Market Definitions of Cyber War

Daniel W. Woods[*], Jessica Weinkle[†]

WORKING PAPER

September 30, 2019

Abstract

Definitions of war found in cyber insurance policies provide a novel window into the concept of cyber war. Changes in policy wording reflect shifting expectations surrounding technology and military strategy as mediated by market forces. In a recent legal case, an insurer refused to pay a property insurance claim by arguing the cause of the claim, a cyber attack, constituted a hostile or warlike action. We build a corpus of 56 cyber insurance policies. Longitudinal analysis reveals distinct market trends. 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". This article explores the economic, strategic, and regulatory forces driving war clauses in cyber insurance policies.

We then discuss how these definitions contest state-formulated narratives around war by arguing that the insurance industry can influence discourses on offensive cyber operations. Insurance policies constitute private contracts that do not confer rights or responsibilities on third-parties, in this case states. Legal cases do, however, provide a symbolic platform to present evidence about offensive cyber operations and subject it to legal reasoning. Nevertheless, states maintain significant structural power in influencing what evidence can be presented in court and in controlling its production by intelligence agencies.

[*]Department of Computer Science, University of Innsbruck, Austria and Department of Computer Science, University of Oxford, UK

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

Daniel W. Woods, Jessica Weinkle. *Market definitions of cyber war and hostility.* In Proceedings of The Hague Conference on Cyber Norms, 2019.

1 Introduction

What constitutes war? Is there a threshold for hostility below which society can 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 have a role to play.

Markets offer answers in the form of war and military clauses in insurance policies. The British Government discovered this when war exclusions in marine insurance threatened to halt sea-trade, forcing the Government to take "responsibility for merchant ships damaged or sunk by enemy action" (Strange, 1996). The naval arms race leading up to World War I led the insurance industry to believe sea voyages were uninsurable. Whereas, 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. Unlike with bomb damage coverage during World War I, insurers selling insurance covering Spanish property during the civil war made considerable losses (Haufler, 1997). Ships trading with Spain could also purchase private insurance against war risks during the Spanish civil war based on the unfounded assumption that British military vessels provided protection. Haufler (1997) argues private insurance should be seen as an enabler of trade and prosperity in the presence of political risk, not as financiers profiting from war.

The social value of insurance 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 began halting construction projects as the buildings could not be insured. The US government responded by passing the Terrorism Risk Insurance Act (2002), which forced all property insurance providers to offer terrorism coverage and committed the US Treasury to covering losses above a pre-defined threshold. In terms of the who gets what of this case, terrorism risk was socialised to the advantage of commercial property owners in dense urban centres.

Shifting risk perceptions influence the terms of insurance policies. Coverage expansion is driven by policyholder fears rising relative to those of insurers, whereas coverage contraction reveals insurers becoming uncomfortable with the potential for catastrophe. Hayek (1945) famously argued market forces aggregate information across society—this view suggests market definitions embody societal expectations about political risk. This article explores what cyber insurance policies reveal about the extent to which society can tolerate offensive cyber operations.

2 Conceptions of Cyber War

Rid (2013) begins his influential work by reflecting on Hollywood narratives around cyber war. He goes on to identify 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 smaller than the conventional alternative. Rid concedes this will not always be true[1] but does not consider criteria for when cyber operations become too damaging[2].

Rid's line of debate around the semantics of war distracts 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. Stone (2013) responded to Rid by considering the conceptual basis of force and violence in the context of (cyber) war. 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" created semantic controversy and distracted from evaluating the damage resulting from these attacks.

The potential benefits of offensive cyber operations is another source of distraction. Arquilla and Ronfeldt (1993) looked forward thoughtfully but failed to meaningfully ask questions beyond how the United States might use technological developments to their strategic advantage. Similarly, Farwell and Rohozinski (2011) considered the cost of developing offensive operations, focusing on how intelligence agencies can harness the non-state actors who specialise in exploiting computer systems[3] without considering the societal costs beyond a brief discussion of collateral damage.

A disparate set of actors believe more attention should be paid to hostile actions falling significantly below 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 (2014) makes a philosophical argument that property rights are violated by state-sponsored cyber attacks, which weighs into the proportionality consideration of *jus in bello*. Researchers within the economics of information security (Anderson et al., 2013; Romanosky, 2016) quantify cyber losses but do not consider the link to international relations.

[1] He states "non-violent cyber attacks 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.

[3] Even though many of the tools and techniques used by cybercriminals were created by intelligence agencies to begin with.

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. The United States would argue establishing what constitutes lawful response creates a meaningful deterrent, whereas norms can be endorsed in a report and disregarded in practice. But when the US realised an agreement on lawful response was not possible, it faced a choice between the symbolism of withdrawal and the benefit of the "implementation of stabilizing measures" (Henriksen, 2019). An estimate of the consequences of ongoing below the threshold activities must weigh into this decision.

The insurance industry is uniquely placed to monitor economic consequences of offensive cyber operations. In 2019, Zurich Insurance Group joined the debate by refusing to pay damages resulting from the NotPetya attack. Media reports suggested Zurich is arguing the NotPetya attack constitutes an "act of war". It falls short of all three of Clausewitz's criteria: there was no known loss of life or even physical injury, the damage to Western companies was likely unintentional[4] let alone instrumental, and Russia failed to claim responsibility undermining any political goal. By his own criteria, 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 exclusion is not based on Clausewitz's definition. The sole grounds for denying coverage was the following clause:

> 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.
>
> ...

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

The legal case turns on a broader definition covering "hostile or warlike actions"[5]. Zurich's argument rests on more than $10 billion in total damages[6] and the joint US–UK attribution of the attack to the Russian military. We argue this legal case is a form of advocacy against military adventurism in cyberspace. We first provide an empirical analysis of how war and hostility is defined in cyber insurance policies.

3 Market Definitions of War

Romanosky et al. (2019) analysed cyber insurance policies filed with regulators in the US and found "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.

War clauses function to invalidate coverage and are found in the exclusions section. Of the policies in our corpus, 42 contained a war clause and 14 did not. The structure of the exclusion in the previous section is broadly representative of those in our sample. War clauses generally exclude any losses covering one from a list of criteria including terms like: war (declared or undeclared), warlike action, hostilities, military force, civil war, insurrection, confiscation, or mutiny. The clauses have not been standardised across companies. The meaning of terms like war or military force are not defined within the document and, consequently, must be interpreted by courts.

The policies contained a number of interesting qualifiers to the war clauses. Such qualifiers expand coverage that would otherwise be denied by a traditional war clause and take the form:

> This exclusion will not apply to X.

where X can relate to terrorism as defined in the Terrorism and Reinsurance Act (TRIA) of 2002, which insurers are required to offer coverage for. In cyber-specific qualifiers, X took the form "Cyber Terrorism", "Network security breaches", or "acts perpetuated electronically". This breaks down into three categories of war clause found in our corpus: no war clause, conventional war or terrorism related clauses, and war clause with cyber-specific qualifier.

Analysing the corpus in terms of the expertise of the insurer and when the policy was filed with the regulator reveals interesting trends. We 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 special-

[5] `https://www.ft.com/content/8db7251c-1411-11e9-a581-4ff78404524e`

[6] `https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/`

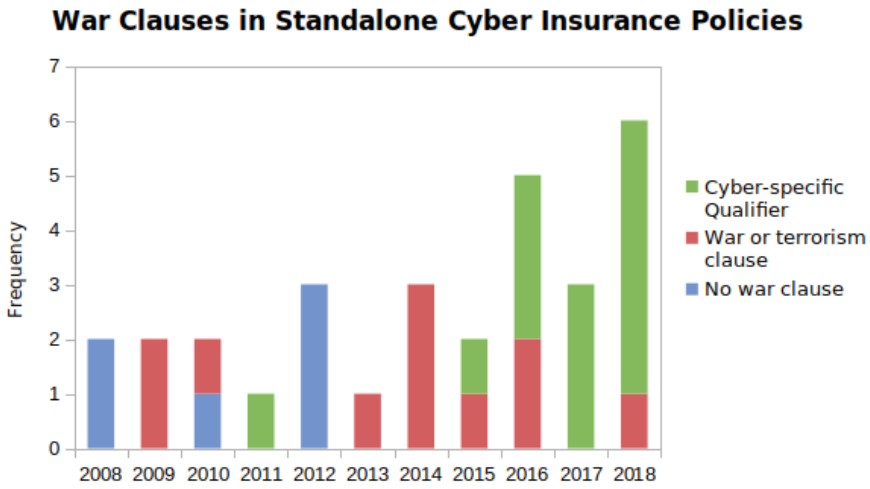

Figure 1: How standalone cyber insurance policies exclude losses related to war.

ising in cyber insurance, whereas flat-rate policies require comparatively little expertise to sell and rarely provide limits greater than $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 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, likely because these policies have smaller limits.

The majority of the cyber-specific qualifiers (13 of 16) functioned to include losses resulting from *cyber terrorism*. The remaining 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,

[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.

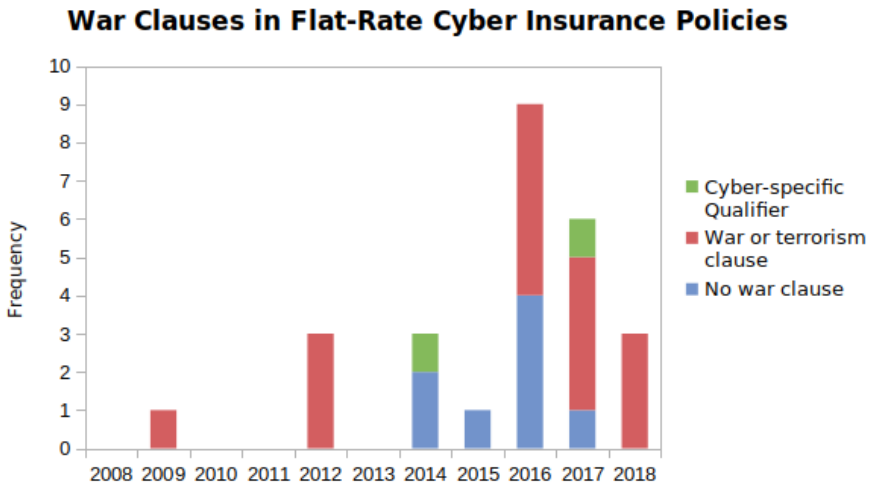

Figure 2: How flat-rate cyber insurance policies exclude losses related to war.

> ideological, or similar purposes including the intention to influence any government and/or put the public, or any section of the public, in fear.

Curiously market entrants did not immediately introduce their own cyber terrorism endorsements. The majority of the cyber-specific qualifiers, which can be found in the Appendix, were introduced five years later. 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.

Policy wordings provide a window into how the insurance industry views war and hostility in the context of cyber insurance, but there are many important factors not captured by contractual analysis.

4 Beyond Insurance Policies

The reality of the market reveals insurers display restraint in the enforcement of exclusions. Despite the Zurich case stealing the headlines after the NotPetya attack[8], there were many more cases in which insurers indemnified victims of this attack. The insurers of Sony Pictures paid out on a 2014 claim even though it resulted from an attack that was attributed to North Korea by the FBI and the Obama administration (Sullivan, 2016). Exclusions reserve the right to deny coverage but do not obligate the insurer to do so.

[8] A similar case garnered less media attention: Merck Co., Inc. v. Ace American Insurance Co., No. UNN-L-002682-18 (N.J. Sup. Ct.)

This gap between policy language and market reality is in part caused by insurance law. Ambiguity in policies is interpreted against the drafter's interest (Thoyts, 2010). This leads insurers to offer policies that exclude losses that will be paid in actuality. Propensity to indemnify losses that are contractually excluded is governed by market norms. Policyholders can punish insurers who exclude losses they reasonably expect to be covered by ending the business relationship[9]. Consequently, the wording of policies cannot be separated from the expectations of market participants.

Legal interpretation is another intervening factor. Policies do not define terms like *war* or *government agent*. Simon (1981) describes a body of case law in which war clauses are interpreted in illuminating ways. Many cases related to Pearl Harbour turned on whether a state of war existed despite war not being declared. In another example, a Supreme court decision[10] ruled property damaged caused by Tribes "acting in hostility to the United States" constituted an act of war. How these precedents apply in the context of offensive cyber operations is a fruitful topic for future study.

Regulatory developments explain the trend towards affirmatively including cyber terrorism. The United States Department of the Treasury (2016) issued guidance stating that cyber liability insurance was considered "property and casualty insurance" under the Terrorism Risk Insurance Act. One such implication is that insurers offering cyber insurance must "make available" coverage for cyber terrorism on materially similar terms[11]. In other words, cyber terrorism cannot be excluded from cyber insurance policies and the United States treasury will cover qualifying losses[12]. Including cyber terrorism under TRIA is not the same as the government acting as a generic (cyber) insurer of last resorts[13]. Woods and Moore (2019) argue this makes little sense while an over-supply of capital for cyber insurance exists, unlike the situation when TRIA was passed (Kunreuther and Michel-Kerjan, 2004).

Prudential oversight over the cyber insurance market is still developing[14]. It concerns the insurer's ability to pay and generally requires the insurer to hold enough capital. Weinkle (2019) argues establishing how much is enough is in part political and not a question of objective risk management. Decisions are driven by a form of stress test provided by so-called catastrophe modeling

[9]This provides little power to buyers of personal insurance but corporate insurance is different. Firms often buy multiple lines of insurance from the same broker. In representing multiple buyers across multiple insurance lines, brokers hold significant market power over insurers.

[10]Montoya v. United States, 180 U.S. 261 (1900).

[11]`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`

[12]The suitability of the criteria for cyber attack is doubtful. For example, the the act needs "to have resulted in damage within the United States". How this geographic criterion applies to losses related to the computer systems of multinational corporations is yet another can of worms.

[13]Woods and Simpson (2017) show that this has been considered as policy by the United States, the United Kingdom and the European Union.

[14]A credit rating firm warned it will downgrade insurers selling cyber insurance "too aggressively" (Eling and Schnell, 2016).

firms. The data inputs for these tests are contested—in Florida the regulatory preference for the long-term catalog has clashed with private market preference for the near-term catalog (Weinkle, 2015). The dearth of systemic cybersecurity incidents forces (or frees) these firms to imagine cyber catastrophe, where imagine is the operative word. Regulators tend to co-develop such tests with insurers who could use the lack of historical record to push for favourable requirements.

5 Strategic Implications

One might expect changes in cyber insurance policies over time follow the contours those found in academic debate. The concept of cyber war is older than our corpus, even so we observed many policies without war clauses. This suggests cyber war is taken less seriously by *some* professional risk managers than the catastrophists warning of an impending "cyber pearl harbour"[15]. And yet, *some* insurers include clauses so broad as to include attacks falling significantly below the criteria applied by Rid (2013). This suggests below-the-threshold attacks threaten the existence of a private insurance market. Concluding that the market is as divided as academic debates would be false. Insurers specialising in cyber insurance have, driven by market and regulatory forces, converged on an equilibrium of excluding war but including cyber terrorism (see Figure 1).

Market definitions create a narrative surrounding war that seem to exist beyond the authority of states. An insurer arguing a cyber attack to be a hostile action or even warlike could contravene the strategic interests of states[16]. 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, such as the Terrorism Risk Insurance Act.

Insurance law is interpreted and enforced within a state's legal system. This has led accusations of political judgements. American courts were accused of wrongly dumping asbestos liability on insurers in the United Kingdom (Tweedale (2000))[17]. What constitutes admissible evidence and the conditions under which it is presented will be more relevant in the case of interpreting insurance cases pertaining to offensive cyber operations. This is especially relevant given states maintain a near monopoly on structural power in the form of (claims to) knowledge about political adversaries. Most attributions rely on observing technical indicators which have already been linked to adversaries by intelligence agencies. Only evidence made public can be presented in court and

[15] Dunn Cavelty (2013) tracks this analogy to a 1991 testimony before the US Congress.

[16] Note that within TRIA, the Treasury retains the right to determine what constitutes an act of terrorism (Kunreuther and Michel-Kerjan, 2004).

[17] Many of these cases were justified by the principle of deep pockets that assigns liability to the party deemed in the best position to pay it. However, liability disproportionately fell on individual investors who had accepted unlimited liability for the most affected syndicates and went bankrupt as a result. The investors were often advised by industry insiders whose personal investments happened to be in syndicates unaffected by the catastrophic losses. Raphael (1994) charts the human tragedy of this.

subjected to scrutiny. Intelligence agencies will no doubt favour secret evidence justified on the grounds of national security.

Nevertheless, the insurance industry influences the formation of norms by influencing the structure of discourse. The institution of insurance law creates a conceptual testing ground providing many features deemed important in norm development. Kratochwil (1991) emphasises the importance of "explicitly formulated rules [that] make it possible to discuss diverging expectations". Court rooms provide a symbolic platform to present and reason over evidence. This creates a public discourse characterised by "argumentative reasoning" (Risse, 2000) in which challenges and counter-challenges to validity claims produce less fragile shared expectations.

Insurers also take a position within the norms debate by advocating against offensive cyber operations—a role predicted by Anderson (1994) in 1994. This provides another instance of a private company acting as a cyber norm entrepreneur (Hurel and Lobato, 2018). As hierarchical networks pursuing shareholder value, insurers are different in structure and purpose to the transnational advocacy networks described by Keck and Sikkink (2014). However, we use their analytical framework to draw comparisons in terms of tactics.

Information politics are used by insurers in aggregating damage across their network of policy holder and drawing attention to public attributions by external actors. Presenting a simple story of a policyholder being attacked by a nation state represents *symbolic politics* by drawing on public preconceptions about hostile states. Fighting the case in a court of law adds an additional layer of symbolism. *Accountability politics* are limited by the lack of formal statements by states about offensive cyber operations. However, insurers offering coverage for cyber terrorism creates a liability for the US treasury[18], which could represent a form of *leverage politics*.

6 Conclusion

In answering the question *what constitutes war?* we suggested ethical, constructionist, and realist arguments appeal to reason, shared expectations, and the self-interest of the powerful respectively. Information provides a similarly simplistic candidate for the legitimacy of market based definitions of war. Markets offer incentives for participants to collect information and negotiate the terms of the contract. Hayek (1945) argued this process aggregates local information that cannot be collected by a central planner.

The evolution of war clauses reflects shifting expectations about technological and strategic developments. The trend towards excluding causes of war in cyber insurance policies may reflect insurers questioning how insurable cyber attacks involving states are. Regulatory forces should not be overlooked. The convergence on affirmatively offering coverage for cyber terrorism was driven by the regulator, not shared expectations.

[18]It can be argued that this represents an increase in complex interdependence (Keohane and Nye, 1977).

Insurers do not, however, provide explicit definitions of war and hostility. War clauses are draped in ambiguity that courts must interpret if a dispute arises. Insurers further rely on external actors, predominantly employed by the state, to produce intelligence linking losses to political actors. But fighting the cases in court provides symbolism, transparency and legal rigour. We will have to wait for court cases like Mondelez vs Zurich to discover how concepts like "hostile or warlike action" apply to offensive cyber operations.

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*, pp. 265–300. Springer.

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

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

Clarke, R. A. and R. K. Knake (2014). *Cyber war*. Tantor Media, Incorporated.

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

Dunn Cavelty, M. (2013). From cyber-bombs to political fallout: Threat representations with an impact in the cyber-security discourse. *International Studies Review 15*(1), 105–122.

Eling, M. and W. Schnell (2016). Ten key questions on cyber risk and cyber risk insurance. *The Geneva Association*.

Farwell, J. P. and R. Rohozinski (2011). Stuxnet and the future of cyber war. *Survival 53*(1), 23–40.

Grigsby, A. (2017). The end of cyber norms. *Survival 59*(6), 109–122.

Haufler, V. (1997). *Dangerous commerce: Insurance and the management of international risk*. 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), tyy009.

Hurel, L. M. and L. C. Lobato (2018). Unpacking cyber norms: private companies as norm entrepreneurs. *Journal of Cyber Policy 3*(1), 61–76.

Keck, M. E. and K. Sikkink (2014). *Activists beyond borders: Advocacy networks in international politics*. Cornell University Press.

Keohane, R. O. and J. S. Nye (1977). *Power and interdependence*. Boston.

Kratochwil, F. V. (1991). *Rules, norms, and decisions: on the conditions of practical and legal reasoning in international relations and domestic affairs*, Volume 2. Cambridge University Press.

Kunreuther, H. and E. Michel-Kerjan (2004). Policy watch: challenges for terrorism risk insurance in the united states. *Journal of Economic Perspectives 18*(4), 201–214.

Lewis, J. A. (2002). *Assessing the risks of cyber terrorism, cyber war and other cyber threats*. Center for Strategic & International Studies Washington, DC.

Raphael, A. (1994). *Ultimate Risk: The Inside Story of the Lloyd's Catastrophe*. Four Walls Eight Windows.

Rid, T. (2013). *Cyber war will not take place*. Oxford University Press, USA.

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., A. Kuehn, L. Ablon, and T. Jones (2019). Content analysis of cyber insurance policies: how do carriers price cyber risk? *Journal of Cybersecurity 5*(1).

Simon, S. I. (1981). The dilemma of war and military exclusion clauses in insurance contracts. *American Business Law Journal 19*, 31.

Simpson, T. W. (2014). The wrong in cyberattacks. In L. Floridi and M. Taddeo (Eds.), *The ethics of information warfare*, Volume 14. Springer Science & Business Media.

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*.

Stone, J. (2013). Cyber war will take place! *Journal of Strategic Studies 36*(1), 101–108.

Strange, S. (1996). *The retreat of the state: The diffusion of power in the world economy*. Cambridge university press.

Strange, S. (2015). *States and markets*. 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.

Thoyts, R. (2010). *Insurance theory and practice*. Routledge.

Tweedale, G. (2000). *Magic mineral to killer dust: Turner & Newall and the asbestos hazard*. Oxford University Press.

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*.

Woods, D. W. and T. Moore (2019). Does insurance have a future in governing cybersecurity? *IEEE Security & Privacy*, to appear.

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.

A Data Collection and Analysis

Our data only relates to the admitted market in California[19]. 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[20] 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 the more sophisticated standalone policies. We then extracted policy wording and the date at 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

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

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

identify any war or terrorism clauses and definitions. These were generally found in the exclusions section. We also searched each document using search-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.

Our analysis was coarse in mapping a policy 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 assigned to cyber-specific qualifier if they contained any terms like cyber, network security, or "acts perpetuated electronically".

B Raw Data

This section displays our raw data. We extracted war clauses and any qualifiers from the insurance policies. For each policy we provide the insurer name and year of filing, we then include the main war clause first and any qualifiers/relevant definitions afterwards.

B.1 Standalone Policies

B.1.1 American Guarantee and Liability Insurance Company, 2017

War clause with network security qualifier:

> Based upon, arising out of or attributable to: a. War, including undeclared or civil war; b. Warlike action by a military force, including action in hindering or defending against an actual or expected attack, by any government, sovereign or other authority using military personnel or other agents; or c. Insurrection, rebellion, revolution, riot, usurped power, or action taken by governmental authority in hindering or defending against any of these. However, this exclusion does not apply to breaches of your network security.

where

> Network security means the use of hardware, software, firmware and written security policies and procedures by insureds, or by others on your behalf to protect against unauthorized access to or the unauthorized use of your computer system including the use of your computer system in a denial of service attack.

B.1.2 Arch Insurance Company, 2016

War clause with cyber terrorism qualifier:

> any war, invasion, acts of foreign enemies, hostilities or warlike operations (whether war is declared or not), strike, lockout, riot, civil war, rebellion, revolution, insurrection, civil commotion assuming

> the proportions of or amounting to an uprising, military or usurped power, however, this exclusion will not apply to Cyberterrorism

where

> "Cyberterrorism" means the premeditated use of disruptive activities against any Computer System by an individual or group of individuals, or the explicit threat by an individual or group of individuals to use such activities, with the intention to cause harm, further social, idealogical, Religious, political or similar objectives, or to intimidate any person(s) in furtherance of such objectives. Cyberterrorism does not include any such activities which are part of or in support of any military action, war or warlike operation.

B.1.3 AXIS Insurance Company, 2016

War clause without any qualifiers:

> war, invasion, hostilities or warlike operations (whether war is declared or not), strike, lock-out, riot, civil war, rebellion, revolution, insurrection, civil commotion assuming the proportions of or amounting to an uprising, military or usurped power, or the confiscation, nationalization or destruction of, or damage to, property under the order of government or other public authority.

B.1.4 Beazley Insurance Company, Inc., 2016

War clause without any qualifiers:

> 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;

B.1.5 Contractors Bonding and Insurance Company, 2014

War clause without any qualifiers:

> any actual or alleged strike or similar action, war, invasion, act of foreign enemy, hostilities or warlike operations (whether declared or not), civil war, mutiny, civil commotion assuming the proportions of or amounting to a popular rising, military rising, insurrection, rebellion, revolution, military or usurped power, or any action taken to hinder or defend against these actions;

B.1.6 CUMIS Insurance Society, Inc., 2010

No war clause.

B.1.7 Discover Property and Casualty Insurance Company , 2012

No war clause.

B.1.8 Everest National Insurance Company, 2018

War clause with cyber terrorism qualifier:

> For, arising out of, or resulting from: war, invasion, acts of foreign enemies, hostilities (whether war be declared or not), civil war, rebellion, revolution, insurrection, military or usurped power or confiscation or nationalization or requisition or destruction of or damage to property by or under the order of any government or public or local authority; provided, that this exclusion will not apply to Cyber Terrorism.

where

> Cyber Terrorism means the premeditated use of disruptive activities, or threat to use disruptive activities, against an Insured's Computer System with the intention to cause harm, further social, ideological, religious, political or similar objectives, or to intimidate any person in furtherance of such Objectives.

B.1.9 Federal Insurance Company, 2009

War clause without any qualifiers:

> any riot or civil commotion, outside the United States of America or Canada, or any military, naval or usurped power, war or insurrection;

B.1.10 Federated Rural Electric Insurance Exchange, 2015

War clause with cyber terrorism qualifier:

> Any claim based upon, arising out of, resulting from, in consequence of, or in any way involving:
>
> 1. Strikes or similar labor actions, war, invasion, act of foreign enemy, hostilities or warlike operations (whether declared or not), civil war, mutiny, civil commotion assuming the proportions of or amounting to a popular uprising, military uprising, insurrection, rebellion, revolution, military or usurped power, or any action taken to hinder or defend against these actions;
>
> 2. The confiscation, nationalization, requisition or destruction of, or damage to, property by or under the order of any government or public or local authority; or

3. Any action taken in controlling, preventing, suppressing or in any way relating to GG(1) or GG(2) above.

This exclusion does not apply to an act of cyber terrorism.

where

Act of cyber terrorism means the premeditated use of disruptive activities, or the threat thereof, against computers, computer systems, networks and/or public internet by any person or group(s) of persons, whether acting alone or on behalf of, or in connection with, any organization(s) or government(s) with the intention to intimidate or cause destruction or harm and/or further social, ideological, religious, political or similar objectives.
Act of cyber terrorism includes, but is not limited to, the use of information technology to organize and execute large-scale attacks against computer systems, networks and/or public internet, resulting in disabling and/or deleting critical infrastructure, data or information.

B.1.11 Freedom Specialty Insurance Company, 2016

War clause with cyber terrorism qualifier:

based upon, arising out of or attributable to any war, invasion, acts of foreign enemies, hostilities (whether war is declared or not), civil war, rebellion, revolution, insurrection, military or usurped power, confiscation, nationalization, requisition, or destruction of, or damage to, property by or under the order of any government, public or local authority; or Terrorism;

where

Terrorism means any act, including without limitation the use of force or violence, or the threat thereof, by any individual or group(s) of individuals, whether acting alone, on behalf of or in connection with any organization(s) or government(s), to cause harm, loss or damage, committed for or to further social, ideological, religious, political or similar objectives, or to intimidate or influence any person(s), organization(s), government(s) or the public, or any segment of the public, in furtherance of such objectives, including without limitation any Security Incident or Privacy Violation (or act related thereto), or threat thereof. Terrorism shall not include Cyberterrorism.

where

Cyberterrorism means the premeditated disruption, or the threat thereof, of computers and/or net- works, with the intent to cause

> harm or further social, ideological, religious, political or similar objectives, or to intimidate any person in furtherance of such objectives. Cyberterrorism shall mean an attack against a Critical Infrastructure Sector as defined in Presidential Policy Directive 21 (PPD-21), and shall not include an attack against the computers and/or networks of a single entity.

B.1.12 Great American Insurance Company, 2012

No war clause.

B.1.13 Hartford Fire Insurance Company, 2009

War clause without any qualifiers:

> any war, invasion, acts of foreign enemies, hostilities or warlike operations (whether war is declared or not), strike, lock-out, riot, civil war, rebellion, revolution, insurrection, civil commotion assuming the proportions of or amounting to an uprising, military or usurped Power;

B.1.14 Key Risk Insurance Company, 2018

War clause with cyber terrorism qualifier:

> War and Seizure of Property based upon, arising out of, or attributable to strikes, riots or similar labor action, war, invasion, acts of foreign nations, hostilities or war-like operations (whether war is declared or not), civil war, mutiny, popular or military uprising, insurrection, rebellion, revolution, military or usurped power, or any action taken to hinder or defend against any of these events, or the confiscation, nationalization or destruction of, or damage to, property under the order of government or other public authority; provided that this exclusion shall not apply to that part of an otherwise covered Loss resulting from Cyber Terrorism;

where

> Cyber Terrorism means an act by an individual or any group of individuals directed against a Computer System, where it is reasonable to conclude that the actors are motivated by social, ideological, religious, economic or political objectives, or for the purpose of intimidating or coercing a government or the civilian population thereof, or disrupting any segment of the economy.

B.1.15 North American Specialty Insurance Company, 2018

War clause with cyber terrorism qualifier:

> War, invasion, acts of foreign enemies, terrorism, hostilities, civil war, rebellion, revolutions, insurrection, military, or usurped power; however, this exclusion will not apply to cyber terrorism.

where

> Cyber terrorism means the premeditated use, or threatened use, of disruptive activities against computer systems by any person, group, or organization, committed with the intention to harm or intimidate you to further social, ideological, religious, or political objectives. However, cyber terrorism does not include any activity which is part of or in support of any military action, war, or war-like operation.

B.1.16 Nova Casualty Company, 2018

War clause without any qualifiers:

> War And Military Action Based upon, arising out of or in any way related to:
>
> 1. War, including undeclared or civil war;
> 2. Warlike action by a military force, including action in hindering or defending against an actual or expected attack, by any government, sovereign or other authority using military personnel or other agents; or
> 3. Insurrection, rebellion, revolution, usurped power, or action taken by governmental authority in hindering or defending against any of these.

B.1.17 Philadelphia Indemnity Insurance Company, 2011

War clause with cyber terrorism qualifier:

> Any act of terrorism, strike or similar labor action, war, invasion, act of foreign enemy, hostilities or warlike operations (whether declared or not), civil war, mutiny, civil commotion assuming the proportions of or amounting to a popular rising, military rising, insurrection, rebellion, revolution, military or usurped power, or any action taken to hinder, defend, control, prevent or suppress any of the foregoing; provided, however, that this exclusion shall not apply to coverage otherwise provided under Insuring Agreement H. Cyber Terrorism Coverage, if purchased.

where

> Cyber terorrism: We will reimburse you for income loss, interruption expenses and special expenses in excess of the applicable deductible shown in the Declarations, incurred by you during the period of

restoration directly as a result of total or partial interruption, degradation in service, or failure of the computer system that exceeds the time retention and which is directly caused by an act of terrorism. Such act of terrorism must be discovered by a knowledgeable person during the policy period and reported to us within sixty (60) days after the end of the policy period.

B.1.18 QBE Insurance Corporation, 2014

Terrorism exclusion without war clause:

> I. We will not pay for any Loss caused directly or indirectly by Terrorism, including action in hindering or defending against an actual or expected incident of Terrorism. Any Loss is excluded regardless of any other cause or event that contributes concurrently or in any sequence to such Loss. However, this exclusion applies only when one or more of the following are attributed to an incident of Terrorism:
>
> 1. The Terrorism is carried out by means of the dispersal or application of radioactive material, or through the use of a nuclear weapon or device that involves or produces a nuclear reaction, nuclear radiation, or radioactive contamination; or
>
> 2. Radioactive material is released and it appears that one purpose of the Terrorism was to release such material; or
>
> 3. The Terrorism is carried out by means of dispersal or application of pathogenic or poisonous biological or chemical materials; or
>
> 4. Pathogenic or poisonous biological or chemical materials are released and it appears that one purpose of Terrorism was to release such materials; or
>
> 5. The total of insured damage to all types of property exceeds $25,000,000. In determining whether the $25,000,000 threshold is exceeded, we will include all insured damage sustained by property of all persons and entities affected by the Terrorism and business interruption losses sustained by owners or occupants of the damaged property. For the purpose of this provision, insured damage means damage that is covered by any insurance plus damage that would be covered by any insurance but for the application of any Terrorism exclusions; or
>
> 6. Fifty (50) or more persons sustain death or serious physical injury. For the purpose of this provision, serious physical injury

> means: (a) Physical injury that involves a substantial risk of death; or (b) Protracted and obvious physical disfigurement; or (c) Protracted loss of or impairment of the function of a bodily member or organ.
>
> Multiple incidents of Terrorism which occur within a 72-hour period and appear to be carried out in concert or to have a related purpose or common leadership will be deemed to be one incident, for the purpose of determining whether the thresholds in paragraphs 5. and 6. are exceeded. Paragraphs 5. and 6. above describe the threshold used to measure the magnitude of an incident of Terrorism and the circumstances in which the threshold will apply for the purpose of determining whether this exclusion will apply to that incident.
> When the exclusion applies to an incident of Terrorism, there is no coverage under this Policy. In the event of any incident of Terrorism that is not subject to this exclusion, coverage does not apply to any Loss that is otherwise excluded by this Policy.
>
> II. Solely for the purposes of this endorsement, this Policy is amended by the addition of the following: Terrorism means activities against persons, organizations, or property of any nature: 1. That involve the following or preparation for the following: (a) Use or threat of force or violence; or (b) Commission or threat of a dangerous act; or (c) Commission or threat of an act that interferes with or disrupts an electronic, communication, information, or mechanical system; and When one or both of the following applies: (a) The effect is to intimidate or coerce a government or the civilian population or any segment thereof, or to disrupt any segment of the economy; or (b) It appears that the intent is to intimidate or coerce a government, or to further political, ideological, religious, social or economic objectives or to express (or express opposition to) a philosophy or ideology.

B.1.19 RLI Insurance Company, 2013

War clause without any qualifiers:

> any actual or alleged strike or similar action, war, invasion, act of foreign enemy, hostilities or warlike operations (whether declared or not), civil war, mutiny, civil commotion assuming the proportions of or amounting to a popular rising, military rising, insurrection, rebellion, revolution, military or usurped power, or any action taken to hinder or defend against these actions;

B.1.20 St. Paul Fire and Marine Insurance Company, 2008

No war clause.

B.1.21 Starr Indemnity Liability Company, 2017

War clause with cyber terrorism qualifier:

> alleging, arising from, based upon or attributable to, in any way involving or in consequence of war, military or usurped power, or any action taken by governmental, public or local authority to confiscate, nationalize, seize, destroy or damage property; invasion, military action (whether or not war is declared), civil war, rebellion, revolution, insurrection, military or usurped power, or any action taken by governmental, public or local authority to confiscate, nationalize, seize, destroy or damage property;

Each of the insuring agreements includes "Security Failure", for example:

> 1. INSURING AGREEMENTS
> A. Security Privacy Liability The Insurer shall pay on behalf of the Insured all Loss, in excess of the Retention, arising from a Claim first made during the Policy Period (or Discovery Period, if applicable) against such Insured for an actual or alleged Security Failure or Privacy Incident, and duly reported to the Insurer in accordance with Section 7 of this policy.
> B. Security Privacy Incident Response Expenses The Insurer shall pay on behalf of the Company the Incident Response Expenses of the Company, in excess of the Retention, resulting from an actual or reasonably suspected Security Failure or Privacy Incident that is first discovered by the Insured during the Policy Period, and duly reported to the Insurer in accordance with Section 7 of this policy.

where

> "Security Failure" means any:
>
> - unauthorized access, unauthorized use, denial of service attack or receipt or transmission of a malicious code due to a failure or violation of the security of the Computer System or any other failure or violation of the Computer System;
> - failure to disclose an event referenced in Sub-paragraphs (1) above in violation of any Security Privacy Law;
> - theft of a password or access code from an Insured's premises, the Computer System, or an Insured Person by non-electronic means;
> - physical theft of hardware controlled by the Insured (or components thereof) on which electronic data is stored from a premises occupied and controlled by the Insured,
>
> including such failure or violation resulting from Cyberterrorism.

Affirmative coverage for cyber terrorism is inherited via the definition of Security failure, where

> "Cyberterrorism" means the premeditated use of disruptive activities against the Computer System by an individual or group of individuals, or the explicit threat by an individual or group of individuals to use such activities, with the intention to cause harm, further social, ideological, religious, political or similar objectives, or to intimidate any person(s) in furtherance of such objectives.
> "Cyberterrorism" does not include Cyberwarfare. "Cyberwarfare" as used herein means actions by a nation-state to penetrate the Computer System for the purposes of causing damage or disruption.

B.1.22 Stratford Insurance Company, 2018

War clause with cyber terrorism qualifier:

> war, invasion, terrorism, acts of foreign enemies, hostilities or warlike operations (whether war is declared or not), strike, lock-out, riot, civil war, rebellion, revolution, insurrection, civil commotion assuming the proportions of or amounting to an uprising, military or usurped power, provided, however, that this exclusion U.4. shall not apply to Cyber Terrorism.

where

> For purposes of this exclusion U.4., Cyber Terrorism means (i) any act expressly directed against an Inured's Network Security by an individual or any group of individuals, whether acting alone, on behalf of or in connection with any entity or government, or for social, ideological, religious, economic or political reasons, including intimidating or coercing a government, a civilian population or disrupting any segment of an economy;

B.1.23 The Hartford Steam Boiler Inspection and Insurance Company, 2015

War clause without any qualifiers:

> War and military action including any of the following and any consequence of any of the following:
>
> 1. War, including undeclared or civil
> 2. Warlike action by military force, including action in hindering or defending against an actual or expected attack, by any government, sovereign or other authority using military personnel or other agents; or
> 3. Insurrection, rebellion, revolution, usurped power, political violence or action taken by governmental authority in hindering or defending against any of these. war;

B.1.24 The Medical Protective Company, 2012

No war clause.

B.1.25 The Travelers Indemnity Company Of Connecticut, 2008

No war clause.

B.1.26 Travelers Casualty and Surety Company of America, 2010

War clause with terrorism qualifier:

> This CyberRisk Policy will not apply to any Claim or Single First Party Insured Event based upon or arising out of war, invasion, acts of foreign enemies, hostilities (whether war is declared or not), civil war, rebellion, revolution, insurrection, military or usurped power, confiscation, nationalization, requisition, or destruction of, or damage to, property by or under the order of any government, public or local authority; provided that this exclusion will not apply to any "act of terrorism" as defined in the Terrorism Risk Insurance Act, as amended.

B.1.27 Zurich American Insurance Company, 2014

War clause without qualifier:

> Based upon, arising out of or attributable to:
>
> 1. War, including undeclared or civil war;
> 2. Warlike action by a military force, including action in hindering or defending against an actual or expected attack, by any government, sovereign or other authority using military personnel or other agents; or
> 3. Insurrection, rebellion, revolution, riot, usurped power, or action taken by governmental authority in hindering or defending against any of these.

B.1.28 Twin City Fire Insurance Company, 2017

War clause with cyber terrorism qualifier:

> based upon, arising from or in any way related to any actual or alleged war, invasion, acts of foreign enemies, hostilities or warlike operations (whether war is declared or not), strike, lock-out, riot, civil war, rebellion, revolution, insurrection, civil commotion assuming the proportions of or amounting to an uprising, military or usurped power; provided, however, that this exclusion will not apply to any act of Cyber Terrorism.

B.1.29 Twin City Fire Insurance Company, 2018

War clause with cyber terrorism qualifier:

> based upon, arising from or in any way related to any actual or alleged war, invasion, acts of foreign enemies, hostilities or warlike operations (whether war is declared or not), strike, lock-out, riot, civil war, rebellion, revolution, insurrection, civil commotion assuming the proportions of or amounting to an uprising, military or usurped power; provided, however, that this exclusion will not apply to any act of Cyber Terrorism.

where

> Cyber Terrorism means the premeditated use, or threatened use, of disruptive activities, including a Cyber Extortion Threat against an Organization's Computer System, by an individual or group of individuals, whether acting alone or on behalf of or in connection with any organization or government, with the intent to demand an Extortion Payment, or cause a Network Intrusion or Data Privacy Incident, in furtherance of stated social, ideological, religious, economic or political objectives, or to intimidate the Insured in furtherance of such Objectives.

B.1.30 Zurich American Insurance Company, 2016

War clause with network security qualifier:

> War or Civil Unrest based upon, arising out of, or attributable to:
>
> - war, including undeclared or civil war;
> - warlike action by a military force, including action inm hindering or defending against an actual or expected attack, by any government, sovereign, or other authority using military personnel or other agents; or
> - insurrection, rebellion, revolution, usurped power, or action taken by governmental authority in hindering or defending against any of these; or
> - civil unrest, including but not limited to protests, striking employees and riots;
>
> provided, however, this Exclusion does not apply to breaches of the Company's Network Security;

B.2 Flat-rate Policies

B.2.1 Acceptance Indemnity Insurance Company, 2016

No war clause.

B.2.2 Alaska National Insurance Company, 2016

No war clause.

B.2.3 Aspen American Insurance Company, 2012

War clause with terrorism qualifier:

> Alleging or arising out of any:
>
> a. War, invasion, acts of foreign enemies, Hostilities or warlike operations (whether war be declared or not), civil war, rebellion, revolution, insurrection, civil commotion Assuming the proportions of or amounting to an uprising, military or usurped power; or
>
> b. Act of terrorism.

B.2.4 AXIS Insurance Company, 2014

No war clause.

B.2.5 BCS Insurance Company, 2014

War clause with acts perpetuated electronically qualifier:

> Any "Act Of Terrorism"; strike or similar labor action, war, invasion, act of foreign enemy, hostilities or warlike operations (whether declared or not), civil war, mutiny, civil commotion assuming the proportions of or amounting to a popular rising, military rising, insurrection, rebellion, revolution, military or usurped power, or any action taken to hinder or defend against these actions; including all amounts, "Damages", or "Claim Expenses" of whatsoever nature directly or indirectly caused by, resulting from or in connection with any action taken in controlling, preventing, suppressing, or in any way relating to the above; however, if "We" allege that by reason of this exclusion any "Damages" or "Claim Expenses" are not covered by this Policy, the burden of proving the contrary shall be upon "You". However this exclusion does not apply to acts perpetuated electronically.

B.2.6 Berkley National Insurance Company, 2017

War clause without any qualifiers:

> War and military action including any of the following and any consequence of any of the following:
>
> a. War, including undeclared or civil war;

b. Warlike action by military force, including action in hindering or defending against an actual or expected attack, by any government, sovereign or other authority using military personnel or other agents; or

c. Insurrection, rebellion, revolution, usurped power, political violence or action taken by governmental authority in hindering or defending against any of these.

B.2.7 Civic Property and Casualty Company, 2012

War clause without any qualifiers:

> Arising out of or resulting from, directly or indirectly occasioned by, happening through or in consequence of war, invasion, acts of foreign enemies, hostilities (whether war be declared or not), civil war, rebellion, revolution, insurrection, military or usurped power or confiscation or nationalization or requisition or destruction of or damage to property by or under the order of any government or public or local authority;

B.2.8 Employers Mutual Casualty Company, 2018

War clause without any qualifiers:

> War and military action including any of the following and any consequence of any of the following:
>
> a. War, including undeclared or civil war;
>
> b. Warlike action by military force, including action in hindering or defending against an actual or expected attack, by any government, sovereign or other authority using military personnel or other agents; or
>
> c. Insurrection, rebellion, revolution, usurped power, political violence or action taken by governmental authority in hindering or defending against any of these.

B.2.9 Everest National Insurance Company, 2014

No war clause.

B.2.10 Farmers Insurance Exchange, 2016

War clause without any qualifiers:

> Arising out of or resulting from, directly or indirectly occasioned by, happening through or in consequence of: war, invasion, acts of foreign enemies, hostilities (whether war be declared or not), civil

> war, rebellion, revolution, insurrection, military or usurped power or confiscation or nationalization or requisition or destruction of or damage to property by or under the order of any government or public or local authority.

B.2.11 Federated Rural Electric Insurance Exchange, 2018

War clause without any qualifiers:

> Any loss arising from war, invasion, act of foreign enemy, hostilities or warlike operations (whether declared or not), civil war, mutiny, civil commotion assuming the proportions of or amounting to a popular uprising, military uprising, insurrection, rebellion, revolution, military or usurped power, or any action taken to hinder or defend against these actions; or the confiscation, seizure, nationalization, requisition or destruction of, or damage to, property by or under the order of any government or public

B.2.12 Foremost Insurance Company Grand Rapids Michigan, 2016

War clause without any qualifiers:

> Arising out of or resulting from, directly or indirectly occasioned by, happening through or in consequence of: war, invasion, acts of foreign enemies, hostilities (whether war be declared or not), civil war, rebellion, revolution, insurrection, military or usurped power or confiscation or nationalization or requisition or destruction of or damage to property by or under the order of any government or public or local authority.

B.2.13 Graphic Arts Mutual Insurance Company, 2017

War clause without any qualifiers:

> War and military action including any of the following and any consequence of any of the following:
>
> a. War, including undeclared or civil war;
> b. Warlike action by military force, including action in hindering or defending against an actual or expected attack, by any government, sovereign or other authority using military personnel or other agents; or
> c. Insurrection, rebellion, revolution, usurped power, political violence or action taken by governmental authority in hindering or defending against any of these.

B.2.14 Great American Insurance Company, 2009

War clause without any qualifiers:

> Based upon, attributable to or arising out of:
>
> 1. war, including undeclared or civil war or civil unrest;
>
> 2. warlike action by military force, including action hindering or defending against an actual or expected attack, by any government, sovereign or other authority using military personnel or other agents; or
>
> 3. insurrection, rebellion, revolution, usurped power, or action taken by government authority in hindering or defending against any of these.

B.2.15 Greenwich Insurance Company, 2015

No war clause.

B.2.16 Harleysville Insurance Company, 2016

No war clause.

B.2.17 National Interstate Insurance Company, 2016

War clause without any qualifiers:

> Arising out of or resulting from, directly or indirectly occasioned by, happening through or in consequence of: war, invasion, acts of foreign enemies, hostilities (whether war be declared or not), civil war, rebellion, revolution, insurrection, military or usurped power or confiscation or nationalization or requisition or destruction of or damage to property by or under the order of any government or public or local authority;

B.2.18 NIPPONKOA Insurance Company Ltd.,(U.S.Branch), 2012

No war clause.

B.2.19 Palomar Specialty Insurance Company, 2018

War clause without any qualifiers:

> War, invasion, acts of foreign enemies or hostilities (whether war is declared or not); rebellion, revolution, insurrection, war-like action, coup, usurped power or military power.

B.2.20 Pennsylvania Lumbermens Mutual Insurance Company, 2016

No war clause.

B.2.21 Pennsylvania Lumbermens Mutual Insurance Company, 2017

War clause without any qualifiers:

> War and military action including any of the following and any consequence of any of the following:
>
> a. War, including undeclared or civil war;
> b. Warlike action by military force, including action in hindering or defending against an actual or expected attack, by any government, sovereign or other authority using military personnel or other agents; or
> c. Insurrection, rebellion, revolution, usurped power, political violence or action taken by governmental authority in hindering or defending against any of these.

B.2.22 Philadelphia Indemnity Insurance Company, 2016

War clause with terrorism qualifier:

> Any act of terrorism, strike or similar labor action, war, invasion, act of foreign enemy, hostilities or warlike operations (whether declared or not), civil war, mutiny, civil commotion assuming the proportions of or amounting to a popular rising, military rising, insurrection, rebellion, revolution, military or usurped power, or any action taken to hinder, defend, control, prevent or suppress any of the foregoing;

where

> Act of terrorism means any violent act or an act that is dangerous to human life, property or infrastructure that is committed by an individual or individuals and that appears to be part of an effort to coerce a civilian population or to influence the policy or affect the conduct of any government by coercion.

B.2.23 QBE Insurance Corporation, 2017

No war clause.

B.2.24 Security National Insurance Company, 2016

War clause without any qualifiers:

> Arising out of or resulting from, directly or indirectly occasioned by, happening through or in consequence of: war, invasion, acts of foreign enemies, hostilities (whether war be declared or not), civil war, rebellion, revolution, insurrection, military or usurped power or confiscation or nationalization or requisition or destruction of or damage to property by or under the order of any government or public or local authority;

B.2.25 State National Insurance Company Inc., 2017

War clause with cyber terrorism qualifier:

> Any claim based upon, arising out of, resulting from, in consequence of, or in any way involving:
>
> 1. Strikes or similar labor actions, war, invasion, act of foreign enemy, hostilities or warlike operations (whether declared or not), civil war, mutiny, civil commotion assuming the proportions of, or amounting to, a popular uprising, military uprising, insurrection, rebellion, revolution, military or usurped power, or any action taken to hinder or defend against these actions;
> 2. The confiscation, commandeering, nationalization, requisition or destruction of, or damage to, property, including computer hardware, by or under the order of any government or public authority for whatever reason; or
> 3. Any action taken in controlling, preventing, suppressing or in any way relating to DD(1) or DD(2) above.
>
> This exclusion does not apply to an act of cyber terrorism.

where

> Act of cyber terrorism means the premeditated use of information technology to organize and execute attacks, or the threat thereof, against computers, computer systems, networks or the internet by any person or group, whether acting alone, on behalf of, or in connection with any organization or government, which is committed for political, religious, or ideological purposes, with the intention to influence any government, put the public in fear, or cause destruction or harm to critical infrastructure or data.

B.2.26 The Dentists Insurance Company, 2017

War clause without any qualifiers:

> War and military action including any of the following and any consequence of any of the following:

a. War, including undeclared or civil war;

b. Warlike action by military force, including action in hindering or defending against an actual or expected attack, by any government, sovereign or other authority using military personnel or other agents; or

c. Insurrection, rebellion, revolution, usurped power, political violence or action taken by governmental authority in hindering or defending against any of these.