ON THE INSURABILITY OF CYBER WARFARE: AN INVESTIGATION INTO THE GERMAN CYBER INSURANCE MARKET

ABSTRACT
Insurance is an important part of a constellation of institutions that assist in the provision of security, resilience and welfare. This is true across a range of threats, including those in the cyber domain. Cyber risks, particularly those associated with cyber warfare, present a considerable threat to the international economy and society owing to their inherent unpredictability and far-reaching consequences. These risks have the potential to impact security and cause significant economic losses, making them a critical concern for governments, businesses, and individuals alike. This research addresses the protection gap arising from cyber warfare exclusions in the context of cyber insurance. Furthermore, this study analyses the impact of war exclusion clauses on cyber insurance coverage during the Ukraine and Russia conflict. A mixed methods approach was employed, analyzing 44 cyber insurance policies in the German SME insurance market, and conducting interviews with 26 cyber insurance experts from various areas of the industry. It is found that insurers employ vaguely worded war exclusion clauses to restrict the scope of their policies. The study finds that such exclusionary provisions fail to account for emerging forms of warfare, including hybrid warfare and rapidly evolving cyber operations. The analysis provides practical solutions to address these challenges by highlighting the problems of the cyber war exclusion clause, demonstrating the perceptions and understanding of cyber insurers, and providing possible solutions to the insurability of cyber war risks. A well-functioning insurance market around cyber warfare would improve the resilience of nation-states in the face of such attacks. This paper provides important insights on the operation of this critical risk transfer market, based on the view of market participants.

Keywords:
Cyber warfare, cybersecurity, cyber risk, cyber insurance, risk management, cyber war risk

Disclosure statement
On behalf of all authors, the corresponding author states that there is no conflict of interest.

1. Introduction

Cyber warfare is a complex, emergent risk residing within the virtual architectures of international security. Unlike traditional threats, physical geography does not protect a state from cyberattack, and distance does not give time for defense or response; cyber transcends traditional precepts of geopolitics. Simultaneous, or proliferating multi-locational viral acts of sabotage at macro and micro levels contain the potential to destabilize an economy. The attacker, in the meantime, collects data that can be monetized as intelligence, which together with other criminal activities, accumulates finance to further evolve the complexity and potency of its technologies. At the same time a cyber-attack is designed to invoke a sense of panic among a target population; and to dilute the effects of sovereignty, political culture and legal procedure. A truly global phenomenon, cyber risks flow along the primary capillaries of human interaction and commerce, operating against individual, local and international security. The traditional terrestrial military response to this existential threat is obsolete (Gartzke, 2013).

In the past, faced with global risks of similar potential, civil society stepped in to address the challenge of maintaining order. The oldest maritime insurance company, Lloyds of London, we need to remember, was begotten as an instrument to counter the sorts of novel risks encountered during early colonial enterprise (Carter & Enoizi, 2020; Martin, 1876). 18th and 19th century European expansion into the global south would have been a loss-making operation were it not for the invention of insurance.

Lloyds regulated the inherent turbulence and risk of maritime trade by redistributing risk and indemnifying loss. It built its business around an extensive network of intelligence agents posted at major ports throughout the world. Lloyds was a repository for data on all maritime activity, both commercial and criminal. The rising cost of insurance during the Revolutionary and Napoleonic wars (1793-1815), and the sudden growth of Britain's maritime empire drastically expanded Lloyds commercial activity (Kingston, 2007). The analogy we wish to draw is found in the role played by Lloyds in securing the interests of the British Empire. It is tautological to observe that whereas once the sea was the domain of risk, adventure and profit, it is now cyber that possesses these attributes—the sea interconnected ports and harbors on planetary-sized sea lanes of communication. Akin to the cyber domain today, sea was a lawless, deterritorialized space shaped by commercial, criminal and military freedom. Insurance thrived in the chaos of criminality, war and colonialism, and brought certainty to the immense and complex foundations of today's global political economy. Certainly, it retains its role in the 21st century in this regard. Most recently, the piracy crisis off the coast of Somalia was managed by the public-private cooperation between NATO and Lloyds (Lobo-Guerrero, 2012).

Thus, insurance has long held an important function in terms of managing risks pertaining to geopolitics. It is an important bulwark against those that would seek to disrupt the economic well-being of the major world economies. That said, in the realm of cyber warfare, there is some evidence of what we might refer to as market failure. Extant insurance policies do not cover many of the risks under this category. All this means that victims of cyberwarfare are less resilient, and those that propagate such attacks are better able to leverage the capacity for attacks through the digital space. The shortcomings of the cyber risk insurance markets are attracting much attention. The Financial Times reported earlier this year that large insurers are in talks with the UK government on whether there is merit in extending the terrorist reinsurance scheme to include State-backed cyber-attacks (Smith, 2023). This is clearly an issue that pertains to international security. This paper offers a view of the rationale of key actors in this market and, as such, is an important

contribution to policy-making in this area. Governments worldwide are now paying more attention to the danger posed by cyber hackers. There are several national initiatives that seek to address the security risks attendant to cyber-crime. In April of 2023, the UK Cabinet Office minister, Oliver Dowden spoke of the dangers of ideologically motivated cyber-attacks and, indeed, issued a “call to arms” to businesses to strengthen their security (Rathbone, 2023). Insurance is an essential line of defense.

Cyber insurance is a commonly used risk transfer mechanism, but it does not extend coverage to losses arising from cyber warfare events, which are usually excluded under the war exclusion clause. The lack of clarity surrounding insurance coverage for cyber warfare incidents and other significant cyber risks impedes the growth of strong and socially beneficial cyber insurance markets (Bateman, 2020). This study investigates the cyber war exclusion clause included in cyber insurance policies offered to Small and Medium-sized Enterprises (SMEs) by both international and local insurance companies operating within the German market. The research creates and analyzes a comprehensive dataset that includes the wording of war exclusions in cyber insurance policies to address the associated challenges. The research is further supported and extended by conducting semi-structured interviews with cyber experts from the insurance sector. The analysis provides important insights into how insurance companies address cyber war risks and identifies potential approaches for the insurability of such risks in the current cyber insurance market.

The war exclusion clause presents a challenge in cyber insurance policies because the definition of war can be interpreted differently across various regulatory jurisdictions, depending on factors such as cultural norms, attitudes, and understanding (Dennen, 2005). The variability in the interpretation of the exclusion clause can result in ambiguity and uncertainty when applying it, has the potential to generate legal complexities and disputes. Furthermore, a lack of global agreement regarding the specific conduct or set of criteria that distinguish a cyber incident as an act of terrorism or warfare further contributes to this issue (Woods & Weinkle, 2020). The absence of a universal understanding of the definitions of these terms could lead to inconsistent applications of exclusion clauses across different jurisdictions and complicate the resolution of disputes (Carter & Enoizi, 2020). The Bank of America has raised concerns with Lloyd's of London about the exclusion of state-sponsored cyberattacks from standard insurance policies (Smith, 2023). This underscores the concerns of financial institutions regarding alterations to a major safeguard.

The far-reaching impact of cyber risks is exploited by actors that financially support or provide information technology (IT) infrastructure to carry out state-sponsored attacks on other countries to cause losses or obtain trade secrets (Maschmeyer, 2021). The Council on Foreign Relations (CFR) Cyber Operations Tracker dataset estimates that at least 700 verified state-sponsored cyber-attacks have been conducted since 2005 (CFR, 2022). The suspected state-sponsored cyber-attack called "NotPetya" had a more significant impact (Ferland, 2019). This data-destruction malware infected hundreds of companies internationally and caused an estimated loss of USD 10 billion (PCS, 2019). In 2010, a computer virus known as Stuxnet led to the destruction of more than 1,000 Iranian centrifuges and delayed Iran's enrichment program (Nye, 2017). Stuxnet is notable for being one of the first examples of a suspected cyber weapon being used in a state-sponsored attack, and it demonstrated the potential for such attacks to have real-world consequences (Gartzke, 2013). These and other international cyber loss events have raised the profile of cybersecurity, leading to increased attention and spurring geopolitical developments (Buchanan, 2020; Vakulchuk et al., 2020).

In parallel to cybersecurity, the transfer of risk via cyber insurance is challenging in the context of cyber warfare. From a risk management perspective, adopting cyber insurance can play a vital role in enhancing the overall resilience of international security and companies in the face of cyber threats (Hausken, 2020; Nye, 2017). Cyber insurance can provide companies with financial protection against potential losses from cyber incidents, including data breaches, cyber-attacks, and other malicious activities (Eling, 2018). With cyber insurance, a significant portion of a company's cyber exposure can be transferred to an insurer by purchasing a cyber insurance policy (Talesh, 2018). Furthermore, the adoption of cyber insurance can encourage corporates to improve their cybersecurity posture, as insurance providers often require companies to meet specific security standards as a condition for coverage (MacColl et al., 2021; Marchant & Stevens, 2017).

By requiring minimum security standards for the insurance coverage, they provide cyber insurers positively influence the cybersecurity measures of companies and thus act as proxy regulators (Marchant & Stevens, 2017). However, concerning cyber warfare, such cyber losses are not covered by the cyber warfare exclusion clause under the terms of the insurance policies in place (Gold, 2019). Reasons for this are the unpredictability of these events due to the lack of data and the limited experience of cyber insurers with cyber conflicts Cremer et al., 2022; Slayton, 2017). However, even in the context of traditional warfare, there exist challenges regarding the interpretation of insurance terms, which are often a subject of frequent debate and discussion among scholars and practitioners (Satariano & Perlroth, 2019). Given the escalating frequency and severity of cyber-attacks, a comprehensive cyber insurance market is imperative. However, for such a market to be effective, it is essential to understand the limitations and exclusions of cyber war coverage (Bateman, 2020). Therefore, conducting research in this area is necessary to guarantee that the cyber insurance market can function optimally and effectively minimize the overall impact of cyber risks on global security.

Research and industry best practices show that cyber insurance is still in its infancy (Eling, 2020; Nurse et al., 2020; Xu & Hua, 2019). Unclear policy wording, a lack of standardization and inconsistent terms in cyber insurance present companies with significant insurance gaps (OECD, 2020). The war exclusion clause is a provision that precludes coverage for losses resulting from the impact of armed conflicts. The imprecise nature of such wordings frequently presents policyholders with uncertainties regarding the scope of coverage, mainly due to the inherent vagueness of the definition of war (Carter & Enoizi, 2020). Cyber conflicts between states present a significant challenge, not just for the demand side of the cyber insurance market (Woods & Weinkle, 2020). These conflicts also challenge providers of cyber insurance (Woods & Simpson, 2017). For instance, the accumulated impact of cyber warfare makes in problematic to adequately insure and calculate such cyber risks (Falco et al., 2019; Marotta et al., 2017). Although there have been some investigations into the war exclusion clauses present in cyber insurance policies, thus far, there has been no interviews conducted with experts in the field of cyber insurance (Bateman, 2020). In addition, due to a lack of open declared cyber conflicts, insight from practitioners in the field are only now becoming available. In the context of an ongoing cyber conflict, the acquisition of qualitative data is a valuable resource for gaining insight into the intricacies of cyber insurance, including its presence, design, and management. The absence of unambiguous guidelines for insurance coverage of cyber war events and other consequential cyber risks poses an obstacle to the emergence of a robust and socially constructive cyber insurance market.

The selection of Germany as the focus of this case study is based on several factors. First, Germany's cybersecurity policy has successfully expanded the protective role of various security institutions, centralized control over critical infrastructure, and implemented a national security strategy to ensure protection across all sectors (Monstadt & Schmidt, 2019; Steiger, 2022). This approach is similar to that taken in the United States (Shafqat & Masood, 2016). Germany also shares a similar objective with the United States: to promote resilience rather than absolute protection (Wagner, 2021). Second, from an insurance perspective, the German insurance market has the second largest premium volume in the EU and, with its large number of insurance companies, is an ideal candidate for investigation within Europe (EIOPA, 2022). Additionally, all insurance companies in Germany are supervised by the Federal Financial Supervisory Authority, which provides publicly available data on all supervised insurers. Overall, the selection of Germany as the case study for this research is based on its robust cybersecurity policy and the relatively more mature insurance market.

German insurance companies demonstrably hold the potential to shape market risk and strengthen the architecture of international security. Focusing upon the Russian invasion of Ukraine, this study mines deep into the attitudes of insurance professionals to cyber warfare events. We highlight the perceptions of cyber insurers to the war risk market, providing insight into the relationship between current global causes of insecurity and the performative power of the modern insurance sector.

A mixed methods approach was selected to achieve this aim as it is particularly useful in integrating findings from various research methods and generating comprehensive knowledge for both academic theory and practical applications (Johnson & Onwuegbuzie, 2004). This approach begins by utilizing an inductive qualitative content analysis to examine war exclusions in cyber policy wordings of both German and international cyber insurers. The cyber policy wordings analyzed in this study represent approximately 82% of the cyber insurers under supervision in Germany. In addition to analyzing policy conditions, semi-structured interviews with cyber insurance experts from insurance, reinsurance, and insurance brokers were conducted and evaluated through thematic analysis. The findings from these interviews are used to describe, validate, and expand on the results obtained from the content analysis.

We highlight that this work on cyber war exclusions using the structured interview methodological approach with cyber insurance professionals, including data on an ongoing cyber conflict (Ukraine/Russia), represents a novel contribution to the field of security studies. The study provides unique insights into how cyber warfare exclusions are currently being handled in the insurance industry (e.g., vague wording to limit the scope of insurance) and explore the implications of this approach in light of real-world cyber conflicts.

The structure of the paper is as follows. In Section 2, related literature on cyber insurance exclusions, with a focus on the cyber war exclusion clause, is presented. Section 3 outlines the mixed research method employed in this study, including the inductive qualitative content analysis and semi-structured interviews with cyber insurance experts. Section 4 presents the results from the thematic analysis of the structured interviews and provides an overview of the cyber warfare exclusion clauses. Section 5 offers additional discussion and interpretation of the results. Finally, Section 6 concludes the article.

2. Related work

Despite the increasing importance of cyber risks, the interdisciplinary field of cyber warfare and cyber insurance remains limited (Eling, 2020; Gorwa & Smeets, 2019). Woods and Weinkle (2020) conducted a comprehensive study of war exclusion clauses in US cyber policies,

analyzing 56 policies through longitudinal analysis. Among the policies scrutinized, 41 policies were found to contain a war clause, while the remaining 15 policies did not exhibit such a provision. In their summary, the authors highlight the need for insurers to provide clear guidelines on the point at which cyber conflict becomes uninsurable if existing war clauses cannot be meaningfully applied. Similar research was conducted by Bateman (2020). The author investigated the ambiguity surrounding the applicability of cyber war and terrorism exclusions clauses, and proposed to abandon the traditional exclusions for war and terrorism for cyber losses. In their research, Ferland (2019) conducted a thorough examination of the war exclusion clause in insurance policies, with a particular focus on the notable case of Mondelez International, Inc. v. Zurich American Insurance Company. This research focused on attributing a cyber-attack to a specific state and the complexities of interpreting a war exclusion clause in the context of cyber incidents.[1] It was noted that there is a growing need for policy wording that is more transparent regarding cyber war exclusions and the possibility of shifting coverage from conventional risks to cyber risks.

Proposing a "call to action," Falco et al. (2019) suggest an agenda for cyber risk and cyber insurance to accelerate the pace of cyber research progress and emphasize the need for greater collaboration across disciplines. The paper's authors comprise a diverse group of individuals, including academics, industry practitioners, and policymakers from various parts of the world. In their agenda, the authors list six major interdisciplinary questions, which also include risk transfer via cyber insurance. Romanosky et al. (2019) conducted a thorough review of the underwriting process for cyber insurance. The authors analyzed 235 publicly available US cyber insurance policies and examined critical components of these policies: coverage, exclusions, application questionnaires, and pricing. Their findings revealed that while some insurers utilized simplistic flat rates based on a single calculation of expected loss, others considered more complex parameters such as the company's asset value, company revenue, standard insurance metrics such as deductibles and limits, and industry-specific factors. Cremer et al. (2022) carried out a comprehensive study on general exclusions in cyber insurance policies and their impact on companies facing cyber risks. The authors employed an inductive qualitative content analysis approach to examine policy terms and conditions from 40 German cyber insurers and compared the results with real-life cyber risk events. The study found that some exclusions could pose significant risks to companies, emphasizing the importance of careful policy selection and understanding.

The study conducted by Li and Liu (2021) investigates the advancements in cybersecurity and the evolving nature of security threats. Through an analytical lens, the authors evaluate the challenges, strengths, and weaknesses of various cybersecurity methods. The research findings reveal that conventional approaches, such as reliance on military and police by governments, are not sufficient to ensure national security to cyber threats such as cyber warfare. Thus, the study suggests that bilateral collaboration between governments and the private sector is imperative, as they share a mutual interest in addressing these threats. A similar analysis on cyber warfare was performed by Trifunović and Bjelica (2020), who looked at trends and technologies in the context of cyber warfare. The study identified that the field of cyber security has assumed a critical role for security services in identifying potential threats emanating from this domain. In the context of security and resilience with respect to cyberspace, Hausken (2020)

[1] It should be noted that this was an all-risk insurance policy from Mondolez covering all risks of loss or damage to Mondelez' property. It was not a specific cyber insurance policy.

conducted a systematic literature analysis. The findings discuss the different actors involved in cyber resilience, including non-threat actors, threat actors, and hybrid actors, and how they operate at different levels. The author also emphasized the significance of cyber resilience as a prerequisite for cyber insurance.

3. Method

This study adopts a mixed methods approach to investigate insurance coverage for cyber war events within typical SMEs cyber insurance policies. In Section 3.1, semi-structured interviews were conducted with experts in the cyber insurance industry to obtain an aggregate view and perception from the insurance industry on cyber war. In Section 3.2, an inductive qualitative content analysis was carried out on the war exclusion clauses in cyber insurance policies to validate and complement the findings from the interviews.

3.1 Semi-structured interviews with cyber insurance experts

The war exclusion clause may not serve as a definitive indication of how cyber insurers perceive and manage cyber war risks. Given the dynamic nature of cyber threats, there is still a need for more qualitative research to bridge gaps in knowledge and draw upon expert insights. This lacuna of research is also highlighted by the cyber research agenda of Falco et al. (2019), in which they call for interviews with cyber insurance providers and reinsurers. Interviews can yield valuable insights into cyber insurers' presence, design, and risk management practices. Additionally, industry experts' experiences and perspectives can contribute to the collection of qualitative data on the cyber war clause, which the scientific community can utilize. Specifically, there is a gap in the collection of qualitative data on the open cyber conflict between Ukraine and Russia, which this research addresses.

The semi-structured e-interviews were conducted following the Format of Bampton and Cowton (2002) and Newcomer et al. (2015). This form of interviewing allows open-ended questions to be asked, allowing industry experts to comment and expand on the topic more freely and ask more specific questions to get more precise answers (DiCicco-Bloom & Crabtree, 2006). The application of semi-structured interviews in cyber insurance has already been conducted by Bahşi et al. (2020) and Franke and Meland (2019). Semi-structured interviews offer a viable method for acquiring data pertaining to cyber insurers' risk management strategies and perceptions of cyber warfare.

In selecting industry experts for interviews, the emphasis was placed on primary insurers, reinsurers, and insurance brokers due to their substantial role in the insurance industry's value chain (Eling & Lehmann, 2018). The insurance broker has a vested interest in safeguarding its insurance clients and ensuring that they have adequate coverage in the event of a cyber-attack (Beenken et al., 2018). Conversely, the primary insurer and reinsurer have a stake in maintaining sufficient insurance coverage and risk exposure relative to the insurance premium (Powell & Sommer, 2007). Given these considerations, the selection of interviewees from these parties is well-suited for gathering valuable insights into the intersection of cyber warfare and the cyber insurance industry. After identifying the relevant areas of interest, various methods were employed to select and invite cyber experts for interviews. Direct contact was initiated when possible, such as through information available on their website. If no information was available on possible contacts, the cyber insurers were contacted via the general communication channels. Regarding insurance brokers and reinsurers, only those who publicly disclosed their reports on cyber insurance were considered.

The selected companies were sent interview requests that provided details on the researchers' background, the research

objectives, and other relevant information. If the interview was accepted, the interviewees received a pre-read memo 48 hours prior to the interview outlining the interview process, the topics to be covered, and the commitments to be made. The interviews were conducted using MS Team or Zoom software, with the industry experts' permission to record. Approximately 72 hours after the interview, a draft of the interview notes was shared with the experts for their review and comments, which could be added, changed, or deleted before signing. Out of 60 companies contacted, 26 participants were available for interviews. The semi-structured interviews were conducted between 10. November 2022, and 3. February 2023, with one hour allotted for each interview.

The interviewees were provided with assurance that the recorded data would be anonymized, meaning that any information that could potentially reveal the identity of the interviewee or their company would be removed. Table 2 in this paper provides a summary of the expertise and experience of the cyber experts involved in the interviews. For a more detailed overview, please refer to section 1 in the appendix.

Organization type	Number of industry experts	Average cyber experience in years
Broker	7	6.4
Primary insurer	14	6.1
Reinsurer	5	6.2

Table 1: Overview of the cyber insurance experts.

The formulation of the interview questions was based on the deductive inference from the analysis of the insurance policy, which revealed that cyber insurers generally exclude claims arising from cyber warfare. The interviews were conducted to gain an understanding of the significance and perception of cyber warfare in relation to cyber insurance from the perspective of cyber insurers. To achieve this aim, the questions were structured in a flexible and interactive manner, allowing for a dynamic interview guide (Kallio et al., 2016). The questions are as follows:

1. War exclusion clauses in cyber insurance products usually only refer to the term war but do not provide any further definition. In your experience, what are the problems regarding the war exclusion clause?

2. In your expert opinion, what is the difference between cyber warfare and traditional warfare?

3. Due to the cyber-attacks, the conflict may also affect insured companies. In your experience, have cyber claims been rejected due to war events? If yes, has there been an increase in declined claims due to the Ukraine/Russia conflict?

4. Even if no state-sponsored cyber-attacks were detected, has the incident loss landscape changed since the conflict?

5. State-sponsored cyber-attacks, like the suspected Notpetya malware, have the potential to cause major losses worldwide. In your expert opinion, what would be necessary to insure against these cyber warfare risks?

Following the work of Bahşi et al. (2020), the interviews were transcribed, and subsequently, codes were assigned to the text segments using MAXQDA software.

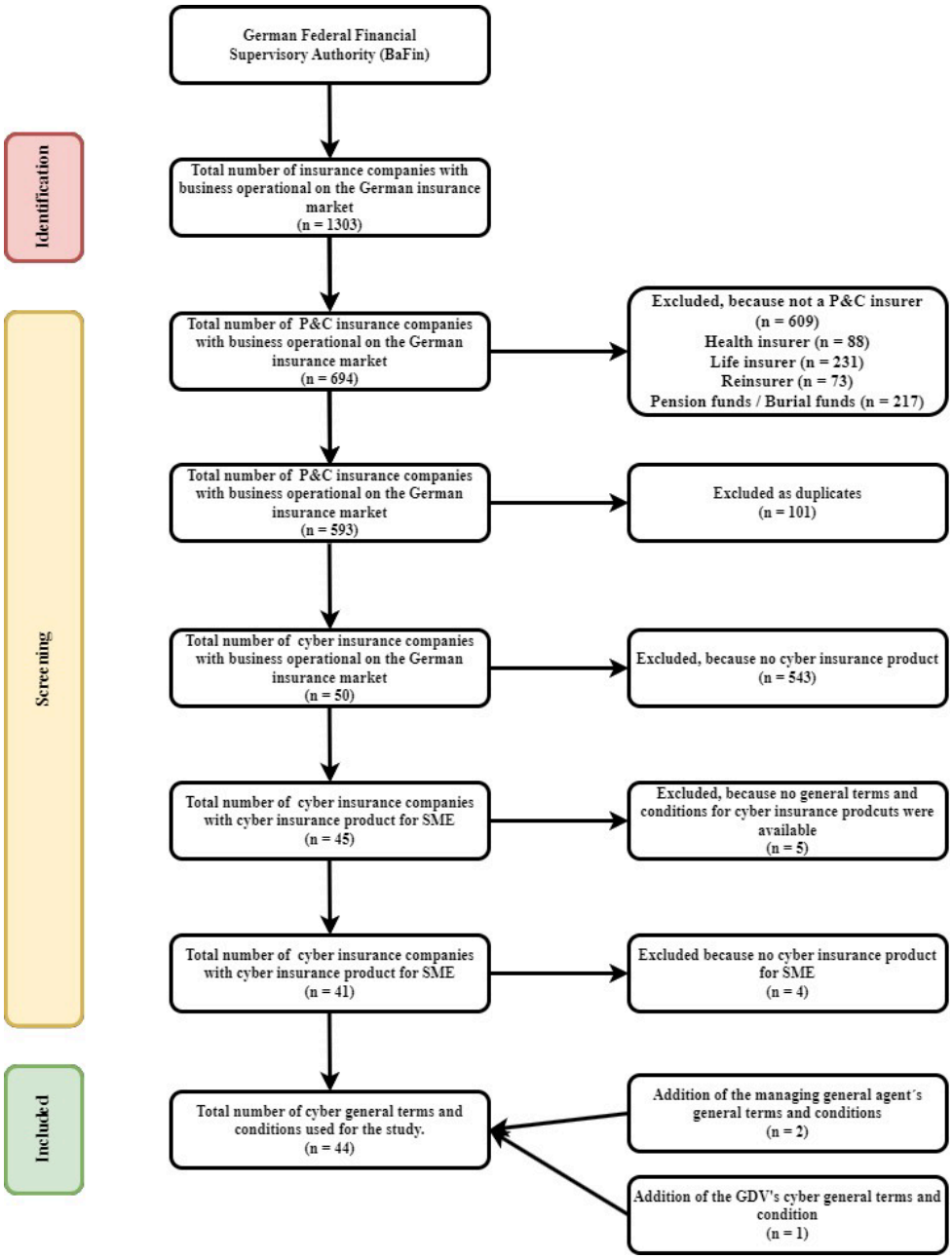

Figure 1: The cyber insurance policy database used in this study was developed using data provided by the German Federal Financial Supervisory Authority. To ensure the accuracy of the data, a PRISMA screening process was applied, which involved the use of stringent eligibility criteria. As a result, 44 cyber general terms and conditions and their respective war exclusion clauses were identified as suitable for inclusion in this study.

3.2 Cyber Insurance policy analysis

For the inductive qualitative content analysis, a database of 44 war exclusions clauses from the cyber insurance terms and conditions was created based on publicly available information. The war exclusion clauses represent approx. 82% of the German cyber insurer. In addition, the war exclusion clauses of general managing agents of and German Insurance Association (GDV) were added.

This study examines the war exclusion clause included in the cyber insurance policies provided to SMEs by international and local cyber insurance companies

operating within the German market. Information on the selected cyber insurance companies was sourced from the German Federal Financial Supervisory Authority (BaFin) to collect the necessary data for this study. With over 1300 insurance companies and the second largest premium income in the EU, the German insurance market represents a prime candidate for investigation within Europe (EIOPA2022).

Following the research Wrede et al. (2020) and Cremer et al. (2022), the dataset was selected for eligible cyber insurers in a multistep process based on the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) (Page et al., 2021), shown in Figure 1. To ensure the dataset used in this study was appropriate, the authors established specific criteria that were applied in a systematic process. First, insurers that do not offer property and casualty (P&C) insurance were excluded, resulting in the removal of 609 insurers from the original dataset. Next, insurers that operated in the insurance market in the form of subsidiaries or similar were removed as duplicates, which left a remaining pool of 593 eligible insurers. To determine if these remaining insurers offered cyber insurance products, the authors manually checked their respective websites, resulting in the identification of 50 cyber insurers in Germany. To evaluate the plausibility of the identified number of 50 cyber insurers, the number of GDV members offering cyber insurance was utilized as a benchmark. The GDV members were selected as a reference point since they constitute approximately 97% of insurance companies in operation within Germany (GDV, 2021). Upon conducting the verification, it was found that 39 members of the insurance association offered policies pertaining to cyber insurance (GDV, 2022).[2] Based on this, it can be inferred that the PRISMA process did not overlook a substantial number of cyber insurers, given the identified count of 50.[3] Between November 2021 and February 2022, the authors collected publicly available general terms and conditions of the identified cyber insurers via their websites to extract the war exclusion clauses for this analysis. If these documents were not available, they were requested via email from the respective insurers. This process resulted in the collection of 41 general terms and conditions for SMEs that were used as a starting point for further analysis. This included the template model terms and conditions of the GDV and two additional cyber insurance terms and conditions of managing general agents.

[2] Originally, the number of cyber insurers included 42, but these were two duplicates as well as one reinsurer.

[3] GDV makes no claim that the list of members of cyber insurers is complete. Nevertheless, in order to create a benchmark, the number of members was used for verification.

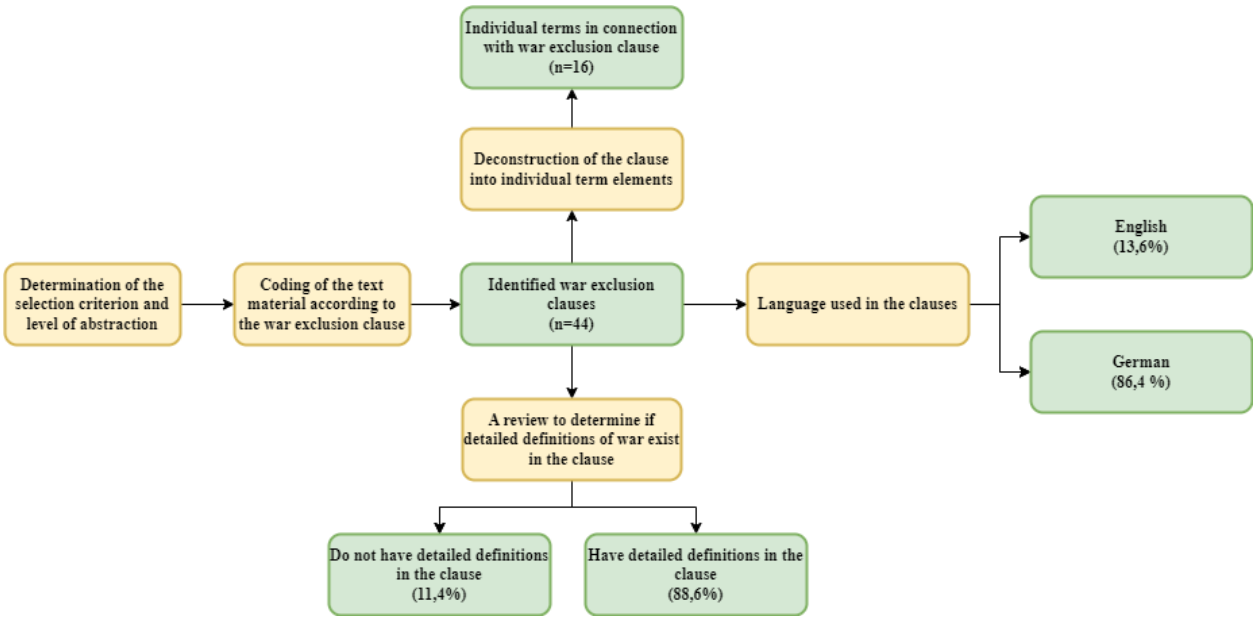

Figure 2: To reduce the text material, relevant sections were identified and coded with "text-related" markers. The aim was to reduce complexity and make the data more accessible. Next, the text was further analyzed by extracting clauses, resulting in a total of.

In the subsequent phase of this research, a comprehensive analysis of textual materials was performed, as illustrated in Figure 2. Specifically, the study focused on analyzing the general cyber terms and conditions of insurance and the content of the war exclusions clause of the cyber insurers that met the eligibility criteria. To facilitate and systematically structure the coding process, the researchers utilized the qualitative data analysis software MAXQDA (MAXQDA, 2022). The analysis was carried out using Maying's model of qualitative content analysis, which is a rule-based and systematic approach to data evaluation (Mayring, 2021). The categories used in the analysis were derived directly from the text material of the war exclusion clause.

In the initial phase, the qualitative data material was systematically coded to reduce complexity. Relevant text segments were identified, marked, and assigned "text-related" codes. Exclusions marked "war" were considered relevant and coded accordingly. The dataset contained cyber insurance terms and conditions in both German and English languages due to the international nature of some cyber insurers. The war exclusion clauses were deconstructed into individual components in the subsequent process, and the terms mentioned were coded into different categories. The texts were further evaluated to check for any detailed formulations or definitions of the exclusion. If such formulations were present, the texts were coded accordingly. The coded text material was analyzed and summarized based on categories. In cases where there were strong similarities in terms, the categories were merged to form uniform summaries. The final category scheme included 16 individual terms and was derived from the analysis of 44 war exclusion clauses of cyber policies.

4. Results

The study's results are divided into three parts. The first part presents the results of the semi-structured interviews with cyber insurance experts. The second part includes the findings of the inductive qualitative content analysis of the war exclusion clause in general cyber wordings, which provide new qualitative data and

serve to both extend and corroborate the findings from the interviews. The last part is a comparison of the results with previous studies in the literature.

4.1 Findings from semi-structured interviews

In the following subsections, the results are presented. These represent a summary of the interviewee's responses to the relevant question. It is important to add a caveat at this point that the insights gained from the interviews are inherently subjective and may not reflect directly measurable variables.

4.1.1 War exclusion clauses in cyber insurance products

The results of the interviews indicate that the war clause poses significant challenges for the cyber insurance industry. An important issue is the lack of a clear definition for the term "war" or "warlike incidents" in the exclusion clauses of cyber insurance products. As a result, policyholders are required to interpret the meaning of these terms themselves, and insurers *must* consider the understanding of the average policyholder when developing their policies. Moreover, given that there is no standard definition of "war," some insurers have intentionally adopted vague language to limit the scope of their policies, citing the lack of case law as a justification. Consequently, cyber insurers have been able to avoid the issue since the war exclusion clauses have never been tested in court. In addition, cyber insurers are awaiting a decision from the Merck case, which is the only ongoing case regarding the war exclusion (Vanderford, 2023).[4]

Another challenge identified by the interviewees is the origin of the war exclusion clause, which arose from other insurance conditions and lines where the focus was on physical warfare. The war exclusion clause does not address new forms of hybrid warfare or cyber operations, which are dynamically evolving. Cyber-attacks pose a unique challenge, as it is difficult to attribute and prove them compared to traditional war actions. Identifying the initiator and assessing the damage is easier in the case of traditional acts of war, such as missile attacks. However, in the case of cyber-attacks, the cybercriminals are often anonymous and unverifiable. Additionally, there is no official declaration of war in cyberspace, which complicates matters further. When states are involved, assessing the potential scope and damage of cyber-attacks can be particularly challenging due to their greater financial resources and capabilities to carry out attacks. For instance, it is unclear whether an attacker using a laptop on behalf of a government can be classified as an act of war. The issue at hand is further compounded by the absence of robust cyber arms control measures and a universally accepted set of international regulations or standards governing the conduct of nation-states during cyber warfare (Eilstrup-Sangiovanni, 2018).

These complexities present significant difficulties for cyber insurers since they bear the burden of proof if a claim is denied. Interviewees expressed skepticism about Lloyds' new war exclusion clauses, believing that they are insufficiently transparent to address these issues (Lloyds Market Association, 2021). Nevertheless, they viewed the inclusion of the clause as a positive step towards greater clarity in the industry.

4.1.2 Differences between cyber warfare and traditional warefare

The diverse views of experts on the distinction between cyber warfare and traditional warfare demonstrate the complexities of defining and understanding

[4] As with the settled case between Mondolez and Zurich, the Merck case involves all-risk insurance and not standalone cyber insurance.

cyber warfare. Despite the varied opinions, common themes emerged from the analysis of the interview data. Consensus existed around the fact that both cyber warfare and traditional warfare are intended to damage and destabilize the targeted.
country. However, the mode of attack used, visibility, and impact are factors that were considered to distinguish the two types of warfare.

influence public opinion). Therefore, according to the interviewees, cyber warfare aims to harm other countries undetected, irrespective of active engagement. The experts also highlighted the potential impact of cyber-attacks, particularly on companies that function as critical infrastructure. Moreover, due to the increased interconnectedness of critical infrastructure, there is a higher potential for collateral damage.

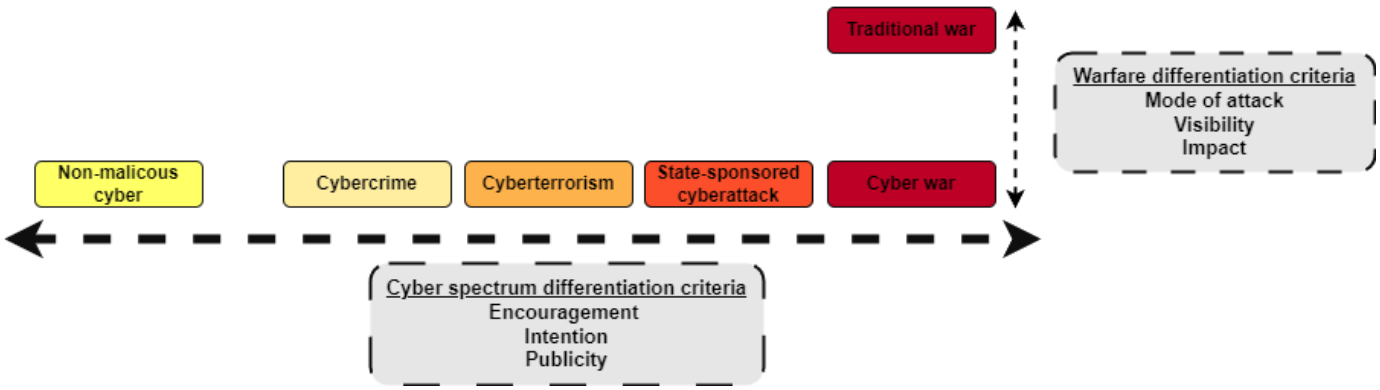

Figure 3: Building upon the research conducted by (Mitoraj, 2020), the present work expands upon the existing spectrum of cyber activity by incorporating warfare criteria into the framework. The spectrum encompasses a wide range of cyber activities significant and potentially devastating effects of cyber warfare.

To further elaborate on the differentiation commonly observed within the insurance sector, Figure 3 serves as a valuable addition to the existing comprehension of critical criteria. Regarding tools, the experts stated that traditional warfare requires sophisticated weapons and equipment that are more difficult to obtain compared to cyber warfare, which only requires a computer with an internet connection. As for visibility, traditional warfare is often characterized by visible military action, such as armies with soldiers and tanks, whereas cyber warfare is often perceived as invisible, preparatory, and supportive (e.g., example, destabilizing critical infrastructure or spreading fake news to

4.1.3 Rejection of cyber claims due to the Ukraine/Russia conflict

All the interviewees reported that at this juncture, since the onset of the Ukraine/Russia conflict on February 24, 2022, they have not come across any instances of insurance claims being rejected due to the cyber war exclusion, either within their own organization or at other insurance companies.[5] To corroborate this finding, another literature review on current news portals focusing on insurance on the part of the authors also came to the same conclusion. Although the insurance industry had anticipated an increased number of cyber claims as a result of the conflict, it was surprising that no cyber insurance claims have been denied based on the cyberwar exclusion since the conflict. Many were surprised as they had assumed that the conflict would result in significant cyber losses.

[5] The authors conducted an extensive literature search from March 13-15, 2023, and reviewed current news portals related to insurance, and they came to the same conclusion as the interviewees.

Furthermore, cyber experts have highlighted that cyber insurers are exercising greater caution when underwriting risks, particularly in the energy and infrastructure sectors, because of the Ukraine/Russia conflict.

4.1.4 Change in cyber insurance claims due to the Ukraine/Russia conflict

Changes in cyber claims reporting varied significantly among the interviewees, with 38,5% reporting a decrease, 11,5% flat, and 50% reporting increased claims frequency in the German cyber insurance market. From those that reported a decrease, there was uncertainty about whether this was because of an actual decrease in cyber-attacks or a temporary pause due to acts of war. Some insurers did not note any changes in the frequency or amount of claims, which could be explained by the differences in customer segments. For instance, cyber insurers serving SMEs were less affected than those serving larger corporations. One possible reason is that hackers see corporations as more lucrative targets, even though cybersecurity measures are generally higher than for SMEs. Furthermore, some experts reported an increase in the frequency and level of losses, particularly in critical infrastructure, despite the overall decrease in average losses. The experts have suggested different explanations for this trend, such as the fact that hackers from Ukraine and Russia are presently deploying their resources for cyber operations on each other due to the Ukraine/Russia conflict. This has resulted in a general decrease in the intensity of cyber-attacks elsewhere, which are now considered less sophisticated and less effective than previous ones. In addition, the lower activity of ransomware groups with suspected proximity to Russia is attributed to the strong sanctions that also affect ransomware payments, significantly impacting the cyber insurer operations. Cyber insurers would not pay claims that violated sanctions, and this has led to a decrease in the frequency of ransomware attacks. Another stated reason for the decrease in cyber-attack frequency is that companies have improved their cybersecurity posture. Commercial enterprises have learned from high-profile cyber events such as Petya, WannaCry, and Lock4J, and have strengthened their security measures accordingly. Companies have also learned from the Covid-19 pandemic that the home office presents a major attack vector. In this context, interviewees have highlighted that companies are more careful with their backups, which has led to smoother and fewer reported attacks, possibly because companies do not want to make the attacks public.

Despite the decrease in the frequency of cyber-attacks, some insurers and reinsurers have warned against assuming the best when the conflict ends. They have pointed out that many people are being trained in cyber operations as hackers due to the conflict, and when it ends, some of the trained hackers may use their skills as a source of income. Furthermore, it is uncertain how many companies have been hacked and the extent of damage that has not been noticed. In this scenario, cyber-attacks could increase significantly as the conflict ends and human resources are freed up. Lastly, it is essential to note that the decrease in cyber losses is not an indicator of a decrease in cyber-attacks since only losses reported by insured parties are included in the analysis. The actual number of cyber-attacks could be higher, and it is important for the insurance market to remain vigilant in the face of these threats.

4.1.5 Insurability of the cyber war risk and possible approaches to insure it

The preceding summaries of interviews illustrate the significance of war exclusion in cyber insurance. In relation to the final inquiry about insurability and potential remedies, all cyber experts unanimously agreed that cyber war risk is currently uninsurable due to its high accumulation and incalculability. Such a risk would lead to insurers being unable to fulfil their obligations to pay benefits, potentially

resulting in their financial ruin. Furthermore, co-insurance of such a risk would lead to a considerable surge in premiums, rendering it unaffordable for numerous companies. Nevertheless, some experts have suggested ways in which this risk could be insured, although the insurance industry will need to agree on which aspects of war and cyberwar to insure and the accumulations of risk involved. However, insuring extreme accumulation risks would be perilous without an adequate assessment of these risks. To manage accumulation risk better, efforts are underway in insurance companies to implement a data standard for cyber risk to better manage accumulation risk. Presently, loss ratios in cyber insurance are exposed, particularly in the large corporate sector. Thus, ensuring the risk of cyber wars without a comprehensive database to evaluate this risk is hazardous. Furthermore, companies must elevate cybersecurity measures to decrease the likelihood of occurrence, emphasizing that risk identification and quantification are critical before deciding what to accept and transfer. This research stresses the importance of focusing on cybersecurity within organizations, as systemic risks cannot be covered by capital alone. Furthermore, transparent and understandable attribution in the war clause is critical in any potential insurance of cyber war risks.

The questionnaire also included inquiries about what an insurance solution for this risk might resemble. All experts agreed that no insurer could bear this cyber risk alone. While not everything needs to be insured, partial compensation should be possible to prevent policyholders from being entirely vulnerable. To make the risk more manageable, some interviewees suggested using a combination of increasing deductibles, deeper risk exclusions, technical obligations, widespread event clauses, accumulation limits, and policyholder participation in the overall risk. An alternative approach to risk transfer would be to integrate a pool solution. For instance, the Extremus pool in Germany could handle accumulated losses (Dick et al., 2022).[6] However, it was noted that the insurance industry is not yet ready to embrace this solution, and there is insufficient political pressure. Another potential solution would be to involve the capital market through Insured Linked Securities (ILS). Although the interviewees were unable to provide specific design options, practical examples demonstrate that ILS has gained popularity for conventional cyber risks. Thus, two cat bonds were issued under the ILS framework, one for USD 45 million by insurer Beazly and the other for USD 100 million by reinsurer Hannover Re (Artemis, 2023; Hannover Re, 2023). Examples of other state-funded backstops are Flood Re or the UK's terrorism-linked Pool Re scheme (Barnes, 2002; Flood Re, 2015).

To enhance academic rigor and clarity, the results summarized in table 2.

[6] Extremus Versicherungs-Aktiengesellschaft was established with the objective of offering policyholders a sense of security and stability, while safeguarding insurers and reinsurers from financial ruin. The insurer's primary focus lies in providing comprehensive coverage for large-scale and significant losses, particularly those caused by fire outbreaks and business interruptions resulting from terrorist attacks.

Section	Key findings
4.1.1 War exclusion clauses in cyber insurance products	• The lack of a clear definition for "war" in cyber insurance exclusion clauses creates challenges for policyholders and insurers. • Insurers use vague language to limit policy scope, citing the absence of relevant case law. • Cyber-attacks, especially in the context of hybrid or cyber warfare, present unique attribution and damage assessment challenges compared to traditional warfare. • The insurance industry awaits the outcome of the Merck case for guidance on applying war exclusions in cyber insurance.
4.1.2 Differences between cyber warfare and traditional warfare	• Cyber and traditional warfare aim to damage and destabilize but differ in attack mode, visibility, and impact. • Traditional warfare involves visible military actions; cyber warfare is invisible and can be conducted with simple tools like a computer with internet access. • Cyber warfare's invisibility and potential for collateral damage, especially on critical infrastructure, present unique challenges.
4.1.3 Rejection of cyber claims due to the Ukraine/Russia conflict	• Despite expectations, no cyber insurance claims have been rejected based on the cyber war exclusion clause since the Ukraine/Russia conflict began. • Insurers are exercising greater caution, especially in underwriting risks in the energy and infrastructure sectors.
4.1.4 Change in cyber insurance claims due to the Ukraine/Russia conflict	• Reports on changes in cyber claims frequency vary, with some insurers experiencing a decrease, attributed to a variety of factors including decreased hacker activity and improved cybersecurity measures by companies. • The conflict has led to a decrease in the intensity and effectiveness of cyber-attacks elsewhere, influenced by sanctions and the redirection of hacker resources.
4.1.5 Insurability of the cyber war risk and possible approaches to insure it	• Cyber war risk is currently considered uninsurable due to high accumulation and incalculability. • Possible approaches to insure this risk include the use of data standards for better risk management, increased cybersecurity measures, and exploring risk transfer options like pool solutions or ILS.

Table 2: Overview of the key results from section 4.1.

4.2 Results of the cyber insurance policy analysis

This section provides the findings of the qualitative content analysis conducted on the general cyber insurance terms and conditions. The study focused on analyzing the war exclusion clause components and language used in 44 cyber policies. The analysis aimed to achieve multiple objectives. Firstly, it aimed to determine the prevalence of the war exclusion clause across all general cyber terms. Additionally, the study aimed to identify the specific components of the war exclusion clause and assess their frequency and occurrence. The analysis also considered the interviewees' statements to determine whether the clause employs detailed definitions for better comprehension or whether it solely refers to the term "war". Lastly, the study aimed to investigate the language used in cyber terms.

The analysis quantified the occurrence of particular terms within the war exclusion clauses of the 44 policies under review. The findings from this analysis are illustrated in Figure 4. All cyber policies that were analyzed in this study included a war exclusion clause. This exclusion clause was the only clause found in all policies. According to the research conducted by Cremer et al. (2022), deliberate or reckless acts of defamation and infrastructure outage ranked second and third, respectively, in terms of the frequency of occurrence of the exclusion clause.

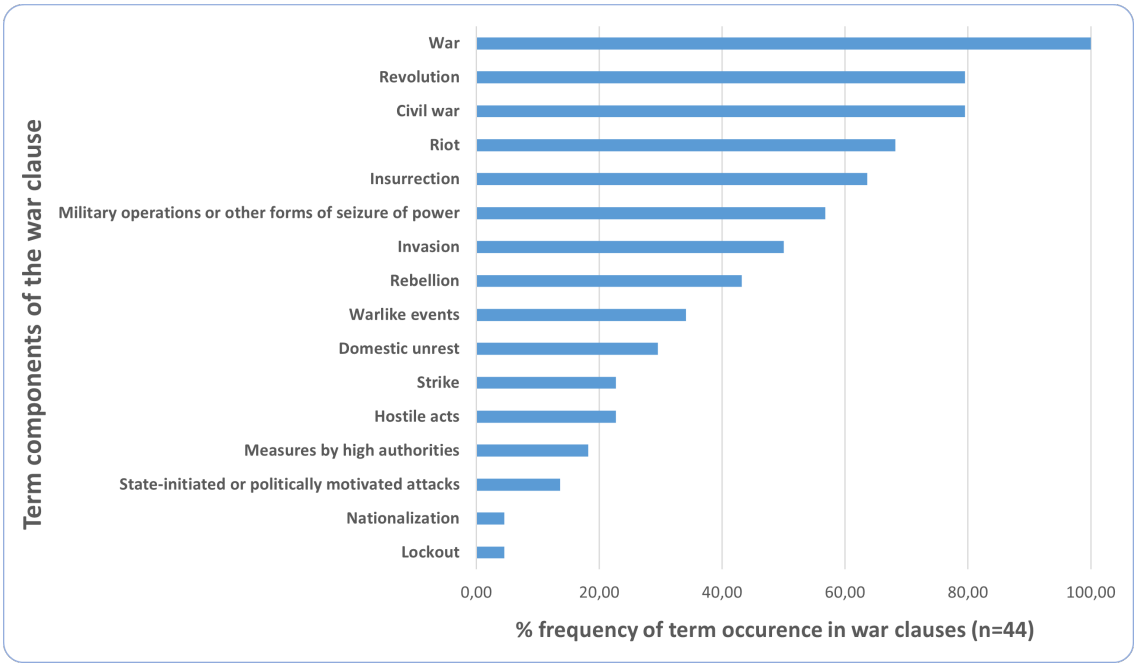

Figure 4: This overview presents the findings related to the identification of specific terms and their frequency within war exclusion clauses in insurance policies, based on a sample size of 44. Each of the 44 cyber insurance policies analyzed in this study includes a clause that excludes coverage for losses associated with war.

Based on the direct wording, the term "war" was present in the term components in every clause, but the frequency of occurrence for the other terms was lower. This supports the findings from the interviews, which indicated that cyber insurance providers opted for vague language in their policies to limit their scope of coverage. It is particularly interesting to note that the term "state-initiated or politically motivated attack" has a very low

frequency, despite the current risk of state-sponsored cyber-attacks.

The analysis highlights that a significant number of cyber insurers relied on either the GDV's cyber standard terms and conditions or the standard terms and conditions for property and casualty insurance when drafting their war clauses. As a result, the wording of many of these clauses was very similar. This result aligns with the findings obtained from the interviews conducted, which indicate that policyholders face challenges due to the lack of clear definitions and interpretation difficulties associated with the wording of the policies. Consequently, policyholders are forced to interpret the meanings of such terms independently. The wording of the war exclusion clause found was as follows [translated]:

“Excluded from insurance coverage regardless of contributory causes are:

Insured events or losses due to war.

War means: war, invasion, civil war, insurrection, revolution, riot, military or other or other form of seizure of power.”

Further examination of the explanations and definitions revealed that only 11.4% of the war clauses contained additional descriptions and definitions of the exclusion. This indicates that 88.6% of cyber insurers only referred to their exclusion terms in their war clauses, which provided insurance coverage. For instance, one of the more detailed policy terms we identified was as follows [translated]:

"Damage caused by war or warlike events, civil war, revolt, rebellion, civil unrest or insurrection. In particular, also by loss of any kind - also in and/or emanating from virtual space (cyberwar) with means predominantly from the field of information technology - which is directly or indirectly based on war events or other hostile acts (regardless of whether war has been declared or not)."

In addition, a war clause was found that had an even more in-depth detail of the exclusion clause [translated]:

"No insurance coverage is provided due to damage arising directly or indirectly in connection with any of the following events:

The use of physical force by one state against another state (War), whether or not a declaration of war has been made, the unauthorized access to an IT system by a state in the territory of another state, or the unauthorized use of an IT system by a state in the territory of another state (cyber operation), if this cyber operation: is carried out in the course of the war and/or leads directly or indirectly to a disruption of the availability, integrity or performance of the critical infrastructure or else the security or defence of the other state."

The subsequent qualitative analysis examined patterns of term co-occurrence within cyberwar clauses. The study found that, in 12 of the 44 cyber policies reviewed, a specific set of terms — namely "war," "invasion," "civil war," "strike," "revolution," "riot," "military operations and other expressions indicating a seizure of power” — appeared simultaneously within the clauses. In a separate finding, it was noted that four policies featured a concurrent appearance of another group of terms: "war," "civil war," "strike," "revolution," "riot," "domestic unrest," and "warlike events." Beyond these patterns of co-occurrence, Figure 5 displays additional patterns that were identified twice in the policy documents. For the remaining policies, the co-occurrence of terms was identified once.

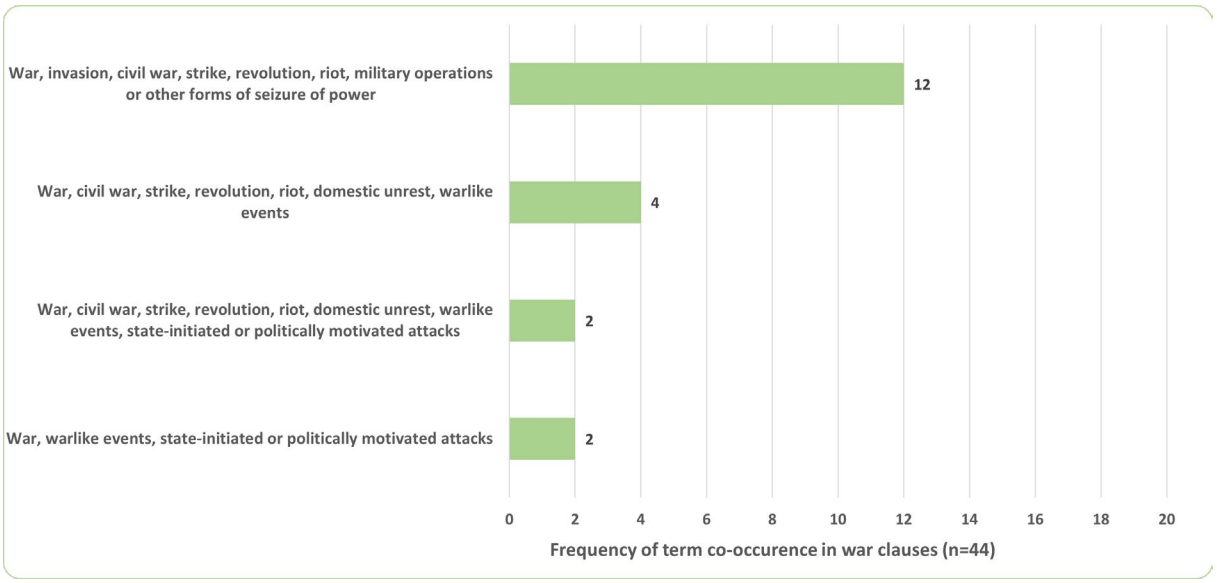

Figure 5: The analysis revealed patterns of term co-occurrence in cyber war clauses. It was observed that certain terms appeared together in 12 out of 44 policies. A different combination of similar terms was found in four other policies. In addition, there were patterns that were identified twice in the clauses. In the rest of the policy cyber war clauses, these term co-occurrences were noted only once.

The last qualitative analysis focused on the language used in cyber war clauses. We found that 86.4% of cyber insurers used German as the language in their insurance terms and conditions, while the remaining percentage used English. All English-language war clauses were translations of the German model terms and conditions. This observation contrasted with our original hypothesis that the [translated] terms would need to be more detailed to accommodate different legal systems. Overall, the study provides insights into the key elements of the war exclusion clause in cyber insurance policies, highlighting any common patterns and providing a comprehensive understanding of the language used in such clauses.

The key findings are summarized in Table 3.

Aspect of analysis	Key findings
Prevalence of war exclusion Clause	All 44 cyber insurance policies analyzed include a war exclusion clause. This clause was the only one found in all policies.
Specific term components and frequency	The term "war" is present in every clause, but other terms such as "state-initiated or politically motivated attack" have very low frequency.
Common wording in the insurance policies	Many policies rely on either the GDV's cyber standard terms and conditions or standard terms for property and casualty insurance, leading to similar wording across policies.
Detailed descriptions of the definitions	Only 11.4% of policies provide additional descriptions and definitions within the war clauses, indicating that 88.6% of insurers refer solely to the exclusion terms without detailed explanation.
Patterns of term co-occurrence	The analysis revealed that specific terms were grouped together in 12 out of 44 policies. A different combination of similar terms was identified in four additional policies. Moreover, certain patterns of term co-occurrence were observed twice within the clauses.
Language used in the policies	86.4% of the policies used German for their terms and conditions, with all English-language clauses being translations of the German model terms.

Table 3: Overview of the key findings from Section 4.2.

No	Author(s)	Year	Title	Focus
1	Ferland	2019	Cyber insurance – What coverage in case of an alleged act of War? Questions raised by the Mondelez v. Zurich case	Analysis of Mondelez v. Zurich case, focusing on insurance policy's war exclusion clause
2	Woods & Weinkle	2020	Insurance definitions of cyber war	Perspective on the evolution of war clauses in cyber insurance policies and their implications on cyber insurance
3	Cremer et al.	2022	Cyber exclusions: an investigation into the cyber insurance coverage gap	Examination of exclusions in German cyber insurance policies and their relation to cyber risk events.
4	Cremer et al.	2024	Bridging the cyber protection gap: An investigation into the efficacy of the German cyber insurance market	Analysis of the German cyber insurance market, focusing on the challenges of rapid cyber threat adaptation, data availability, and risk understanding.
5	Romanosky et al.	2019	Content analysis of cyber insurance policies: how do carriers price cyber risk?	Thematic analysis of cyber insurance policies to understand coverage, risk assessment, and premium calculation.
6	Shackelford	2020	Wargames: Analyzing the act if war exclusions in insurance coverage and its implications for cybersecurity policy	Discussion on the act of war exclusion in insurance and its implications for U.S. cybersecurity policy.
7	Wolff	2024	The role of insurers in shaping international cyber-security norms about cyber-war	Analyzing insurers' influence on international cybersecurity norms through coverage decisions for state-sponsored cyberattacks.
8	Brunner	2022	Insurance policies and the attribution of cyber operations under international law: a commentary	Legal consideration of the relationship between cyber insurance policies, international law and the attribution of cyber operations to states.
9	Wan	2020	Notpetya not warfare: Rethinking the insurance war exclusion in the context of international cyberattacks	Examination of the war exclusion in insurance policies in the context of state-sponsored cyber-attacks.
10	Bateman	2020	War, Terrorism, and Catastrophe in Cyber Insurance: Understanding and Reforming Exclusions	Analysis of traditional war and terrorism exclusions in cyber claims and proposals for reform.
11	Rovetto Jr	2022	Cyberwarfare & Cyber Insurance: Exploring When a Cyberattack Can Negate a Cyber Insurance Claim	Exploration of the legal and insurance implications of cyberwarfare on cyber insurance claims.
12	Chopra	2021	Cyberattack - Intangible Damages in a Virtual World: Property Insurance Companies Declare War on Cyber-Attack Insurance Claims	Discussion on the challenges and implications of insuring against cyber-attack damages.

Table 4: Overview of the literature that has addressed the exclusions in cyber insurance and, in particular, the war exclusion.

4.3 Comparison

In the final part of the results, the results from sections 4.1 and 4.2 are compared with similar research. This results in the two categories, definition and clarity of war exclusions as well as litigation and insurability of cyber war losses. An overview of the articles used for the comparison and other articles with similar topics can be found in Table 4.

This study emphasizes the challenges the cyber insurance sector faces in defining and implementing war exclusion clauses. It points out the ambiguity in defining 'war' or 'war-like events and insurers dependence on vague terminology due to the absence of relevant legal precedents. Both earlier and more recent research uncover identical issues. Specifically, Woods and Weinkle (2020), along with Cremer et al. (2022), investigate how definitions in cyber insurance policies have evolved and identify a coverage gap stemming from definitions that are not explicitly stated. Furthermore, Cremer et al. (2024) conduct semi-structured interviews with industry practitioners to understand the rationale behind such exclusions. These studies collectively underscore the difficulty in interpreting and applying war exclusion clauses amid state-sponsored cyber-attacks, and highlight the broader implications for both the insurance industry and policyholders.

The next comparison category analyzes the legal aspects and insurability of damages from cyber warfare, detailing contributions from various authors on the subject. Shackelford (2020) and Wolff (2024) discuss the implications of war exclusions on cybersecurity policies and the influence of insurers in establishing international cybersecurity standards. Brunner (2022) and Wan (2020) offer critiques on the use of international law for attributing cyber operations, arguing against the widespread application of war exclusions to state-sponsored cyber-attacks. Bateman (2020) suggests a revision of exclusion clauses to better meet the challenges posed by cyber warfare and state-sponsored cyber incidents. In contrast, this work emphasizes the practical challenges faced in cyber insurance claims, particularly in the context of the Ukraine/Russia conflict. This comparison highlights how the industry is navigating contemporary conflicts and cyber operations. Additionally, the analysis extends to the insurability of cyber war risks, pointing out the insurance industry's difficulty with the significant accumulation and unpredictability of such risks.
The comparison consistently underscores the difficulties encountered by the cyber insurance industry in managing war exclusion clauses, especially concerning the definitions of "war" and "warlike events." Both earlier and more recent research point out the issue of imprecise wording and the consequent coverage gaps. Legal examinations and demands for change stress the importance of precise definitions and adjustments to the unique aspects of cyber warfare. The widespread implications of these uncertainties for policyholders and the industry at large highlight the critical need to revise exclusion clauses to enhance the insurability of cyber war risks.

5. Discussion

This research highlights the lack of clarity in the cyber war exclusion clause of the market in the German cyber insurance industry. The analysis of German cyber insurance policies shows that war exclusion clauses are present in every cyber policy. However, the lack of standardization, different components, and unclear definitions by insurers make it difficult to understand the scope of the exclusion. The absence of a clear delineation of insurance coverage for cyber warfare events and other significant cyber risks creates barriers to developing cyber insurance markets. It is also hampered by the lack of comparability between insurance terms and conditions. The study suggests that the varying interpretation of the exclusion clause can lead to ambiguity and uncertainty in its application, resulting in legal complexity and disputes. Overall, the findings highlight

the need for greater standardization and transparency of the war exclusion clause to improve the effectiveness of insurance coverage and reduce SMEs' exposure to cyber risks.

The interviews yielded insightful perspectives, as interviewees unanimously emphasized that the absence of clear definitions for terms such as "war" or "warlike incidents" in cyber insurance products presents significant challenges for the industry. This issue was predominantly raised by primary insurers, who cited the lack of case law as the reason for choosing vague wording to limit the scope of their policies. The reason given for this was that no war exclusion clauses had yet been tested in court for their stability. Additionally, the origin of the war exclusion clause, which stemmed from other insurance terms and business lines that focused on physical warfare, also poses a challenge. Cyber warfare, in particular, presents a unique challenge as they are difficult to attribute and prove compared to traditional acts of war.

This study has some limitations. The research collected cyber terms and conditions between November 2021 and February 2022 (before the Ukraine/Russia conflict), which means that some insurers may have revised their war exclusion clause since then. In addition, interviews with cyber experts were conducted between November 10, 2022, and February 3, 2023, via MS Teams or Zoom, which changes perceptions depending on the course of the war.

The findings of this study indicate that the German cyber war exclusion clause is still in its developmental stage, resulting in uncertainties that must be addressed. To mitigate cyber risks, both the insurance industry and policymakers must take measures to offer transparent and comprehensive insurance coverage, along with appropriate safeguards. It should be noted that cyber accumulation risks can have an impact on organizations worldwide, regardless of their physical location.

As a result, we argue that standardized and all-encompassing cyber insurance policies will serve to absorb and redistribute the risk within the world wide web. By doing so, market forces will contribute to constructing an order that is so far proving resistant to will of sovereign power and legal codification.

This paper offers significant insights into the current state of war exclusion within the German cyber insurance market. The study evaluates the effectiveness of the war clause and its impact on corporate cyber risk resilience. Policymakers can leverage the research findings to emphasize the significance of recognizing risks that are not presently covered by the insurance industry. Furthermore, the outcomes underscore the criticality of cybersecurity for businesses. The study highlights the links between unclear exclusions and cyber risk exposures, emphasizing the need for companies to take more proactive measures. The findings offer a valuable opportunity for cyber insurers to evaluate their cyber insurance products and war exclusion clauses. The research also emphasizes the need for standardization and transparency in the terms and conditions of cyber insurance across the industry. Finally, the interview results offer potential starting points for addressing the insurability of cyber war risks and their transfer possibilities.

6. Conclusion

The conflict between Ukraine and Russia has made the cyber warfare exclusion clause an issue of global interest. From the perspective of academy, this research highlights the needs for more cross-disciplinary engagement. It is clear insurance is an actor in international relations that has an important role to play in providing for more resilience in the face of cyber-attacks. Thus, insurance companies - and indeed regulatory community are important stakeholders in

the conversation around the security implications of cyber risk. Without insurance, the cyber domain represents a vulnerability in the defense of state interests and the maintenance of interstate relations.

Assessing and comprehending cyber risk is a formidable challenge for all stakeholders in the cyber insurance domain, owing to the dynamic and ever-changing nature of risks in tandem with the rapid progression of technology. From a strategic perspective, the research highlights the importance of transparent and comprehensible exclusions, especially the war exclusion clause. The results of the content analysis and interviews show that different definitions and components of the cyber war exclusion clause make it difficult for policyholders to understand insurance coverage. In addition, the research highlights the importance of the exclusion clause and cyber war risk to the insurance industry. It clearly shows that the insurance industry is reaching its limits with such a risk and that this risk has enormous loss potential. The results should show companies that cyber insurance does not cover all cyber risks and that a cybersecurity strategy and coordinated security measures are essential to minimize these risks. For policymakers, the study clarifies the challenges facing the insurance industry regarding the war exclusion clause and how it is currently perceived. From a resilience perspective, the study points to weaknesses in the current cyber insurance landscape and the importance of cyber war risks.

In summary, the paper contributes to the perceptions of cyber insurance experts concerning cyber war risks, revealing essential issues such as the lack of a clear definition of war and the difficulty in attributing and proving cyber war events. The results ultimately demonstrate that security in turbulent political times, in times of war and change, rests on strategies of public-private cooperation.

Disclosure statement
On behalf of all authors, the corresponding author states that there is no conflict of interest.

References

Artemis. (2023). *Beazly cyber cat bond*. from https://www.artemis.bm/deal-directory/beazley-cyber-cat-bond-2023-1/ (accessed 16 January 2023)

Association, L. M. (2021). *Cyber War and Cyber Operation Exclusion Clauses*. from https://www.lmalloyds.com/LMA/News/LMA_bulletins/LMA_Bulletins/LMA21-042-PD.aspx (accessed 18 January 2023)

Authority, E. I. a. O. P. (2022). *European Insurance Overview*. from https://www.eiopa.europa.eu/publications/european-insurance-overview-2022_en (accessed 26 October January 2022)

Bahşi, H., Franke, U., & Friberg, E. L. (2020). The cyber-insurance market in Norway. *Information & Computer Security, 28*(1), 54-67. https://doi.org/10.1108/ICS-01-2019-0012

Bampton, R., & Cowton, C. J. (2002). The e-interview. Forum Qualitative Sozialforschung/Forum: Qualitative Social Research. https://doi.org/10.17169/fqs-3.2.848

Barnes, L. (2002). A closer look at Britain's Pool Re. *Risk Management, 49*(5), 18.

Bateman, J. (2020). *War, Terrorism, and Catastrophe in Cyber Insurance: Understanding and Reforming Exclusions*. Carnegie Endowment for International Peace. from https://carnegieendowment.org/files/Bateman_-_Cyber_Insurance_-_Final.pdf (accessed 25 November 2022)

Beenken, M., Knörrer, D., Moormann, J., & Schmidt, D. (2018). *Digital Insurance: Strategien, Geschäftsmodelle, Daten*. Frankfurt School Verlag.

Brunner, I. (2022). Insurance policies and the attribution of cyber operations under international law: a commentary. *NYUJ Int'l L. & Pol., 55*, 179.

Buchanan, B. (2020). *The Hacker and the State: Cyber Attacks and the New Normal of Geopolitics*. Harvard University Press.

Carter, R. A., & Enoizi, J. (2020). *Cyber war and terrorism: Towards a common language to promote insurability*. Geneva Association-International Association for the Study of Insurance. from https://www.genevaassociation.org/sites/default/files/research-topics-document-type/pdf_public/cyber_war_terrorism_commonlanguage_final.pdf (accessed 3 January 2023)

CFR. (2022). *Cyber Operations Tracker*. from https://microsites-live-backend.cfr.org/index.php/cyber-operations#Timeline (accessed 2 June 2023)

Chopra, A. (2021). Cyberattack-Intangible damages in a virtual world: Property insurance companies declare War on cyber-attack insurance claims. *Ohio St. LJ, 82*, 121.

Cremer, F., Sheehan, B., Fortmann, M., Mullins, M., & Murphy, F. (2022). Cyber exclusions: An investigation into the cyber insurance coverage gap. 2022 Cyber Research

Conference-Ireland (Cyber-RCI), 10.1109/Cyber-RCI55324.2022.10032678

Cremer, F., Sheehan, B., Fortmann, M., Mullins, M., Murphy, F., & Materne, S. (2024). Bridging the cyber protection gap: An investigation into the efficacy of the German cyber insurance market. *Risk Management and Insurance Review*. https://doi.org/10.1111/rmir.12261

Dennen, J. M. G. (2005). *On War: Concepts, Definitions, Research Data: a Short Literature Review and Bibliography*. Rijksuniversiteit [Host]. https://books.google.ie/books?id=jKVsMwEACAAJ

DiCicco-Bloom, B., & Crabtree, B. F. (2006). The qualitative research interview. *Medical education, 40*(4), 314-321. https://doi.org/10.1111/j.1365-2929.2006.02418.x

Dick, L., Heep-Altiner, M., & Sonnefeld, M. (2022). Risiko und Versicherbarkeit. In *Klima-und Nachhaltigkeitsrisiken für die Versicherungswirtschaft* (pp. 49-90). Springer. https://doi.org/10.1007/978-3-658-35290-5_2

Eilstrup-Sangiovanni, M. (2018). Why the world needs an international cyberwar convention. *Philosophy & Technology, 31*(3), 379-407. https://doi.org/10.1007/s13347-017-0271-5

EIOPA. (2022). *EIOPA Statistics - Accompanying note*. from https://register.eiopa.europa.eu/Publications/Insurance%20Statistics/SA_Accompanying_note.pdf (accessed 29 April 2023)

Eling, M. (2020). Cyber risk research in business and actuarial science. *European actuarial journal, 10*(2), 303-333. https://doi.org/10.1007/s13385-020-00250-1

Eling, M., & Lehmann, M. (2018). The impact of digitalization on the insurance value chain and the insurability of risks. *The Geneva Papers on Risk and Insurance-Issues and Practice, 43*, 359-396. https://doi.org/10.1057/s41288-017-0073-0

Falco, G., Eling, M., Jablanski, D., Miller, V., Gordon, L. A., Wang, S. S., Schmit, J., Thomas, R., Elvedi, M., & Maillart, T. (2019). A research agenda for cyber risk and cyber insurance. Workshop on the Economics of Information Security (WEIS). from https://weis2016. econinfosec. org/wp-content/uploads/sites/6/2019/05/WEIS_2019_paper_35. pdf. (accessed 20 December 2022)

Ferland, J. (2019). Cyber insurance–What coverage in case of an alleged act of War? Questions raised by the Mondelez v. Zurich case. *Computer Law & Security Review, 35*(4), 369-376.

Franke, U., & Meland, P. H. (2019). Demand side expectations of cyber insurance. 2019 International Conference on Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA), https://doi.org/10.1109/CyberSA.2019.8899685

Gartzke, E. (2013). The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth. *International Security, 38*(2), 41-73. https://doi.org/10.1162/ISEC_a_00136

GDV. (2021). *Wie die Versicherungsbranche schützt, was Menschen am Herzen liegt*. from https://www.gdv.de/gdv/visual-stories/visual-story (accessed 4 September 2022)

GDV. (2022). *Wer versichert was?* from https://www.gdv.de/service/wer-versichert-was/de/47406?productQuery=Cyberversicherung&channelId=82 (accessed 9 September 2022)

Gold, J. (2019). War Risk Exclusions Threaten Cyber Coverage. *Risk Management, 66*(3), 12-13.

Gorwa, R., & Smeets, M. (2019). Cyber conflict in political science: a review of methods and literature. https://doi.org/10.31235/osf.io/fc6sg

Hausken, K. (2020). Cyber resilience in firms, organizations and societies. *Internet of Things, 11*, 100204. https://doi.org/10.1016/j.iot.2020.100204

Johnson, R. B., & Onwuegbuzie, A. J. (2004). Mixed methods research: A research paradigm whose time has come. *Educational researcher, 33*(7), 14-26. https://doi.org/10.3102/0013189X033007014

Kallio, H., Pietilä, A. M., Johnson, M., & Kangasniemi, M. (2016). Systematic methodological review: developing a framework for a qualitative semi-structured interview guide. *Journal of advanced nursing, 72*(12), 2954-2965. https://doi.org/10.1111/jan.13031

Kingston, C. (2007). Marine insurance in Britain and America, 1720–1844: a comparative institutional analysis. *The Journal of Economic History, 67*(2), 379-409. https://doi.org/10.1017/S0022050707000149

Li, Y., & Liu, Q. (2021). A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. *Energy Reports, 7*, 8176-8186. https://doi.org/10.1016/j.egyr.2021.08.126

Lobo-Guerrero, L. (2012). Lloyd's and the moral economy of insuring against piracy: towards a politicisation of marine war risks insurance. *Journal of Cultural Economy, 5*(1), 67-83. https://doi.org/10.1080/17530350.2012.640555

MacColl, J., Nurse, J. R., & Sullivan, J. (2021). Cyber insurance and the cyber security challenge. *RUSI Occasional Paper*.

Marchant, G. E., & Stevens, Y. A. (2017). Resilience: a new tool in the risk governance toolbox for emerging technologies. *UCDL Rev., 51*, 233.

Marotta, A., Martinelli, F., Nanni, S., Orlando, A., & Yautsiukhin, A. (2017). Cyber-insurance survey. *Computer Science Review, 24*, 35-61. https://doi.org/10.1016/j.cosrev.2017.01.001

Martin, F. (1876). *The History of Lloyd's and of Marine Insurance in Great Britain: With an Appendix Containing Statistics Relating to Marine Insurance*. Macmillan.

Maschmeyer, L. (2021). The Subversive Trilemma: Why Cyber Operations Fall Short of Expectations. *International Security, 46*(2), 51-90. https://doi.org/10.1162/isec_a_00418

MAXQDA. (2022). *Organize. Analyze. Visualize. Present.* from https://www.maxqda.com/ (accessed 12 December 2023)

Mayring, P. (2021). *Qualitative content analysis: a step-by-step guide*. Sage.

Mitoraj, S. (2020, 24.02.2020). *Cyber crimes, cyber terror and cyber war* Geneva Association and IFTRIP Cyber Terrorism and Cyber Warfare Task Force Workshop, London. https://www.genevaassociation.org/sites/default/files/research-topics-document-type/pdf_public/cyber_war_terrorism_commonlanguage_final.pdf (accessed 8 January 2023)

Monstadt, J., & Schmidt, M. (2019). Urban resilience in the making? The governance of critical infrastructures in German cities. *Urban Studies, 56*(11), 2353-2371. https://doi.org/10.1177/0042098018808848

Newcomer, K. E., Hatry, H. P., & Wholey, J. S. (2015). Conducting semi-structured interviews. *Handbook of practical program evaluation, 492*, 492. https://doi.org/10.1002/9781119171386

Nurse, J. R., Axon, L., Erola, A., Agrafiotis, I., Goldsmith, M., & Creese, S. (2020). The data that drives cyber insurance: A study into the underwriting and claims processes. 2020 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA). https://doi.org/10.1109/CyberSA49311.2020.9139703

Nye, J. S., Jr. (2017). Deterrence and Dissuasion in Cyberspace. *International Security, 41*(3), 44-71. https://doi.org/10.1162/ISEC_a_00266

OECD. (2020). *Encouraging Clarity in Cyber Insurance Coverage*. from https://www.oecd.org/finance/insurance/Encouraging-Clarity-in-Cyber-Insurance-Coverage.pdf (accessed 2 January 2023)

Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., Shamseer, L., Tetzlaff, J. M., Akl, E. A., & Brennan, S. E. (2021). The PRISMA 2020 statement: an updated guideline for reporting systematic reviews. *International Journal of Surgery, 88*, 105906. https://doi.org/10.1136/bmj.n71

PCS. (2019). *Could NotPetya's Tail Be Growing?* from https://www.verisk.com/siteassets/media/pcs/pcs-cyber-catastrophe-notpetyas-tail.pdf (accessed 20 March 2023)

Powell, L. S., & Sommer, D. W. (2007). Internal versus external capital

markets in the insurance industry: The role of reinsurance. *Journal of Financial Services Research, 31*, 173-188. https://doi.org/10.1007/s10693-007-0007-2

Rathbone, J. P. (2023). *UK warns of attacks from new 'Wagner-like' Russian cyber hackers*. from https://www.ft.com/content/18872afa-8758-48e2-a135-6103f9541d41 (accessed 24 April 2023)

Re, F. (2015). *What is Flood Re?* Retrieved from Flood Re: http://www. floodre. co. uk/about-us. Retrieved 02.03. from https://www.floodre.co.uk/about-us/ (accessed 2 March 2023)

Re, H. (2023). *Hannover Re partners with Stone Ridge in first cyber risks transfer to the capital markets through proportional reinsurance*. from https://www.hannover-re.com/1932493/hannover-re-transfers-cyber-risks-to-the-capital-market-for-the-first-time-through-a-proportional-reinsurance-solution.pdf (accessed 15 March 2023)

Romanosky, S., Ablon, L., Kuehn, A., & Jones, T. (2019). Content analysis of cyber insurance policies: How do carriers price cyber risk? *Journal of Cybersecurity, 5*(1), tyz002. https://doi.org/10.1093/cybsec/tyz002

Rovetto Jr, J. M. (2022). Cyberwarfare & cyber insurance: exploring when a cyberattack can negate a cyber insurance claim. *J. Bus. & Tech. L., 18*, 309.

Satariano, A., & Perlroth, N. (2019). Big Companies Thought Insurance Covered a Cyberattack. They May Be Wrong. *The New York Times*. from https://courses.cs.duke.edu/spring20/compsci342/netid/news/nytimes-cyber-attack.pdf. (accessed 20 September 2022)

Shackelford, S. J. (2020). Wargames: Analyzing the Act of War Exclusion in Insurance Coverage and Its Implications for Cybersecurity Policy. *Yale J.L. & Tech., 23*, 362.

Shafqat, N., & Masood, A. (2016). Comparative analysis of various national cyber security strategies. *International Journal of Computer Science and Information Security, 14*(1), 129-136.

Slayton, R. (2017). What Is the Cyber Offense-Defense Balance? Conceptions, Causes, and Assessment. *International Security, 41*(3), 72-109. https://doi.org/10.1162/ISEC_a_00267

Smith, I. (2023). *Bank of America warns Lloyd's over state-backed cyber attack exclusion*. Financial Times. Retrieved 25.04. from https://www.ft.com/content/52cc6be9-b88c-4b68-9ab0-da6b771e8d09?accessToken=zwAF-jgcaWTYkc9SzGvpuIxLaNOasNprdx6NCQ.MEYCIQC_vOhrwijtzNmtYXi00CPocpJ-T_n0e-eFVUMGOgTsZwIhAPc0-y61gUZAnXgg9jHfg1PVA54zQnZzjFrTFbBOvaFG&sharetype=gift&token=1d409980-5530-442f-9e3e-5367f5a80913 (accessed 25 April 2023)

Steiger, S. (2022). Cyber securities and cyber security politics. *Cyber Security Politics*, 141. https://doi.org/10.4324/9781003110224-12

Talesh, S. A. (2018). Data breach, privacy, and cyber insurance: How insurance companies act as "compliance managers" for businesses. *Law & Social Inquiry, 43*(2), 417-440. https://doi.org/10.1111/lsi.12303

Trifunović, D., & Bjelica, Z. (2020). CYBER WAR-TRENDS AND TECHNOLOGIES. *National Security & the Future, 21*(3). https://doi.org/10.37458/nstf.21.3.2

Vakulchuk, R., Overland, I., & Scholten, D. (2020). Renewable energy and geopolitics: A review. *Renewable and Sustainable Energy Reviews, 122*, 109547. https://doi.org/10.1016/j.rser.2019.109547

Vanderford, R. (2023). *Insurers Say Cyberattack That Hit Merck Was Warlike Act, Not Covered*. Retrieved 03.03. from https://www.wsj.com/articles/insurers-say-cyberattack-that-hit-merck-was-warlike-act-not-covered-11675897657 (accessed 3 March 2023)

Wagner, P. (2021). Critical infrastructure security. *Available at SSRN 3762693*. http://dx.doi.org/10.2139/ssrn.3762693

Wan, K. S. (2020). NotPetya, not warfare: rethinking the insurance war exclusion in the context of international cyberattacks. *Wash. L. Rev., 95*, 1595.

Wolff, J. (2024). The role of insurers in shaping international cyber-security norms about cyber-war. *Contemporary Security Policy, 45*(1), 141-170. https://doi.org/10.1080/13523260.2023.2279033

Woods, D., & Simpson, A. (2017). Policy measures and cyber insurance: a framework. *Journal of Cyber Policy, 2*(2), 209-226. https://doi.org/10.1080/23738871.2017.1360927

Woods, D. W., & Weinkle, J. (2020). Insurance definitions of cyber war. *The Geneva Papers on Risk and Insurance-Issues and Practice, 45*(4), 639-656. https://doi.org/10.1057/s41288-020-00168-5

Wrede, D., Stegen, T., & von der Schulenburg, J.-M. G. (2020). Affirmative and silent cyber coverage in traditional insurance policies: qualitative content analysis of selected insurance products from the German insurance market. *The Geneva Papers on Risk and Insurance-Issues and Practice, 45*(4), 657-689. https://doi.org/10.1057/s41288-020-00183-6

Xu, M., & Hua, L. (2019). Cybersecurity insurance: Modeling and pricing. *North American Actuarial Journal, 23*(2), 220-249. https://doi.org/10.1080/10920277.2019.1566076

Appendix

1) Detailed overview of the cyber insurance experts

Industry experts	Organization type	Cyber experience in years
B1	Broker	6 years
B2	Broker	4 years
B3	Broker	8 years
B4	Broker	8 years
B5	Broker	5 years
B6	Broker	8 years
B7	Broker	5 years
P1	Primary insurer	6 years
P2	Primary insurer	10 years
P3	Primary insurer	4 years
P4	Primary insurer	7 years
P5	Primary insurer	8 years
P6	Primary insurer	7 years
P7	Primary insurer	10 years
P8	Primary insurer	8 years
P9	Primary insurer	4 years
P10	Primary insurer	7 years
P11	Primary insurer	6 years
P12	Primary insurer	8 years
P13	Primary insurer	6 years
P14	Primary insurer	6 years
R1	Reinsurer	5 years
R2	Reinsurer	5 years
R3	Reinsurer	10 years
R4	Reinsurer	7 years
R5	Reinsurer	4 years