to elaborate on what they meant with a 'tunnel', Non-Expert 2 said (when creating the illustration in Figure 1):

"I see it a bit as a kind of protective cover that surrounds the data. [. . .] a kind of protective layer, so that you cannot see through it, say from the outside, and where data then passes through. Instead of just being open." [Non-Expert 2]

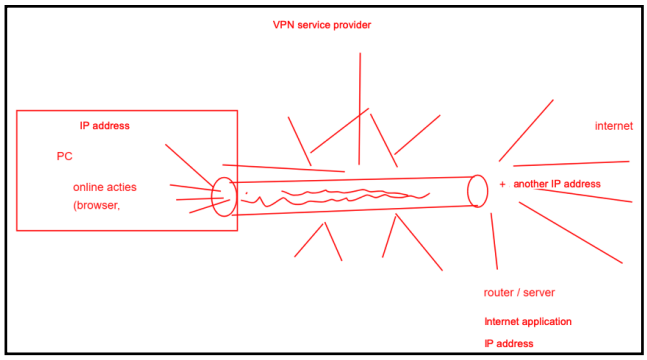

Figure 1: Illustration of the 'tunnel' metaphor by Non-Expert 2. The interview was conducted in Dutch.

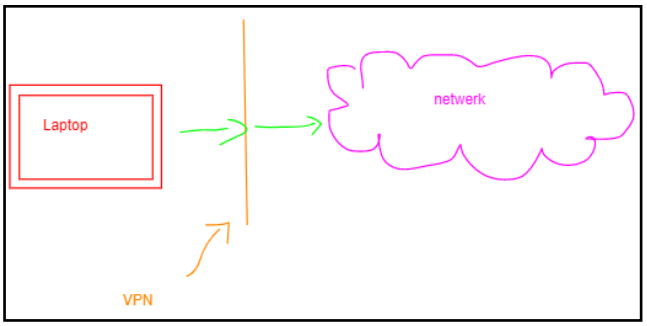

Figure 2: Illustration of the 'shield' metaphor by Expert 6. The interview was conducted in Dutch.

The system *to* which the connection is made was correctly identified as the VPN 'server', even though not all non-experts were able to describe what a server is:

> *"[. . .] actually a folder on eh, so, yeah, just really a documents folder [. . .]"* [Non-Expert 1]

Minor variations exist between different participants (see D.13.–D.15. in Table 2), with, for example, one expert mentioning that the VPN server is most likely located in the demilitarized zone (DMZ) of the company's network. In this context, experts used metaphors like a *"safe", "gate", "door", "shield"*, or *"secured zone"*. For example:

> *"[. . .] it is a certain zone that you basically have to go through. [. . .] I'm not quite sure if it's a zone, yeah, some sort of secured zone that you have to go through first [. . .]."* [Expert 6]

Please see Figure 2 for the drawing created by Expert 6 to accompany this metaphor. Others assumed that not all traffic is routed through the VPN. In general, 6 experts and one non-expert discussed split or complete VPN types (see E.5. in Table 2) and that data can be transmitted in encrypted or decrypted form between client and receiving points (see F.1.–F.2. in Table 2). This may, however, depend on different configurations being used depending on the department, i.e., some only use the VPN for accessing internal content, while other departments route all network traffic via the VPN.

In addition to these aspects, experts also provided more information on implementation details within the corporation. They outlined that, while the VPN connection *does* provide access to the corporate network, it does not provide access to *all* parts of it. Statements from 2 experts were coded with *'internal network segmentation'*. Furthermore, as mentioned before, they iterated that VPN services may be outsourced (4 E / 1 NE) or managed in-house (2 E / 1 NE), and multiple external providers might be used for different purposes (1 E).

Encryption: Both groups noted that the established connection is secured by 'encrypting' traffic flowing via it. (6 E / 1 NE, see F.7. in Table 2). The descriptions of encryption were, however, different. Experts would follow common textbook style analogies of (symmetric) encryption, i.e., applying a secret key that ciphers text in a way that ensures only those in possession of the key can decipher it.

> *"[. . .] if you send from one point to another, information encrypt need to have like the key to actually read the encryption, if you don't, if you see from here, you just see a lot of symbols, let's say inside. So, if you don't have the key to decrypt them, they have no sense for you. Have no meanings. [sic]"* [Expert 8]

Non-Experts similarly expressed the idea of keys being involved, but also stayed closer to the idea of a protected 'tube', most likely superimposed by the cryptographic application scenario of VPNs. For example, Non-Expert 7 remarks:

> *"[. . .] but the message you send, 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."* [Non-Expert 7]

Additionally, one of the experts discussed steps where encrypted data goes through deep packet inspection, decrypting the packets on the path, before reaching the company's network:

> *"[. . .] there's data that you encrypt, that's sent to a server [. . .] that doesn't come directly into the network via a server on the other side, there are steps in between. And [. . .] often that is done through a load balancer or a firewall or a web application firewall, and they often have a way to certificate to use. They then have the certificate on the other side to decrypt the data]"* [Expert 1]

Addressing and Routing: While non-experts and experts were both aware that traffic flowing through the VPN might change the IP address seen by destinations on the Internet, for clients, addressing itself remained unclear, even to experts. This is supported by 7 experts and 2 non-experts discussing that VPN *masks IP-address*. Still, experts at least noted that network addressing and—for IPv4—NAT (Network Address Translation) [21] play important roles in operating a VPN. Expert 8, for example, describes NAT as follows:

"[. . .] it protects the, or it confuse your region IP. For instance, I can visit a website now from The Netherlands, but with some VPN connection, I can appear as I am in Italy." [Expert 8]

Still, even experts were sometimes imprecise in the language used around IP addressing, and, e.g., around what public IP and private addresses [54] are, and which implications they have (see F.5.–F.6. in Table 2):

"Normally I would connect to [the company] using my IP, which is my Internet name. [. . .] [The company] 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 company]." [Expert 4]

Impact of VPN Providers: While the question of whether the operators of VPNs can be trusted remained a common theme, see also the statement of Non-Expert 7 in Section 3.2, only Expert 4 brought up the issue of different *external* VPN providers, and how they inflict on the security of a VPN:

"[. . .] 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's] server. So, this [company's] 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 company], they have provided their own VPN, this is known, this is the highest level. [. . .] There is no way of anyone intervening in the middle." [Expert 4]

This contextualizes the blurry lines of commercial vs. corporate VPNs even in our study population and despite the focus on corporate VPNs. Please see Sections 5.1 and 5.2 for a discussion of this point.

4 Mental Models

In this section, we synthesize experts' and non-experts' mental models from the results of our interviews, and then compare the mental models for the two groups. We create the mental models along three dimensions: *How* each group *uses* VPNs, how each group envisions the *technical operation/implementation* of VPNs, and which *threat models* the groups construct around using VPNs. While both groups were aligned on basic usage perspectives, we found major differences in their understanding of VPN infrastructure and VPN related threat models. Section 4 provides a visual representation of the mental models we identified.

Usage: We find that the mental models of experts and non-experts align when considering *how* they are using VPNs. As expected from the study's scope, both groups share the perspective that they use a VPN to *access corporate resources* and to mitigate threats, with non-experts holding a broader perspective on threats. Both groups were coherent about devices using a VPN and the steps necessary to start the connection.

We find that—among experts and non-experts alike—there is significant uncertainty *when* to use a VPN. Given new threats some experts see, we found some reporting that they sometimes actively *do not* use a VPN in risky situations, as they assume using a VPN might make them more of a target. Both of these observations are tied in with limitations (in both groups) in understanding *how* a VPN actually works.

VPN Operation/Technology Understanding: Both groups demonstrate the same *fundamental* understanding of how VPNs work. In both cases, the common 'tunnel' analogy for a secure connection between a client and a VPN server captures our participants basic mental model of the technical aspects well. However, while non-experts demonstrated a general understanding of how a VPN is organized, they do not completely understand *what* a VPN actually *does*. As expected, experts provided a more detailed mental model of VPN infrastructure. Their technical explanations reach further depth, and include concepts like external authentication and authorization, as well as aspects of the corporation's network topology and segmentation, e.g., the use of a DMZ. In general, though, their mental model is a *super set* of the mental model we found for non-experts.

Threat Modelling: When we look at the threat modeling of our participants, i.e., which threats they consider to be mitigated by using a (corporate) VPN, and which they see being introduced by a VPN, we again find their mental models to be dominated by their operational conceptualization. In Section 4 we denote the threats that are mitigated or introduced by a VPN according to our participants with an anonymous-style hacker pictogram. For mitigated threats, the pictograms are accompanied by a green shield, while introduced threats' pictograms are accompanied by a red warning sign. A dotted line shows if one or both groups brought up the threats.

We find that for non-experts the general understanding of threats and mitigations around VPNs follows the 'tunnel' metaphor. Once the VPN connection is established, the information goes through a secure 'tunnel' that mitigates specific threats, which remain 'outside' of that tunnel. Also, experts were concerned about their *privacy*, i.e., their personal information being routed via and inspected on a corporate VPN.

Again, as to be expected, experts identified more threats mitigated and introduced by VPNs. The general theme here was that experts took a more *operational* perspective on threats, in addition to the basic threats also identified by non-experts. When looking at *new* threats introduced by VPNs,

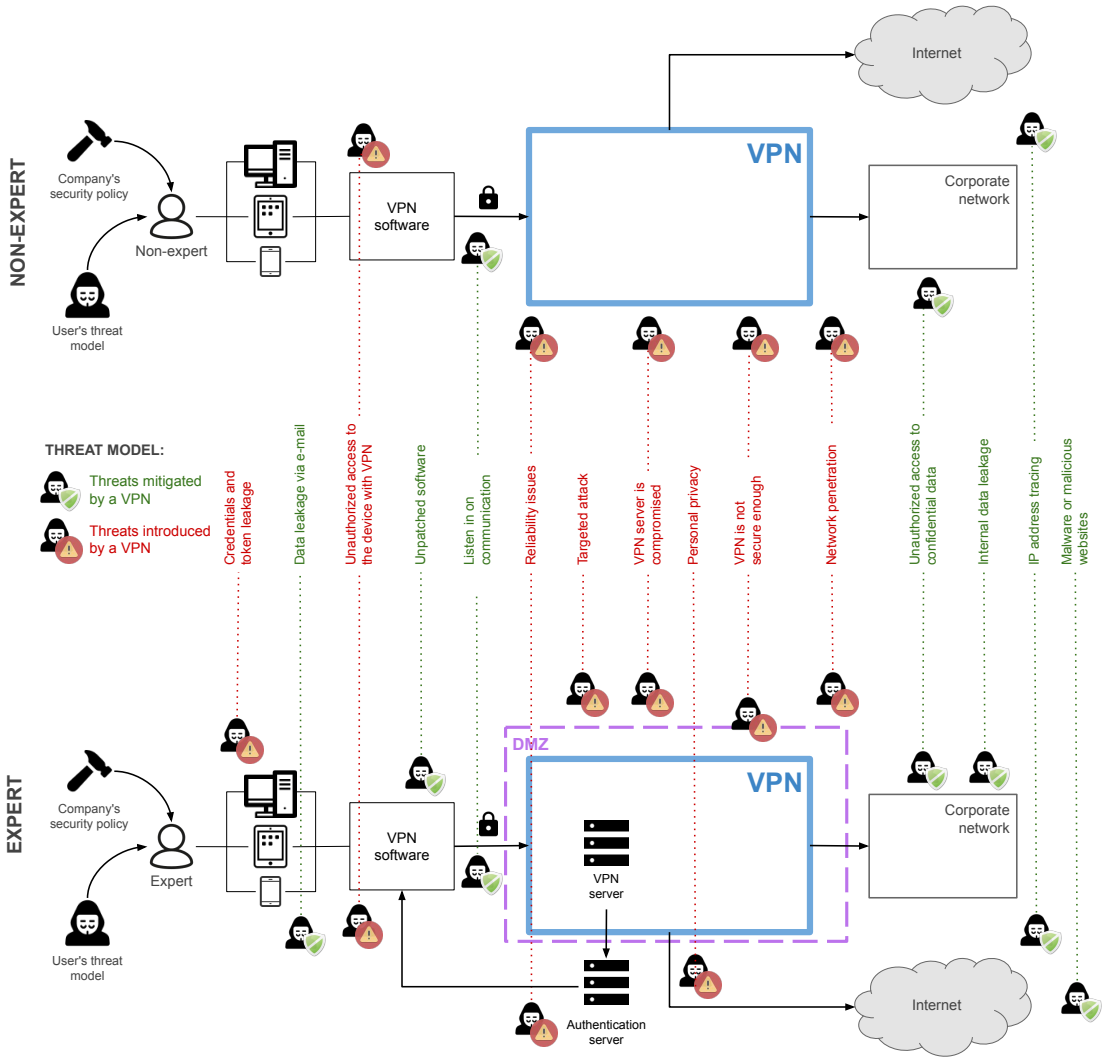

Figure 3: Mental models of experts/non-experts for VPNs along the dimensions of *usage*, *threat modelling*, and *implementation*. *In this figure we used icons by Chanut Industries, Font Awesome, Pixel Bazaar, Umar, DesignModo, RemixIcon, Altop Media, Nick Roach, Webdesigner Depot.

our participants also considered the VPN service itself as a potential threat. This included direct attacks on the VPN service, threats of compromised endpoints connected via the VPN and lost or stolen credentials.

Furthermore, in contrast to non-experts, experts also considered better control and device management capabilities due to the VPN as a part of the threats mitigated by a VPN. They noted that systems connected via VPN could be better monitored and corporate security policies could be better enforced. In this context, they mentioned, for example, monitoring clients' software update state and monitoring users' network traffic by passing it through corporate intrusion detection systems. Interestingly, this point actually relates to the privacy threats *introduced* by a VPN mentioned by our participating experts. Still, these mitigations are also not *necessarily* related to the VPN itself. Rather, they are additional services *enabled* by using a VPN. The same general way of thinking reappears in experts seeing a VPN mitigating data leaks due to accidental or intentional actions by insiders. For example, accidentally uploading sensitive files to public clouds or intentionally sharing confidential data via email. According to experts, this can be more easily monitored with a VPN.

5 Discussion

In this section, we first discuss our key observations with regard to our participants' mental models. We then continue from there to identify recommendations for practitioners and suggestions for further research. Finally, we discuss the limitations of our study.

5.1 Our Population & The State of the World

With the global outbreak of COVID-19, remote work became mandatory for the majority of office workers around the world (see, for example, Brynjolfsson et al. [12]). As the company from which we recruited our participants also mandate working from home while using the corporate VPN to retain access to corporate resources, all participants in our sample have—at least—working knowledge of using the corporate VPN. In turn, this priming on using VPNs may affect our results, e.g., participants might be more familiar with which applications need the VPN. However, we find that participants are, for example, still uncertain on which applications require the VPN. We conjecture that this is connected to changes in policies to accommodate remote work without a VPN, e.g., see our participants' reflections on whether the VPN is necessary for using email services, see also Section 5.3.

With our participants (forced to be) familiarized with VPN technology, we are looking at a primed sample concerning VPN technology. This means that our results have to be understood under these constraints and may deviate for a population interviewed before the emergence of COVID-19 as a global pandemic in 2020. At the same time, given the global impact of COVID-19, these conditions *may* actually be considered representative for populations *at this point in time*.

In any case, these considerations and our results imply a series of new research questions for follow-up work. We suggest investigating *if* and *how* the introduction of mandatory remote work impacted users' mental models. For this work, our findings can serve as a first data point for users mental models in a corporate setting during work-from-home orders.

5.2 Impact of Specific VPN Technology

As detailed in Section 2.4, the organization in which we executed our study uses a specific commercial VPN integration tailored to their corporate design. This aspect naturally begs the question of how this *specific* technology has impacted our analysis of users' mental models.

When we revisit our mental model, see Figure 4, we find that the specific tunneling technology being used is not part of the users' mental models. Instead, non-expert and expert users alike consider the actual encapsulation part of the VPN a 'black box' that links their own system via a local 'VPN software' to the corporate network and the Internet.

However, besides the *specific* technology used for the VPN, we find that other aspects of the VPN's implementation *did* have an impact on our participants mental model. The largest impact is certainly in redirecting the default route of VPN users via the corporate network. While this is the case in the corporation from which we recruit, it is not necessarily the case for all corporate VPNs, especially when they are only targeted at providing access to internal services. However, as the default route is redirected here, we find both groups describing Internet access as being facilitated *via* the VPN.

Similarly, as we are dealing with a corporate VPN, and our users' mental model heavily involves the workflow and local VPN application, our results most certainly differ from what would be expected when interviewing a population familiar with end-user VPNs. While the actual technology in that communication—which often will be comparable to the TLS based tunneling used here to reduce the potential for user-visible connectivity failures—most likely will not play a major role either, the procedural and workplace dependent factors we find will not be present. Instead, we conjecture, that for example, the *location* of VPN servers will play a bigger role, as these usually take a prominent position in marketing and user interfaces for end-user VPNs, see, e.g., NordVPN [48].

5.3 When to use a VPN

In our study, experts and non-experts were often unsure when to use a VPN. This finding tied into a variety of factors, including different policies between endpoint types (an application needing the VPN on a PC but not on a tablet), changing policies (An application suddenly being usable (only) with(out) the VPN), and an unclear threat model on the users' side (for experts and non-experts alike). While the first two points can be addressed by a more straightforward policy and risk communication, the latter is more difficult to address. We found that experts' and non-experts' conceptualization of threats heavily depends on their understanding of how a VPN works. However, we also found limitations in experts' and non-experts' understanding of the inner workings of VPNs and—in the corporate context—uncertainty of what services are affected by using a VPN. These beliefs— as in the case of one expert being worried about *becoming* a target when using a VPN—relate to a fear of becoming more of a target when using a VPN. As users are uncertain about *how* a VPN works and may hold *false beliefs* of the protection (or limitations of protection) it offers, they decide to *not* use the VPN, even though it might be beneficial, e.g., when using a public WiFi. These challenges can be further amplified if a corporate policy is inconsistent regarding which applications are accessible with(out) a VPN or if the policy changes without notifying users sufficiently.

5.4 Limitations in Experts' Knowledge

The limitations in experts' knowledge regarding VPNs outlined above, especially in the context of threats around VPNs are a notable observation. Given our population, recruitment channel, and the associated ability to verify these experts' credentials and certifications—see Section 2.3—it is unlikely that we accidentally interviewed non-experts as experts.

There must be different root causes for the observed limitations in knowledge and misconceptions about threat modeling

around VPNs and security. We conjecture that there is a multitude of factors leading to the observed behavior. Computer security has become a complex issue, preventing individuals from attaining a general end-to-end understanding of *all* facets of security. The credentials and certifications held by our experts may only test person compliance with a certain perspective on security, e.g., in the case of ISO27001 on information security management. Furthermore, not only since Snowden the capabilities of state threat actors seem to be limitless, casting doubt and fear even among experts, e.g., see Expert 3 in Section 3.2. Finally, the industry sees 'groundbreaking' vulnerabilities nearly every other day—often partially overhyped with a logo and accompanying social media campaign—casting further fear, uncertainty, and doubt.

However, as we did not aim to investigate the specific issue of experts' knowledge not matching their certified expertise, our data does not hold sufficient explanatory value for making causal claims in this regard. Still, the observed issue is alarming and might have widespread implications for society at large. Hence, we strongly suggest investigating this issue with a targeted explanatory study in future work.

5.5 Recommendations for Practitioners

We argue that operators can significantly improve the efficacy of existing VPN infrastructure by improving their corporate policies, risk communication, and training efforts:

- **VPN Automation:** users reported uncertainty about when to use a VPN; still, they usually internalized the process of using the VPN. We hence recommend improving further the process of using a corporate VPN, so it becomes *invisible* and the *default* for users.
- **Privacy Communication:** experts were concerned about the privacy implications of using a corporate VPN. Corporations should hence find a privacy policy that accommodates a degree of private VPN uses and actively communicate this to their employees. An intrusion detection system configured to ignore specific traffic via the VPN may be better than an intrusion detection system missing important threats because the user turned the VPN off to browse, for example, Facebook.
- **Device Management:** especially expert users found VPNs to be an integral part of device management and policy/compliance enforcement. Given the increasing work-from-home situation the white-collar world finds itself in, we suggest investigating adjusting device management solutions to securely work even without a VPN.
- **Technical Training:** risk communication should focus on what people need to know, and the mental model approach can help facilitate such a design [23]. We find that even non-experts in general *do* have a basic understanding of *how* VPNs work. Following the work of Demjaha et al., we hence suggest utilizing the tunnel metaphor commonly used by participants to make training more accessible [19]. In line with our observations on experts' knowledge, following work by Wash and Cooper, we also recommend focusing the training on story-based peer interactions to improve training outcomes [68].

Finally, we emphasize the importance of IT operators considering users' perspectives and needs, e.g., in terms of clearly communicating the impact of security technologies when deploying mitigations. For example, in our case, several participants reported uncertainty about *when* a VPN should or must be used, see Section 3.1, which could be improved upon.

5.6 Further Research Directions:

While we found a generally similar understanding of threats and mitigations—among experts and non-experts—our results are not directly transferable to end-user VPNs. Especially the privacy concerns noted by experts in our study are of significantly higher relevance in the context of privately used VPNs, see Khan et al. [34]. Users seem to have an imbalanced trust relationship with their local Internet Service Providers (ISPs), while they tend to trust commercial VPN providers more—often unjustly [34]. We hence argue that the trust interdependence between end-users and their local ISPs should be investigated in future studies. Such studies can leverage the mental model we constructed for non-experts to create appropriate interview scripts to explore this trust relationship and how it interacts with the perceived threat landscape.

Furthermore, we suggest studying the use of VPNs—in a corporate as well as a private context—quantitatively to obtain a more general perspective, also spanning different cultural dimensions. Our mental model provides the necessary foundation for such studies to design appropriate questionnaires. Similarly, our mental model can serve as the basis for more controlled studies regarding VPN use, i.e., assessments of the efficacy of the interventions we outlined for practitioners.

Finally, our findings regarding limitations in (certified) experts' knowledge require further research to explain better and quantify these issues.

5.7 Limitations

As qualitative research [6, 11], our work has limitations. Hence, we document these limitations and describe how we reduced their impact, so readers can appropriately contextualize our results. Our study's scope revolves around VPN use in a professional context, where the population is familiar with a specific type of VPN, see Section 2.4. Hence, our results should not be directly transferred to end users' use of VPN software in a non-professional setting or professional use of other VPN technologies. Furthermore, our sample population has been recruited from a single consulting services firm with global operations. As such, the company culture and branch office location in the Netherlands, i.e., cultural environment,

may have impacted our results. Hence, we encourage independent reproduction of our results in other countries.

Our results might be influenced by the work-from-home reality due to the COVID-19 pandemic: Currently, VPN usage is mandatory for corporate users who mostly work remotely.

Our study may suffer from a self-reporting or social desirability bias as we rely on self-reported information. Moreover, as participants volunteered to participate, we may suffer from a self-selection bias, especially among non-experts. We are confident that the impact of this factor is limited due to our sample size and reached theoretical saturation.

The participants were not necessarily familiar with the video conferencing platform and drawing tools used. To counter this, we provided them with a test room to try out the available features before the meeting. Furthermore, we introduced the capabilities of the drawing tools before each interview. We did not collect video from all participants for privacy reasons. Hence, we might have missed some relevant facial expressions for participants opting out of sharing their video. On the other hand, disabling the video link ensures that participants were not biased by the researcher's facial expressions or body language.

6 Related Work

In this section, we compare our work with related studies that either i) compare mental models of experts and non-experts for security and privacy-related topics or ii) investigate the adoption of VPN technology.

Mental Models for Security and Privacy: In order to understand how and why users interact with complex security technology, researchers from usable security and HCI start to leverage users' mental models more frequently to understand human decision-making [33, 60]. We cluster the related work in three broad categories:

i) Mental models of a security-*technology* [1–3, 20, 25, 32, 36, 38, 55, 62, 70]
ii) Mental models of security and privacy best practices (prescriptive knowledge) [4, 5, 9, 40, 49, 50, 67, 69]
iii) Mental models of software development and end users' *practices* (descriptive) [51, 64, 65]

Common examples for the first group are, e.g., Krombholz et al.investigating users' understanding of HTTPS [36], Abu-Salma et al.'s work on secure communication tools [2, 3], and mental models of Tor by Gallagher et al. [25]. Based on our scope, our work follows the approach of these earlier papers. However, while, e.g., Krombholz et al.and Gallagher et al.found experts' and non-experts' mental models to be fundamentally different, we found that the mental models of experts and non-experts for VPNs are fundamentally aligned but diverge on threat and mitigation assessment.

An example from the second group is Asgharpour et al. [5] who quantitatively examine five risk mental models around security risks using a card-sorting methodology on a population of 33 experts and 76 non-experts. Similar to us, they found that risk perception and mental models thereof diverge between experts and non-experts. This finding aligns with ours, where we found general alignment in the basic concepts around VPN technology but diverging mental models concerning the threat environment.

An example for the third category is Votipka et al., who conduct an *observational* study on reverse engineers' work processes. As our study relies on self-reported data, instead of using an observational methodology, our results can not be directly compared to findings from observational studies.

Studies of VPN Adoption: Studies on VPN adoption usually focus on end-user VPNs. Sombatruang et al. [61] studied attributes affecting VPN adoption in the UK ($N = 15$) and Japan ($N = 17$). They found security and privacy considerations to be secondary concerns when users choose a VPN service. Instead, users focus on app review ratings, the price, and recommendations—see also Redmiles et al. [52, 53]—for choosing a service. This aligns with our observation that, e.g., corporate policy and integration into the workflow play a major role in corporate VPN usage.

Namara et al. [45] surveyed 90 end-users already using public VPNs on their usage patterns in the context of the Technology Acceptance Model [18] in combination with the risk-as-feeling theory [37] to investigate emotional and practical aspects of VPN adoption. While this study again focuses on public VPNs, their results are comparable insofar that we also observe a connection between *perceived* risks not necessarily rooted in facts, i.e., fears, and users reported behavior around using VPNs.

7 Conclusion

We find that—in general—the mental models of VPNs between experts and non-experts are similar. Naturally, experts exhibit a deeper understanding of the underlying technology and specific configuration of that technology within the corporations' infrastructure. As the threat modelling aspects of our participants' mental models depend on the depth of their technical understanding, these differences—experts mental models being a superset of non-experts'— can also be found for users' threat modeling. This point is supported by the diverse views our experts have regarding network monitoring enabled by VPNs: While they *do* see it as a new threat, they *also* recognize it as an important feature *mitigating* threats. Nevertheless, both experts and non-experts partially hold inaccurate assumptions of a corporate VPN effect on the threat landscape. These inaccuracies do reflect on participants' threat assessment—partially leading to them overestimating risks introduced by VPNs—and should be addressed appropriately. Based on our findings, we drafted guidelines for improving training, communication, and deployment processes around corporate VPNs, see Section 5.5.

Data Availability: The data consisting of the summarized demographic information, anonymized transcriptions, and anonymized drawings are accessible in the 4TU.Centre for Research Data for a minimum period of 10 years [8].

Acknowledgements: This material is based on research supported by the European Commission (EC) under grant CyberSecurity4Europe (#830929), and the Nederlandse Organisatie voor Wetenschappelijk Onderzoek (Dutch Research Council, NWO) under grants RAPID (CS.007) and INTERSECT (NWA.1160.18.301).

Any views, opinions, findings, recommendations, or conclusions contained or expressed herein are those of the authors and do not necessarily reflect the position, official policies, or endorsements, either expressed or implied of their host institutions, or those of the EC, or NWO.

References

[1] Noura Abdi, Jose M. Such, and Kopo 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 (SOUPS)*. 2019, pp. 451–466.

[2] Ruba Abu-Salma, Elissa M Redmiles, Blase Ur, and Miranda Wei. "Exploring User Mental Models of End-to-End Encrypted Communication Tools". In: *Proceedings of the 8th USENIX Workshop on Free and Open Communications on the Internet (FOCI)*. 2018.

[3] Ruba Abu-Salma, M. Angela Sasse, Joseph Bonneau, Anastasia Danilova, Alena Naiakshina, and Matthew Smith. "Obstacles to the Adoption of Secure Communication Tools". In: *Proceedings of the 38th IEEE Symposium on Security & Privacy (S&P)*. 2017, pp. 137–153.

[4] Bilal Al Sabbagh and Stewart Kowalski. "Developing social metrics for security modeling the security culture of it workers individuals (case study)". In: *Proceedings of the 5th International Conference on Communications, Computers and Applications (MIC-CCA)*. IEEE. 2012, pp. 112–118.

[5] Farzaneh Asgharpour, Debin Liu, and L. Jean Camp. "Mental Models of Security Risks". In: *Proceedings of the 12th International Workshop on Usable Security (USEC)*. 1st ed. Vol. 4886. Lecture Notes in Computer Science. 2007, pp. 367–377. URL: http://link.springer.com/10.1007/978-3-540-77366-5%7B%5C_%7D34.

[6] Rosaline S Barbour. "Quality of Data Analysis". In: *The SAGE Handbook of Qualitative Data Analysis*. 2014, pp. 496–510.

[7] Veroniek Binkhorst. *Improving Cyber Risk Communication: Mental Models of VPN in a professional services firm in the Netherlands*. Tech. rep. 2020. URL: https://repository.tudelft.nl/islandora/object/uuid%3Ac92f8e21-d935-4406-ae89-6cb7abb74f4a.

[8] Veroniek Binkhorst, Tobias Fiebig, Katharina Krombholz, Wolter Pieters, and Kate Labunets. *Data underlying the research of VPN Mental Models Among Experts and Non-Experts in a Corporate Context*. Dec. 2021. URL: https://doi.org/10.4121/17118491.v1.

[9] Cristian Bravo-Lillo, Lorrie Faith Cranor, Julie Downs, and Saranga Komanduri. "Bridging the gap in computer security warnings: A mental model approach". In: *IEEE Security & Privacy* 9.2 (2011), pp. 18–26. URL: https://ieeexplore-ieee-org.tudelft.idm.oclc.org/abstract/document/5669245.

[10] Mark de Bruijne, Michel van Eeten, Carlos Gañán, and Wolter Pieters. *Towards a new cyber threat actor typology*. Tech. rep. 2017. URL: https://www.wodc.nl/onderzoeksdatabase/2740-categorisering-en-motieven-cyberactoren.aspx.

[11] Alan Bryman. *Social Research Methods*. 4th ed. Oxford University Press, 2012.

[12] Erik Brynjolfsson, John J Horton, Adam Ozimek, Daniel Rock, Garima Sharma, and Hong-Yi TuYe. *COVID-19 and remote work: an early look at US data*. Tech. rep. National Bureau of Economic Research, 2020.

[13] Terry Anthony Byrd, Kathy L. Cossick, and Robert W. Zmud. "A synthesis of research on requirements analysis and knowledge acquisition techniques". In: *MIS Quarterly* 16 (1 1992), pp. 117–138.

[14] Tim Casey. *Understanding Cyberthreat Motivations to Improve Defense*. Tech. rep. 2015. URL: https://www.intel.com/content/dam/www/public/us/en/documents/white-papers/understanding-cyberthreat-motivations-to-improve-defense-paper.pdf.

[15] Timothy Casey. *Threat Agent Library Helps Identify Information Security Risks*. Tech. rep. 2007. URL: https://www.researchgate.net/publication/324091298%7B%5C_%7DThreat%7B%5C_%7DAgent%7B%5C_%7DLibrary%7B%5C_%7DHelps%7B%5C_%7DIdentify%7B%5C_%7DInformation%7B%5C_%7DSecurity%7B%5C_%7DRisks.

[16] Juliet Corbin and Anselm Strauss. "Grounded theory research: Procedures, canons, and evaluative criteria". In: *Qualitative Sociology* 13.1 (1990), pp. 3–21. URL: http://link.springer.com/10.1007/BF00988593.

[17] Juliet Corbin and Anselm Strauss. *Basics of Qualitative Research: Techniques and Procedures for Developing Grounded Theory*. 3rd ed. SAGE, 2008.

[18] Fred D Davis. "A Technology Acceptance Model for Empirically Testing New End-user Information Systems: Theory and Results". PhD thesis. Massachusetts Institute of Technology, 1985.

[19] Albese Demjaha, Jonathan M Spring, Ingolf Becker, Simon Parkin, and M Angela Sasse. "Metaphors considered harmful? An exploratory study of the effectiveness of functional metaphors for end-to-end encryption". In: *Proc. USEC*. Internet Society. 2018.

[20] Constanze Dietrich, Katharina Krombholz, Kevin Borgolte, and Tobias Fiebig. "Investigating system operators' perspective on security misconfigurations". In: *Proceedings of the 25th ACM SIGSAC Conference on Computer and Communications Security (CCS)*. 2018, pp. 1272–1289.

[21] K. Egevang and P. Francis. *The IP Network Address Translator (NAT)*. RFC 1631. IETF, May 1994. URL: http://tools.ietf.org/rfc/rfc1631.txt.

[22] Anja Feldmann, Oliver Gasser, Franziska Lichtblau, Enric Pujol, Ingmar Poese, Christoph Dietzel, Daniel Wagner, Matthias Wichtlhuber, Juan Tapiador, Narseo Vallina-Rodriguez, et al. "The Lockdown Effect: Implications of the COVID-19 Pandemic on Internet Traffic". In: *Proceedings of the 20th Internet Measurement Conference (IMC)*. 2020, pp. 1–18.

[23] Baruch Fischhoff. "Risk Perception and Communication Unplugged: Twenty Years of Process". In: *Risk Analysis* 15.2 (1995), pp. 137–145. URL: http://doi.wiley.com/10.1111/j.1539-6924.1995.tb00308.x.

[24] Marsha E. Fonteyn, Benjamin Kuipers, and Susan J. Grobe. "A Description of Think Aloud Method and Protocol Analysis". In: *Qualitative Health Research* 3 (4 1993), pp. 430–441. URL: http://journals.sagepub.com/doi/10.1177/104973239300300403.

[25] Kevin Gallagher, Sameer Patil, and Nasir Memon. "New Me: Understanding Expert and Non-Expert Perceptions and Usage of the Tor Anonymity Network". In: *Proceedings of the 13th Symposium On Usable Privacy and Security (SOUPS)*. 2017.

[26] Nelly Ghaoui. *Policy strategies for VPN for consumers in the Netherlands*. Tech. rep. 2016. URL: https://studentntheses.universiteitleiden.nl/access/item%3A2666258/view.

[27] Devon Greyson, Heather O'Brien, and Jean Shoveller. "Information world mapping: A participatory arts-based elicitation method for information behavior interviews". In: *Library & Information Science Research* 39.2 (2017), pp. 149–157.

[28] Jassim Happa and Graham Fairclough. "A Model to Facilitate Discussions About Cyber Attacks". In: *Ethics and Policies for Cyber Operations*. 2017, pp. 169–185.

[29] International Organization for Standardization. *ISO 3100:2018*. 2018. URL: https://www.iso.org/obp/ui/%7B%5C#%7Diso:std:iso:31000:ed-2:v1:en:term:3.1 (visited on 10/05/2020).

[30] Natalie A. Jones, Helen Ross, Timothy Lynam, Pascal Perez, and Anne Leitch. "Mental models: An interdisciplinary synthesis of theory and methods". In: *Ecology and Society* 16.1 (2011). URL: http://ro.uow.edu.au/smartpapers/81.

[31] Juniper Networks. *Juniper Remote Access VPNs with NCP Exclusive Remote Access Client*. 2021. URL: https://www.juniper.net/documentation/us/en/software/junos/vpn-ipsec/topics/topic-map/security-remote-access-vpns-with-ncp-exclusive-remote-access-client.html (visited on 12/21/2021).

[32] Ruogu Kang, Laura Dabbsih, Nathaniel Fruchter, and Sarah Kiesler. ""My Data Just Goes Everywhere:" User Mental Models of the Internet and Implications for Privacy and Security". In: *Proceedings of the 11th Symposium On Usable Privacy and Security (SOUPS)*. 2015, pp. 39–52.

[33] Mannat Kaur, Michel van Eeten, Marijn Janssen, Kevin Borgolte, and Tobias Fiebig. "Human Factors in Security Research: Lessons Learned from 2008-2018". In: *arXiv preprint arXiv:2103.13287* (2021).

[34] Mohammad Taha Khan, Joe DeBlasio, Geoffrey M Voelker, Alex C Snoeren, Chris Kanich, and Narseo Vallina-Rodriguez. "An empirical analysis of the commercial VPN ecosystem". In: *Proceedings of the 18th Internet Measurement Conference (IMC)*. 2018, pp. 443–456.

[35] Klaus Krippendorff. *Content Analysis: An Introduction to Its Methodology*. 2nd ed. SAGE, 2004.

[36] Katharina Krombholz, Karoline Busse, Katharina Pfeffer, Matthew Smith, and Emanuel von Zezschwitz. ""If HTTPS Were Secure, I Wouldn't Need 2FA" - End User and Administrator Mental Models of HTTPS". In: *Proceedings of the 40th IEEE Symposium on Security & Privacy (S&P)*. 2019, pp. 246–263.

[37] George F Loewenstein, Elke U Weber, Christopher K Hsee, and Ned Welch. "Risk as feelings". In: *Psychological bulletin* 127.2 (Mar. 2001), pp. 267–286.

[38] Alexandra Mai, Katharina Pfeffer, Matthias Gusenbauer, Edgar Weippl, and Katharina Krombholz. "User Mental Models of Cryptocurrency Systems-A Grounded Theory Approach". In: *Proceedings of the 16th Symposium On Usable Privacy and Security (SOUPS)*. 2020.

[39] Janosch Maier, Arne Padmos, Mortaza S Bargh, and Wolfgang Wörndl. "Influence of Mental Models on the Design of Cyber Security Dashboards." In: *Proceedings of the 12th International Conference on Communications, Computers and Applications (MIC-CCA)*. 2017, pp. 128–139.

[40] Heike Märki, Miriam Maas, Michaela Kauer-Franz, and Marius Oberle. "Increasing software security by using mental models". In: *Advances in Intelligent Systems and Computing*. 2016, pp. 347–359.

[41] Allison McDonald, Matthew Bernhard, Luke Valenta, Benjamin VanderSloot, Will Scott, Nick Sullivan, J Alex Halderman, and Roya Ensafi. "403 Forbidden: A Global View of CDN Geoblocking". In: *Proceedings of the 18th Internet Measurement Conference (IMC)*. 2018, pp. 218–230.

[42] MITRE ATT&CK. *Enterprise Tactics*. URL: https://attack.mitre.org/tactics/enterprise/ (visited on 09/11/2020).

[43] Maria D Molina, Andrew Gambino, and S Shyam Sundar. "Online Privacy in Public Places: How do Location, Terms and Conditions and VPN Influence Disclosure?" In: *Proceedings of the 2019 ACM SIGCHI Conference on Human Factors in Computing Systems (CHI)*. 2019, pp. 1–6.

[44] M. Granger Morgan, Baruch Fischhoff, Ann Bostrom, and Cynthia J Atman. *Risk Communication: A Mental Models Approach*. Cambridge University Press, 2002.

[45] Moses Namara, Daricia Wilkinson, Kelly Caine, and Bart P Knijnenburg. "Emotional and Practical Considerations Towards the Adoption and Abandonment of VPNs as a Privacy-Enhancing Technology". In: *Proceedings of the 20th Privacy Enhancing Technologies Symposium (PETS)*. 2020, pp. 83–102.

[46] National Coordinator for Security and Counterterrorism. *Nederlandse Cybersecurity Agenda*. Tech. rep. 2019. URL: https://www.nctv.nl/onderwerpen/ncsa/documenten/publicaties/2018/04/21/nederlandse-cybersecurity-agenda.

[47] Daiyuu Nobori and Yasushi Shinjo. "VPN Gate: A Volunteer-Organized Public VPN Relay System with Blocking Resistance for Bypassing Government Censorship Firewalls". In: *Proceedings of the 11th USENIX Symposium on Networked Systems Design and Implementation (NDSI)*. 2014, pp. 229–241.

[48] Nord VPN. *All you need to know: TLS vs. SSL*. 2021. URL: https://nordvpn.com/blog/tls-vs-ssl/ (visited on 07/23/2021).

[49] Maggie Oates, Yama Ahmadullah, Abigail Marsh, Chelse Swoopes, Shikun Zhang, Rebecca Balebako, and Lorrie Faith Cranor. "Turtles, Locks, and Bathrooms: Understanding Mental Models of Privacy Through Illustration". In: *Proceedings of the 18th Privacy Enhancing Technologies Symposium (PETS)*. 4. 2018, pp. 5–32.

[50] Celeste Lyn Paul and Kirsten Whitley. "A taxonomy of cyber awareness questions for the user-centered design of cyber situation awareness". In: *Proceedings of the 1st International Conference on Human Aspects of Information Security, Privacy and Trust (HAS)*. 1st ed. 2013, pp. 145–154.

[51] Kopo Marvin Ramokapane, Awais Rashid, and Jose Miguel 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 (SOUPS)*. 2017, pp. 241–256.

[52] Elissa M Redmiles, Sean Kross, and Michelle L Mazurek. "How I Learned to Be Secure: A Census-Representative Survey of Security Advice Sources and Behavior". In: *Proceedings of the 23rd ACM SIGSAC Conference on Computer and Communications Security (CCS)*. 2016, pp. 666–677.

[53] Elissa M Redmiles, Amelia R Malone, and Michelle L Mazurek. "I Think They're Trying to Tell Me Something: Advice Sources and Selection for Digital Security". In: *Proceedings of the 37th IEEE Symposium on Security & Privacy (S&P)*. IEEE. 2016, pp. 272–288.

[54] Y. Rekhter, B. Moskowitz, D. Karrenberg, G. J. de Groot, and E. Lear. *Address Allocation for Private Internets*. RFC 1918. IETF, Feb. 1996. URL: http://tools.ietf.org/rfc/rfc1918.txt.

[55] Karen Renaud, Melanie Volkamer, and Arne Renkema-Padmos. "Why doesn't Jane protect her privacy?" In: *Proceedings of the 14th Privacy Enhancing Technologies Symposium (PETS)*. 2014, pp. 244–262.

[56] A. Retana, R. White, V. Fuller, and D. McPherson. *Using 31-Bit Prefixes on IPv4 Point-to-Point Links*. RFC 3021. IETF, Dec. 2000. URL: http://tools.ietf.org/rfc/rfc3021.txt.

[57] Bernd Rohrmann. "The evaluation of risk communication effectiveness". In: *Acta Psychologica* 81.2 (1992), pp. 169–192. URL: https://www.sciencedirect.com/science/article/pii/000169189290004W.

[58] Johnny Saldaña. *The Coding Manual for Qualitative Researchers*. SAGE, 2016.

[59] Liz Sanders and Pieter Jan Stappers. *Convivial Toolbox*. BIS Publishers B.V., 2012.

[60] Martina-Angela Sasse. "How to T(R)AP Users' Mental Models". In: *Human Factors in Information Technology*. Vol. 2. Feb. 12, 1991, p. 572.

[61] Nissy Sombatruang, Tan Omiya, Daisuke Miyamoto, M Angela Sasse, Youki Kadobayashi, and Michelle Baddeley. "Attributes affecting user decision to adopt a Virtual Private Network (VPN) app". In: *Proceedings of the 22nd International Conference on Information and Communications Security (ICICS)*. 2020, pp. 223–242.

[62] Eric Spero, Milica Stojmenovic, Zahra Hassanzadeh, Sonia Chiasson, and Robert Biddle. "Mixed Pictures: Mental Models of Malware". In:

Proceedings of the 17th International Conference on Privacy, Security and Trust (PST). 2019.

[63] Anselm Strauss and Juliet Corbin. *Basics of Qualitative Research: Techniques and Procedures for Developing Grounded Theory*. 2nd ed. SAGE, 1998.

[64] K. Vaniea, E. Rader, and R. Wash. "Mental models of software updates". In: *International Communication Association* (2014), pp. 1–39. URL: https://scholar.google.com/scholar?cluster=9993021985847634727.

[65] Daniel Votipka, Seth Rabin, Kristopher Micinski, Jeffrey S Foster, and Michelle L Mazurek. "An Observational Investigation of Reverse Engineers' Processes". In: *Proceedings of the 29th USENIX Security Symposium (USENIX Security)*. 2020, pp. 1875–1892.

[66] Zhongjie Wang, Yue Cao, Zhiyun Qian, Chengyu Song, and Srikanth V Krishnamurthy. "Your State is Not Mine: A Closer Look at Evading Stateful Internet Censorship". In: *Proceedings of the 17th Internet Measurement Conference (IMC)*. 2017, pp. 114–127.

[67] Rick Wash. "Folk models of home computer security". In: *Proceedings of the 6th Symposium On Usable Privacy and Security (SOUPS)*. 2010, pp. 1–16.

[68] Rick Wash and Molly M Cooper. "Who provides phishing training? facts, stories, and people like me". In: *Proceedings of the 2018 ACM SIGCHI Conference on Human Factors in Computing Systems (CHI)*. 2018.

[69] Rick Wash and Emilee 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 (SOUPS)*. 2015, pp. 309–325.

[70] Justin Wu and Daniel Zappala. "When is a Tree Really a Truck? Exploring Mental Models of Encryption". In: *Proceedings of the 14th Symposium On Usable Privacy and Security (SOUPS)*. 2018, pp. 395–409.

A Interview Protocol

This appendix contains the interview protocol in English. At the beginning of the interview, a short introduction was provided. The native language version of the interview protocol can be found in the thesis report [7].

A.1 Interview Introduction

The aim of this research is to determine the differences between experts and non-experts in their perception of VPN. The focus is on the VPN in [the professional services firm]. In this interview, I will ask you some questions, and the intention is that you tell as much as possible about what you know about VPN. I would like to emphasize that there are no right and wrong answers, so tell everything you can think of. During the interview I will ask you to make a drawing based on an assignment. I ask you to think out loud as much as possible while making this drawing. For the drawing we will use the whiteboard in Big Blue Button. I will now show the whiteboard and briefly explain how it works. <Show the whiteboard and give a brief overview of the possibilities>. I would like to inform you again that this interview will be recorded. The recording will be used to transcribe the interview and will not be viewed by anyone outside the research group. I have sent you a consent form by e-mail, have you been able to read this and do you have any questions about this? Do you have any other questions before we start the interview?

A.2 Interview Structure

The complete overview is presented in Table A.1. First, a general question was asked (A), after which each topic mentioned was asked to elaborate. Continuation to the next section (B, C, or D) happened when either no new topics came up in the current section or when an interviewee naturally continued to a new section. When an interviewee continued to a new section, the interviewer let the interviewee continue and revisited the previous section when appropriate.

A Starting question

1. What is a 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>.

C Questions how VPN works (not necessarily in this order)

1. Why do you use VPN?
   - When?
   - 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
   - Basis scenario: Make a VPN connection at home
   - Second scenario (different location): Make a VPN connection at a coffee bar
   - Third scenario (specific task): Send an e-mail with an active VPN connection

D Questions changes in threat landscape

1. What is the influence of a VPN connection on your computer security?
   - Why?
   - How?
   - In drawing: draw influence in previous drawing.
2. What kinds of digital threats do you deal with on a normal day?
   - How does the threat change because of the VPN connection?
3. What kinds of social threats do you deal with on a normal day?
   - How does the kind of attacker change because of the VPN connection?
   - What would be an attacker's intention?
   - What would be an attacker's capability?
4. What could be the impact of an attack?
   - Why?
   - How?

   Vulnerabilities of VPN
5. How secure is a VPN connection?
6. If not 100% secure:
   - Why?
   - In drawing: draw where it is not secure and the cause
   - How do your actions change because of this?
   - What are the consequences of these insecurities?

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 . . . ?

B Informed Consent Form

Dear <name>,

In this e-mail I send you the consent form for the interview upcoming <day>. In this consent form you will find more information regarding the study and you can find to what you agree by participating in the study. Giving consent can by replying on this e-mail, stating that you give consent. If you have any questions regarding the interview or the consent form, you can e-mail me or ask the questions at the beginning of the interview.

Information regarding the study, data processing, and questions.

1. Background and aims of the study
The purpose of this research is to determine the similarities and differences between experts and non-experts of their perception of VPN in a professional services firm in the Netherlands. This study aims at empirically investigating the perception of experts and non-experts on: 1) What a VPN is, 2) For what purpose a VPN is used, 3) What the technical infrastructure of a VPN looks like, 3) What the security benefits and/or risks of using a VPN are, 4) What changes occur in the threat landscape when using a VPN, and 5) What the impact of a possible attack could be when using VPN.

2. Do I have to participate?
You can ask questions about the study before deciding whether or not to participate. If you do agree to participate, you may withdraw yourself from the study at any time, without giving a reason and without penalty, by informing the researchers of this decision.

3. What will happen in the study?
If you agree to take part in the study, you will be asked to participate in an approximately 60 minute semi-structured interview in English or your native language. The researcher will conduct the interview by using the conferencing software Big Blue Button. As part of the interview a drawing task will be completed using the whiteboard in the Big Blue Button. The interview will be recorded, and transcribed to text after the interview has taken place. The recording consists of audio, and video if the participants chooses to enable video.

4. Are there any potential risks in taking part?
Interviews will be held with employees in a professional services firm on their beliefs of how a VPN works. The knowledge of participants may be different than expected from experts and/or non-experts. We aim to address such concerns by:

a. Storing e-mail addresses, the recordings of the interviews, demographic information, and a pdf file of the consent e-mail securely.
b. Anonymizing the transcriptions.
c. Summarizing demographic information.
d. Deleting the original e-mail from the e-mail inbox.
e. Destroying the collected e-mail addresses, recordings, original demographic data, and pdf file of the consent e-mails after the end of the study.

5. Are there any benefits in taking part? There are no benefits involved for the participants of the study.

6. What happens to the data provided? We will securely store all collected data at the [company] laptop of the researcher. A back-up of the collected data will be securely stored on [private cloud service used by the university]. Nobody except the project research team will have access to the data during the study period. The collected e-mail address, recording of the interview, original demographic data, and pdf file of the consent e-mail will be destroyed after the end of the study.

At no point will we ask for your name except to confirm your consent. Consent will be confirmed by replying in an e-mail stating the participant gives consent. We will ask for the participant's educational qualifications, education area, role in the firm, and years active in the firm. As this can be used to identify certain individuals, we will treat this as personal data and store it securely. The answers on the questions regarding personal data will not be published per individual participant, but will be presented in the study results in a summarized matter.

The participant has the right to request access to and rectification or erasure of personal data.

The anonymized transcription, drawings made during the interview, and summarized demographic data will be shared in products of the study and in will be stored on the [public research data repository] for a minimum retention period of 10 years after publication or public release of the work of the research.

We ask participants for their permission to use direct quotes, these will be attributed to a participant number.

7. Will the research be published?
The results will contribute to the completion of a master's thesis project and a paper submitted to an academic venue. To protect the participants' anonymity we will anonymize all information relating to the participants and the employer of the participants.

8. Who has reviewed this study?
This study has been reviewed by, and received ethics clearance through, the Delft University of Technology Human Research Ethics Committee (reference number: 55223).

9. Who do I contact if I have a concern about the study or I wish to file a complaint?
If you have a concern about any aspect of this study, please speak to the relevant researcher [first author], who will do their best to answer your query. The researcher should acknowledge your concern within 10 working days and give you an indication of how they intend to deal with it. If you remain unhappy or wish to make a formal complaint, please contact the relevant chair of the Human Research Ethics Committee at the [University] who will seek to resolve the matter in a reasonably expeditious manner:

Chair, Human Research Ethics Committee; Email: HREC@tudelft.nl.

10. Contact details
If you would like to discuss the research with someone beforehand (or if you have questions afterwards), please contact:

[First Author]
Email: [First Author's email]

Consent Form

Taking part in the study
I have read and understood the study information dated <date>, or it has been read to me. I have been able to ask questions about the study and my questions have been answered to my satisfaction.
I consent voluntarily to be a participant in this study and understand that I can refuse to answer questions and I can withdraw from the study at any time, without having to give a reason.
I understand that taking part in the study involves participating in an audio recorded interview. I understand that if I decide to enable video during the interview this will also be recorded. I understand that part of the interview includes a drawing task. I understand that the recorded interview will be transcribed as text and anonymized and the recording will be destroyed after the end of the study.

Use of the information in the study
I understand that information I provide will be used for a master thesis report and publications in academic venues (like conferences or journals).
I understand that personal information collected about me that can identify me, such as my name or email address, will not be shared beyond the study team.
I agree that my information can be quoted in research outputs.
I agree to joint copyright of the drawings created during the interview to [First Author].

Future use and reuse of the information by others
I give permission for the anonymized interview transcript, drawings made during the interview, and summarized demographic information that I provide to be archived in the 4TU.Centre for Research Data so it can be used for future research and learning.

I look forward to your reply,

Kind regards,

[First Author]

C Codebook

Table 2: Final codebook used during the qualitative analysis.

The table reports the codebook developed in our study. For each code we report how often it occurred (Total) and how many participants mentioned the code during their interviews at all (Part.)

Code	Experts ($N=11$) Total	Experts ($N=11$) Part.	Non-Exp. ($N=7$) Total	Non-Exp. ($N=7$) Part.
A. Reason for use				
A.1. Access internal network	34	11	14	7
A.2. Internal network: accessible w/o VPN connection	2	1	-	-
A.3. Internal network: impossible to directly connect	16	9	8	4
A.4. Mobile network used instead of unsecured network	8	5	-	-
A.5. Not necessary when in office	8	5	-	-
A.6. Not used when using mobile network	1	1	-	-
A.7. Secure communication	3	1	3	1
A.8. Secure connection	13	9	3	2
A.9. Security purpose general	3	3	2	2
A.10. Use unsecured network if mobile network is expensive	1	1	-	-
A.11. Used when using mobile network	5	3	-	-
A.12. Used when using unsecured network	7	6	3	3
A.13. Virtual Private Network	7	6	2	2
B. Device				
B.1. Mobile	9	6	5	4
B.2. Personal computer	12	11	10	7
B.3. Tablet	2	2	1	1
C. User actions to establish a connection				
C.1. Access token	12	7	-	-
C.2. Access token: hardware token	15	10	7	6
C.3. Access token: software token	19	10	9	6
C.4. Click connect to VPN	3	3	4	3
C.5. Connect to Internet	6	5	2	2
C.6. Enter code access token	13	10	8	7
C.7. Enter password	13	10	8	6
C.8. Enter username	8	7	-	-
C.9. Launch VPN software	7	7	9	7
D. Basic configuration				
D.1. Authentication	15	8	5	3
D.2. Authentication by server	10	4	-	-
D.3. External server can function for only authorisation	3	2	-	-
D.4. Internal network	35	9	9	5
D.5. Internal network: uses allowlist for access management	2	2	-	-
D.6. Internet	54	10	11	5
D.7. Internet service provider	4	3	4	1
D.8. IP address	10	6	-	-
D.9. IP used to identify endpoint	9	5	-	-
D.10. Make connection	7	3	9	5
D.11. Make connection with server	24	9	1	1
D.12. Server	45	7	11	4
D.13. Server: in demilitarized zone	1	1	-	-
D.14. Server: inside corporate network	6	3	-	-
D.15. Server: outside corporate network	4	2	-	-
D.16. Webtraffic is routed through server	24	7	2	1
E. Additional specifications				
E.1. Internal network segmentation	7	2	-	-
E.2. One company can have multiple VPN providers	1	1	-	-
E.3. Own VPN provider	4	2	1	1
E.4. Third party is VPN provider	13	4	1	1
E.5. VPN complete or split	5	2	-	-
E.6. VPN provider	4	2	-	-
F. Secured connection				
F.1. Data is send to receiving point (RP) decrypted	6	4	-	-
F.2. Data is send to RP encrypted	5	5	3	1
F.3. Encryption	37	8	9	4
F.4. Firewall can decrypt communication	1	1	-	-
F.5. Private IP for VPN server	4	1	-	-
F.6. Private IP is only known by VPN server and endpoint	1	1	-	-
F.7. Is encrypted between own device and VPN server	10	6	1	1
F.8. Load balancer can decrypt comm.	2	1	-	-
F.9. Protocol	11	4	-	-
F.10. Secured connection	41	11	7	4
F.11. VPN filters traffic	20	5	-	-
F.12. VPN includes antivirus	5	1	-	-
G. Metaphors				
G.1. Tunnel	29	8	9	1
G.2. Shield	3	3	-	-
H. Threats mitigated				
H.1. Block you from accessing a website	13	3	-	-
H.2. Does not mitigate all computer security threats	18	8	2	1
H.3. Listening in on communication	15	8	12	4
H.4. Masks IP	22	7	2	2
H.5. More difficult for threat actor	8	6	6	4
H.6. No access to files when access to device	4	4	2	2
H.7. Single point of attack from webtraffic threats	4	2	-	-
H.8. Stop malicious software	15	3	-	-
H.9. Updates pushed	1	1	-	-
I. Change in user behavior				
I.1. Do not use VPN for private matters	2	2	-	-
I.2. Does not change	3	3	2	2
I.3. Only use VPN when necessary	2	2	-	-
I.4. Prevent access by other persons	2	2	-	-
I.5. Separate devices for work and private use	2	2	-	-
J. New threats due to VPN				
J.1. Access to device while VPN is connected	8	3	2	2
J.2. Authentication measures	5	3	3	2
J.3. Hacking	18	8	5	3
J.4. Listening in on communication	1	1	1	1
J.5. Malfunction	1	1	-	-
J.6. Malicious traffic can go through sec. layer	2	1	-	-
J.7. More suspicious for state actor	2	1	-	-
J.8. Server is compromised	11	5	1	1
J.9. Trace back IP	1	1	-	-
J.10. Use VPN when using unsecured network	2	1	1	1
J.11. VPN provider	10	3	2	2