Researching cybersecurity governance: insights from fieldwork with cybersecurity experts and end-users

Real, C. del; Steen, T. van; Díaz-Fernández, A.M.; Del-Real, C.; Molnar, L.

Researching cybersecurity governance: Insights from fieldwork with cybersecurity experts and end-users

Cristina Del-Real
Institute of Security and Global Affairs, Leiden University (The Netherlands)
Email: c.del.real@fgga.leidenuniv.nl (corresponding author)
ORCID: https://orcid.org/0000-0003-3069-4974

Tommy van Steen
Institute of Security and Global Affairs, Leiden University (The Netherlands)
Email: t.van.steen@fgga.leidenuniv.nl
ORCID: https://orcid.org/0000-0002-5805-4664

This is an Author Accepted Manuscript version of the following chapter: Del-Real, C., van Steen, T. (2023). Researching Cybersecurity Governance: Insights from Fieldwork with Cybersecurity Experts and End-Users. In: M. Díaz Fernández, A., Del-Real, C., Molnar, L. (eds) Fieldwork Experiences in Criminology and Security Studies*. Springer, Cham. https://doi.org/10.1007/978-3-031-41574-6_26*

Researching cybersecurity governance: Insights from fieldwork with cybersecurity experts and end-users

Abstract

The field of cybersecurity governance research strives to understand, rationalize, and propose effective solutions for the complex task of safeguarding cyberspace as a secure environment. Concurrently, social research focuses on comprehending the institutions, policies, and behaviours that foster a safer online realm. This type of inquiry often relies on the expertise of professionals or involves research conducted directly with end-users. However, conducting fieldwork with these specific groups presents unique challenges pertaining to the subject matter. In this chapter, we aim to share our first-hand experiences of conducting fieldwork in cybersecurity, engaging with both experts and end-users. Our experiences stem from three distinct projects centred around governance, culture, and cybersecurity training. Throughout this chapter, we delve into the logistical, ethical, and emotional challenges we encountered along the research journey, highlighting the successes and missteps we encountered. By sharing our experiences and lessons learned, we contribute to the ongoing discourse in this field and offer valuable insights for future research endeavours.

Keywords: Delphi, hackers, gatekeeper, engagement, focus group

1. Untangling cybersecurity governance

Cyberspace stands as humanity's most complex creation. The vast deployment of millions of kilometres of optical fibre, composed of glass and plastic, spanning across land and sea, has birthed an entirely novel ecosystem of virtual domains, agents, social and political structures, and unparalleled norms throughout history. In a mere span of 30 years, since the commercialization of Internet access commenced, society has undergone transformative changes. Consequently, criminality, violence, and conflicts between individuals, groups, and even nations have adapted to new manifestations. The field of cybersecurity governance research endeavours to comprehend, rationalize, and propose solutions to the intricate task of preserving cyberspace as a secure place. However, such an undertaking is not without its challenges. A comprehensive grasp of cybersecurity governance is only achievable through meticulous analysis of its constituent components and the intricate relationships that bind them into a cohesive whole.

In the studies of cybersecurity governance, two primary approaches have emerged: top-down and bottom-up. The first approach, top-down, seeks to comprehend cybersecurity governance by zooming out the analysis. It delves into the macro level, examining the behaviour of states, international and national norms, policies, etc., and the meso level, including organizational behaviour and business practices. From the macro perspective, for instance, scholars aim to understand how states define their sovereignty in cyberspace (e.g., Jensen, 2015), retaliate or not against other states for destructive or disruptive cyber operations (e.g., Kaminska, 2021), or create policies to protect their data and systems (e.g., De Busser,

2009; Porcedda, 2018). From the meso level, studies aim to determine the most effective cybersecurity practices (e.g., Buil-Gil et al., 2021a), assess an organization's cybersecurity maturity (e.g., Maleh et al., 2021), or establish measures to prevent and manage threats within companies (e.g., Moneva and Leukfeldt, 2023; Trim and Upton, 2013). The second approach, bottom-up, explores cybersecurity governance from the end users' perspective, also known as the micro level. This level aims to understand secure behaviours (e.g., Moustafa et al., 2021), explain why some individuals adopt these behaviours more easily than others (e.g., De Kok et al., 2020), and propose solutions to make secure behaviour the easiest or default option (van Steen and De Busser, 2021).

In this chapter, we have brought together our research expertise in exploring both perspectives. On the one hand, we have examined the top-down perspective, seeking to understand the role of public institutions, private organizations, and professional communities, as well as the dynamics among them, in cybersecurity governance, with a particular focus on Spain (Del-Real, 2022; Del-Real and Díaz-Fernández, 2022; Del-Real and Rodríguez Mesa, 2022). On the other hand, we have adopted the bottom-up approach to investigate strategies for influencing user behaviour and enhancing awareness and training of employees in cybersecurity (Van Steen and Deeleman, 2021). To accomplish our research goals, the fieldwork involved the participation of cybersecurity experts from intelligence services, law enforcement agencies, the military, cybersecurity firms, major technology corporations, national and regional governments, ethical hacking communities, as well as employees and end-users.

The following sub-section will present the characteristics of our three projects. Subsequently, in Section 2, we describe the phases of our fieldwork. Section 3 we explain the methods employed, including interviews, Delphi, focus groups, and surveys. The ethical and emotional challenges associated with conducting research involving cybersecurity experts and end-users will be explored in Section 4. Finally, the chapter concludes by summarizing the lessons learned throughout the authors' research journey.

1.1. Project 1: Exploring the Spanish cybersecurity landscape

The first fieldwork experience is Del-Real's PhD project on actors and collaboration networks in cybersecurity in Spain (2017–2021). This research had three objectives: i) to understand how organizations and hackers mobilize their capital[1] and interact with other entities to foster cybersecurity, ii) to map the collaboration networks among these organizations and the hackers communities, and iii) to determine the most likely future cybersecurity model for Spain in 2035. The fieldwork for this project involved face-to-face and online interviews, as well as a

[1] For my study on cybersecurity governance in Spain, I employed the conceptual framework of resource exchange through various forms of capital, adapted to security studies by Dupont (2004), and based on Bourdieu's notion of capital as exchange units (Bourdieu, 1986). Therefore, when referring to "capital", I encompass five types: economic, political, cultural, symbolic, and social. For further details on the conceptual framework, please refer to Dupont (2004) and Del-Real and Díaz-Fernández (2022).

study using the Delphi method[2] (see Figure 1). The interviews, both pre and post-Delphi, were semi-structured (Flick, 2007). The Delphi study was conducted in three rounds: an introductory round, a second round consisting of closed-ended questions, and a final round for feedback and consensus-building among the experts (for more details, see section 3.2).

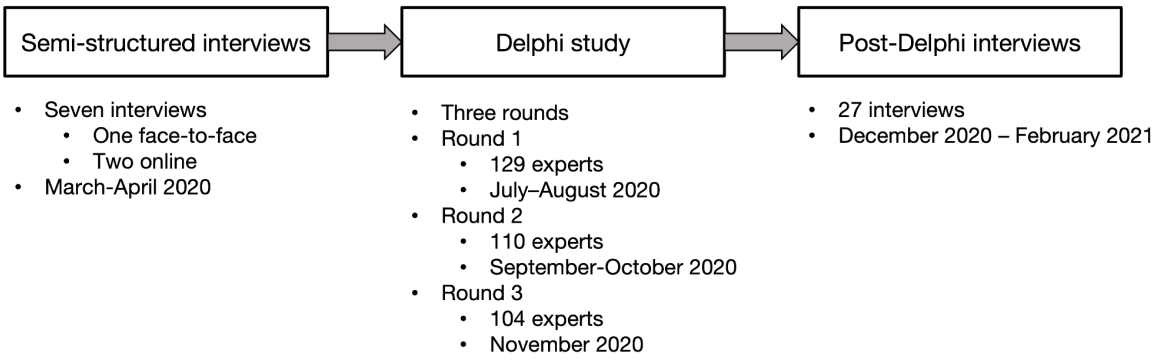

Figure 1. Project 1 fieldwork design.

The study engaged a total of 134 cybersecurity experts in Spain, combining both interviews and the Delphi method. The literature in the field of social science often employs the terms "experts" and "elites" interchangeably. However, it is important to note that these concepts refer to distinct types of assets. While an individual can possess expertise and simultaneously be a member of the elite, the two concepts convey different meanings. Expertise, as commonly defined in the majority of literature drawing from the sociology of knowledge, pertains to individuals with professional knowledge and specialized skills (Meuser and Nagel, 2009; Petintseva et al., 2020). On the other hand, elites are characterized by their social position, which is based on factors such as power, authority, and high social status (Van Audenhove and Donders, 2019). Although this conceptual distinction is theoretically significant, in practice, the link between knowledge and power often becomes blurred (Petintseva et al., 2020). Because in the domain of cybersecurity individuals with the highest levels of knowledge and expertise may not always hold positions of power (Tanczer, 2020), I define cybersecurity experts as those individuals who demonstrate exceptional knowledge and possess a comprehensive understanding of cybersecurity matters – i.e., these individuals were my research's participants.

As a highly fragmented field (Cavelty and Wenger, 2022), studying cybersecurity governance required integrating a wide range of perspectives and experiences from experts with diverse backgrounds (following the advice by Rowe and Wright, 1999). Therefore, I incorporated participants from the five clusters of organizations that I had identified during the literature review and analysis of policy documents as being part of the cybersecurity system in

[2] The Delphi method was developed in the 1950s by Olaf Helmer and Theodore J. Gordon (Gordon and Helmer, 1964; Helmer, 1967) at the RAND Corporation as a technique for studying expert consensus on defence futures (Dalkey and Helmer, 1963; Rowe et al., 1991). In the Delphi method, consensus is achieved through a structured and iterative process in which experts anonymously express their opinions over multiple rounds. The data analysis aims to determine the degree of consensus among participants on each of the questions.

Spain: i) public sector (i.e., the National Cryptologic Centre –CCN–[3] the National Cybersecurity Institute –INCIBE–[4] government offices such as the Department of Homeland Security, regional cybersecurity agencies,[5] courts of justice, and prosecution services); ii) law enforcement and armed forces (i.e., *Guardia Civil* and *Policía Nacional,*[6] and the military's Joint Cyberspace Command); iii) private technology sector companies (i.e., telecommunications, technology firms, internet service providers, etc.), iv) other private companies (i.e., banking, security, transportation, etc.), and v) universities and research centres. Having access to these agencies, I was able to reach out to and gather data from a diverse range of individuals from judges, police officers, military personnel, company CISOs,[7] intelligence service members, government officials, full professors, and ethical hackers. The information from the participants was analysed from the epistemological approach of positivism (Miller and Glassner, 1997), considering the experts as a source of data that would be complemented with documentary analysis.

1.2. Project 2: Cybersecurity culture in organisations

This postdoc project (van Steen) consisted of three focus groups within a single organisation in the United Kingdom to investigate the views of end-users towards cybersecurity culture (2017-2018). The project was funded by the National Cyber Security Centre (NCSC) of the United Kingdom who wanted to support research on improving organisational cybersecurity. The focus groups were proposed as we were interested in the views of end-users of all levels within the organisation to get a complete overview of the organisation's cybersecurity culture compared to only interviewing security specialists. The organisation that took part in the case study was contacted by the NCSC and agreed to act as a testbed on the basis that they wanted to support the developments in the field of cybersecurity and they saw the project as a way to better understand their own practices and areas for improvement. As the anonymity of the organisation in public reporting was a prerequisite for participation, no further information

[3] The National Cryptologic Centre (*Centro Criptológico Nacional*, CCN) is an entity affiliated with the National Intelligence Centre (*Centro Nacional de Inteligencia*), the intelligence service in Spain. Its primary mandate is to contribute to the cybersecurity of networks and systems within the public sector, as well as companies and organizations of strategic interest.

[4] The National Cybersecurity Institute (*Instituto Nacional de Ciberseguridad,* INCIBE) is a Spanish public corporation whose primary role is to provide public services to citizens, businesses, and private companies of critical sectors.

[5] In addition to the national cybersecurity agencies in Spain, autonomous communities are also establishing their own regional cybersecurity agencies. For instance, examples include the Catalonia Cybersecurity Agency (*Agència de Ciberseguretat de Catalunya*) and the Andalusia Cybersecurity Centre (*Centro de Ciberseguridad de Andalucía*).

[6] In Spain, there are two law enforcement agencies with jurisdiction across the entire national territory: the *Guardia Civil* and the *Policía Nacional*. These two nationwide bodies serve as the primary law enforcement entities responsible for investigating cybercrime in Spain. The *Guardia Civil* operates two specialized groups dedicated to combating cybercrime: the Cybercrime Unit (*Grupo de Delitos Telemáticos, GDT*) and the Cyberterrorism Group (*Grupo de Ciberterrorismo*). Similarly, the *Policía Nacional* has its own Technological Investigation Unit (*Unidad de Investigación Tecnológica*) focused on investigating cyber-related offenses.

[7] Chief Information Security Officer.

regarding the type, name of the organisation or sector they worked in can be shared. The decision to only include three focus groups was made in agreement with the case study organisation, as they were interested in us running focus groups in three different sites across the U.K. where they had organised security events in the past. An additional reason was that the organisation had to balance the importance of the project with the time it would cost for their employees to attend. Participants were recruited by a gatekeeper within the organisation with the goal of including people from various layers and job titles in the organisation in every focus group. The focus groups were carried out by two researchers. One researcher with expertise in running focus groups and one with expertise on the topic of cybersecurity culture. Audio recordings were made, transcribed, and analysed for a report for the NCSC and the partnering organisation.

1.3. Project 3: Gamification of cybersecurity training

This project by van Steen aimed to design a playable game to train end-users from the general public to behave more cybersecure. The format of the project was an MSc thesis supervised by van Steen. The project entailed both the design of the cybersecurity game, as well as testing whether the game had improved the factors encompassed by the Theory of Planned Behaviour (Ajzen, 1991): attitudes, subjective norms, perceived behavioural control, intentions and self-reported behaviour. We designed a single player game using the online survey software Qualtrics as the environment for the game, as well as for the outcome measurements. The reason for choosing an online setting was that the COVID-19 pandemic hit the world during the runtime of the project. Initially, we intended to create an offline multiplayer game, but as it was impossible for participants to meet face-to-face, we had to redesign the game for an online setting. As creating an online environment for a multiplayer game was not feasible given the short timeframe of the project –only five months from start to finish– we opted for a single player experience instead. Members from the general public were invited to play a game in which they were presented with various ‘rounds’ in which they could spend a virtual pot of money to buy assets for their department. Some assets were good for business, others for cybersecurity. In between rounds, our 258 participants were presented with cybersecurity challenges. In those challenges they could benefit from assets they had bought, and had to make decisions to respond to the cybersecurity challenges they were confronted with. Qualtrics was a useful tool for this study, as it is versatile in the type of questions and information that can be shared on screen, and the routing option of the software. Using the routing option, participants’ decisions in the game were used as input for later rounds. For participants it looks like the software is responding directly to their unique choices, but they are in fact routed to a limited set of options throughout the game. After the game ended, outcome measures were recorded in the Qualtrics survey software, exported, analysed and written up as MSc thesis and later as journal article (Van Steen and Deeleman, 2021).

2. Phases of the fieldwork

This section outlines the challenges and solutions we encountered during our fieldwork with cybersecurity experts and end-users of cybersecurity technologies.

2.1. Understanding cybersecurity concepts

Research in cybersecurity from the social sciences perspective is complex. As a complex socio-technical system (van den Berg et al., 2014), studying the dynamics surrounding cyberspace requires a minimum understanding of the technical aspects and acquisition of the language. Otherwise, there is a risk of misinterpreting the information we gather or missing relevant details (e.g., overlooking a technical concept). This is exactly what happened to me (Del-Real) at the beginning of my research. I decided to gather expert feedback on the questionnaire for each of the three Delphi rounds to ensure its accuracy. The first setback came with the comments from a computer science academic. Despite having dedicated endless hours to prepare the questionnaire, I received very negative feedback on the initial version, including the statement: "My advice is that you should first inform yourself better or formulate the questions more effectively, otherwise you won't get any meaningful results. I say this from experience", and he recommended that I acquire more technical knowledge "before attempting to ask questions". Specifically, he pointed out in his comments that it was evident in the questionnaire that I did not understand the technical tasks carried out by each institution. And he was right. At that time, I would not have been able to explain the distinguishing activities between a Security Operation Center (SOC) and a Computer Security Incident Response Team (CSIRT).

Understanding technical concepts is not only important for asking appropriate questions, but also for obtaining and interpreting information. For instance, during the interviews following the Delphi study, I discovered a point of contention between the CCN and the police forces. The CCN have real-time monitoring probes installed in the networks of public administrations to identify threats and incidents. However, the police officers I interviewed complained that their organizations did not have easy access to this information, even though one of their mandates is to protect citizens' rights, freedoms, and security, including in cyberspace, in their opinion (Del-Real and Díaz-Fernández, 2022). The lack of infrastructure that would enable them to conduct this "virtual patrolling" compromised their ability to take action. In this instance, the fact that I was familiar with the concept the interviewees referred to as "SAT INET"[8] when discussing these probes offered me two advantages. First, I could interpret this finding. I had followed the advice given to me by that computer science academic, and thanks to a better understanding of the technical concepts, I could identify and delve into a governance problem that would have otherwise gone completely unnoticed. And second, I was able to build trust with the participants by demonstrating my knowledge and understanding of their language (Petintseva et al., 2020).

[8] In reference to the CCN's Internet Early Warning System. More information: https://www.ccn-cert.cni.es/en/incident-management/early-warning-system-sat/sat-inet.html

Aside from the potential to mistakenly explain concepts wrongly, in my experience (van Steen), another issue with a limited understanding of the cybersecurity field is that participants in focus groups might use a range of abbreviations to describe their procedures or an organisational structure. It was our task during the focus groups in Project 2 to then ask for clarification and ensure that we get it right. However, when a focus group participant uses large amounts of jargon, constantly asking for clarification or summarising to see whether you as researcher have understood the point they are trying to make can disrupt the flow of the focus group and the intra group discussion, thereby denying us access to important information. In addition to the earlier mentioned reading up on technical aspects of cybersecurity, a second tool can be to first have a conversation with one or two experts in the organisation to understand the various procedures and key events that have taken place before collecting data. For instance, when we conducted the focus groups, we first sat down with two security experts from the organisation to hear about their awareness campaigns and other security culture initiatives so that we would more easily understand what the focus group participants could be referring to.

2.2. Finding the target group: cybersecurity experts and end-users

Accessing cybersecurity experts is relatively straightforward. One simply needs to attend one of the dozens of cybersecurity conferences organized each year. However, gaining access to the most suitable cybersecurity experts for the study's objectives, especially during a pandemic, is more complex. Based on the five clusters of organizations for Project 1, I (Del-Real) initially sent emails to these organizations to request an interview with one of their members. This strategy soon proved completely futile. Most of my emails went unanswered, and the few organizations that did respond cited a lack of time as the reason for their refusal.

This result –which was, on the other hand, expected– led me to reorganize my field access strategy. Two decisions proved successful in gaining access to participants: attending specialized conferences and drawing on the networks of one of my thesis supervisors. Firstly, attending conferences and technology fairs allowed me to expand my network of contacts. In particular, my participation in various editions of the *Smart City World Expo Congress* in Barcelona, the *Hackplayers' Hacking Conference* (H-C0N), and the *International Security Exhibition* in Madrid proved highly fruitful. During this field access phase at conferences, I observed that it was much more effective to approach executives in the conference rooms where they delivered presentations or attended as listeners, rather than at the stands of technology fairs, where it was less likely to find these high-level experts of interest. To maximize my effectiveness in contacting potential participants at conferences, it was crucial to prepare in advance a list of target participants, enabling me to locate them once at the conference, and to have a concise and compelling pitch about my study ready.

The second decision was to leverage the networks and reputation of one of my thesis supervisors, Dr. Antonio Díaz Fernández. In the field of security studies in Spain, Dr. Díaz Fernández is known as one of the pioneering scholars in the study of the *Centro Nacional de*

Inteligencia (CNI, the Spanish National Intelligence Centre) (Díaz-Fernández, 2005). His research on the history and evolution of the CNI led him to interview –and to still be in touch with– numerous intelligence agents, military personnel, and political elites. Additionally, he is one of the Spanish experts on ethical issues in sensitive research topics in criminology and security studies (Díaz-Fernández, 2019). Associating my name with his supervision, in my opinion, offered two main advantages in accessing the field. Firstly, I gained access to his contacts in the intelligence service, police, and armed forces, which undoubtedly saved me months of work in reaching out to experts from these organizations. Secondly, I benefited – perhaps due to the halo effect (Beckwith and Lehmann, 1975)– from his reputation as a respected researcher who is trustworthy and committed to research ethics. As one of the interviewees expressed: "If you're doing your thesis with Antonio, I trust you".

To contact participants, I firstly compiled a list of potential names, including those contacts identified through conferences and my supervisors (as well as other colleagues). I sent them an email following the template outlined in Figure 2. In conversations with participants following the completion of my Delphi study, some highlighted the elements of my email that had made them take me seriously and, as they put it, "reassured" them: i) including what I expected from them (i.e., participation) from the beginning of the email; ii) promptly emphasizing in the email that their participation would be anonymous and their opinions would not be associated with their organization (see section 4 below); and iii) clearly explaining the study's dynamics (i.e., dates, deadlines, effort required, etc.), which allowed them to make an informed decision based on the study's timeline and expectations. Of the invited contacts, some responded positively, while others referred me to other contacts who, in their opinion, could be of greater utility. In total, I invited 275 Spanish experts, including both initial contacts and those obtained through the snowball sampling method.

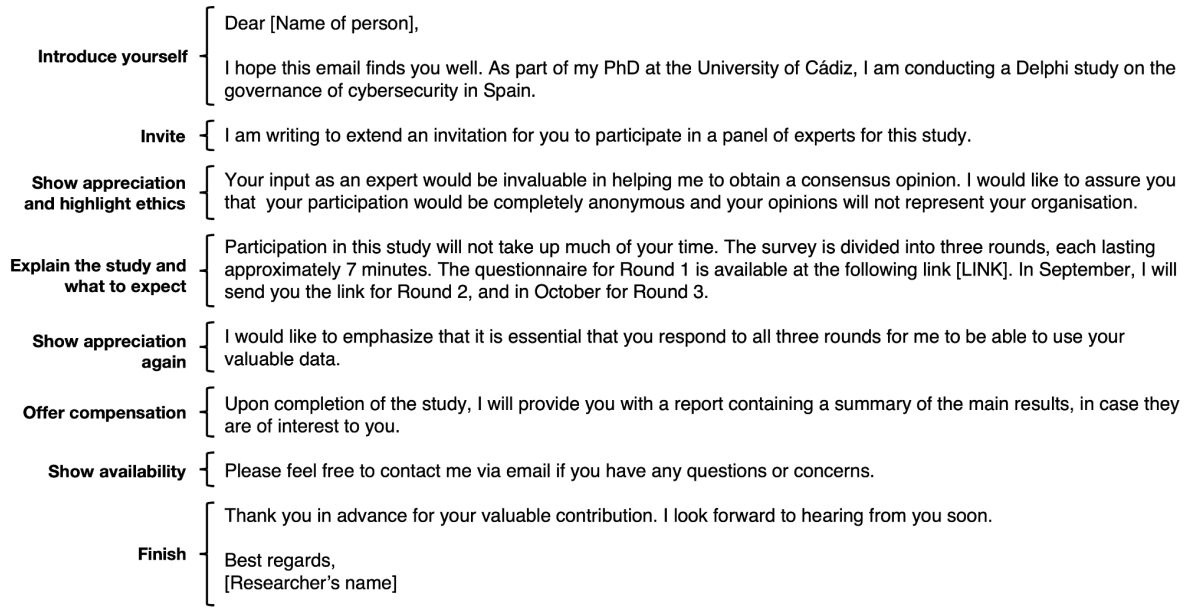

Figure 2. Example of an invitation email.

Another method to find participants for qualitative studies is through gatekeepers. This is particularly crucial when trying to access hard-to-reach groups. For instance, in Project 1, I (Del-Real) encountered two challenging groups to reach: women who are cybersecurity experts and ethical hackers. To engage the first group, given the existing gender bias in cybersecurity, I sought assistance from the *Women in Cybersecurity in Spain* association in Spain. They acted as gatekeepers by sharing the invitation to my study with their extensive network of over 300 members. As for the second group, having the support of a highly-connected cybersecurity journalist with deep knowledge of ethical hacking proved to be immensely valuable.

In Project 2 (van Steen) we worked with an organisation that had an interest in the research being carried out. In that study, it was helpful to use the gatekeeper to get access to relevant people as our focus groups required a range of job titles to be present at the same time and location. A potential downside to using a gatekeeper is that it might also prevent access to relevant participants (Maramwidze-Merrison, 2016). For example, they can select people who are supportive of the views of the gatekeeper, leading to potentially biased findings. However, in our focus group project the gatekeeper was able to recruit a variety of participants due to him having been travelling around the various sites to deliver security training in the past. This trusted individual from within the own organisation allowed us to recruit more people who were willing to spend time talking to us and sharing their experiences in the focus groups.

2.3. Collecting data

In our fieldwork experiences, we have encountered two main issues when asking questions to participants: disparities in cybersecurity knowledge and reluctance to answer sensitive questions. Firstly, disparities in cybersecurity knowledge pertain to both vocabulary and content. For instance, in Project 1 (Del-Real), striking a balance to make the Delphi questionnaire accessible to both technically oriented participants (e.g., ethical hackers) and those with less technical expertise (e.g., judges) posed a challenge. To address this issue, I sought experts from diverse backgrounds to review the questionnaire for all three rounds before its launch. While this decision undoubtedly increased accessibility to a wider range of profiles, achieving full accessibility in such a complex topic is difficult to achieve. For example, four experts who had completed the Round 1 questionnaire opted not to proceed to Round 2. Their choice was influenced by the high level of specialization required to adequately respond to the questions. Additionally, three other experts requested to answer the questionnaires while speaking with me over the phone, as they had some doubts about the questions.

In Project 2, the focus was on the organisational aspects instead of the technical aspects of cybersecurity. As we invited end-users from all layers in the organisation, some had a more thorough understanding of what the organisation was currently doing to build a cybersecurity culture than others. Therefore, the questions we formulated had to be broad enough to ensure that all participants could take part in the conversation that followed. Once the conversation started, it was then our responsibility to make sure that all participants were understanding the comments made by others. Sometimes we did that by briefly clarifying a statement that we

thought might be too complex. Other times, we asked the participant who brought up a certain point to elaborate. A complicating factor here was that not all end-users had been with the company long. Some of the examples then shared by the end-users did not resonate with the end-users who had joined the company only recently which at one or two occasions caused confusion for some end-users.

Secondly, we encountered instances where participants attempted to evade answering contentious or sensitive questions. For instance, in Project 1, participants provided information with varying levels of depth. Experts from the private sector offered insightful and detailed perspectives on the challenges and issues related to collaboration between public organizations and the private sector (see Del-Real and Díaz-Fernández, 2022). However, a few experts from the public sector simply repeated during the interviews that "everything was going smoothly" without offering any further details. Specifically, in two cases, I had to cut short the interviews with representatives from public organizations shortly after they began, as it became evident that my attempts to inquire only resulted in scripted, politically correct responses lacking substantial content. Consequently, it became crucial to gather information about the same organizations from multiple sources and assign greater validity to results that were consistently reported by multiple experts in separate sessions.

2.4. Engaging participants

Obtaining and maintaining participant engagement is another challenge in cybersecurity research with experts and end-users. As Bulmer (1982, p. 3) stated, "no-one gives anything away for nothing, especially the truth". Additionally, participation is always voluntary. Therefore, it is important to try to understand why participants agree to take part in our research. In Project 1 (Del-Real), I identify two reasons that may explain why I obtained such a high participant sample in the Delphi process – i.e., 129 experts in the first round, exceeding 83% of Delphi studies (Gargon et al., 2019). Firstly, because the research topic –cybersecurity governance– is still evolving. Previous studies have described how participants sometimes choose to participate in order to provide insights into the changes occurring within their group (Clark, 2010). In this regard, I believe that participants saw in my research an opportunity to inform the scientific community about the advancements being made by public organizations and companies in the field of cybersecurity. Secondly, because my research focused on understanding the roles of and collaborative relationships between public and private organizations. Therefore, the contacted experts may have interpreted their participation as an opportunity for their organization to be represented in the study (Clark, 2010).

During Project 1, I employed three techniques to ensure the engagement of the participants. Firstly, I aimed to streamline the interaction with participants through email and phone communication. I made sure to respond to messages and emails from invited experts within 10 minutes, conveying a sense of complete availability to address any questions or concerns they had. Secondly, I offered to provide a copy of the research findings. This may have increased their curiosity about the results (Clark, 2010), keeping them motivated to

participate in all three rounds. Lastly, I sent two to three reminders in each round. Starting from Round 2, the initial invitation email was generic, but I personalized the subsequent reminders to enhance their perception of commitment and encourage consistency in their behaviour (Becker, 1960). Consistent with studies on the effect of reminders in increasing response rates (e.g., Blumenberg et al., 2019; Svensson et al., 2012), Figure 3 illustrates how responses increased after each reminder.

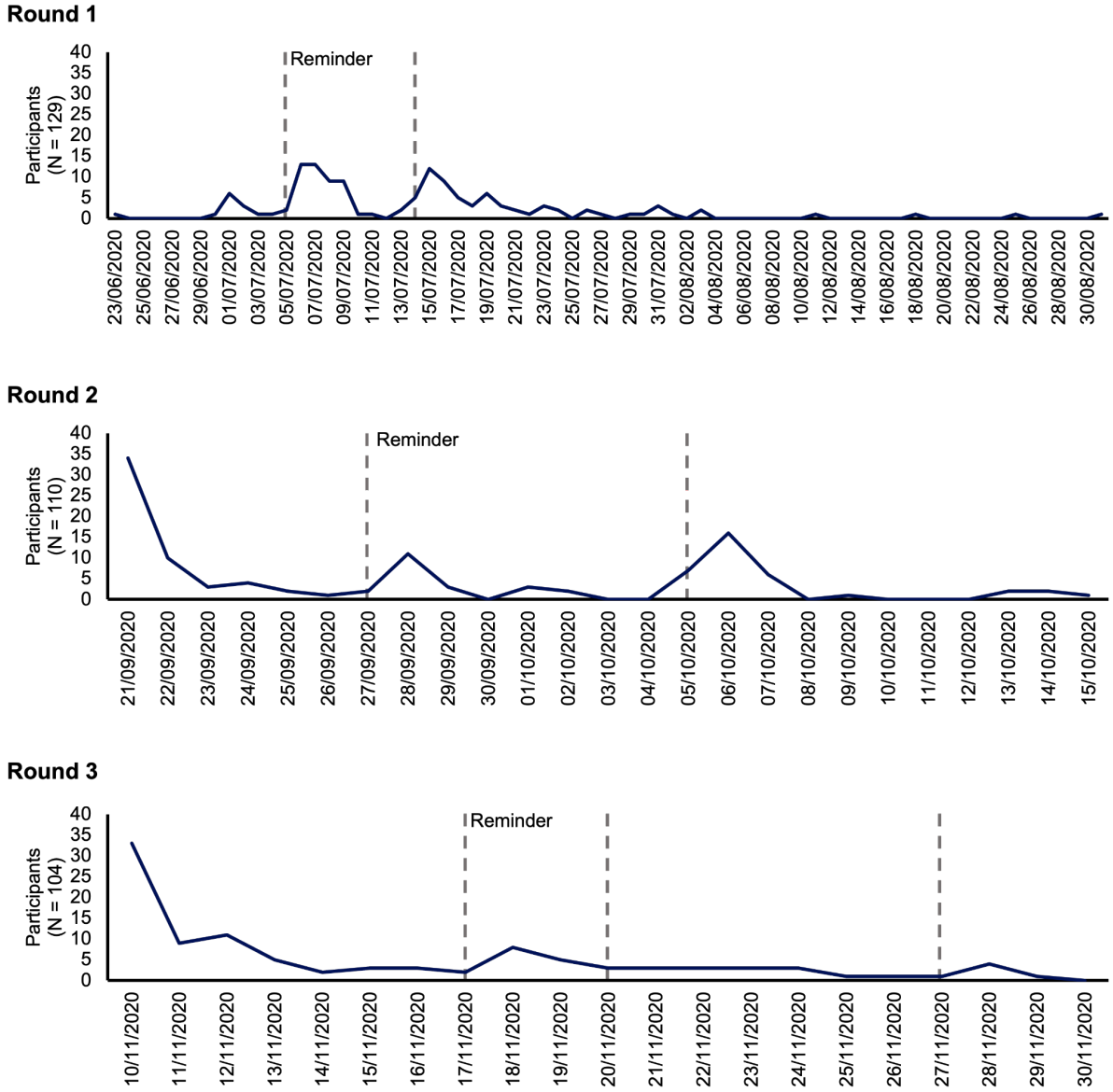

Figure 3. Relationship between responses received and reminders in Project 1.

3. Data collection techniques

This section outlines the research techniques employed in our investigation of cybersecurity governance. Specifically, we discuss four techniques: interviews, the Delphi method, focus groups, and surveys.

3.1. Interviews

For Project 1 (Del-Real), I deemed it most appropriate to conduct semi-structured interviews given the complexity and sensitivity of the study's objectives. The interviews were aligned with Brinkmann's doxastic interview (2007), which aims at understanding the functioning of practices or events. The choice to conduct semi-structured interviews was particularly driven by the characteristics of the participants, who were experts, predominantly senior executives and individuals with over fifteen years of experience in the cybersecurity sector. This specificity necessitated semi-structured interviews, allowing for the emergence of new themes and avoiding participants' sense of being scrutinized (Díaz-Fernández, 2019).

At that time, I was pursuing my PhD at the Faculty of Law of the University of Cádiz (Spain), while residing in Sevilla. However, the majority of my potential participants were based in Madrid and Barcelona, the economic and political centres of Spain. Therefore, I planned two research visits to academic institutions in Madrid and Barcelona. In the case of Madrid, the *General Gutiérrez Mellado University Institute* affiliated with the Open University (UNED), kindly agreed to host me as a visiting researcher during the months of April and May 2020, under the supervision of Prof. Carlos Echeverría. The choice of this institution was due to its extensive faculty of professors and researchers in security studies. Additionally, the research visit in Madrid would allow for extensive fieldwork based on the contacts I had established in previous months (see Section 2.2). In Barcelona, the Research and Analysis Group of Public Administration at the University of Barcelona, led by Prof. Rafael Martínez, director of the Master's Program in Strategic Security and Policing Management, accepted the research visit for the month of June 2020. The selection of this research group was based on their extensive work in security management (e.g., Martínez and Durán, 2017) and the opportunity to access telecommunication companies and major technology corporations headquartered in Catalonia. However, I was unable to carry out any of the research visits due to unforeseen circumstances.

On March 14, 2020, the Spanish government declared a State of Alarm in response to the health crisis caused by Covid-19. The State of Alarm lasted for a total of 98 days, during which social distancing measures were implemented to contain the spread of the virus. These measures included restrictions on leaving home, holding gatherings, and traveling outside the province of residence. As a result of these social distancing measures, the planned research visits to Madrid and Barcelona had to be cancelled. Prior to the lockdown, I was only able to conduct one of the fifteen scheduled interviews for the months of March and April, some of which had already been scheduled with specific dates and times. When mobility restrictions were announced, I contacted the participants to propose conducting the interviews via video call. Six of them agreed to proceed with the interviews through video calls, two did not respond, and the rest requested to be contacted once the crisis had ended.

Given such a low rate of positive response, I decided to reach out to other potential participants whose profile aligned with the objectives of my study through LinkedIn and email, as well as through recommendations from other participants using the snowball sampling technique. However, this approach proved to be unsuccessful. During the lockdown, there was

an increase in cybercrime incidents (e.g., Buil-Gil et al., 2021b), which significantly heightened the workload of cybersecurity experts. As a result, they progressively started to cancel the scheduled interviews. Moreover, newly contacted cybersecurity experts declined the interview requests, largely due to their overwhelming workload stemming from crisis management and their high-level managerial roles within their organizations.

The inability to conduct fieldwork in Madrid and Barcelona led to significant changes in the study's methodology. Initial discussions with the experts revealed that various professional and personal factors, along with the impersonal nature of video calls, would hinder and complicate the original interview process. Moreover, the experts declined to participate in online interviews due to their confidentiality obligations with their respective companies, which required them to maintain privacy. These obligations sometimes involved surveillance to ensure adherence to these commitments. After considering different options for several weeks, it was decided to conduct a comprehensive Delphi study consisting of three rounds (see section 3.2).

In the questionnaire of the third round of the Delphi study, I asked the participants if they would be available for an interview. A total of 68 agreed to be interviewed. I then extended invitations to the 30 expert participants in the Delphi study who had shared the most compelling and, in some cases, contrasting opinions. Out of these 30 experts, 27 accepted the invitation. All interviews were conducted via video call or telephone, according to the preference of the interviewees. No interviews were audio-recorded, as I considered that this privacy would allow participants to feel more comfortable and express their opinions with greater freedom (Díaz-Fernández, 2019), which was crucial for profiling and understanding elusive causes and elements of the study. I transcribed the interview in real-time on a blank Word document while conversing with the interviewee. Although this method initially seemed like a good option to gather as much material as possible, it became impossible to capture all the nuances mentioned by the interviewees. To mitigate the loss of valuable information, I shared my research notes with those participants who expressed willingness to review them and provide additional insights after the interview. Unfortunately, I am aware that valuable material was lost due to my decision not to record the interviews. Therefore, for subsequent studies, I decided to prioritize offering the possibility of a non-recorded interview as an exception rather than the norm. This way, it is much more likely to ensure transparency, rigor, and accuracy in the collected data.

The adaptation I had to make to the data collection technique taught me three main lessons. First, virtual tools can be an alternative when conducting in-person research is not possible, but they are not a substitute for in-person interviews. Specifically, I noticed a significant difference between the initial in-person interviews compared to the online interviews. Online interviews feel more impersonal, making it more challenging to establish rapport with the interviewee. Additionally, in my experience, fewer spontaneous topics emerged, and the interviewees became fatigued more quickly. Second, every research design should have a rigorous and detailed contingency plan as robust as the primary plan. This

practice, well-established in EU funded projects, saves a lot of time and resources in case the planned collection method fails. Lastly, I learned that different research designs can support each other beyond scientific aspects (e.g., data triangulation). For instance, I was surprised when, after implementing the Delphi study, a total of 68 experts (out of the 134 participants) agreed to be interviewed. Despite being already in the middle of a pandemic and understanding their likely busy schedules, the Delphi study served as a gateway to gaining their trust, increasing their willingness to be interviewed. Therefore, it is advisable to design research and contingency plans from both a scientific and as well strategic perspective.

3.2. Delphi method

For Project 1 (Del-Real), I designed a three-round Delphi study with cybersecurity experts. This methodology replaced the in-depth interviews that had to be cancelled due to the health crisis caused by the Covid-19 pandemic. At the time when I designed my study, I did not find precedents for the use of the Delphi method in the study of cybersecurity. Previous studies have predominantly employed this method to investigate the priorities in violence prevention (e.g., Mikton et al., 2017) and formulate indicators for its measurement (e.g., de Melo et al., 2018). However, I decided to proceed with this method because it has been widely employed in prospective studies on the impact of technology in various fields (e.g., Keller and von der Gracht, 2014).

Although different from in-depth interviews, the Delphi method allows for similar conclusions and offers some additional advantages compared to interviews, as stated in various research studies (e.g., Gargon et al., 2019). Firstly, the utilization of the Delphi method enabled me to significantly reduce the time commitment required from participants. Instead of conducting lengthy interviews lasting anywhere from 30 minutes to over an hour, I employed an online questionnaire hosted on SurveyMonkey, which took approximately 15 minutes to complete. Secondly, Delphi is a method that can –and should– be conducted remotely. Unlike interviews, which were better suited for physical interaction to accurately analyse participants' non-verbal language, the choice of the Delphi method was consistent with the circumstances during which a significant portion of my fieldwork had to be conducted –the Covid-19 pandemic– when other forms of social interaction beyond the virtual realm were not possible. Lastly, the data collection dynamics of the Delphi method reduce biases that may arise from researcher-participant interaction, which can affect the quality of research outcomes. All this represented an advantage over interviews.

During Project 1 fieldwork, I made several choices regarding the design, execution, and exiting fieldwork strategy that may be of help to future researchers. In the *design phase*, I made two decisions that, in my opinion, enhanced the results' quality. Firstly, although the majority of Delphi studies consist of two rounds (see e.g., Camara et al., 2019), I opted for a three-round Delphi: an introductory round, a second round of closed-ended questions, and a final round for feedback and consensus-building among the experts. This choice allowed me to design open-ended questions in the first round, capturing the complexity of the problem more effectively.

While two-round Delphi studies are less time-consuming for both researchers and participants, the introductory round provided valuable and nuanced information that enriched the subsequent rounds. Secondly, I ensured that the questionnaires for all three rounds were reviewed by at least five experts from diverse backgrounds who could offer comments and suggestions before their implementation.

During the *execution phase* it was crucial to understand and empathize with the characteristics of the participants. 70.3% of them had a minimum of six years of experience in the field of cybersecurity, 72.9% held managerial positions, and they came from different types of organizations with distinct organizational cultures. This presented two challenges for the execution of the Delphi. Firstly, I had to transparently communicate with my participants and ensure that I would not waste their time. While I recognize that this requirement should characterize all research, it is particularly important when working with experts who may perceive their involvement as an act of generosity towards the researcher (Van Audenhove and Donders, 2019). Secondly, I had to adapt my language to suit the diverse profiles of the experts. I quickly realized that with private sector professionals and with policymakers, I could establish a more informal and friendly language (some even ended their emails with affectionate phrases like "sending hugs"). However, with personnel from the military, police, and intelligence services –very hierarchical organisations– I always maintained a formal language and showed respect for their rank. For instance, I maintained an Excel spreadsheet where I recorded their respective ranks, such as "Colonel" or "Inspector," to ensure I addressed them appropriately using the correct protocol.

Finally, during the *exiting phase,* it is crucial to acknowledge the efforts made by the participants. Exiting the field is just as important as entering it, as the manner in which this phase is conducted can either open the door to future research opportunities or close it indefinitely – not only for us, but also for future researchers (Díaz-Fernández, 2019). This holds even greater significance in the context of my own investigation. In a world engulfed by chaos, amidst a global pandemic that disrupted every facet of life, these individuals kindly offered their valuable time to help me make sense of the complex network of institutions and organizations governing cybersecurity in Spain. Consequently, it was paramount to express my appreciation by personally sending each participant a tailored *thank-you* email. Additionally, I provided interested participants with copies of my thesis and relevant publications. To this day, I maintain contact with some individuals who have shown interest in my professional trajectory and future research endeavours.

3.3. Focus groups

For Project 2 on cybersecurity culture (van Steen) we conducted three focus groups. Focus groups are a method to elicit new insights through the interaction of the participants (Morgan, 1996). The participants in the focus groups were employees from a range of layers within a single organisation, which we analysed using thematic analysis (Glaser and Strauss, 1967). The number of participants per focus group ranged from 6 to 16 end-users and covered a wide range

of job roles, including Human Resources staff, Information Technology personnel, Health and Safety officers, personal assistants and project engineers. The focus groups lasted about 1.5 to 2 hours and two researchers were present. One researcher acted as facilitator, leading the discussion, posing questions and asking for clarification, while the other observed and took notes, and occasionally interjected a follow-up question to a response of one of the participants. This division helped in streamlining the focus groups, as well as double checking that all relevant areas of the discussion were covered and any required clarification in terms of abbreviations or organisational processes was achieved. This was necessary, as it would have been impossible to go back to a single participant with follow up questions once the audio recordings of the focus groups had been transcribed. Additionally, adding a second researcher ensured that in case of technical failure of the audio recordings, notes and basic insights were still available. As stated before, the goal of these focus groups was to further investigate the findings of an earlier series of interviews with security specialists in the same organisation. The set of questions used in the focus groups were designed by the two researchers who facilitated the discussion during the focus groups, and was then sense checked by a third researcher from the same department as well as the point of contact in the partnering organisation. Organising the focus groups helped us in two ways.

First, the focus groups were ideal in examining whether there was any truth in the perceptions and views expressed by gatekeepers in a set of preliminary meetings where the goals and logistics of the focus groups were discussed. There, the gatekeepers outlined that security specialists within the organisation viewed themselves as enablers of working in a secure fashion, while they felt that the rest of the organisation sees them as blockers. This tension was confirmed in the focus groups where the participants acknowledged that they viewed the security specialists as blocking them from meeting their job goals instead of enabling them. The second way in which the focus groups helped us understand the current security culture at the organisation was through testing their experiences with cybersecurity training materials. In the focus groups we could investigate whether the views of the security experts aligned with those of the end-users, and dive deeper into why these views of ‘enablers’ and ‘blockers’ exist and what might be done to change that in the future.

3.4. Surveys

In contrast to interviews, focus groups and Delphi studies, surveys are used for large scale data collection, where the in-depth experiences, views and perceptions of people are of lesser importance, and the wider view together with the option to draw conclusions about relationships between variables is key. Where surveys are a useful tool is in determining the effectiveness of campaigns to improve end-user security. While surveys are a great way to conduct research in the field of cybersecurity governance, its applicability depends greatly on the specific research question and target group. Some projects require such in-depth knowledge from participants that a survey study cannot possibly result in enough participants taking part,

or the survey questions are inadequate to tease out the intricacies of the phenomenon under investigation.

When we designed our survey on the gamification of cybersecurity training (Project 3), we used the survey tool to deliver the cybersecurity training, as well as measure the effectiveness of the training. The advantage of combining both the delivery of the training and the outcome measurement in the same tool is that we can more easily export the data for analysis, that we do not need participants to move between platforms and that we could register additional data on the survey process, such as the time passed between starting the game and finishing the survey. Given the five-month timeframe of the project, we did not have the opportunity to design and validate a complete new set of survey questions for the outcome measures. Instead, we based our outcome measures on earlier research on the Theory of Planned Behaviour (Mcmillan and Conner, 2003; Poulter *et al*., 2008). We chose the Theory of Planned Behaviour factors as outcome measures, as these factors are often used to investigate the effectiveness of cybersecurity training (e.g., Cook *et al.*, 2017).

One potential issue with surveys is that participants cannot ask for clarification while filling out the surveys. When designing surveys, we are often prone to use jargon. It is key for us to ensure that the participants in a survey study understand the various concepts they are asked about. In some cases, this means that we need to word concepts differently so that participants understand. While the same issue can arise in a qualitative interview or focus group study, participants in those studies can ask for clarification if they do not understand the interviewer, or the interviewer can clarify when it seems that the answer to a particular question does not capture the concepts they were asking about. In survey research you only get one chance to explain the tasks and questions correctly and unless you pilot your study extensively, you will only find out at the analysis stage whether or not participants understood what was asked of them.

4. Ethical and emotional challenges

In this section, we explain three challenges that we have encountered in our research with cybersecurity experts and end-users: ensuring anonymity and confidentiality, managing participant demands, and striking the right balance in the participant relationship. Generally, research studies require approval from ethics committees. However, in Project 1 (Del-Real), I did not obtain any approval as the University of Cádiz only has a bioethics committee that has recently started evaluating social science projects. In Project 2 (van Steen), we obtained ethical approval from the ethics committee through a standardised form and standardised informed consent sheet. In the form, the ethics committee wants to see clear answers on questions regarding both participant and researcher safety, as well the goal and methods of the study. The informed consent sheet included the standard sections on voluntary participation and the option to stop participating at any time without requiring to provide a reason.

Project 3 (van Steen) was interesting in terms of ethical approval, as the data was collected by a student I supervised as part of her MSc programme. The programme at the time

required a light touch ethical approval process for MSc thesis projects. This process consisted of a brief questionnaire students had to complete. Based on their answers, specific themes were flagged by the online system and these themes were then discussed with the thesis supervisor and changes to the research design were implemented if needed. While this way of working was the standard for MSc projects within the department at the time, it raised some questions from one of the reviewers of the journal *Cyberpsychology, Behavior, and Social Networking* when we submitted the paper for publication. They were worried that we did not do a full ethical approval process through an Institutional Review Board (IRB). We were able to explain that the followed method was the standard practice within the department and after clarifying the procedure in the main body of the article, the reviewer accepted the ethical approval method used by the department for this study. For future projects involving student researchers it is beneficial to proactively seek advice from the IRB to avoid delays in the publication process.

4.1. Ensuring anonymity and confidentiality

Ensuring anonymity is crucial for participants to share their information without the risk of negative consequences (Nespor, 2000). In Project 1 (Del-Real), I implemented four strategies to guarantee participant anonymity, protect the data collected, and prevent deductive disclosure (Boruch and Cecil, 1979). Firstly, I replaced participants' names with a unique code composed of three elements: sex (e.g., F for female experts), sector of expertise (e.g., PS for Public Sector), and interview order (e.g., F-PS7 for the seventh female expert from the public sector). Secondly, I eliminated references to specific organizations, replacing them with an "X" (see Del-Real and Rodriguez Mesa, 2022). In some cases, the interviewees themselves requested not to include this information in writing. Thirdly, I kept a record of participating experts in a password-protected folder on a computer that was also password-protected. Lastly, in my research, I only collected email addresses as personally identifiable information in accordance with the General Data Protection Regulation (GDPR) (2016), the norm that informs the Data Protection in EU countries. During the three rounds of the Delphi, I informed participants that the email address provided by them would be solely used for communication purposes and to match their responses across the three rounds. Once the three rounds were completed, I replaced each participant's email address with a generated code, and subsequently deleted the email list.

In Project 2, similar methods were used. However, we also added more safeguards to ensure that the organisation as a whole was also kept anonymous. This included conversations with gatekeepers on specific lingo used in the organisation, such as how they refer to their security culture team, specific slogans that were unique to teams within that organisation, as well as leaving out some identifying details in descriptions of specific awareness campaigns they ran. The conversations with gatekeepers are of importance as there might be some wording of specific organisational structures that seem quite generic, but that together with other information about the organisation (such as whether it is a national/international organisation, the sector they are in etc.) might make the organisation instantly identifiable for people working

in the same sector. We require independence as researchers in terms of our analysis and conclusions and the quotes we incorporate in our reports and publications. However, it is important to work together with organisations regarding naming specific instances, initiatives or incidents, when these can also be described in broader terms if possible and without sacrificing scientific rigour and validity. We achieved this through sharing draft versions of our reports that included specific quotes by participants with the gatekeepers. The gatekeepers could then check whether some wording in the quotes needed a higher level of anonymisation, for example through the use of generic placeholders such as [*security slogan*] or [*company department*] or whether the level of anonymity was already appropriate.

4.2. Managing demands from participants

As mentioned earlier, participants may have certain expectations from the research (Bulmer, 1982). They may expect you to provide them with information about other participants, take a stance, or solve a particular problem. For instance, in Project 1 (Del-Real), I encountered instances where some participants inquired about who had already participated and what had been said about their organizations (see Harvey, 2011 for a similar case). While these inquiries were always conducted respectfully, I must admit that certain participants from the public sector were somewhat persistent in seeking information about what other participants had said about them. In such cases, it is important to maintain neutrality, adopt a professional role, and decline to provide information, especially if it has not yet been verified from other sources. Although this refusal may initially disrupt the interview dynamic, it can be redirected towards a positive outcome by emphasizing that any information the participant shares will also remain confidential and undisclosed to others if they inquire.

4.3. Striking the right balance in the relationship with participants

A final challenge in research with cybersecurity experts and end-users is finding a balance in the relationship with the participants. Particularly, in the case of cybersecurity experts, many of the recommendations for researching vulnerable populations such as minors, victims of violence, or incarcerated offenders do not apply (Liamputtong, 2007). In these cases, the researcher may be perceived as holding a position of power over the participants. However, in research with cybersecurity experts, the power dynamics are reversed. My participants (Del-Real) were highly specialized professionals, with 80.6% of them being male and an average of 11 and a half years of experience in cybersecurity. Meanwhile, I conducted the research as a 27-year-old female PhD student. Therefore, my challenge was to convey to them the value of my research and their participation in it, while also ensuring that I did not reproduce gender and age power structures in respect for my own work and my position as early career researcher (Lefkowich, 2019).

In particular, apart from repeatedly emphasizing the study objectives, I took three measures to prevent any uncomfortable situations with the participants. Firstly, the few in-

person interviews I conducted always took place in public spaces, such as a café. Secondly, I dressed in formal and neutral attire during the interviews. And thirdly, in all communications with the participants, I made sure to include the names of my thesis supervisors, who were often copied on the emails. I must say that during the course of the research, the majority of participants were respectful and assertive, and to this day, I maintain a good professional relationship with some of them. However, I did have three uncomfortable encounters with three experts. The first two incidents were a result of paternalistic behaviours exhibited by two experts. In both cases, their critical remarks about my study were characterized by condescension and arrogance, causing me to doubt my credibility as a researcher.[9] The third incident involved another participant who displayed a clear interest in maintaining contact after the interview had concluded. I started feeling uneasy when this individual persisted in asking me personal questions via WhatsApp for several days following the interview. Upon discussing the matter with my supervisors, I decided to respond in a direct and professional manner, consistently redirecting the conversation towards the objectives of my study. This approach ultimately put an end to the participant's attempts to reach out to me.

As the Netherlands is a small country, working in the Dutch cybersecurity field means that you are likely to run into former participants at some point during conferences and other meetings. As we promise anonymity when we invite people to take part in our research, we should not disclose that people took part in our research to others. When meeting former participants in a group setting, my approach (van Steen) is that I do not bring up that they participated in a research project that I conducted and do not say anything about it, unless they bring it up themselves. In some cases it is difficult or even impossible to pretend you have never met before, but acknowledging that you know each other is different from disclosing you know them as participant in your research. Making that distinction is key in ensuring anonymity and striking the right balance in the relationship with participants.

5. Lessons learned and methodological perspectives

This chapter finishes with a summary of the lessons learned during our research projects. Firstly, regardless of whether it is qualitative or quantitative research, piloting the study is key. The pilot phase of the study may involve gathering feedback from experts on the measurement tools (questionnaire, interview script, etc.) and conducting pre-tests. For instance, the pilot study can assist us in striking an appropriate balance between the use of technical concepts and accessibility to a broad range of participants.

A second valuable lesson we learned, closely tied to the intricacies of studying cybersecurity within the realm of social sciences, is the importance of conducting extensive preliminary research to grasp technical concepts. For instance, we highly recommend preparing a comprehensive glossary of essential terms and acronyms for the project. This glossary can be continually expanded and refined with new terms and acronyms that emerge during the pilot

[9] I have chosen not to provide further information about these cases to avoid deductive disclosure.

study and fieldwork phase. Having a robust technical vocabulary not only enhances our data interpretation but also builds rapport with the participants. It enables us to establish a level of understanding and credibility as researchers.

Thirdly, it is of utmost importance to have a well-developed contingency plan in case the primary data collection method encounters any issues. It is recommended to strategically design this contingency plan, ensuring its alignment with the primary data collection method. Such a decision enables the possibility of repurposing prior work in the event that the primary method needs to be abandoned.

Finally, the demonstration of availability and trustworthiness, along with the facilitation of direct communication and timely reminders, plays a pivotal role in fostering participant engagement with the research. However, it is of paramount importance for researchers, particularly early career researchers investigating individuals in positions of power, to navigate this delicate balance with utmost care and consideration. By doing so, we can create an environment of mutual respect and professionalism that not only enhances the quality of our research but also safeguards against potential discomfort or misuse of power dynamics.

References

Ajzen, I., 1991. The theory of planned behavior. Organizational Behavior and Human Decision Processes 50, 179–211. https://doi.org/10.1016/0749-5978(91)90020-T

Becker, H.S., 1960. Notes on the Concept of Commitment. American Journal of Sociology 66, 32–40. https://doi.org/10.1086/222820

Beckwith, N.E., Lehmann, D.R., 1975. The Importance of Halo Effects in Multi-Attribute Attitude Models. Journal of Marketing Research 12, 265–275. https://doi.org/10.1177/002224377501200302

Blumenberg, C., Menezes, A.M.B., Gonçalves, H., Assunção, M.C.F., Wehrmeister, F.C., Barros, F.C., Barros, A.J.D., 2019. The role of questionnaire length and reminders frequency on response rates to a web-based epidemiologic study: a randomised trial. International Journal of Social Research Methodology 22, 625–635. https://doi.org/10.1080/13645579.2019.1629755

Boruch, R.F., Cecil, J.S., 1979. Assuring the confidentiality of social research data. University of Pennsylvania Press, Philadelphia.

Bourdieu, P., 1986. The forms of capital, in: Handbook of Theory and Research for the Sociology of Education. Greenwood Press, New York, pp. 241–258.

Brinkmann, S., 2007. Could Interviews Be Epistemic?: An Alternative to Qualitative Opinion Polling. Qualitative Inquiry 13, 1116–1138. https://doi.org/10.1177/1077800407308222

Buil-Gil, D., Lord, N., Barrett, E., 2021a. The Dynamics of Business, Cybersecurity and Cyber-Victimization: Foregrounding the Internal Guardian in Prevention. Victims & Offenders 16, 286–315. https://doi.org/10.1080/15564886.2020.1814468

Buil-Gil, D., Miró-Llinares, F., Moneva, A., Kemp, S., Díaz-Castaño, N., 2021b. Cybercrime and shifts in opportunities during COVID-19: a preliminary analysis in the UK. European Societies 23, S47–S59. https://doi.org/10.1080/14616696.2020.1804973

Bulmer, M. (Ed.), 1982. Social research ethics: an examination of the merits of covert participant observation. Holmes & Meier Publishers, New York.

Camara, Y., Sow, F., Govoeyi, B., Moula, N., Sissokho, M.M., Antoine-Moussiaux, N., 2019. Stakeholder involvement in cattle-breeding program in developing countries: A Delphi survey. Livestock Science 228, 127–135. https://doi.org/10.1016/j.livsci.2019.08.014
Cavelty, M.D., Wenger, A., 2022. Cyber Security Politics: Socio-Technological Transformations and Political Fragmentation, 1st ed. Routledge, London. https://doi.org/10.4324/9781003110224
Clark, T., 2010. On 'being researched': why do people engage with qualitative research? Qualitative Research 10, 399–419. https://doi.org/10.1177/1468794110366796
Dalkey, N.C., Helmer, O., 1963. An Experimental Application of the DELPHI Method to the Use of Experts. Management Science 9, 458–467. https://doi.org/10.1287/mnsc.9.3.458
De Busser, E., 2009. Data protection in EU and US criminal cooperation: a substantive law approach to the EU internal and transatlantic cooperation in criminal matters between judicial and law enforcement authorities. Maklu Publishers ; International Specialized Book Services, Antwerpen : Portland, OR.
De Kok, L.C., Oosting, D., Spruit, M., 2020. The Influence of Knowledge and Attitude on Intention to Adopt Cybersecure Behaviour. ISIJ 46, 251–266. https://doi.org/10.11610/isij.4618
de Melo, R.A., Cavalcante Valença Fernandes, F.E., Tassitano, R.M., Randau, K.P., 2018. Validation of Questionnaire on Violence in Affective Relationships. J Interpers Violence 088626051881279. https://doi.org/10.1177/0886260518812793
Del-Real, C., 2022. Panorama institucional de la gobernanza de la ciberseguridad en España. REJUCRIM. https://doi.org/10.25267/REJUCRIM.2022.i6.03
Del-Real, C., Díaz-Fernández, A.M., 2022. Understanding the plural landscape of cybersecurity governance in Spain: a matter of capital exchange. Int. Cybersecur. Law Rev. 3, 313–343. https://doi.org/10.1365/s43439-022-00069-4
Del-Real, C., Rodriguez Mesa, M.J., 2022. From black to white: the regulation of ethical hacking in Spain. Information & Communications Technology Law 1–33. https://doi.org/10.1080/13600834.2022.2132595
Díaz-Fernández, A.M., 2019. La investigación de temas sensibles en criminología y seguridad.
Díaz-Fernández, A.M., 2005. Los servicios de inteligencia españoles: desde la guerra civil hasta el 11-M: historia de una transición. Alianza Editorial, Madrid.
Dupont, B., 2004. Security in the Age of Networks. Policing and Society 14, 76–91. https://doi.org/10.1080/1043946042000181575
European Parliament, Council of Europe, 2016. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).
Flick, U., 2007. Designing Qualitative Research. SAGE Publications, Ltd, 1 Oliver's Yard, 55 City Road, London England EC1Y 1SP United Kingdom. https://doi.org/10.4135/9781849208826
Gargon, E., Crew, R., Burnside, G., Williamson, P.R., 2019. Higher number of items associated with significantly lower response rates in COS Delphi surveys. Journal of Clinical Epidemiology 108, 110–120. https://doi.org/10.1016/j.jclinepi.2018.12.010
Glaser, B.G., Strauss, A.L., 1967. The discovery of grounded theory: strategies for qualitative research, 4. paperback printing. ed. Aldine, New Brunswick.
Gordon, T.J., Helmer, O., 1964. Report on a Long-Range Forecasting Study. RAND Corporation, Santa Monica, CA.

Harvey, W.S., 2011. Strategies for conducting elite interviews. Qualitative Research 11, 431–441. https://doi.org/10.1177/1468794111404329
Helmer, O., 1967. Analysis of the Future: The Delphi Method. RAND Corporation, Santa Monica, CA.
Jensen, E.T., 2015. Cyber Sovereignty: The Way Ahead. Texas International Law Journal 50, 275–304.
Kaminska, M., 2021. To retaliate or not: a matter of cyber risk perception (Doctoral Thesis). University of Oxford, Oxford.
Keller, J., von der Gracht, H.A., 2014. The influence of information and communication technology (ICT) on future foresight processes — Results from a Delphi survey. Technological Forecasting and Social Change 85, 81–92. https://doi.org/10.1016/j.techfore.2013.07.010
Lefkowich, M., 2019. When Women Study Men: Gendered Implications for Qualitative Research. International Journal of Qualitative Methods 18, 160940691987238. https://doi.org/10.1177/1609406919872388
Liamputtong, P., 2007. Researching the vulnerable: a guide to sensitive research methods. SAGE, London ; Thousand Oaks, Calif.
Maleh, Y., Sahid, A., Belaissaoui, M., 2021. A maturity framework for cybersecurity governance in organizations. EDPACS 63, 1–22. https://doi.org/10.1080/07366981.2020.1815354
Maramwidze-Merrison, E., 2016. Innovative Methodologies in Qualitative Research: Social Media Window for Accessing Organisational Elites for interviews. Electronic Journal of Business Research Methods 14, 157–167.
Martínez, R., Durán, M., 2017. International Missions as a Way to Improve Civil–Military Relations: The Spanish Case (1989–2015). Democracy and Security 13, 1–23. https://doi.org/10.1080/17419166.2016.1236690
Meuser, M., Nagel, U., 2009. The Expert Interview and Changes in Knowledge Production, in: Bogner, A., Littig, B., Menz, W. (Eds.), Interviewing Experts. Palgrave Macmillan UK, London, pp. 17–42. https://doi.org/10.1057/9780230244276_2
Mikton, C.R., Tanaka, M., Tomlinson, M., Streiner, D.L., Tonmyr, L., Lee, B.X., Fisher, J., Hegadoren, K., Pim, J.E., Wang, S.-J.S., MacMillan, H.L., 2017. Global research priorities for interpersonal violence prevention: a modified Delphi study. Bull. World Health Organ. 95, 36–48. https://doi.org/10.2471/BLT.16.172965
Miller, J., Glassner, B., 1997. The 'Inside' and the 'Outside': Finding Realities in Interviews, in: Silverman, D. (Ed.), Qualitative Research. Theory, Method and Practice. SAGE Publications, London, pp. 99–112.
Moneva, A., Leukfeldt, R., 2023. Insider threats among Dutch SMEs: Nature and extent of incidents, and cyber security measures. Journal of Criminology 263380762311618. https://doi.org/10.1177/26338076231161842
Morgan, D.L., 1996. Focus Groups. Annu. Rev. Sociol. 22, 129–152. https://doi.org/10.1146/annurev.soc.22.1.129
Moustafa, A.A., Bello, A., Maurushat, A., 2021. The Role of User Behaviour in Improving Cyber Security Management. Front. Psychol. 12, 561011. https://doi.org/10.3389/fpsyg.2021.561011
Nespor, J., 2000. Anonymity and Place in Qualitative Inquiry. Qualitative Inquiry 6, 546–569. https://doi.org/10.1177/107780040000600408
Petintseva, O., Faria, R., Eski, Y., 2020. Interviewing Elites, Experts and the Powerful in Criminology.
Porcedda, M.G., 2018. 'Privacy by Design' in EU Law: Matching Privacy Protection Goals with the Essence of the Rights to Private Life and Data Protection, in: Medina, M.,

Mitrakas, A., Rannenberg, K., Schweighofer, E., Tsouroulas, N. (Eds.), Privacy Technologies and Policy, Lecture Notes in Computer Science. Springer International Publishing, Cham, pp. 183–204. https://doi.org/10.1007/978-3-030-02547-2_11
Rowe, G., Wright, G., 1999. The Delphi technique as a forecasting tool: issues and analysis. International Journal of Forecasting 15, 353–375.
Rowe, G., Wright, G., Bolger, F., 1991. Delphi: A reevaluation of research and theory. Technological Forecasting and Social Change 39, 235–251. https://doi.org/10.1016/0040-1625(91)90039-I
Svensson, M., Svensson, T., Hansen, A.W., Trolle Lagerros, Y., 2012. The effect of reminders in a web-based intervention study. Eur J Epidemiol 27, 333–340. https://doi.org/10.1007/s10654-012-9687-5
Tanczer, L.M., 2020. 50 shades of hacking: How IT and cybersecurity industry actors perceive good, bad, and former hackers. Contemporary Security Policy 41, 108–128. https://doi.org/10.1080/13523260.2019.1669336
Trim, P.R.J., Upton, D., 2013. Cyber security culture: counteracting cyber threats through organizational learning and training. Gower, Farnham.
Van Audenhove, L., Donders, K., 2019. Talking to People III: Expert Interviews and Elite Interviews, in: Van den Bulck, H., Puppis, M., Donders, K., Van Audenhove, L. (Eds.), The Palgrave Handbook of Methods for Media Policy Research. Palgrave Macmillan, Cham, pp. 179–197. https://doi.org/10.1007/978-3-030-16065-4_10
van den Berg, J., Zoggel, J. van, Snels, M., Leeuwen, M.W.V., Boeke, S., Koppen, L. van de, Lubbe, J.C.A. van der, Berg, B. van den, Bos, T. de, 2014. On (the Emergence of) Cyber Security Science and its Challenges for Cyber Security Education. Presented at the NATO STO/IST-122 symposium, Tallinn, Tallinn.
van Steen, D.T., De Busser, E., 2021. Security by Behavioural Design: A Rapid Review (Final report for NCSC-NL). Institute of Security and Global Affairs, Leiden University.
Van Steen, T., Deeleman, J.R.A., 2021. Successful gamification of cybersecurity training. Cyberpsychology, Behavior, and Social Networking 24, 593–598. https://doi.org/10.1089/cyber.2020.0526
Van Steen, T., Norris, E., Atha, K., Joinson, A., 2020. What (if any) behaviour change techniques do government-led cybersecurity awareness campaigns use? Journal of Cybersecurity 6, tyaa019. https://doi.org/10.1093/cybsec/tyaa019