The Geneva Papers on Risk and Insurance - Issues and Practice
https://doi.org/10.1057/s41288-020-00168-5

Insurance definitions of cyber war

Daniel W. Woods[1] · **Jessica Weinkle**[2]

Received: 7 October 2019 / Accepted: 28 March 2020

Abstract
Definitions of war found in cyber insurance policies provide a novel window into the concept of cyber war. Mediated by market forces, changes in policy wording reflect shifting expectations surrounding technology and military strategy. Legal cases contesting war clauses probe state-formulated narratives around war and offensive cyber operations. In a recent legal case, an insurer refused to pay a property insurance claim by arguing the cause of the claim—the NotPetya cyberattack—constitutes a hostile or warlike action. To understand the implications, we build a corpus of 56 cyber insurance policies. Longitudinal analysis reveals some specialist cyber insurance providers introduced policies without war clauses until as late as 2012. Recent years have seen war exclusions weakened as cyber insurance policies affirmatively cover "cyber terrorism". However, these clauses provide few explicit definitions, rather they prompt a legal discourse in which evidence is presented and subjected to formal reasoning. Going forward, war clauses will evolve so insurers can better quantify and control the costs resulting from offensive cyber operations. This pushes insurers to affirmatively describe the circumstances in which cyber conflict is uninsurable.

Keywords Cyber war · Cyber insurance · Politics · Terrorism · International relations

Electronic supplementary material The online version of this article (https://doi.org/10.1057/s41288-020-00168-5) contains supplementary material, which is available to authorized users.

✉ Daniel W. Woods
daniel.woods@uibk.ac.at

[1] Department of Computer Science, University of Innsbruck, Innsbruck, Austria

[2] Department of Public and International Affairs, University of North Carolina Wilmington, Wilmington, USA

Published online: 06 May 2020

Introduction

What constitutes war? Where is the threshold for hostility at which society can no longer tolerate the resulting damage? Ethical arguments suggest the answers can be found in reason. Realists assert that these questions are decided by the powerful. Constructionists argue shared expectations about reasonable behaviour shape such decisions.

Markets offer answers in the form of war clauses in insurance policies. Such clauses are used to withdraw coverage for losses related to military operations. Insurers draw the line between war and peace because the underwriting assumptions fundamentally differ. Doing so necessitates anticipating and defining which war-related events threaten the existence of a private market. Disputes over whether war clauses apply may prompt a legal discourse resulting in a symbolic ruling. War clauses, however, have significance beyond the insurance industry and its customers (Strange 1996; Lobo-Guerrero 2012a).

The British government discovered this when war exclusions in marine insurance threatened to halt sea trade in the lead up to World War I, forcing the government to take financial responsibility for merchant ships damaged or sunk by enemy action (Lobo-Guerrero 2012a). The naval arms race led the insurance industry to believe sea voyages were uninsurable; meanwhile property owners could purchase insurance for bomb damage. The insurance industry made a considerable profit selling such policies because expectations of damage exceeded the realised losses (Haufler 1997).

Insurance against war risks has not always turned a profit. The actuarial assumption that past losses predict future losses is undermined by developments in military technology and tactics. In contrast to bomb damage coverage during World War I, insurers selling property insurance in Spain during the civil war made considerable losses (Haufler 1997). Ships trading with Spain could also purchase private insurance against war risks based on the unfounded assumption that British military vessels provided protection.

Haufler (1997) argues that private insurers should be seen as enablers of trade and prosperity in the presence of political risk, not as financiers profiting from war. This is made clear when private markets collapse. Following the September 11 attacks, reinsurers began excluding coverage for terrorist attacks, which forced insurers to include similar exclusions (Thoyts 2010). Investors responded by halting construction projects as buildings could not be insured. The U.S. government responded by passing the Terrorism Risk Insurance Act (TRIA) 2002, which forced all property insurance providers to offer terrorism coverage and committed the U.S. Treasury to covering losses above a pre-defined threshold. In terms of who gets what in this case, terrorism risk was socialised to the advantage of commercial property owners in dense urban centres.

Shifting risk perceptions influences the terms of insurance policies (Lobo-Guerrero 2012b). Coverage expansion is driven by rising policyholder fears relative to those of insurers, whereas coverage contraction is an indication of insurers becoming uncomfortable with the potential for catastrophe. Hayek (1945) argued

Table 1 Describing the possible functions of war clauses, which apply differently to each case

	Type	Description
F1	Financial	Unavailability of risk transfer prompts risk withdrawal
F2a	Discursive	New terms are introduced to describe war risks
F2b	Discursive	War-related terms are defined in policies or via case law
F2c	Discursive	How these terms apply to specific cases is contested
F3	Informational	Evidence is produced and made public
F4	Symbolic	Decisions inherit status and power from the legal system
F5	Active	Insurers actively shape security risks

market forces aggregate information across society. This view suggests war clauses embody societal expectations about political risk. However, war clauses are more than artifacts to be analysed.

A political platform is created when insurance disputes contest the meaning and applicability of war clauses. The history of the Israeli–Palestinian conflict was disputed in Pan Am v. Aetna (1973), which hinged on whether a plane hijacking could trigger a war clause. The legal process of discovery was used successfully to call government agencies to give evidence (and was unsuccessful in the case of the CIA). More recently, a war clause was invoked to deny a claim resulting from the NotPetya cyber attack in Mondelez v. Zurich (2018). It is speculated that the U.S. government's attribution of the attack to the Russian military will be used as evidence (Corcoran 2019).

The preceding examples motivate the relationship between war clauses and international relations, but the nature of this relationship is unclear. We aim to capture the diversity of possible effects. The result is a functional framework that cuts across theories about the structure of the international system. Our case study applies the framework to offensive cyber operations—an unsettled issue within international relations (Arquilla and Ronfeldt 1993; Cavelty 2008; Rid 2013; Kello 2017; Smeets 2018).

Functions of war clauses

Our descriptive framework (summarised in Table 1) speaks to different accounts of power within the international system. The first function emphasises the role of finance in the international political economy (Strange 2015). The discursive functions (F2a–c) draw on both a constructivist school of thought (Wendt 1992) and the role of argumentation emphasised by Risse (2000). The ability of insurers to mobilise and produce information (F3) speaks to information economics. This function, along with the fourth, also speak to the structural power of states over the production of intelligence and the legal system (Strange 2015). The final function draws on literature rooted in sociolegal research (Baker 2010) and

governance studies (Lobo-Guerrero 2012b). Mobilising these diverse strands of literature is necessary to fully account for the interaction between war clauses and international relations.

The first-order function of war clauses is to deny financial access if a qualifying event occurs (F1). If a war clause is introduced or broadened, the covered events become more salient to policyholders who are left exposed to the risk. The lack of insurance can cause policyholders to withdraw from the risk-generating activity (Haufler 1997). This withdrawal of economic activity may cause the state to intervene by socialising the risk. This was seen when builders halted construction projects in response to the terrorism exclusions following 9/11 and the state responded by passing TRIA (Thoyts 2010).

The discursive functions of war clauses can be separated according to when they take effect. The choice of terms describing war risks (F2a) takes place regardless of whether the war clause is contested. Clauses tend to be structured as lists of excluded criteria like war, warlike action, revolution and insurrection. Baker and Simon (2010) describe how such insurance imaginaries "animate the development of insurance technologies, institutions, and forms", but these industry terms can also spill over into common use, as with the concept of moral hazard (Baker 1996). A securitisation lens suggests the choice of war clauses has implications for the distribution of societal attention and resources (Buzan et al. 1998).

The terms in war clauses can be defined by insurers or in case law (F2b). Ambiguity resulting from the lack of definition has received continual criticism in the context of marine insurance (United Nations 1978). The industry maintains that explicit definitions would sacrifice "the body of market practice, case law, statutory interpretation and specially tailored clauses which had developed over the 200 or more years" (Vicente 1995). This case law is infrequently tested and covers conflicts as diverse as the American Civil War, Pearl Harbour and the 9/11 attacks.

The reasoning employed in legal cases represents a shift in the mode of discourse (F2c). The resulting "argumentative reasoning" (Risse 2000) allows for challenges and counter-challenges to validity claims about the conflicts or issues under consideration, which need not be limited to narrow disputes. For example, Pan Am v. Aetna (1973) forced a U.S. court to hear and consider the political history of the Israeli–Palestinian conflict.

The adversarial nature of legal cases incentivises the production and distribution of evidence (F3). Insurers control information collecting infrastructure in the form of claims investigators and the ability to aggregate claims across many clients (Ben-Shahar and Logue 2012). Pan Am v. Aetna (1973) highlighted how these cases can entangle external actors, in which "several inches of secret and otherwise classified State Department papers have been made a peculiar sort of secret annex to the record". Publication can range from full transparency through to being presented in secret or even refusal to provide evidence, as in the case of the CIA in Pan Am v. Aetna (1973).

Deciding ambiguities in a court of law represents a symbolic function of war clauses (F4). Symbolism may be completely absent when ambiguities are resolved without mediation, or it may inherit the "final truth" of the Supreme Court (Lerner 1937). A Supreme Court decision in Montoya v. United States (1901) ruled that

property damage caused by indigenous tribes "acting in hostility to the United States" triggered a war clause.

Lobo-Guerrero (2012b) documents how differentiating war risks allows insurers to actively shape the "strategic security environment" (F5). This includes maintaining a "War List" of regions with heightened risk and recommending risk mitigation measures, which ties into a broader theory of insurance as governance (O'Malley 1991; Ericson et al. 2003; Baker 2010). Taxonomising the ways in which insurers can actively influence risks is beyond the scope of this paper.

We now consider offensive cyber operations as a case study to illustrate this framework. We begin by sketching a discourse that has focused on the concept of cyber war and obscured societal costs resulting from so-called below the threshold operations. Later sections will argue that war clauses function to shift attention towards the private actors who absorb the cost of military adventurism in cyberspace.

Conceptions of offensive cyber operations

Rid (2013) begins his influential work by reflecting on Hollywood narratives around cyber war, identifying a common thread between these cultural themes and the metaphors invoked in policy discussions. These fears distract from "the real significance of cyber security", which is the reduction in physical violence. This consequentialist perspective suggests trade-offs exist and the cost imposed by cyber operations is less than the alternative of conventional operations. Rid concedes this will not always be true[1] but does not consider criteria for when cyber operations become too damaging.[2]

Clarke and Knake (2014) drew attention to the cost of "skirmishes in cyberspace" by identifying attacks in Estonia, Georgia and South Korea as problematic military developments. Unfortunately, claims like "cyber war has begun" (Clarke and Knake 2014) distracted from evaluation of the damage resulting from these attacks. Debating the semantics of war diverts attention away from the question of whether society can tolerate those operations falling below the threshold for war. Lewis (2002) made this point fifteen years ago: "if the risks of cyber-terrorism and cyber-war are overstated, the risk of espionage and cyber crime may be not be fully appreciated by many observers", a point that was unfortunately borne out.

A disparate set of actors believe more attention should be paid to hostile actions falling significantly below the contested threshold for cyber war. Singer and Shachtman (2011) argue online crime and espionage constitute "a real national security danger", which is being ignored in theoretical discussions about cyber war. Simpson

[1] He states "non-violent cyberattacks could cause economic consequences without violent effects that could exceed the harm of an otherwise smaller physical attack" (p. 3) and points to Waxman (2011).

[2] This abstract formulation of damage obscures the political question of damaging for whom. For example, focusing on economic consequences alone ignores privacy harms suffered by users, which do not translate into economic cost.

(2014) makes a philosophical argument that property rights are violated by state-sponsored cyberattacks, which weighs into the proportionality consideration of jus in bello. Researchers in the field of economics of information security quantify cyber losses but do not consider the link to international relations (Anderson et al. 2013; Romanosky 2016).

Henriksen (2019) argues the Group of Governmental Experts did not pay enough attention to such costs when they failed to agree upon a consensus report in June 2017. Explanations for the failure centred on the issue of lawful responses to cyber operations, which states like Cuba feared would be used to justify military action (Grigsby 2017). Henriksen (2019) suggests this deflected attention away from "various forms of espionage, manipulation of data, criminal activities and different and novel forms of coercion that cause little physical destruction" that are more concerning for Western states.

In 2019, Zurich Insurance Group joined the debate by refusing to pay damages resulting from the NotPetya attack claimed on a property insurance policy. Media reports suggested Zurich is arguing the NotPetya attack constitutes an act of war. The attack falls short of all three of Clausewitz's criteria upon which Rid (2013) is based: there was no known loss of life or even physical injury, the scope of the damage was likely unintentional,[3] let alone instrumental, and Russia failed to claim responsibility, undermining any political goal. If we accept the relevance of Clausewitz, Rid (2013) is correct: cyber war has still not taken place. Zurich are not fighting a legal case that can be dismissed in a paragraph. The sole grounds for denying coverage was the following clause in Mondelez's property insurance[4] policy (Mondelez v. Zurich 2018):

"This Policy excludes loss or damage directly or indirectly caused by or resulting from any of the following regardless of any other cause or event, whether or not insured under this Policy, contributing concurrently or in any other sequence to the loss: hostile or warlike action in time of peace or war, including action in hindering, combating or defending against an actual, impending or expected attack by any:

(i) government or sovereign power (de jure or de facto);
(ii) military, naval, or air force; or
(iii) agent or authority of any party specified in i or ii above."

Zurich are expected to point to more than USD 10 billion in total damages (McQuade 2018) and the joint U.S.–U.K. attribution of the attack to the Russian military (Corcoran 2019). Even if these facts do not meet the threshold for cyber war, they are still relevant to responsible state behaviour.

[3] Many of the victims resided in Russia, including the state oil company.

[4] Although this was a property policy, it contained terms affirmatively providing coverage for "damage to electronic data, programs, or software" (Corcoran 2019). The industry differentiates between affirmative cyber insurance coverage, which explicitly covers costs resulting from cyberattacks, and silent cyber coverage, which provides coverage for cyberattacks due to unintentional ambiguity. One can expect that affirmative cyber insurance policies reflect expectations about cyber risk, whereas silent cyber coverage does not. The industry is moving to eradicate silent cyber coverage (Woods and Simpson 2017).

Our functional framework is applied to consider how war clauses in cyber insurance forms impact the discourses and practice of offensive cyber operations. We first conduct an empirical analysis of war clauses within cyber insurance policies. This analysis can help establish trends in coverage availability and the specific terms and definitions used to define war clauses. However, it cannot probe the discursive, symbolic and informational impact of legal cases as they are yet to be concluded.

Market definitions of war

Romanosky et al. (2019) analysed cyber insurance policies filed with regulators in the U.S. and found that "acts of terrorism, war, or a military action were covered in rare cases". They discovered no significant trends over time but the scope of their study made detecting subtle changes unlikely. We used the same data source to build a corpus of 56 cyber insurance policies filed in the state of California since 2008. Both the corpus and our data collection methodology can be found in the Appendix.

Of the policies in our corpus, 41 contained a war clause and 15 did not. War clauses function to invalidate coverage if the claim resulted from any of a long list of terms broadly related to political violence. Table 2 counts the frequency of each term across all the cyber insurance policies. Categories like "Foreign conflict" are introduced for illustrative purposes.

The majority of the terms and language in Table 2 predate cyber insurance. Although these terms constitute the war clause, many fall significantly below the threshold of war. Some terms cover the actions of labour movements like strikes or lockouts. Disrupting the status quo is perhaps a better unifying theme than military operations. Insurers rely on predictable power relations, most often provided by states.[5] This view suggests that war clauses test the broader question of whether power relations have shifted in an uninsurable way. We observed no trend in the use of traditional language in cyber insurance policies.

New terms are added (F2a) when the existing list does not capture such a power shift. No insurers in our sample added cybersecurity-specific exclusions. In fact, after 2015 terms like "cyber terrorism" or "acts perpetuated electronically" were increasingly used by insurers to affirmatively cover cyber events that might otherwise be excluded, known as a carve-back by insurers. This suggests that the insurers in our corpus believe either that cyber operations do not disrupt power relations in an uninsurable way or that existing concepts cover the risk. This expansion of coverage for cyber operations (F1) casts doubt over the exceptionalism at the heart of cybersecurity politics.

Exclusions reserve the right to deny coverage but do not obligate the insurer to do so. The folk wisdom that insurers fight to deny every claim is misguided. Insurers indemnify claims related to publicly attributed cyberattacks in actuality. Sony were

[5] Physical kidnap insurance provides a fascinating counter-example in which insurers bring order to regions where the state's monopoly on violence has broken down (Lobo-Guerrero 2012b; Shortland 2019).

Table 2 Existence of war clauses and qualifying events included in each of the 56 cyber insurance policies at the date of filing

	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018	All
No war clause	2	0	1	0	4	0	2	1	4	1	0	15
War or terrorism clause	0	3	1	0	2	1	3	1	7	4	4	26
Cyber carve-back	0	0	0	1	0	0	1	1	3	4	5	15
Foreign conflict												
War	0	3	1	1	2	1	3	2	10	8	9	41
Undeclared war	0	2	1	1	2	1	3	2	10	8	8	38
Warlike action	0	2	0	1	1	1	3	2	4	8	5	27
Invasion	0	1	1	1	2	1	1	1	8	3	6	25
Hostilities	0	1	1	1	1	1	2	1	6	3	6	23
Actual or alleged strike	0	0	0	0	0	1	1	0	0	0	0	2
Acts of foreign enemies	0	1	1	1	1	1	1	1	7	3	5	22
Using military personnel or other agents	0	1	0	0	0	0	1	1	0	6	3	12
Response to an actual or expected attack	0	1	0	0	0	0	1	1	1	6	2	12
Internal conflict												
Civil war	0	2	1	1	2	1	3	2	10	8	7	37
Coup	0	0	0	0	0	0	0	0	0	0	1	1
Insurrection	0	3	1	0	2	1	3	2	10	9	9	40
Rebellion	0	2	1	0	2	1	3	2	10	9	9	39
Revolution	0	2	1	0	2	1	3	2	10	9	9	39
Military uprising	0	0	1	1	1	0	1	1	6	3	6	20
Usurped power	0	2	1	1	1	1	2	1	7	9	9	34
Civil unrest												
Civil commotion	0	2	0	1	1	1	2	1	3	3	2	16
Riot	0	2	0	0	0	0	1	0	3	3	2	11

Table 2 (continued)

	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018	All
Strike or labor action	0	1	0	1	0	0	0	1	4	3	2	12
Lockout	0	1	0	0	0	0	0	0	2	2	1	6
Response to the above	0	1	0	1	0	1	3	2	3	7	5	23
Miscellaneous												
Nationalisation	0	0	1	0	1	0	0	0	7	1	3	13
Mutiny	0	0	0	1	0	1	2	1	1	1	2	9
Terrorism	0	0	0	1	1	0	2	0	1	1	1	7
Cyber clauses												
Cyber terrorism	0	0	0	1	0	0	0	1	2	3	5	12
Network security	0	0	0	0	0	0	0	0	1	1	0	2
Perpetuated electronically	0	0	0	0	0	0	1	0	0	0	0	1
Total number of policies	2	3	2	1	6	1	6	3	14	9	9	56

An example of an exclusion is “due to war, whether or not declared, civil war, insurrection, rebellion or revolution or to any act or condition incident to any of the foregoing;”

indemnified for costs resulting from a 2014 attack (Sullivan 2016) and there were no publicly disputed exclusions from (the unknown number of) claims related to Wannacry (Ralph 2017), even though both attacks were attributed to North Korea. Despite the press coverage focusing on two exclusions related to NotPetya, the industry anticipates a total of USD 3 billion worth of claims (Evans 2019) and we are yet to hear of further exclusions.

The proliferation of "cyber terrorism" carve-backs is strange given its infrequent use in cybersecurity discourses. It was most prevalent in the aftermath of 9/11, after which threat perceptions shifted towards state-sponsored actors (Bendrath et al. 2007; Cavelty 2008). The most significant use was an Estonian official's claim that the 2007 denial of service attack represented "a kind of terrorism" (Blomfield 2007). Hansen and Nissenbaum (2009) argue the analogy was used to differentiate cyberattacks from the image of juvenile hackers and tap into support for the Global War on Terror.

The proliferation of cyber terrorism carve-backs results from a law passed in response to 9/11. The United States Department of the Treasury (2016) issued guidance stating that cyber liability insurance was considered "property and casualty insurance" under TRIA. One such implication is that insurers offering qualifying cyber coverage must "make available" coverage for cyber terrorism on materially similar terms.[6] This represents a partial socialisation of cybersecurity risk to ensure coverage availability (F1).

Cover under TRIA falls significantly short of the government acting as a generic (cyber) insurer of last resorts, which has been considered as policy by the United States, the United Kingdom and the European Union (Woods and Simpson 2017). Events must be certified by the Secretary of the Treasury, which introduces uncertainty. The Boston attack is yet to be certified despite being condemned as a "terrorist act" by President Obama (North 2013). Uncertainties also result from applying requirements such as damages being suffered "within the United States" to victims with multinational computer systems, which ties into the broader problem of applying state sovereignty to cyberspace (Mueller 2019). Government-backed reinsurance schemes are normally justified by receding coverage.

Changes in these policies can be tracked via the date of filings. We classify each policy in our corpus into: no war clause, conventional war- or terrorism-related clauses without cyber carve-back and war clause with cyber carve-back. We then use the sophistication of the insurer's pricing algorithm as a proxy for expertise. Romanosky et al. (2019) differentiate standalone cyber insurance priced using an advanced pricing algorithm from cyber insurance sold using a flat rate pricing scheme. Standalone policies are generally sold to larger firms by underwriters specialising in cyber insurance, whereas flat rate policies require comparatively little expertise to sell and rarely provide limits greater than USD 1 million.

Figure 1 reveals 2012 was the last time a standalone cyber insurance provider filed a policy without a war exclusion in California. This suggests providers

[6] https://www.lloyds.com/~/media/files/the-market/i-am-a/delegated-authority/market-bulletin/2017/y5065--us-tria-compliance-for-cyber-insurance-policies.pdf.

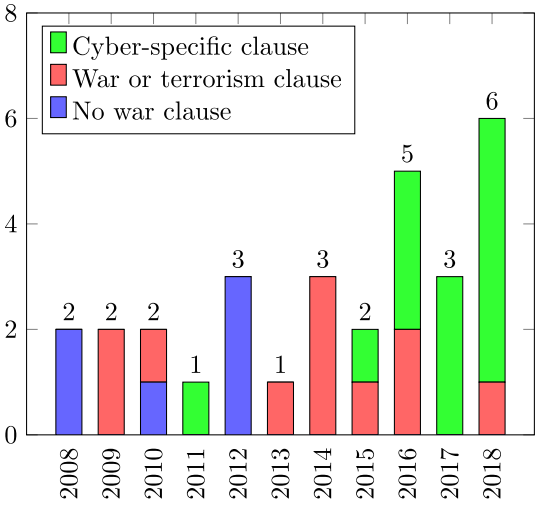

Fig. 1 How standalone cyber insurance policies exclude losses related to war

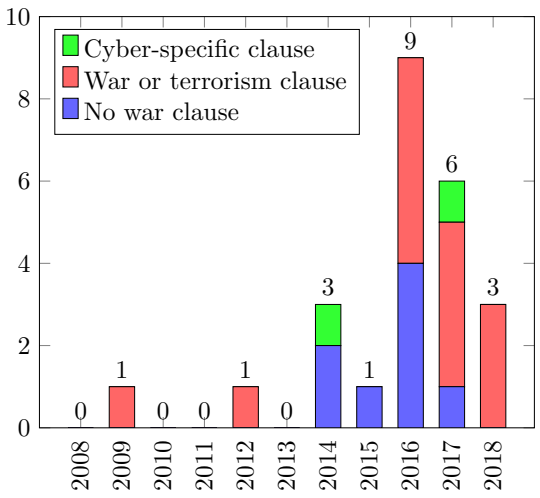

Fig. 2 How flat rate cyber insurance policies exclude losses related to war

specialising in cyber insurance believe some of the losses covered by war clauses are uninsurable.[7] The proliferation of cyber-specific qualifiers to war clauses since 2015 represents the clearest trend in the market. Figure 2 shows a significant increase in market entrance for flat rate insurance around 2016. However, policies without a war clause were introduced as recently as 2017 and only 2 of 26 were sold with a cyber-specific qualifier. This suggests these carriers are less concerned by catastrophic losses.

[7] Conversations with industry insiders suggest the biggest cyber insurance providers were all including war exclusions around this time. Unfortunately, regulatory filings do not provide the market share of a given policy so we cannot evaluate this.

The majority of cyber-specific qualifiers (12 of 15) functioned to include losses resulting from cyber terrorism. The remaining three qualifiers explicitly offered coverage for any attacks perpetrated electronically or that compromise the policyholder's network security. Cyber terrorism coverage was first introduced in 2011 as an optional endorsement the policyholder could purchase for an additional 5% of the premium. The first definition of cyber terrorism was:

"an act, including but not limited to, the use of force or violence and/or the threat thereof, of any person or group(s) of persons, whether acting alone or on behalf of, or in connection with any organization(s) or government(s), committed for political, religious, ideological or similar purposes including the intention to influence any government and/or put the public, or any section of the public, in fear."

Market entrants did not begin including cyber terrorism clauses until the regulatory guidance of the Department of the Treasury (2016). Most required the act to result from "social, ideological, religious, economic or political objectives'', or similar wordings. The actor was always described as an individual or group, although some definitions provided coverage even if they were acting on behalf of a government. This analysis suggests that insurance for state-sponsored cyberattacks is becoming more available, with relevance to F1.

Beyond insurance policies

The remaining functions of war clauses rely on factors beyond contractual wording. These are more difficult to probe as they depend on how legal disputes unfold and how insurers respond to the risk. With this in mind, we identify available evidence and discuss the issues at hand in the knowledge that definitive answers can only be provided by future work.

The question of how terms like warlike action apply to cyberattacks (F2c) is beyond our scope and will be probed in Mondelez v. Zurich (2018). Our analysis does, however, speak to the availability of alternative language, which was a consideration in Pan Am v. Aetna (1973). The judge criticised insurers for drafting a policy without language specific to the "contemporaneously vivid" risk of hijacking when more certain clauses were used by other insurers. Our analysis suggests cybersecurity-specific terms are not used to exclude coverage via war clauses and, in fact, cyber terms were only used to expand coverage. These insights may not generalise beyond our sample of cyber insurance policies to traditional lines, which tend to have broader exclusions.

If courts find that the "antiquated terminology" (United Nations 1978) of today's war clauses does not apply to offensive cyber operations, then insurers will be forced to introduce new terms that specifically describe which cyberattacks are excluded. Such a move would see the insurance industry formulate which offensive cyber operations are uninsurable and, consequently, prohibitively damaging to society.[8]

[8] Slupska (2020) argues that the metaphor of cyber war undermines international collaboration, leading to a self-fulfilling prophecy.

These explicit formulations are favoured in norm development as they clarify the relationship between actions and responses (Kratochwil 1991). War clauses emerging from this negotiation could provide the evolution of cyber norms with concepts, legal language and arguments fortified with market information (F2).

This argument belies a contested assumption that insurance policies accurately capture the risk landscape. An information economics view emphasises how market forces mediate between the informational infrastructure of the insurance industry (Ben-Shahar and Logue 2012), the local information of policyholders (Hayek 1945) and the availability of capital to absorb shocks. A more critical lens highlights endemic risk-taking in the insurance industry (Ericson and Doyle 2004) and the subtle politics that pervade insurance modelling (Weinkle 2019). Whereas the industry normally uses historical events to shape scenarios, the dearth of systemic cybersecurity incidents forces modelling firms to imagine cyber catastrophes with little historical basis (Coburn et al. 2018).

In terms of the evidence producing informational function (F3), insurers demand widely agreed and neutral attributions of cyberattacks to political actors (Mueller et al. 2019). Romanosky and Boudreaux (2019) differentiate technical attribution (code, computers and communications) from political attribution (people, organisations and motives). Computer security firms collect evidence about patterns of technical indicators that cannot be directly linked to political actors without information traditionally collected by intelligence agencies. Discovery could be used, as it was in Pan Am v. Aetna (1973), to gain access to classified documents about attributions by governments.

Agencies already face an uneasy balance between the secrecy necessary to protect sources and the pressure to publicise information to influence adversaries (Rid and Buchanan 2015). Egloff (2020) describes frustration with public scepticism about the methods used to attribute the Sony hack to North Korea. These methods would face greater scrutiny in a court of law (F2c), though secret evidence can be used to avoid public disclosure. On the other hand, these legal cases provide a symbolic platform for intelligence agencies to present evidence that may function to amplify attributions (F4).

The question of how actively insurers are shaping the strategic security landscape is very much open (F5). Following the insurance as governance concept, the industry can provide the private actors who are targeted by offensive cyber operations with incentives to improve security levels (Schneier 2001; Talesh 2018; Herr 2019). However, a review of empirical studies suggests this is less effective in practice (Woods and Moore 2020). Further, insurance as governance is focused on basic cyber hygiene, not preventing state-sponsored attacks.

Actively shaping the norms that govern state behaviour may be a more effective pursuit of F5. Anderson (1994) predicted that insurers would take a position within the norms debate by advocating against offensive cyber operations. This makes economic sense given that they directly indemnify the victims. Yet, technology companies have taken the lead as cyber norm entrepreneurs (Hurel and Lobato 2018)

and no traditional insurers have yet signed the Cybersecurity Tech Accord led by Microsoft.[9]

Conclusion

In answering the question of what constitutes war, we suggested ethical, constructionist and realist arguments appeal to reason, shared expectations and the self-interest of the powerful, respectively. Information and market discipline are similarly simplistic candidates for the validity of market-based definitions of war. Markets offer incentives for participants to collect information and negotiate the terms of the contract. Too many exclusions and the policyholder will choose another insurer, too few and claims will bankrupt the insurer.

War clauses emerging from this evolutionary process reflect market expectations about uninsurable events rooted in political conflict. Uncertainty forces insurers to drape such clauses in ambiguity and instead rely on an infrequently tested body of case law (Vicente 1995). Disputes over these terms represent a novel discourse around political conflict characterised by legal reasoning, evidential standards and higher burdens of proof. In this way, private actors force ostensibly apolitical courts to consider political conflicts.

Strange (2015) warned against rejecting a state-centric perspective only to overemphasise markets. The power of markets is granted "by whoever wields power" and there are many ways the state exhibits authority over insurance markets. Pan Am v. Aetna (1973) showed that government agencies can provide evidence for these cases in secret and use national interest as a justification for refusing to do so. More concretely, states have responded to retracting private markets by socialising the risk (Strange 1996; Thoyts 2010).

Our analysis of 56 cyber insurance policies revealed that insurers specialising in cyber insurance have, driven by market and regulatory forces, converged on an equilibrium of excluding circumstances significantly below the threshold of war but including cyber terrorism (see Fig. 1). Insurance for cyber terrorism or cyberattacks more generally has the potential to make these "normal risks", in which losses are tolerated and expected as part of economic activity in modern times. If state and market experience with natural hazard catastrophe loss over the past several decades is any indication, unexpected insured losses instigate volatile social and market dynamics over the causes and consequences of a 'new normal' (Weinkle 2015; Elliott 2019; Taylor 2020).

At least three problematic issues arise. First, there are questionable ethics in making the risk of terrorism or any sort of attack socially acceptable (Lubin 2019). Private insurance functions to legitimate both state-orchestrated cyber operations and the risk-generating business models in which personal data is collected at an unprecedented scale and basic risk management measures are often flaunted. Insurers may in turn fall victim to the wrath of public opinion as privacy conceptions shift and

[9] A data analytics company, QOMPLX, who have recently launched an MGA, are the exception.

regulation evolves. The insurance industry's history with U.S. asbestos liability suits demonstrates the financial costs of the public's ire (Carroll et al. 2005).

Second, governments may seek to extend the normality of the current situation in which insurance absorbs the consequences of offensive cyber operations. In 2016, the U.S. clarified that TRIA applied to cybersecurity, which means that some cyber risk held by private companies will be socialised by the U.S. Treasury. While losses thus far have been modest, the potential for catastrophe can be seen in the scale of the NotPetya attack (Greenberg 2019) or in some of the industry's so-called realistic disaster scenarios (Coburn et al. 2018).

Third, it is not clear whether a line between war and peace can be meaningfully drawn in the context of cybersecurity. Kello (2017) describes the current situation as "unpeace". Traditionally the industry has relied on case law to uncover this line. Cases like Mondelez v. Zurich (2018) will test how exceptional cybersecurity is in the history of military conflict considered in war clause cases. If existing war clauses cannot be meaningfully applied, then the industry will be forced to affirmatively describe the point at which cyber conflict becomes uninsurable.

Acknowledgements The authors would like to thank the reviewers for the thoughtful comments on an exploratory research project. It began as an abstract submitted to The Hague Program for Cyber Norms, who were very generous in offering support to early career researchers crossing disciplines. A second round of insightful, if slightly bruising, comments were offered by the The Center for Security Studies at ETH Zurich, thanks in particular to Myriam Dunn Cavelty for making that happen.

Appendix: data collection and analysis

Our data only relates to the admitted market in California.[10] We obtained regulatory filings using the same search as Woods et al. (2019):

"We extracted rate schedules related to cyber insurance by searching with keywords "cyber", "security" and "privacy", as in Romanosky et al. (2019)."

We only collected filings with type "new program" because these represent entirely new filings[11] and they also contain documents related to how insurance is priced. This allowed us to determine whether the insurer was selling a flat rate policy or more sophisticated standalone policies. We then extracted policy wording and the date on which the policy was filed. Note the regulator must approve the filing before policies can be sold.

Our inductive approach consisted of first reading through the policy. We consider the policy to be both the general provisions and the specific endorsements found within the filing. We cannot track terms and conditions contained in other filings nor any wordings that are negotiated after the fact. We aimed to identify any war or terrorism clauses and definitions. These were generally found in the exclusions section.

[10] Refer to Romanosky et al. (2019) for a more detailed explanation. They suggest there is little variation across admitted and non-admitted markets.

[11] Future work could track how wordings are updated over time. This may reveal war clauses offered by one insurer changing over time.

We also searched each document for terms including "war", "terrrorism" and "hostility". Each exclusion was extracted, along with any sub-clauses and relevant definitions, and can be found in the following section.

The clauses are essentially lists with little grammatical complexity. We thus conducted a simplistic inductive content analysis to identify which terms are included in this list. The similarities in wordings across documents made this task relatively straightforward. The main difficulties lay in deciding which terms could be grouped together. The results are described in Table 2.

Figures 1 and 2 result from a coarse mapping of each clause to one of three categories: no war clause, war or terrorism clause, and cyber-specific qualifier. A policy without any war clause was mapped to the first. War clauses were classified as cyber-specific qualifier if they contained any terms like cyber, network security or "acts perpetuated electronically".

References

Anderson, R., C. Barton, R. Böhme, R. Clayton, M.J. Van Eeten, M. Levi, T. Moore, and S. Savage. 2013. Measuring the cost of cybercrime. In *The economics of information security and privacy*, ed. R. Böhme, 265–300. Berlin: Springer.

Anderson, R.J. 1994. Liability and computer security: Nine principles. In *Proceedings of the European Symposium on Research in Computer Security*, pp. 231–245. Berlin: Springer.

Arquilla, J., and D. Ronfeldt. 1993. Cyberwar is coming! *Comparative Strategy* 12 (2): 141–165.

Baker, T. 1996. On the genealogy of moral hazard. *Texas Law Review* 75: 237.

Baker, T. 2010. Insurance in sociolegal research. *Annual Review of Law and Social Science* 6: 433–447.

Baker, T., and J. Simon. 2010. *Embracing risk: The changing culture of insurance and responsibility*. Chicago: University of Chicago Press.

Ben-Shahar, O., and K.D. Logue. 2012. Outsourcing regulation: How insurance reduces moral hazard. *Michigan Law Review* 111: 197.

Bendrath, R., J. Eriksson, and G. Giacomello. 2007. From 'Cyberterrorism'to 'Cyberwar', back and forth: How the United States securitized cyberspace. In *International relations and security in the digital age*, ed. J. Eriksson and G. Giacomello, 77–102. London/New York: Routledge.

Blomfield, A. 2007. Estonia calls for a NATO strategy on 'Cyber-terrorists' after coming under attack. *The Daily Telegraph*, May 18.

Buzan, B., O. Wæver, O. Wæver, J. De Wilde, et al. 1998. *Security: A new framework for analysis*. Boulder: Lynne Rienner Publishers.

Carroll, S.J., D.R. Hensler, J. Gross, E.M. Sloss, and M. Schonlau. 2005. *Asbestos litigation*. Santa Monica: Rand Corporation.

Cavelty, M.D. 2008. Cyber-terror—looming threat or phantom menace? The framing of the US cyber-threat debate. *Journal of Information Technology & Politics* 4 (1): 19–36.

Clarke, R.A., and R.K. Knake. 2014. *Cyber war*. New York: Tantor Media, Incorporated.

Coburn, A., E. Leverett, and G. Woo. 2018. *Solving cyber risk: Protecting your company and society*. New Jersey: Wiley.

Corcoran, B. 2019. *What Mondelez v. Zurich may reveal about cyber insurance in the age of digital conflict*. Lawfare. https://www.lawfareblog.com/what-mondelez-v-zurich-may-reveal-about-cyber-insurance-age-digital-conflict.

Department of the Treasury. 2016. *Guidance concerning stand-alone cyber liability insurance policies under the terrorism risk insurance program*. [Online; accessed 27-Jan-2020].

Egloff, F.J. 2020. Contested public attributions of cyber incidents and the role of academia. *Contemporary Security Policy* 41 (1): 55–81.

Elliott, R. 2019. 'Scarier than another storm': Values at risk in the mapping and insuring of us floodplains. *The British Journal of Sociology* 70 (3): 1067–1090.

Ericson, R.V., and A. Doyle. 2004. *Uncertain business: Risk, insurance and the limits of knowledge*. Toronto: University of Toronto Press.
Ericson, R.V., A. Doyle, and D. Barry. 2003. *Insurance as governance*. Toronto: University of Toronto Press.
Evans, S. 2019. *Petya cyber industry loss passes $3bn driven by Merck silent cyber: PCS Reinsurance News*.
Greenberg, A. 2019. *Sandworm: A new era of cyberwar and the hunt for the Kremlin's most dangerous hackers*. New York: Doubleday.
Grigsby, A. 2017. The end of cyber norms. *Survival* 59 (6): 109–122.
Hansen, L., and H. Nissenbaum. 2009. Digital disaster, cyber security, and the Copenhagen school. *International Studies Quarterly* 53 (4): 1155–1175.
Haufler, V. 1997. *Dangerous commerce: Insurance and the management of international risk*. New York: Cornell University Press.
Hayek, F.A. 1945. The use of knowledge in society. *The American Economic Review* 35 (4): 519–530.
Henriksen, A. 2019. The end of the road for the UN GGE process: The future regulation of cyberspace. *Journal of Cybersecurity* 5 (1): 1–9.
Herr, T. 2019. Cyber insurance and private governance: The enforcement power of markets. *Regulation & Governance*. https://doi.org/10.1111/rego.12266.
Hurel, L.M., and L.C. Lobato. 2018. Unpacking cyber norms: Private companies as norm entrepreneurs. *Journal of Cyber Policy* 3 (1): 61–76.
Kello, L. 2017. *The virtual weapon and international order*. London: Yale University Press.
Kratochwil, F.V. 1991. *Rules, norms, and decisions: On the conditions of practical and legal reasoning in international relations and domestic affairs*, vol. 2. Cambridge: Cambridge University Press.
Lerner, M. 1937. Constitution and court as symbols. *The Yale Law Journal* 46 (8): 1290–1319.
Lewis, J.A. 2002. *Assessing the risks of cyber terrorism, cyber war and other cyber threats*. DC: Center for Strategic & International Studies Washington.
Lobo-Guerrero, L. 2012a. *Insuring war: Sovereignty, security and risk*. Oxon/New York: Routledge.
Lobo-Guerrero, L. 2012b. 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.
Lubin, A. 2019. *The insurability of cyber risk*. Available at SSRN: https://ssrn.com/abstract=3452833 or https://doi.org/10.2139/ssrn.3452833.
McQuade, M. 2018. *The untold story of NotPetya, the most devastating cyberattack in history*. Wired.
Mondelez v. Zurich. 2018. *Complaint in Mondelez International, Inc. v. Zurich American Insurance Company WL 4941760* (Circuit Court of Illinois.) (Trial Pleading).
Montoya v. United States. 1901. *Verdict 180 U.S. 261* (U.S. Supreme Court).
Mueller, M., K. Grindal, B. Kuerbis, and F. Badiei. 2019. Cyber attribution. *The Cyber Defense Review* 4 (1): 107–122.
Mueller, M. L. 2019. *Against Sovereignty in Cyberspace*. International Studies Review. viz044.
North, M. 2013. Boston bombings: Obama condemns 'act of terrorism'. *BBC*.
O'Malley, P. 1991. Legal networks and domestic security. *Studies in Law, Politics and Society* 11 (1): 165–184.
Pan Am v. Aetna. 1973. *Pan American World Airways, Inc. v. Aetna Cas. Sur. Co. Verdict 368 F. Supp. 1098* (S.D.N.Y. 1973).
Ralph, O. 2017. Cyber insurance market expected to grow after wannacry attack. *The Financial Times*.
Rid, T. 2013. *Cyber war will not take place*. New York: Oxford University Press.
Rid, T., and B. Buchanan. 2015. Attributing cyber attacks. *Journal of Strategic Studies* 38 (1–2): 4–37.
Risse, T. 2000. "Let's argue!": Communicative action in world politics. *International Organization* 54 (1): 1–39.
Romanosky, S. 2016. Examining the costs and causes of cyber incidents. *Journal of Cybersecurity* 2 (2): 121–135.
Romanosky, S., and B. Boudreaux. 2019. Private sector attribution of cyber incidents. *RAND Corporation working paper series*.
Romanosky, S., A. Kuehn, L. Ablon, and T. Jones. 2019. Content analysis of cyber insurance policies: How do carriers price cyber risk? *Journal of Cybersecurity*. https://doi.org/10.1093/cybsec/tyz002.
Schneier, B. 2001. Insurance and the computer industry. *Communications of the ACM* 44 (3): 114–114.
Shortland, A. 2019. *Kidnap: Inside the ransom business*. Oxford: Oxford University Press.
Simpson, T.W. 2014. The wrong in cyberattacks. In *The ethics of information warfare*, vol. 14, ed. L. Floridi and M. Taddeo. Cham: Springer International Publishing.

Singer, P. W., and N. Shachtman. 2011. *The wrong war: The insistence on applying cold war metaphors to cybersecurity is misplaced and counterproductive*. Brookings Government Executive 12.
Slupska, J. 2020. War, health, & ecosystem: Generative metaphors in cybersecurity governance. *Philosophy & Technology*, Forthcoming.
Smeets, M. 2018. A matter of time: On the transitory nature of cyberweapons. *Journal of Strategic Studies* 41 (1–2): 6–32.
Strange, S. 1996. *The retreat of the state: The diffusion of power in the world economy*. Cambridge: Cambridge University Press.
Strange, S. 2015. *States and markets*. London: Bloomsbury Publishing.
Sullivan, C. 2016. The 2014 Sony hack and the role of international law. *Journal of National Security Law & Policy* 8 (3): 1–27.
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.
Taylor, Z.J. 2020. The real estate risk fix: Residential insurance-linked securitization in the Florida metropolis. *Environment and Planning A Economy and Space*. https://doi.org/10.1177/0308518x19896579.
Thoyts, R. 2010. *Insurance theory and practice*. Oxon/New York: Routledge.
United Nations. 1978. *Legal and documentary aspects of the marine contract*. United Nations Conference on Trade and Development.
Vicente, C. 1995. War risk insurance. *Neptunus Law Review* 1 (4): 1–19.
Waxman, M.C. 2011. Cyber-attacks and the use of force: Back to the future of article 2 (4). *Yale Journal of International Law* 36: 421.
Weinkle, J. 2015. A public policy evaluation of Florida's citizens property insurance corporation. *Journal of Insurance Regulation* 34: 1.
Weinkle, J. 2019. Experts, regulatory capture, and the "governor's dilemma": The politics of hurricane risk science and insurance. *Regulation & Governance*. https://doi.org/10.1111/rego.12255.
Wendt, A. 1992. Anarchy is what states make of it: The social construction of power politics. *International Organization* 46 (2): 391–425.
Woods, D.W., and T. Moore. 2020. Does insurance have a future in governing cybersecurity? *IEEE Security Privacy* 18 (1): 21–27.
Woods, D. W., T. Moore, and A. C. Simpson (2019). The county fair cyber loss distribution: Drawing inference from insurance prices. In *Proceedings of The 18th Workshop on the Economics of Information Security (WEIS 2019)*.
Woods, D.W., and A.C. Simpson. 2017. Policy measures and cyber insurance: A framework. *Journal of Cyber Policy* 2 (2): 209–226.

About the authors

Daniel W. Woods is a post-doctoral researcher in the Department of Computer Science at the University of Innsbruck, Austria. His research interests include cyber insurance, the economics of security and privacy and quantifying risk. He received his Ph.D. in Cybersecurity from the University of Oxford, U.K.

Jessica Weinkle is an assistant professor in the Department of Public and International Affairs at the University of North Carolina Wilmington. Her research and writing examines the science and politics of catastrophe risk governance. Jessica's work appears in a diverse range of academic journals, such as Regulation & Governance and Nature Sustainability. Current projects include examining the politicisation of insurance in the face of large-scale policy dilemmas, such as climate change.