Yale Journal of Law & Technology
Volume 23, Spring 2021

WARGAMES: ANALYZING THE ACT OF WAR EXCLUSION IN INSURANCE COVERAGE AND ITS IMPLICATIONS FOR CYBERSECURITY POLICY

Scott J. Shackelford*

Cyber risk insurance coverage has become an increasingly vital tool permitting both public and private-sector organizations to mitigate an array of cyber risks, including the prevalent issue of ransomware. However, despite the rapid uptake of these policies, a series of issues have emerged. Litigation has centered on issues ranging from what constitutes "covered computer systems" to questions of negligence.

Among the most vexing issues, with arguably wide-ranging implications for not only the cyber risk insurance industry, but for U.S. cybersecurity policy generally, consist of when a cyber attack attributed to a foreign nation constitutes an act of war thus excluding coverage. As one example, the 2017 NotPetya cyber attack resulted in more than $10 billion in damages globally, including more than $100 million to the multination food conglomerate, Mondelez International. However, when Mondelez filed a claim with its insurance firm, Zurich International, to recover these costs its claim was denied because NotPetya was considered a "hostile or warlike action" by a "government or sovereign power." Mondelez countersued, alleging breach of contract, and the case remains pending in Illinois state court as of this writing. A similar case involving damage from NotPetya on Merck is likewise

* Executive Director, Ostrom Workshop; Chair, Indiana University-Bloomington Cybersecurity Program; Associate Professor of Business Law and Ethics, Indiana University Kelley School of Business. Special thanks are owed to Noah Holloway and Jalyn Rhodes for their invaluable research support, and to Professor Asaf Lubin, and Stephen Vina for their incredibly helpful comments and critiques on this project.

pending in New Jersey. Yet, the literature to date has largely ignored this vital issue.

This Article makes several original contributions to this debate. First, it couches this issue as part a set of cybersecurity dilemmas facing organizations that are manifest in the ransomware epidemic. Relatedly, it summarizes findings from a statewide cybersecurity survey that was conducted in collaboration with the Indiana Attorney General's Office. Second, it analyzes current pending litigation related to the act of war exclusion, and the impact of Universal Cable Productions LLC v. Atlantic Specialty Insurance Company (9th Cir. 2019), which called into question the efficacy of these exclusions in certain cases. Third, it brings in lessons not only from U.S. cybersecurity policy, but also on the applicable international law on defining acts of cyber war and related challenges of attribution. The Article concludes by suggesting a standard to courts, policyholders, and insurance companies in navigating these issues going forward.

Table of Contents

INTRODUCTION

On October 15, 2020, six Russian nationals that are alleged to be officers in Russia's main Intelligence Directorate (GRU) were indicted by the U.S. Department of Justice for their roles in a host of recent high-profile cyber attacks including those targeting Ukraine, Georgia, France, South Korea, and the United States.[1] These attacks included some of the most costly and destructive incidents in the history of cyber attacks, including the 2017 NotPetya cyber attack that resulted in more than $10 billion in damages globally.[2] Public attributions of such cyber attacks from the U.S. government back to individual nations, organizations, and even individuals, have been an important lynchpin of the evolving U.S. cyber deterrence strategy (i.e., naming and shaming, despite the difficulties of follow-up prosecution given a lack of necessary extradition and robust mutual legal assistance treaties in many instances).[3] Debate continues to rage about the effectiveness of this approach given the ongoing cascade of cyber attacks targeting both the public and private sectors in the United States—prompting a focus post-2018 on "Defending Forward"[4]—but a perhaps

---

[1] *See* Press Release, Six Russian GRU Officers Charged in Connection with Worldwide Deployment of Destructive Malware and Other Disruptive Actions in Cyberspace, U.S. DEP'T JUSTICE (Oct. 19, 2020), https://www.justice.gov/opa/pr/six-russian-gru-officers-charged-connection-worldwide-deployment-destructive-malware-and.

[2] *See* Andy Greenberg, *The Untold Story of NotPetya, the Most Devastating Cyberattack in History*, WIRED (Aug. 22, 2018), https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world.

[3] *See* Jon R. Lindsay, *Tipping the Scales: The Attribution Problem and the Feasibility of Deterrence Against Cyberattack*, 1 J. CYBERSECURITY 53, 53 (2015), https://academic.oup.com/cybersecurity/article/1/1/53/2354517.

[4] *See* Robert Chesney, *The 2018 DOD Cyber Strategy: Understanding 'Defense Forward' in Light of the NDAA and PPD-20 Changes*, LAWFARE (Sept. 25, 2018), https://www.lawfareblog.com/2018-dod-cyber-strategy-understanding-defense-forward-light-ndaa-and-ppd-20-changes. There are two strategies for improving cyber deterrence: (1) so-called deterrence-by-denial, which may be understood as hardening your networks against cyber attacks and thus increasing the cost to

unanticipated knock-on effect has been on shaping the insurance industry.

Cyber risk insurance coverage has become an increasingly vital tool permitting both public and private-sector organizations to mitigate an array of cyber risks, including the prevalent issue of ransomware.[5] However, despite the relatively rapid uptake of these policies, a series of issues and barriers emerged.[6] Litigation has centered on issues ranging from what constitutes "covered computer systems" as many employees are working from home, to questions of negligence.[7]

Among the most vexing issues, with arguably wide-ranging implications for not only the insurance industry, but on U.S. cybersecurity policy generally, consist of when a cyber attack attributed to a foreign nation constitutes an act of war thus excluding coverage. As one example, among those firms impacted by NotPetya was the multination food conglomerate, Mondelez International, which lost more than $100 million in the breach.[8] However, when Mondelez filed a claim with its property insurance

---

attackers; and (2) active defense, i.e., defending forward to underscore the real and perceived costs of attacking. *See* Scott J. Shackelford et al., *From Russia with Love: Understanding the Russian Cyber Threat to U.S. Critical Infrastructure*, 96 NEB. L. REV. 320, 321 (2017).

[5] *Cf.* Julie Bernard, *Overcoming Challenges to Cyber Insurance Growth*, DELOITTE INSIGHTS (Mar. 16, 2020), https://www2.deloitte.com/us/en/insights/industry/financial-services/cyber-insurance-market-growth.html (noting that, in fact, the growth in cyber risk insurance premiums has not been nearly as rapid as many commentators predicted due to an array of barriers including cost).

[6] *See id*.

[7] *See, e.g.*, Alexander Osipovich, *High-Speed Trader Virtu Discloses $6.9 Million Hacking Loss*, WALL ST. J. (Aug. 11, 2020), https://www.wsj.com/articles/high-speed-trader-virtu-discloses-6-9-million-hacking-loss-11597165615.

[8] Mondelez Intern'l, Inc. v. Zurich Am. Ins. Co., 2018 WL 4941760 (Ill. Cir. Ct. 2018). *See* Aaron Klein & Scott R. Anderson, *A Federal Backstop for Insuring Against Cyberattacks*?, BROOKINGS INSTITUION (Sept. 27, 2019), https://www.brookings.edu/blog/techtank/2019/09/27/a-federal-backstop-for-insuring-against-cyberattacks/.

firm,[9] Zurich International, to recover these costs, its claim was denied because NotPetya was considered a "hostile or warlike action" by a "government or sovereign power."[10] Mondelez countersued, alleging breach of contract, and the case remains pending in Illinois state court as of this writing. A similar case involving damage from NotPetya on Merck is likewise pending in New Jersey.[11] Yet, the literature to date has largely ignored this pressing issue,[12] which holds the potential to inhibit, or even remove, a useful risk mitigation tool from companies that are already struggling to manage their cyber risk exposure. The absence of this issue from discussions about U.S. cyber deterrence strategy, despite the importance of insurance to many policymakers,[13] is likewise questionable.

This Article makes several original contributions to this debate. First, it couches this issue as part a set of cybersecurity dilemmas facing organizations that are manifest in the ransomware epidemic, the costs of which by some estimates reached nearly $200

---

[9] It is important to note that much of this litigation centers on property policies, not cyber risk insurance per se. *See* Michael Menapace, *Property Insurance, Cyber Insurance, Coverage and War: Losses From Malware May Not Be Covered Due To Your Policy's Hostile Acts Exclusion*, 11 NAT'L L. REV. (Jan. 29, 2021), https://www.natlawreview.com/article/property-insurance-cyber-insurance-coverage-and-war-losses-malware-may-not-be-0.

[10] *See* Klein & Anderson, *supra* note 8.

[11] *See* Michael F. Aflward, *U.S. Courts Set Their Sights on the War Exclusion*, LEXOLOGY (Sept. 10, 2019), https://www.lexology.com/library/detail.aspx?g=6acb490d-e8fc-48d8-9512-572bd41bd1fd.

[12] *Cf.* Carole J. Buckner, *Ethical Obligations Regarding Data Security*, 2 ORANGE CTY. LAWYER 54, 55 (2020) ("Unlike some traditional insurance policies, cyber insurance policy coverages vary significantly and it is important to understand the policy. All insurance policies include exclusions from coverage. A cyber policy may include an act of war exclusion, and at least one insurance carrier has taken the position that the exclusion applies to actions by hostile governments.").

[13] *See* Robert Morgus et al., *Deterrence-by-Denial: The Missing Element of U.S. Cyber Strategy*, LAWFARE (Mar. 11, 2020), https://www.lawfareblog.com/deterrence-denial-missing-element-us-cyber-strategy; Anne Hobson & Ian Adams, *California Dreams About Cyber Insurance, and Federal Lawmakers Should Pay Attention*, HILL (Mar. 7, 2020), https://thehill.com/opinion/cybersecurity/486427-california-dreams-about-cyber-insurance-federal-lawmakers.

billion in 2019 alone.[14] Relatedly, it summarizes findings from a statewide cybersecurity survey that we conducted in collaboration with the Indiana Attorney General's Office that featured a range of questions on cyber risk insurance coverage. Second, it summarizes current pending litigation related to the act of war exclusion, and the impact of the 2019 Ninth Circuit's *Universal Cable Productions LLC v. Atlantic Specialty Insurance Company* holding, which called into question the efficacy of these exclusions in certain cases.[15] Third, it brings in lessons not only from U.S. cybersecurity policy, but also on the applicable international law on defining acts of cyber war and related challenges of attribution. By way of conclusion, the Article suggests a standard to guide courts, policyholders, and insurance companies in navigating these issues going forward.

The Article is structured as follows. Part I discusses the ransomware epidemic that is an array of public and private-sector organizations, digging into the reasons driving this trend including how certain nation states such as North Korea and Russia are benefiting.[16] Part II then pivots to the issue of defining cyber war, both as a matter of U.S. policy and international law. Part III summarizes the current state of cyber risk insurance coverage through the lens of survey findings undertaken in partnership with the Indiana Attorney General's Office.[17] Part IV reviews pending cases centering on the act of war exclusion, including *Mondelez* and

---

[14] *See* Phil Muncaster, *Ransomware Costs May Have Hit $170bn in 2019*, INFO. SEC. MAG. (Feb. 13, 2020), https://www.infosecurity-magazine.com/news/ransomware-costs-may-have-hit-170/.

[15] Universal Cable Productions, LLC, et al. v. Atlantic Specialty Ins. Co., 929 F.3d 1143 (9th Cir. 2019).

[16] *See, e.g.*, Michelle Nichols, *North Korea Took $2 Billion in Cyberattacks to Fund Weapons Program: U.N. Report*, REUTERS (Aug. 5, 2019), https://www.reuters.com/article/us-northkorea-cyber-un/north-korea-took-2-billion-in-cyberattacks-to-fund-weapons-program-u-n-report-idUSKCN1UV1ZX.

[17] *See* Shackelford et al., *State of Hoosier Cybersecurity 2020*, IND. EXEC. COUNCIL ON CYBERSECURITY (Dec. 2020), https://www.ibrc.indiana.edu/studies/State-of-Hoosier-Cybersecurity-2020.pdf.

Merck. Finally, by way of conclusion Part V offers a proposed standard to help both victims, and the cyber risk insurance industry, find a more equitable approach to this vexing issue.

I. UNPACKING NOTPETYA, WANNACRY, AND THE RANSOMWARE EPIDEMIC

The types of cyber risks that organizations are facing are nearly as numerous as the number of victims. They include spyware, malware, logic bombs, distributed denial-of-service (DDoS) attacks, zero-day exploits, and phishing, just to name a few.[18] Any of these cyber incidents and attacks could trigger cyber risk insurance coverage, and each presents its own set of complex policy issues and potential responses. The following discussion, though, specifically addresses the issue of ransomware and its treatment in insurance policies.

Ransomware is a type of malware that locks access to a computer until a ransom is paid. It has been a component of the cyber threat landscape since the mid-2000s.[19] There are no comprehensive datasets about exactly how many ransomware attacks are occurring, and how much they are costing victims, but from what limited survey data that is available, ransomware rates increased by more than 300 percent in 2020 even as losses to other types of cyber threats decreased.[20] In 2017, for example, the FBI's Internet Crime Complaint Center (IC3) received nearly 2,000

[18] For an in-depth discussion of the prevailing cyber risks facing oranizations, see Chapter 3 in SCOTT J. SHACKELFORD, MANAGING CYBER ATTACKS IN INTERNATIONAL LAW, BUSINESS, AND RELATIONS: IN SEARCH OF CYBER PEACE (2014).

[19] *See* Juliana De Groot, *A History of Ransomware Attacks: The Biggest and Worst Ransomware Attacks of All Time*, DIGITAL GUARDIAN (Oct. 6, 2020), https://digitalguardian.com/blog/history-ransomware-attacks-biggest-and-worst-ransomware-attacks-all-time.

[20] *See* Steve Kaaru, *Digital Currency Crime Reduced by 83% in 2020, But Ransomware Attacks up 311%*, COIN GEEK (Jan. 31, 2021), https://coingeek.com/digital-currency-crime-reduced-by-83-in-2020-but-ransomware-attacks-up-311.

ransomware complaints costing victims over $2.3 million, though according to surveys, the real annual figure is likely in the hundreds of millions of ransomware attacks.[21] High-profile incidents have included ransomware attacks on series of cities including Baltimore and Atlanta,[22] as well as the U.S. Treasury Department in December 2020.[23] Less understood is how widespread and costly ransomware attacks have been against towns and counties such as Riviera Beach in Florida, which had to pay $600,000 to unlock its data,[24] not to mention schools and hospitals such as Hancock Regional in Indiana, which had to pay $55,000 to attackers in 2020.[25]

As with an array of groups that benefit from the proliferation of ransomware including criminal organizations, some nation states are likewise using this tactic to cause service disruptions and sew confusion in other nations,[26] but also to raise funds.[27] North Korea, for example, has raised more than $2 billion through cyber attacks including ransomware to fund its weapons of mass destruction

---

[21] *Id.* There is some evidence, though, that despite the high-profile nature of ransomware attacks in 2019 and 2020, their use actually peaked in 2016 with as many as three times as many incidents that year as in 2019. *See Annual Number of Ransomware Attacks Worldwide from 2014 to 2019*, STATISTA, https://www.statista.com/statistics/494947/ransomware-attacks-per-year-worldwide.

[22] *See* Kate Fazzini, *City Ransomware Attacks and Huge Payouts Mean a Once-Private Corporate Problem has Gone Public*, CNBC (June 26, 2019), https://www.cnbc.com/2019/06/26/baltimore-florida-ransomware-attacks-kick-off-new-era-for-ransomware.html.

[23] *See* Amanda Macias, *White House Acknowledges Reports of Cyberattack on U.S. Treasury by Foreign Government*, CNBC (Dec. 13, 2020), https://www.cnbc.com/2020/12/13/cyber-hack-on-us-treasury-by-foreign-government-.html.

[24] Fazzini, *supra* note 22.

[25] *See* Chris Brook, *Following Ransomware Attack Indiana Hospital Pays $55K to Unlock Data*, DATA INSIDER (Aug. 12, 2020), https://digitalguardian.com/blog/following-ransomware-attack-indiana-hospital-pays-55k-unlock-data; Leandra Bernstein, *K-12 Schools Increasingly the Target of Ransomware Attacks During Pandemic*, CBS (Sept. 15, 2020), https://cbsaustin.com/news/coronavirus/k-12-schools-increasingly-the-target-of-ransomware-attacks-during-pandemic.

[26] *See, e.g.*, Evans F. Horsley, *State-Sponsored Ransomware Through the Lens of Maritime Piracy*, 47 GA. J. INT'L & COMP. L. 669, 671–73 (2019).

[27] *See* Nichols, *supra* note 16.

programs.[28] All told, according to a 2019 U.N. Security Council report, the North Korean regime has been linked to "at least 35 reported instances of DPRK actors attacking financial institutions, cryptocurrency exchanges and mining activity designed to earn foreign currency" spread across seventeen nations.[29] North Korea is not alone in sponsoring these attacks, which leave local governments in a difficult position of deciding whether or not to pay the ransom to recover their data and, in so doing, risk encouraging the aggressors to attack more victims.[30] The situation is so problematic that some states, such as Louisiana, have had to declare emergency declarations in response to a wave of ransomware attacks on municipalities across the state.[31] The total number of such attacks "is largely unknown."[32]

Among the most damaging ransomware attacks to date were the 2017 WannaCry and NotPetya malware attacks. Indeed, for many, the May 2017 WannaCry incident was "the first time they

---

[28] *Id.*
[29] *Id.*
[30] *See* Jenni Bergal, *Ransomware Attacks Prompt Tough Question for Local Officials: To Pay or Not to Pay?*, PEW (Mar. 3, 2020), https://www.pewtrusts.org/en/research-and-analysis/blogs/stateline/2020/03/03/ransomware-attacks-prompt-tough-question-for-local-officials-to-pay-or-not-to-pay; Scott J. Shackelford & Megan Wade, *Deal with Ransomware the Way Police Deal with Hostage Situations*, CONVERSATION (Mar. 25, 2020), https://theconversation.com/deal-with-ransomware-the-way-police-deal-with-hostage-situations-129213.
[31] *See* Lauren Frias, *Louisiana's Governor Declared a State of Emergency After a Cybersecurity Attack on Government Servers*, BUS. INSIDER (Nov. 22, 2019), https://www.businessinsider.com/louisiana-declares-state-of-emergency-after-cybersecurity-attack-2019-11. *See also* Bobby Allyn, *22 Texas Towns Hit With Ransomware Attack In 'New Front' Of Cyberassault*, NPR (Aug. 20, 2019), https://www.npr.org/2019/08/20/752695554/23-texas-towns-hit-with-ransomware-attack-in-new-front-of-cyberassault ("Texas is the latest state to be hit with a cyberattack, with state officials confirming this week that computer systems in 22 municipalities have been infiltrated by hackers demanding a ransom. A mayor of one of those cities said the attackers are asking for $2.5 million to unlock the files.").
[32] *See* Dan Lohrmann, *The Year Ransomware Targeted State & Local Governments*, GOVTECH (Dec. 23, 2019), https://www.govtech.com/blogs/lohrmann-on-cybersecurity/2019-the-year-ransomware-targeted-state--local-governments.html.

heard of 'ransomware'" as it took down NHS clinics across the United Kingdom[33] The incident was fueled by the Shadow Brokers breach of the NSA's vault of advanced cyber weapons, which included stockpiled vulnerabilities in Microsoft Windows that were code-named EternalBlue.[34] One month later, NotPetya struck using the same Windows weaknesses but this time could not hop from network to network.[35] Instead, the hackers used "a hacked version of a major accounting program widely used in Ukraine," among the local branches of Western multinationals.[36] The fact that this particular exploit, which as we will see had devastating impacts on dozens of firms including Mondelez and Merck, originated in Ukraine was an early sign that Russia should be considered a leading culprit. Simply put: "If a nation were to write malware with the aim of crippling the economy of its target, it might look a lot like NotPetya."[37] Indeed, in February 2018, the White House released a statement saying that NotPetya "was part of the Kremlin's ongoing effort to destabilize Ukraine and demonstrates ever more clearly Russia's involvement in the ongoing conflict."[38]

Many insurance firms are bearing the brunt of this ransomware onslaught.[39] The next Part discusses the extent to which such policies are being tailored to protect organizations from various kinds of cyber risk, including ransomware. From this foundation, I

---

[33] Alex Hern, *WannaCry, Petya, NotPetya: How Ransomware Hit the Big Time in 2017*, GUARDIAN (Dec. 30, 2017), https://www.theguardian.com/technology/2017/dec/30/wannacry-petya-notpetya-ransomware.
[34] *Id.*
[35] *Id.*
[36] *Id.*; Greenberg, *supra* note 2.
[37] *Id.*
[38] WHITE HOUSE, STATEMENT FROM THE PRESS SECRETARY (Feb. 15, 2018), https://trumpwhitehouse.archives.gov/briefings-statements/statement-press-secretary-25.
[39] *See* Shawn Tuma, *With Ransomware Attacks Increasing, Cyber Insurance Now Seen as a Necessity, Not a Luxury*, SEC. MAG. (June 22, 2020), https://www.securitymagazine.com/articles/92653-with-ransomware-attacks-increasing-cyber-insurance-now-seen-as-a-necessity-not-a-luxury.

discuss the act of war and hostile acts exclusion in more detail before moving on to recent litigation testing the bounds of this potential lifeline.

II. DEFINING "CYBER WAR"

These cases highlight larger issues discussed above in the cybersecurity field generally, which include: (1) the challenge of recognizing the wide array of cyber risks faced by organizations, (2) the difficulty of pricing these costs that could range from a fraudulent wire transfer to a ransomware attack on an entire network, (3) the reality of immature liability structures, and (4) using outdated analogies and tools (such as the act of war exclusion) to manage these risks.[40] In *Mondelez* and *Merck*, the insurance providers will likely face challenges under international law for the reasons discussed above in making its case that NotPetya crossed the armed attack threshold. The vast majority of cyber incidents fall below the threshold and thus constitute covered criminal activity.[41] The insurance industry has struggled to operationalize this concept, which is derived from a combination of existing international law and emerging state practice. This Section examines the applicable international law on cyber war focusing on the armed attack threshold in the context of cyber attacks, before moving to discuss the U.S. approach to this topic in the context of evolving U.S. cybersecurity strategy.

---

[40] *See* Jon Bateman, War, Terrorism, and Catastrophe in Cyber Insurance: Understanding and Reforming Exclusions, Carnegie Endowment for Int'l Peace (Oct. 5, 2020), https://carnegieendowment.org/2020/10/05/war-terrorism-and-catastrophe-in-cyber-insurance-understanding-and-reforming-exclusions-pub-82819.

[41] *See infra* Part I; *see, e.g.*, Ryan Goodman, *Cyber Operations and the U.S. Definition of "Armed Attack*," JUST SEC. (Mar. 8, 2018), https://www.justsecurity.org/53495/cyber-operations-u-s-definition-armed-attack.

A. Applicable International Law

When does a cyber attack constitute an act of war? Much ink has been spilled and spent on this question since the early 2000s.[42] The Law of Armed Conflict, or International Humanitarian Law (IHL), is broken down into two main fields. The first describes "when . . . [it is] legal for a nation to use force against another nation[.]"[43] This is called *jus ad bellum*,[44] Latin for the "right to declare and wage war."[45] The second body of law addresses what rules "govern the behavior of combatants" during war.[46] This is known as *jus in bello*, or justice in wartime.[47] *Jus ad bellum* dates back to just war theory pioneered by Cicero.[48] Today, *jus ad bellum* is governed by customary international law and the U.N. Charter, particularly Articles 2(4), 39, 42, and 51.[49] *Jus in bello*, in contrast, is regulated by the Hague Conventions of 1899 and 1907, as well as "the Geneva Conventions, and customary international law."[50] *Jus*

---

[42] TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICATION TO CYBER WARFARE 17 (Michael N. Schmitt ed., 2013) (discussing when a cyber attack could trigger the right of self-defense) [hereinafter TALLINN MANUAL].

[43] NAT'L RESEARCH COUNCIL, TECHNOLOGY, POLICY, LAW, AND ETHICS REGARDING U.S. ACQUISITION AND USE OF CYBERATTACK CAPABILITIES 242 (William A. Owens, Kenneth W. Dam, & Herbert S. Lin eds., 2009) [hereinafter TECHNOLOGY, POLICY, LAW, AND ETHICS REGARDING U.S. ACQUISITION AND USE OF CYBERATTACK CAPABILITIES].

[44] *Id*.

[45] Edmund Jan Ozmanczky, 2 *Encyclopedia of the United Nations and International Agreement* 1209 (Anthony Mango ed., 2003).

[46] TECHNOLOGY, POLICY, LAW, AND ETHICS REGARDING U.S. ACQUISITION AND USE OF CYBERATTACK CAPABILITIES, *supra* note 43, at 242.

[47] *Id.*; OZMANCZKY, *supra* note 45, at 1209; Robert Kolb, *Origin of the Twin Terms* Jus Ad Bellum/Jus In Bello, 320 INT'L REV. RED CROSS (1997), http://www.icrc.org/eng/resources/documents/misc/57jnuu.htm.

[48] *See* Mark Edward DeForrest, Note, *Just War Theory and the Recent U.S. Strikes Against Iraq*, 1 GONZAGA J. INT'L L. 11, 14 (1997) (citing St. Augustine of Flippo, *Against Faustus the Manichaean* XXII 73–79, *in* AUGUSTINE: POLITICAL WRITINGS 222 (Michael W. Tkacz & Donald Kries, trans., Ernest L. Fortin & Donald Kries, eds., 1994)).

[49] *See* TECHNOLOGY, POLICY, LAW, AND ETHICS REGARDING U.S. ACQUISITION AND USE OF CYBERATTACK CAPABILITIES, *supra* note 43, at 242.

[50] *Id*. at 246.

ad bellum is likewise important in legal analyses involving the act of war exclusion in cyber risk insurance policies.[51]

The U.N. Charter divides conflict into three zones.[52] The first threshold is defined by Article 2(4), which makes the threat or use of force illegal without prior U.N. Security Council (UNSC) authorization.[53] Various state actions have been found to not breach this prohibition, including space-based surveillance, espionage, and economic sanctions.[54] It remains unclear to what extent cyber attacks may be used consistently with Article 2(4), for example, "[d]oes introducing vulnerabilities into an adversary's system . . . constitute a threat of force . . . ?"[55] The *Tallinn Manual*, which is a study from numerous (though largely Western) law of war experts on law applies to cyber conflict, envisions that not all cyber attacks would necessarily constitute interventions in violation of Article 2(4), especially those "lacking a coercive element" such as cyber espionage campaigns.[56] The authors contend that even the "breaching of protective virtual barriers" may not in itself constitute an act of intervention in violation of Article 2(4).[57]

The second zone includes the thresholds encompassed in Articles 39 and 42, at which point the UNSC may designate a breach

---

[51] For further background on this topic, see Chapter 6 in SHACKELFORD, *supra* note 18; Oona A. Hathaway et al., *The Law of Cyber-Attack*, 100 CALIF. L. REV. 817 (2012) (discussing how cyber warfare fits into existing bodies of law that regard war); Reese Nguyen, *Navigating Jus Ad Bellum in the Age of Cyber Warfare*, 101 CALIF. L. REV. 1079 (2013) (suggesting new analytical framework to determine whether a cyber attack constitutes an act of war).

[52] *See* LAW OF ARMED CONFLICT DESKBOOK, INT'L & OPERATIONAL L. DEP'T 16, 32, 34 (2012), https://www.loc.gov/rr/frd/Military_Law/pdf/LOAC-Deskbook-2012.pdf.

[53] *See* Bruno Simma, *NATO, the UN, and the Use of Force*, 10 EUR. J. INT'L L. 1, 2–3 (1999).

[54] TECHNOLOGY, POLICY, LAW, AND ETHICS REGARDING U.S. ACQUISITION AND USE OF CYBERATTACK CAPABILITIES, *supra* note 43, at 242.

[55] *Id.* at 242, 257 (noting that prohibited threats under Article 2(4) might include "verbal threats, initial troop movements, initial movement of ballistic missiles, [or the] massing of troops on a border . . . .").

[56] TALLINN MANUAL, *supra* note 42, at 47.

[57] *Id.* at 47.

to international peace and security and take action to restore order.[58] Examples of times in which the UNSC has used this authority include cases of ethnic cleansing, apartheid, and genocide.[59] The final barrier is Article 51, which allows for the "right of individual or collective self-defense" in response to an armed attack.[60] Such acts of self-defense are warranted until the UNSC takes action "to maintain international peace and security."[61] International law requires that for self-defense to be permissible, there must be an attack "so egregious that the victim would be justified" in responding in kind.[62] An armed attack is more serious than a use of force according to many nations (though not the United States, as discussed below),[63] and constitutes the equivalent of an invasion by military forces.[64] The natural question, then, is whether a cyber attack can meet that threshold, activating the laws of war.

Although there are varying definitions describing when a cyber operation constitutes a use of force that, in turn, may activate the act of war exclusion in a cyber risk insurance policy,[65] the

---

[58] TECHNOLOGY, POLICY, LAW, AND ETHICS REGARDING U.S. ACQUISITION AND USE OF CYBERATTACK CAPABILITIES, *supra* note 43, at 242 (discussing Articles 39 and 42 as "exceptions to this prohibition on the use of force.").

[59] *See* John Quigley, *Repairing the Consequences of Ethnic Cleansing*, 29 PEPP. L. REV. 33, 34, 37 (2002).

[60] UN Charter, art. 51; TECHNOLOGY, POLICY, LAW, AND ETHICS REGARDING U.S. ACQUISITION AND USE OF CYBERATTACK CAPABILITIES, *supra* note 43, at 243.

[61] UN Charter, art. 51.

[62] G.A. Res. 2625 (XXV) (Oct. 24, 1970) (declaring a war of aggression "a crime against the peace" and exhorting states to refrain from "acts of reprisal involving the use of force . . . [and] from organizing, instigating, assisting, participating in acts of civil strife or terrorist acts in another State."); Definition of Aggression, G.A. Res. 3314 (XXIX), art. 1, U.N. GAOR, 29th Sess., Supp. No. 31, at 142, U.N. Doc. A/9631 (1975), 13 I.L.M. 710 (Dec. 14, 1974).

[63] *See supra* Part V.2.

[64] *See* JEFFERY CARR, INSIDE CYBER WARFARE: MAPPING THE CYBER UNDERWORLD 49–51 (2009).

[65] These include considering the "scope, duration, and intensity" of a cyber attack and was propounded by Walter Gary Sharp, and the Schmitt analysis, which calls for the examination of a number of factors on a case-by-case basis to determine whether or not a cyber attack constitutes a use of force. *See* Graham H. Todd, *Armed Attack in Cyberspace: Deterring Asymmetric Warfare with an Asymmetric*

dominant test focuses on equivalent effects.[66] *Tallinn Manual* Rule 11, for example, states that "[a] cyber operation constitutes a use of force when its scale and effects are comparable to non-cyber operations rising to the level of a use of force."[67] In the act of war exclusion context, this high bar means that the vast majority of cyber incidents would not rise to the level of an act of war breaching the armed attack threshold. However, different countries have chosen to interpret this line differently, which is important to assess particularly in the U.S. context since the lower threshold it maintains, along with the undeclared cyber war doctrine discussed in reference to *Bergara*,[68] could drive radically different holdings on the same exclusion.

B. U.S. Approach

For a nation to legally use force in self-defense under international law, there must be a showing of an armed attack, which has been described as "the gravest forms of force in scale and effects."[69] As opposed to this equivalent effects test described above in reference to *Tallinn Manual* Rule 11, the United States has long maintained that a nation should be able to "use force in self-defense in response to any amount of force by another State."[70] This interpretation was crafted in an earlier analogue era and there is reason to believe that it "worked well when it came to bombs and

---

Definition, 64 A.F. L. REV. 65, 69 n.9 (2009); Michael N. Schmitt, *Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework*, 37 COLUM. J. TRANSNAT'L L. 885, 900 (1999).

[66] *See, e.g.*, Aliya Sternstein, *Threat of Destructive Coding on Foreign-Manufactured Technology is Real*, NEXTGOV (July 7, 2011), https://www.nextgov.com/cybersecurity/2011/07/threat-of-destructive-coding-on-foreign-manufactured-technology-is-real/49363/

[67] TALLINN MANUAL, *supra* note 42, at 45-47. *See also* Matthew C. Waxman, *Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)*, 36 YALE J. INT'L L. 421 (2011) (analyzing the offensive potential and permissibility of international cyber-attacks).

[68] *See infra* note 183.

[69] Goodman, *supra* note 41.

[70] *Id.*

battleships" but may well be less suited to managing cyber attacks, with implications on the cyber risk insurance debate.

The lower use of force threshold advocated by the United States could have some benefits for reducing the risk of international armed conflict by making nations reticent to engage in conduct that would risk being construed as an armed attack.[71] However, given that other nations do not enjoy the same array of economic, diplomatic, and political tools at their disposal as the U.S. enjoys to influence state behavior,[72] this could put pressure on other states to either similarly lower their own use of force thresholds or foster alliances in response. It remains an open question whether a world in which more nations follow the U.S. approach to defining the armed attack threshold would be more peaceful.[73] After all, rather than cyber attacks breaching the armed attack threshold being the extraordinary exception, they would become more the norm, opening up the possibility of states engaging in a wide array of kinetic and cyber responses in self-defense.

C. Evolution of U.S. Cybersecurity Strategy to Defend Forward

The modern course of U.S. cybersecurity policy was largely charted in 1998 when President Bill Clinton signed Presidential Decision Directive (PDD) 63.[74] This directive was for all intents and purposes the founding charter for how the U.S. government would attempt to organize in response to a growing array of cyber threats facing the nation's critical infrastructure systems.[75] For example, it led to the sector-specific approach to cybersecurity risk management

---

[71] *Id.*
[72] *Id.*
[73] *See infra* Part V.
[74] RICHARD CLARKE & ROBERT KNAKE, THE FIFTH DOMAIN: DEFENDING OUR COUNTRY, OUR COMPANIES, AND OURSELVES IN THE AGE OF CYBER THREATS 89 (2019).
[75] *Id.*

that has continued for decades, with each sector being organized through an Information Sharing and Analysis Center (ISAC).[76] Subsequent administrations have tinkered around the edges of this policy, but by and large there was widespread agreement that these policies should be "enhanced," not replaced.[77]

Since the late 1990s running through the Obama Administration, the emphasis of the U.S. government has been on deterring cyber attacks through so-called deterrence by denial. An exception to this strategy occurred during the George W. Bush Administration's Operation Olympic Games, which involved a successful attempt to exploit vulnerabilities in Siemens-manufactured nuclear centrifuges in Iran.[78] The Bush Administration viewed the clandestine program as a success and encouraged the incoming Obama Administration to continue it.[79] Yet the Obama Administration backed away from this active defense policy in the wake of the widespread damage caused by Stuxnet once it got out into the wild, instead outlining a policy of cyber deterence built on the back of the the National Institute for Standards and Technology (NIST) Cybersecurity Framework.[80] This approach seeks to harden systems against cyber risks by increasing the costs to attackers, thus deterring them from expending the necessary time and resources and contributing to overall

---

[76] *Id*.
[77] *Id*.
[78] *See generally* KIM ZETTER, COUNTDOWN TO ZERO DAY: STUXNET AND THE LAUNCH OF THE WORLD'S FIRST DIGITAL WEAPON (2015).
[79] *See* David E. Sanger, *Obama Order Sped Up Wave of Cyberattacks Against Iran*, N.Y. TIMES (June 1, 2012), https://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html.
[80] *See* Max Smeets, *Cyber Deterrence is Dead. Long Live Cyber Deterrence!*, COUNCIL FOREIGN REL. (Feb. 18, 2020), https://www.cfr.org/blog/cyber-deterrence-dead-long-live-cyber-deterrence; *President Obama's Pursuit of Cyber Deterrence Ends in Failure*, COUNCIL FOREIGN REL. (Jan. 4, 2017), https://www.cfr.org/blog/president-obamas-pursuit-cyber-deterrence-ends-failure.

cybersecurity. Yet the U.S. cybersecurity strategy under the Obama administration received criticism for not being more active in responding to an array of cyber threats, including on the 2016 U.S. elections, despite its successes in cyber norm-building efforts.[81]

The Trump administration elected to change course and in its 2018 U.S. Department of Defense Cyber Strategy argues that, along with defending the nation's critical infrastructure from significant threats, it also vital to "persistently contest malicious cyber activity in day-to-day competition" short of armed conflict.[82] What this amounts to is a pivot away from a strategy of 'deterrence-by-denial' and toward a renewed active defense doctrine. U.S. Cyber Command (USCYBERCOM) has been empowered to achieve this goal, including the use of offensive cyber attacks such as the November 2018 takedown of a Russian bot farm without prior Presidential approval.[83] In short, the 2018 DoD Strategy may be read as a full-throated endorsement of active defense, saying that the DoD is empowered to employ "offensive cyber capabilities and innovative concepts that allow for the use of cyberspace operations across the full spectrum of conflict."[84] A significant focus of these efforts is the protection of vulnerable critical infrastructure, with the DoD stating that it "seeks to preempt, defeat, or deter malicious cyber activity" targeting these networks.[85]

---

[81] *See* Adam Segal, *The U.S.-China Cyber Espionage Deal One Year Later*, COUNCIL ON FOREIGN REL. (Sept. 28, 2016), https://www.cfr.org/blog/us-china-cyber-espionage-deal-one-year-later.

[82] *Cyber Strategy*, DEP'T OF DEFENSE 4 (2018), https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF.

[83] This Trump Administration cybersecurity policy, which shared characteristics with the more assertive George W. Bush Administration Cybersecurity Strategy that preceded it, has been encapsulated in National Security Presidential Memorandum 13. *See* Mark Pomerleau, *After Tug-of-War, White House Shows Cyber Memo to Congress*, FIFTH DOMAIN (Mar. 13, 2020), https://www.fifthdomain.com/congress/2020/03/13/after-tug-of-war-white-house-shows-cyber-memo-to-congress/.

[84] *Cyber Strategy*, *supra* note 82, at 1.

[85] *Id.* at 2.

There is some evidence that this new more proactive approach of "Defending Forward" to deter cyber attacks may well be working, as seen in the security of the 2020 U.S. elections,[86] though its failure to deter SolarWinds calls that assertion into question.[87] However, there is concern as to the degree to which other nations could copy this U.S. cybersecurity strategy, as Canada already has.[88] If more nations are compromising one another's networks, there is an open question to whether overall cybersecurity will be enhanced or destabilized. Coupled with the move on the part of other nations – such as Japan[89] – to lower their own use of force thresholds to mirror the U.S. approach discussed above, there seems to be a trend toward both an increasing array of proactive cyber attacks being used, and a decreasing degree of tolerance on the part of more nations to treat these breaches as low-intensity cyber conflict short of war.[90]

As applied to insurance, these trends are meaningful given that they make it more likely both that state-sponsored cyber attacks would occur and target vulnerable civilian critical infrastructure, and that States would treat such attacks as uses of force constituting an armed attack, thus activating U.N. Charter Article 51. Courts will have to undertake a difficult balancing act in these cases, weighing how the jurisdictions in question define the armed attack threshold

---

[86] *Cf.* Erica D. Borghard, *Cyber Command's Role in Election Defense: Important, But Not a Panacea*, LAWFARE (Oct. 30, 2020), https://www.lawfareblog.com/cyber-commands-role-election-defense-important-not-panacea (noting the limitations of USCYBERCOM in the election security context).

[87] This notable episode, despite its scale, though, is better classified as cyber espionage, which is traditionally even harder to deter. *See, e.g.*, Gary Corn, *SolarWinds Is Bad, but Retreat From Defend Forward Would Be Worse*, LAWFARE (Jan. 14, 2021), https://www.lawfareblog.com/solarwinds-bad-retreat-defend-forward-would-be-worse.

[88] National Cybersecurity Strategy, GOV'T OF CANADA (2018), https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg/index-en.aspx.

[89] Goodman, *supra* note 41.

[90] *Id.*

in the context of cyber attacks – a task potentially made easier depending on the outcome of ongoing U.N. cyber norm-building discussions.[91] Attribution challenges will also continue to bedevil both policymakers and courts, which is the topic we turn to next.

D. Attribution Challenges

Given that the *Mondelez* case is civil in nature, Zurich must prove that the Russian government was involved in NotPetya by a preponderance of the evidence.[92] Although applicable in a common law court considering a civil case, there is no clear guidance under international law as to the applicable burden of proof for state-sponsored cyber attacks. The U.S. National Research Council emphasizes the difficulty of identifying "even the nature of the involved party (e.g., a government, a terrorist group, an individual), let alone the name of the country or the terrorist group or the individual."[93] Article 8 of the International Law Commission's Articles on the Responsibility of States for International Wrongful Acts applies when there is a question about State-sponsored cyber attacks, which implicates State control when individuals are "acting on the instructions of, or under the direction or control of, that State in carrying out the conduct."[94]

The International Court of Justice has confirmed states are responsible for the internationally wrongful acts that they conduct, which the *Tallinn Manual 2.0* discussed in reference to "cyber-

---

[91] *See* Christian Ruhl et al., *Cyberspace and Geopolitics: Assessing Global Cybersecurity Norm Processes at a Crossroads*, CARNEGIE ENDOWMENT (Feb. 26, 2020), https://carnegieendowment.org/2020/02/26/cyberspace-and-geopolitics-assessing-global-cybersecurity-norm-processes-at-crossroads-pub-81110.

[92] *See* Lubin, *supra* note 146, at 43.

[93] TECHNOLOGY, POLICY, LAW, AND ETHICS REGARDING U.S. ACQUISITION AND USE OF CYBERATTACK CAPABILITIES, *supra* note 43, at 252.

[94] *State Responsibility*, UN Y.B. INT'L. L., VOL. II 47 (2001), https://casebook.icrc.org/case-study/international-law-commission-articles-state-responsibility.

related act[s]."[95] The *Tallinn Manual* likewise makes clear under Rules 14-16 that a State and its organs are responsible for cyber-related acts that breach its international responsibilities.[96] Thus, if the Russian GRU is indeed proven to have launched NotPetya, then it could be held in breach of its international legal obligations. A more challenging case involves the actions of private groups that may, or may not, be under the direction of a State. There, "a State, either by specific directions or by exercising control over a group, in effect assume[s] responsibility for their conduct."[97]

The terms "direction" and "control" are often conflated by courts even though the International Law Commission indicated that they should be disjunctive, which has resulted in two main competing approaches: the effective and overall control standards.[98] In brief, the effective control doctrine applies when a State "determines the execution and course of the specific operation and the cyber activity engaged in by the non-State actor is an integral part of that operation."[99] This standard is distinct from the lower, more flexible overall control doctrine used to classify armed conflicts, which requires that where a state has a role in organizing and coordinating a group's acts, then it has sufficient overall control so that the group's acts are attributable to the state.[100] The *Tallinn Manual* editors, consistent with the International Court of Justice,

---

[95] TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE 84 (2017) (noting that such acts require both "a breach of an international legal obligation applicable to that State" and that the act is "attributable under international law.").
[96] *Id.* at 88-94.
[97] *Id.* at 95 (quoting Articles on State Responsibility, Art. 8, para. 7 of commentary).
[98] *See* TALLINN MANUAL, *supra* note 42, at 31–33 (noting that state responsibility arises when the non-state actor is "exercising elements of governmental authority").
[99] TALLINN MANUAL 2.0, *supra* note 95, at 96.
[100] *See id.* Prosecutor v. Tadic, Case No. IT-94–1-I ICTY (Oct. 2, 1995), at 1541 [hereinafter Tadic]; ADEMOLA ABASS, COMPLETE INTERNATIONAL LAW 258–61 (2011) (discussing the competing standards of state responsibility).

have argued for the imposition of the effective control standard in attributing cyber attacks made by non-State actors back to nations,[101] even though this relatively higher burden of proof could make it less likely for such attribution to be found, thus limiting the utility of act of war exclusion. So far, there is insufficient State practice to conclude how major cyber powers, to say nothing of the majority of States, view this issue. This makes it much more difficult for courts to determine which standard to follow in cases involving act of war exclusions.

While it is true that "the United States appears to have an increasingly impressive ability to determine attribution," other nations are not so fortunate, which could result in "costly errors" being made in attributing cyber attacks.[102] Consider *Mondelez.* Although public attributions of NotPetya have been made, including by the government, they have not been matched with accompanying showings of proof. This is by design, of course, given the nature of the attribution challenge.[103] As such, the Illinois court could well require additional evidence to prove attribution beyond these statements.[104] Although there is significant public domain reporting that has been done on this linkage, along with how the earlier actions of Shadow Brokers fit into the ransomware campaign,[105] intelligence agencies will most likely not be forthcoming in this analysis, meaning that non-State groups—such as Citizen Lab—may be called upon to testify in this and similar cases.

The need for better guidance for courts, clients, and insurance providers prompts an examination of other avenues for

---

[101] *Id.*
[102] Goodman, *supra* note 41.
[103] *See* Florian J. Egloff, *Public Attribution of Cyber Intrusions*, 6 J. CYBERSECURITY (2020), https://casebook.icrc.org/case-study/international-law-commission-articles-state-responsibility.
[104] Lubin, *supra* note 146, at 44.
[105] *See, e.g.*, Hern, *supra* note 33; GREENBERG, *supra* note **Error! Bookmark not defined.**.

reform beyond reaching a consensus on thorny issues of use of force and attribution that have bedeviled reformers and lawyers alike for decades. Part V takes up the task, both by distilling the core lessons stemming from the preceding analysis, and analyzing what options exist for organizational, national, and international reforms to promote transparency for the act of war exclusion specifically, and cyber risk insurance coverage generally during an era of increasing cyber insecurity. First, though, it is important to discuss how to cyber risks may be managed through insurance.

III. MANAGING CYBER RISKS THROUGH INSURANCE

Insurance firms have been experimenting with cyber risk insurance policies for decades.[106] By some estimates, the market was worth more than $2.5 billion in 2020, with projections that it could triple by 2030 due in part to first-party losses related to ransomware.[107] A growing number of insurance companies are entering the field to meet this surging demand: around 500 carriers now offer cyber risk insurance policies.[108] This trend could be reinforced by regulatory developments such as the California Consumer Privacy Act (CCPA) as well as the European Union's General Data Protection Regulation (GDPR).[109] Indeed, there is a

---

[106] Jon Swartz, *Firms' Hacking-Related Insurance Costs Soar*, USA TODAY (Feb. 9, 2003), http://usatoday30.usatoday.com/tech/news/computersecurity/2003-02-09-hacker_x.htm.

[107] *Insurance 2020 & Beyond: Reaping the Dividends of Cyber Resilience*, PWC (2020), https://www.pwc.com/gx/en/industries/financial-services/publications/insurance-2020-cyber.html. Marsh Insurance, for example, "reports cyber insurance growth rates of 27% across all industries, ranging from 6% in health care to 63% in manufacturing, for US-based clients in 2015." Sasha Romanosky et al., *Content Analysis of Cyber Insurance Policies: How Do Carriers Price Cyber Risk?*, 5 J. CYBERSECURITY (2019), https://academic.oup.com/cybersecurity/article/5/1/tyz002/5366419.

[108] Romanosky et al., *supra* note 107.

[109] *See* Carolyn Cohn, *Europe's New Data Privacy Law Boosts Cyber Insurance Sales*, INSURANCE J. (May 22, 2018), https://www.insurancejournal.com/news/international/2018/05/22/489977.htm

history of state-level data breach notification laws galvanizing uptake for cyber risk insurance coverage.[110] U.S. companies are increasingly eyeing cyber insurance as they potentially face millions of dollars in liability under CCPA, under which state residents can seek up to $750 per data security incident.[111] CCPA originally directed the California Attorney General to take enforcement actions for privacy violations,[112] but the passage of Proposition 24 in 2020 strengthened these protections with a new state agency designed to enforce CCPA and make it more difficult for tech firms to collect data that was collected by third-party sites.[113]

In addition to protecting organizations against financial fallout from cyber incidents, organizations can use cyber risk insurance to inform their security practices in other ways. For example, insurers can use tactics like cyber meteorology to audit companies against cyber risks such as ransomware and help them prioritize their security efforts.[114] The process of applying for cyber insurance also requires organizations to assess cyber controls and

("Insurers say the directive, together with major cyber attacks like last year's WannaCry and NotPetya viruses, is driving demand in Europe for cyber insurance – a sector seen as relatively profitable.").

[110] *See, e.g.*, Yakir Golan, *The Next Five Years: Cyber Insurance Predictions Through 2025*, FORBES (Jan. 19, 2021), https://www.forbes.com/sites/theyec/2021/01/19/the-next-five-years-cyber-insurance-predictions-through-2025/?sh=1d872b863fa6.

[111] *See* Jeffrey N. Rosenthal & David J. Oberly, *Biometric Privacy Regulation May Soon Be Coming to Pennsylvania*, LAW.COM (Oct. 9, 2020), https://www.law.com/thelegalintelligencer/2020/10/09/biometric-privacy-regulation-may-soon-be-coming-to-pennsylvania/?slreturn=20201017110326.

[112] *See* Daniel R. Stoller, *Cyber Insurance Purchases Will Surge With California Privacy Law*, BLOOMBERG L. (Feb. 5, 2020), https://news.bloomberglaw.com/privacy-and-data-security/cyber-insurance-purchases-will-surge-with-california-privacy-law.

[113] *See* Aaron Holmes, *California Just Passed a Major Privacy Law that will make it Harder for Facebook and Google to Track People and Gather Data*, BUS. INSIDER (Nov. 4, 2020), https://www.businessinsider.com/prop-24-privacy-california-data-tracking-facebook-google-2020-11.

[114] *See* Vishaal Hariprasad, *Introducing 'Cyber Meteorology:' A New Strategy for Cyber Insurance*, DARK READING (Feb. 3, 2020), https://www.darkreading.com/risk/introducing-cyber-meteorology-a-new-strategy-for-cyber-insurance-/d/d-id/1336924.

make enhancements in an effort to achieve more favorable pricing from insurers including premium discounts. The insurance industry has also focused extensively on their own cybersecurity practices. Model laws like the National Association of Insurance Commissioners (NAIC) Insurance Data Security Model Law seek to establish data security standards for regulators and insurers in order to mitigate the potential damage of future data breaches.[115] This Model Law, which had been enacted in at least eleven states as of September 2020, requires insurers and other entities licensed by a state department of insurance to "develop, implement, and maintain an information security program" based on a recognized risk assessment tool, with a designated employee in charge of the information security program.[116] The model does not create a private cause of action, nor does it limit an already-existing private right of action.[117] As such, it is less a new approach to regulating cyber risk insurance than an encouragement for covered insurance providers to adopt an approved set of cybersecurity tools and frameworks.

However, with no states mandating cyber insurance as of July 2021 despite a proposed 2020 law in California that failed to pass, adoption has been slow.[118] Deloitte's *2019 Middle Market Cyber Insurance Survey* reported cost and coverage limits being the main deterrent from purchasing cyber risk insurance.[119] However,

---

[115] *2019 Cybersecurity Legislation*, NAT'L CONF. ST. LEGIS. (Jan. 10, 2020), https://www.ncsl.org/research/telecommunications-and-information-technology/cybersecurity-legislation-2019.aspx; *Cybersecurity*, NAIC, National Association of Insurance Commissioners (NAIC) Insurance Data Security Model Law (last updated May 27, 2021).

[116] *2019 Cybersecurity Legislation*, *supra* note 115.

[117] Insurance Data Security Model Law, https://content.naic.org/sites/default/files/inline-files/MDL-668.pdf.

[118] *See* Shoeb Mohammed, *State-Mandated Cyber Insurance Bill Fails Passage*, CALCHAMBER ALERT (May 8, 2020), https://calchamberalert.com/2020/05/08/state-mandated-cyber-insurance-bill-fails-passage.

[119] Julie Bernard, *Overcoming Challenges to Cyber Insurance Growth*, DELOITTE (Mar. 16, 2020), https://www2.deloitte.com/us/en/insights/industry/financial-services/cyber-insurance-market-growth.html.

much is still unknown about how companies decide whether to adopt cyber risk insurance and the broader role that cyber risk insurance plays in cyber risk mitigation practices.

A. Coverage and Cost

Cyber risk insurance does not protect companies against all types of cyber risks.[120] For example, coverage for intellectual property, which comprises eighty-four percent of the value of many S&P 500 companies,[121] is nearly impossible to attain given the challenges of quantifying its value.[122] Moreover, emerging trends such as active defense[123] and the Internet of Things[124] make it challenging for insurance firms or their clients to understand the potential risks to the broader digital ecosystem that may be created by certain activities. Insurance policies may also exclude coverage of incidents that happen under certain circumstances, such as a cyber-attack that is attributed to a foreign nation that may be defined as an act of war, which is the subject of Section II.3. Such catastrophic attacks constitute a "perfect storm" of uncertainty for insurance firms, while terrorist incidents are so rare that it is

---

[120] *See* Adam Satariano & Nicole Perlroth, *Big Companies Thought Insurance Covered a Cyberattack. They May Be Wrong*, N.Y. TIMES (Apr. 15, 2019), https://www.nytimes.com/2019/04/15/technology/cyberinsurance-notpetya-attack.html.

[121] *See* Sarah Ponczek, *Epic S&P 500 Rally Is Powered by Assets You Can't See or Touch*, BLOOMBERG (Oct. 21, 2020), https://www.bloomberg.com/news/articles/2020-10-21/epic-s-p-500-rally-is-powered-by-assets-you-can-t-see-or-touch.

[122] *See How Intellectual Property Compares with Cyber*, INSURANCE J. (Aug. 19, 2019), https://www.insurancejournal.com/magazines/mag-features/2019/08/19/536535.htm. It is possible, though, to attain media liability policies to help with intellectual property infringement. *See* Dan Burke, *Cyber 101: Understand the Basics of Cyber Liability Insurance*, WOODRUFF SAWYER (Nov. 2, 2020), https://woodruffsawyer.com/cyber-liability/cyber-101-liability-insurance-2021.

[123] *See* Scott J. Shackelford et al., *Rethinking Active Defense: A Comparative Analysis of Proactive Cybersecurity Policymaking*, 41 UNIV. PENN. J. INT'L L. 377, 378 (2020).

[124] *See* Scott J. Shackelford & Scott O. Bradner, *Have You Updated Your Toaster? Transatlantic Approaches to Governing the Internet of Everything*, 72 HASTINGS L.J. 627(2021).

challenging for insurers to price them appropriately.[125] Businesses must carefully review policies to ensure that their expectations about what types of incidents are covered aligns with their policies given the wide array of terminology used and coverage offered, which can create barriers to adopting policies.[126]

One 2019 study found that many insurance firms are focusing on the amount and type of data being held by potential clients in deciding whether to offer coverage.[127] Less well appreciated, they found, is the "technical and business infrastructure" of the potential clients related to "organizational processes and practices"; indeed, in only one instance they could identify was an International Standards Organization (ISO) cybersecurity standard mentioned, and at no time was the NIST CSF discussed.[128] These findings, though, do not necessarily dovetail with emerging industry norms of major insurance firms such as AIG, Chubb, and Zurich using cybersecurity standards to assess insureds.[129] The relative lack of engagement with the NIST CSF is particularly surprising given the extent to which it is becoming the default standard for cybersecurity due diligence, particularly in the

---

[125] Adam B. Shniderman, *Prove It! Judging the Hostile-or-Warlike-Action Exclusion in Cyber-Insurance Policies*, 129 YALE L.J. F. 64 (2019) (exploring challenges facing insurers and insured litigating coverage denials under hostile-or-warlike action exclusions, and noting that "[c]yberbreaches, being unpredictable, highly correlated, and costly, possess several of the qualities that make pricing coverage difficult.").

[126] *See* Satariano & Perlroth, *supra* note 120.

[127] Romanosky et al., *supra* note 107 (noting that oftentimes coverage is limited to the tens of millions, and perhaps only in rare occasions up to $200-300 million).

[128] *Id*.

[129] *See, e.g.*, *The NIST Cybersecurity Framework and its Role in Cyber Risk Management and Cyber Insurance*, ZURICH (May 28, 2020), https://www.advisenltd.com/the-nist-cybersecurity-framework-and-its-role-in-cyber-risk-management-and-cyber-insurance.

critical infrastructure context.[130] This particular finding, moreover, is inconsistent with our Indiana-based survey in Section II.2.

As for other risk factors informing pricing and coverage, the study determined that the firms' asset value as a proxy for firm size are the driving feature in risk assessments, "rather than specific technology or governance controls."[131] This fact places small and medium-sized firms, even those with relatively sophisticated cybersecurity expertise, at a relative disadvantage. This can, in turn, contribute to systemic market risk. We discuss this consideration further in Part V.[132]

B. Indiana Survey Findings

Given the relative paucity of data available in cybersecurity policy generally and cyber risk insurance in particular, I have made it a priority to engage in empirical work to get a more complete picture of the cyber threat landscape and how organizations are meeting it. The Indiana Executive Council on Cybersecurity and the Indiana Attorney General's Office reached out to me in 2019 to create a first-of-its-kind statewide cybersecurity survey. I partnered with Professor Anne Boustead, along with the Indiana Business Research Center, which helped create, vet, and field the survey.[133]

The survey itself included a range of questions on both cybersecurity preparedness and cyber risk insurance uptake. We sent survey soliciations and links to a mailing list of more than 3,000 public and private organizations in Indiana. We received 336 responses, including 197 complete responses and 139 incomplete

---

[130] *See* Scott J. Shackelford et al., *Toward a Global Standard of Cybersecurity Care?: Exploring the Implications of the 2014 Cybersecurity Framework on Shaping Reasonable National and International Cybersecurity Practices*, 50 TEX. INT'L L.J. 287, 288 (2015).

[131] Romanosky et al., *supra* note 107.

[132] *See* David Hake et al., *Cyber Insurance and Systemic Market Risk*, EASTWEST INST. (June 5, 2019), https://www.eastwest.ngo/cyberinsurance.

[133] *See Indiana Governor's Council on Cybersecurity Survey*, https://cybersecurity.iu.edu/state-cyber-survey.html (last visited Nov. 17, 2020).

responses. Incomplete responses were dropped from the analysis. This left us with an overall response rate of 6%. From these findings, we drafted a report for distribution to policymakers, practitioners, law enforcement professionals, and the general public.[134]

It is beyond the scope of this Article to summarize all of these results, but several are pertinent to the question at hand.[135] First, the vast majority of respondents (95%) were either somewhat or very concerned about cyber attacks, fueling interest in mitigation tools and techniques including insurance. Second, 82% of respondents reported that they had taken some affirmative steps to manage the cyber risks facing their organizations, including the installation of antivirus software and employee cyber hygiene training. Third, there was a clear lack of planning uncovered among the respondents: only 27% reported that they had created incident response plans. This would make it less likely that the organizations would be able to acquire cyber risk insurance policies if they were sought. Fourth, 58 respondents (29%) stated that their organization consulted an externally developed tool, framework, or control when making decisions about cyber practices. Among respondents who indicated that their organization used an externally developed framework to guide their cybersecurity decision-making, the most common framework was the NIST Cybersecurity Framework, which had been adopted by 58% of those organizations adopting a framework. 36% had adopted the Center for Internet Security (CIS)

---

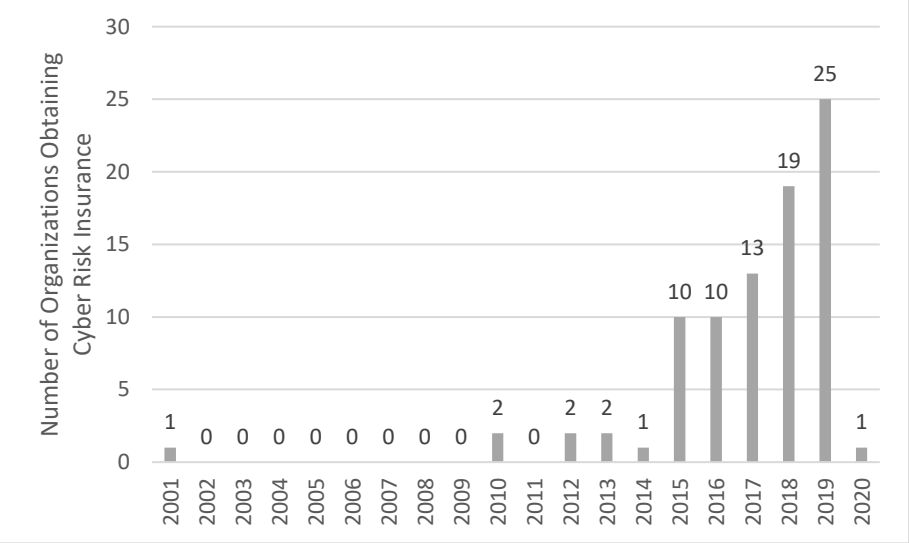
[134] *See* Shackelford et al., *supra* note 17.

[135] At the same time, important limitations should be kept in mind. In particular, representatives from organizations that are more concerned about cybersecurity decision-making may be more likely to respond to the survey, as the issues it raises are more salient to them and their employers. Combined with the relatively low response rate of the survey, this suggests that the results of this analysis should not be seen as representing the exact parameters of cybersecurity decision-making in general. Further, it is important to note that the geographic and economic position of Indiana, being situated as it is in the U.S. Midwest and quite dependent on manufacturing, means that the findings of this survey should not be extrapolated nationally, or globally.

Critical Security Controls. As noted above, this percentage is higher than that reported in the 2019 Romanosky study.[136]

Fifth and finally, roughly half of respondents indicated that their organization had cyber risk insurance. 26% indicated that their organization did not have cyber risk insurance, and remaining respondents were either unsure or declined to answer. Notably, more than half of those covered reported purchasing their policies in response to media coverage involving recent breaches. There was also a notable temporal uptick in the purchasing of such policies, with 2019 being the most active year to date, as shown in Figure 1.

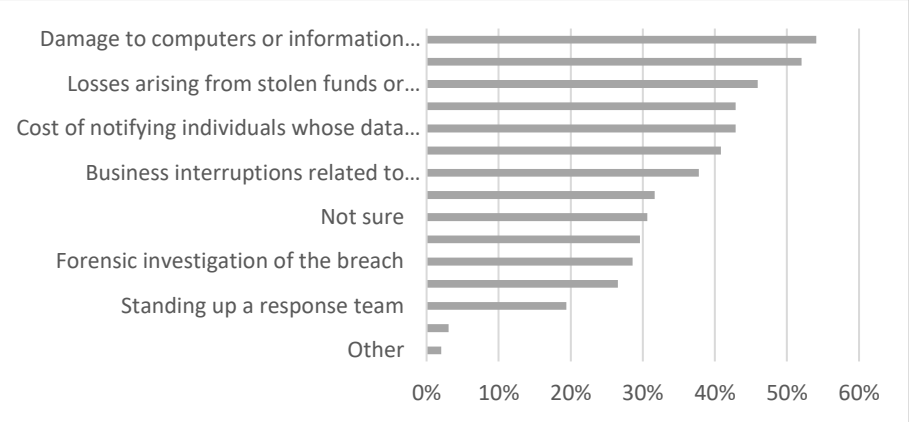
Figure 1: Year Cyber Risk Insurance Was Obtained



Regarding coverage, respondents whose organizations had cyber risk insurance most commonly reported that their organization's insurance policy covered losses due to damage to computers or information systems (54%), with a similar but slightly smaller number of respondents indicating that their organization's cyber insurance policy covered expenses related to responding to the breach (52%):

[136] *See* Romanosky et al., *supra* note 107.

Figure 2: First Party Losses Covered By Cyber Insurance



Over 60% of respondents with cyber insurance policies reported a limit on policy coverage; the remainder were largely unsure as whether their policy included such a limit. Out of the 35 respondents who reported the amount of their coverage limit, the most commonly reported limit was $1 million; however, some respondents reported a coverage limit in the hundreds of millions of dollars. In addition to limitations on coverage amount, insurers may also exclude certain categories of incidents from coverage under a policy. The majority of respondents who indicated that their organization had insurance coverage were unsure whether that insurance policy excluded coverage in certain circumstances, although almost 20% of respondents whose organizations had cyber risk insurance reported that this policy had coverage exclusions. Of those respondents who were able to provide information about these exclusions, the most frequently cited reason for exclusion was acts of war or terrorism, with losses that occurred because the organization failed to provide and maintain adequate security.

C. Act of War Exclusion

Insurance carriers have become increasingly likely to use exclusions to mitigate their exposure to a wide range of difficult-to-quantify risks emanating from IoT devices, drones, critical

infrastructure attacks, and acts of war or terrorism.[137] For example, in the 2019 Romanosky study, nearly 40% of policies surveyed were found to include act of war or terrorism exclusions.[138] In the *State of Hoosier Cybersecurity* survey discussed in Section II.2, 13% of the 98 participants who responded that they had coverage indicated that the policy included an exclusion for acts of war or terrorism. Cyber risk insurance exemptions for acts of war or terrorism were slightly less common amongst respondents who described their organizations as being in a critical infrastructure sector; however, the small number of respondents in this group suggests caution in drawing strong conclusions. In all, the survey found that price and complexity, including with regard to exclusions, were the overriding reasons for why more firms were not purchasing such policies.[139]

To be clear, the exclusion of acts of war or terrorism in property or specific cyber risk insurance policies is not unique to cybersecurity, and in fact dates back centuries.[140] To encompass a broader range of potential conflicts, some policies include language barring coverage from warlike acts "whether declared or undeclared."[141] The reason to exclude such "war risks" from insurance policies is "to prevent the insurer from being bankrupted

---

[137] Romanosky et al., *supra* note 107.
[138] *Id*.
[139] On the other hand, the reasons why such policies were purchased ranged from it being an agent recommendation to the idea being highlighted in a training course to simply "being proactive."
[140] *See* Asaf Lubin, *Public Policy and the Insurability of Cyber Risk*, 6 J.L. & TECH. TEX. __ (forthcoming, 2021), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3452833.
[141] Michael Sean Quinn, *A Look at Invoking War Exclusions*, INSURANCE J. (Oct. 8, 2001), https://www.insurancejournal.com/magazines/mag-legalbeat/2001/10/08/18482.htm. Many policies exclude losses for "(1) war, including undeclared war or civil war; and (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." JEFFEREY W. STEMPEL, LAW OF INSURANCE CONTRACT DISPUTES § 1.02[a] (2001).

by shouldering countrywide losses from war . . . ."[142] Some industries, such as industry and shipping, specifically need insurance coverage if they are to operate in war-torn regions.[143] Though the issue became a particularly hot topic following the September 11, 2001 terrorist attacks,[144] the literature to date exploring the act of war exclusion as applied to state-sponsored cyber attacks remains relatively immature, but is developing. For example, Adam Shniderman has helpfully explored this topic in terms of the challenges surrounding attribution, though not the related question of state sponsorship under international law, and has suggested potential policy options including establishing a National Cybersecurity Safety Board, as is discussed in Part V.[145] Shniderman and others[146] have likewise noted the challenge faced by courts in defining terms like "hostile" and "warlike."[147] Professor Asaf Lubin has taken a broad view of cyber risk insurance, including exclusions such as act of war while also noting the more recent trend of insurance firms moving away from such language and toward sovereign act exclusions, which is likewise discussed in Part V.[148] Daniel Woods and Jessica Weinkle have pointed in particular to the

---

[142] Christopher A. Jennings, Cong. Research Serv., RL31166, *Insurance Exclusion Clauses: Excluding War Risks and Terror Risks from Insurance Contracts* 29 (2001).

[143] Chad Boonswang, *Does Life Insurance Cover Acts of War or Terrorism?*, BOONSWANG L. (Oct. 15, 2019), https://www.boonswanglaw.com/life-insurance-claim/life-insurance-war-exclusion.

[144] *See* Julia Kagan, *War Exclusion Clause*, INVESTOPEDIA (June 23, 2020), https://www.investopedia.com/terms/w/war-exclusion-clause.asp.

[145] Shniderman, *supra* note 125; Scott J. Shackelford & Austin Brady, *Is It Time for a National Cybersecurity Safety Board? Examining the Policy Implications and Political Pushback*, 28 ALBANY L.J. OF SCI. & TECH. 56, 57 (2018).

[146] *See* Lubin, *supra* note 140.

[147] For further discussion, see *infra* Part III.

[148] *Id*. This effort is sweeping in scope, rather than being focused on the act of war exclusion in a comparative context.

need for insurance firms to be more specific about the situations in which the exclusion would apply.[149]

The following Part analyzes recent litigation testing the act of war exclusion in the U.S. context before comparing these interpretations to Britain, and then investigating the applicable international law pertaining to attribution, state responsibility, and opportunities for reform.

IV. REVIEW OF PENDING CASES

This section reviews significant pending cases that are testing the bounds of the act of war exclusion. In particular, the focus here is on *Mondelez*, *Merck*, and *Universal Cable*, the latter of which has been significant in framing a potential reinterpretation of the act of war exclusion. The results of other recent litigation and pending cases are similarly analyzed. This Part conclused by comparing these findings with how another common law jurisdiction with a well-developed insurance industry—the United Kingdom—is approaching this same issue.

A. Mondelez

So far, courts have offered little guidance on what constitutes "hostile acts" in cyberspace,[150] even though there is a history of courts grappling with "hostile or warlike actions" exclusion clauses in other contexts dating back to the 1700s.[151] This issue has been at the fore of *Mondelez*, which involved Zurich Insurance's sale of a

[149] Daniel W. Woods & Jessica Weinkle, *Insurance Definitions of Cyber War*, SPRINGERLINK (May 6, 2020), https://link.springer.com/article/10.1057%2Fs41288-020-00168-5.
[150] Shniderman, *supra* note 125.
[151] *See* Jon Bateman, *War, Terrorism, and Catastrophe in Cyber Insurance: Understanding and Reforming Exclusions*, CARNEGIE ENDOWMENT FOR INT'L PEACE (Oct. 5, 2020), https://carnegieendowment.org/2020/10/05/war-terrorism-and-catastrophe-in-cyber-insurance-understanding-and-reforming-exclusions-pub-82819.

property insurance policy to Mondelez.[152] The policy provided annual coverage for "all risks of physical loss or damage" to Mondelez's property, specifically including "physical loss or damage to electronic data, programs, or software, including physical loss or damage caused by the malicious introduction of a machine code or instruction . . . ."[153] However, there was a broad exclusion in the policy for "'hostile or warlike action in time of peace or war,' whether carried out by a government or its 'agent.'"[154] Such umbrella terms are confusing given that they conflate cyber incidents both above and below the armed attack threshold.[155]

Mondelez fell victim to two separate cyber attacks in 2017 stemming from the NotPetya ransomware epidemic, resulted in the theft of personally identifiable information and the encrypting of approximately 1,700 servers and 24,000 laptops.[156] Mondelez's supply chains were thrown into chaos as network access and associated email systems went down.[157] Recovery took weeks and cost tens of millions of dollars.[158]

In the aftermath of the breach, Zurich informed Mondelez that it was denying coverage under its hostile-or-warlike action exclusion.[159] As of July 2021, the Illinois Circuit Court was

---

[152] Complaint at 2, *Mondelez Int'l, Inc. v. Zurich Am. Ins. Co.*, No. 2018L011008, 2018 WL 4941760 (Ill. Cir. Ct. Oct. 10, 2018).
[153] *Id.*
[154] Bateman, *supra* note 151.
[155] *Id.* For further discussion, see *infra* Part V.
[156] Complaint at 3, *Mondelez Int'l, Inc. v. Zurich Am. Ins. Co.*, No. 2018L011008, 2018 WL 4941760 (Ill. Cir. Ct. Oct. 10, 2018).
[157] Satariano & Perlroth, *supra* note 120.
[158] *Id.*
[159] Complaint at 4, *Mondelez Int'l, Inc. v. Zurich Am. Ins. Co.*, No. 2018L011008, 2018 WL 4941760 (Ill. Cir. Ct. Oct. 10, 2018). Zurich allegedly promised Mondelez via email that Zurich would formally rescind its coverage denial and resume the adjustment of the insurance claim. On July 24, 2018, Zurich sent an email committing to advance a $10,000,000 partial payment toward the claim. Zurich initially sought to place conditions on the advance, but later represented to Mondelez that the promised advance would be unconditional and "not subject to

grappling with a series of claims stemming from this episode, including breach of contract,[160] promissory estoppel,[161] and vexatious and unreasonable conduct.[162] The court granted Zurich's motion to dismiss or withdraw allegations, but which specific allegations the motion referred to are unclear. Core issues remain unresolved, including both the nature of the attack and identity of the perpetrator.[163] To succeed, Zurich must establish by a preponderance of the evidence that Russia, or its agent, was responsible for the NotPetya attack on Mondelez and that the breach constituted a "hostile or warlike action."[164] So far, this has not been done.[165]

B. Merck

As with Mondelez, NotPetya infiltrated Merck's servers in 2017.[166] Merck estimated that the malware caused $870 million in direct damages, crippled Merck's vaccine production facilities, and thereby affected the U.S. emergency supply of human papillomavirus vaccines.[167]

Like Mondelez, Merck had a property policy this time from Allianz SE and American International Group Inc that covered

---

a 'claw back' provision." *Id*. at 5. Mondelez alleged that it refrained to its detriment from instituting immediate litigation challenging the original June 1, 2018 denial letter. *Id*. at 6. Zurich sent a letter on October 9, 2018 to reassert its original declination of coverage. *Id.* This letter also sought to raise new coverage defenses in addition to assertion of the "hostile-or-warlike action" exclusion. *Id.*

[160] *Id*. at 7.

[161] *Id.* at 8.

[162] *Id.* at 9.

[163] *See* Shniderman, *supra* note 125, at 65. For further discussion, see *infra* Part V.

[164] *Id.* at 64.

[165] *Id.* at 81.

[166] Riley Griffin et al., *Was It an Act of War? That's Merck Cyber Attack's $1.3 Billion Insurance Question*, INSURANCE J. (Dec. 3, 2019), https://www.insurancejournal.com/news/national/2019/12/03/550039.htm.

[167] *Id*.; MERCK, FORM 10-K (2019), https://www.sec.gov/Archives/edgar/data/310158/000031015819000014/mrk1231201810k.htm.

$1.75 billion for catastrophic risks.[168] However, Merck's insurers denied coverage, citing an "act of war" exclusion.[169] This points to a key issue: property policies include act of war or terrorism exclusions that are involved in a good degree of this litigation, which is not as common in more tailored cyber-specific policies. Merck sued its insurers, alleging breach of contract and claims of $1.3 billion in total losses. These alleged losses include computer repair expenses, network repair expenses, and the costs of business interrupted by the cyber attack.[170] The insurers argued that NotPetya was a "hostile or warlike" act or an act of terrorism, which are expressly excluded by their insurance policies:[171] according to Philip Silverberg, a lawyer for the insurance companies, "[t]he insurers are confident that there is evidence to demonstrate attribution of NotPetya to the Russian military."[172]

As of this writing, it remains to be seen how the New Jersey courts will decide whether Merck's insurers breached the insurance contract when they cited a war exclusion in denying coverage following the NotPetya cyber attack, and whether the NotPetya attack, if orchestrated by Russia, is the type of cyber operation that could be considered warfare. In making this determination, the court will doubtless rely on *Universal Cable Productions LLC*, which is discussed next.

C. Universal Cable Productions LLC

The Ninth Circuit in 2019 focused on the issue of the "act of war" exclusion in an insurance policy unrelated to a cyber attack,

---

[168] *See* Merck & Co., Inc. v. Ace American Insurance Co., No. UNN-L-002682-18 (N.J. SUP. CT.).
[169] Griffin et al., *supra* note 166.
[170] *Id.*
[171] *Id.*
[172] *Id.*

but involving a terrorist incident.[173] In this case, Universal Studios sought to recover for losses incurred after moving the production of a television series out of Jerusalem after the terrorist group Hamas fired rockets into Israel. Atlantic, the insurer, denied coverage based on its "act of war" policy exclusions.[174] The Ninth Circuit held that Cal. Civ. Code § 1644 required the district court to apply the specialized meanings of "war" and "warlike action by a military force."[175] The court reasoned that because both contractual terms required the hostilities to be between either de jure or de facto sovereigns and because Hamas was neither, the war exclusions did not apply.[176] Thus, the insurer breached its contract with Universal Studios in denying its claim.[177]

---

[173] *See* Michael F. Aylward, *U.S. Courts Set Their Sights on the War Exclusion*, MORRISON MAHONEY (Sept. 10, 2019), https://www.lexology.com/library/detail.aspx?g=6acb490d-e8fc-48d8-9512-572bd41bd1fd.

[174] Universal Cable Prods., LLC, et al. v. Atl. Specialty Ins. Co., 929 F.3d 1143, 1159 (9th Cir. 2019).

[175] *Id.* at 1157. In making this decision, the court wrestled with the special meaning of 'war' in the insurance context. It found that, "[c]ontrary to the district court's holding, California law does not require Universal to introduce 'specific evidence from the negotiation or drafting of the Policy reflecting the parties' intention' to use any 'special meaning of "war"' . . . [T]he only requirement is that the parties had at least constructive notice of the usage, which they did here." *Id.* at 1156. Cal. Civ. Code § 1644 does not provide qualifications or an intent requirement to its mandate on application of customary usage. *Id.* Atlantic did not provide any evidence to contradict the conclusion that "war" has a specialized meaning in this case. The cases used by Atlantic to support its position here are distinguishable for three reasons. *Id.* First, the Israeli-Hamas conflict was not a war between de jure governments. *Id.* Second, the Tenth Circuit's interpretation of "undeclared war" does not apply under California law. *Id.* Third, Universal's expert testified that the current customary usage of the word "war" was developed to distinguish between acts of terror and acts of war in the insurance context. *Id.* Finally, the court found that the cases relied on by Atlantic finding that the 9/11 terrorist attacks were acts of war took place outside of the insurance context. *Id.* Some of these cases explicitly stated that its ruling should be read narrowly and not applied to the insurance context. *Id.*

[176] The court noted that, in particular, Hamas has never declared itself independent from Palestine. *Id.* at 1158. Moreover, the U.S. Secretary of State has consistently designated Hamas as a terrorist organization. *Id.* Customary usage dictates that both of the exclusions require a showing of either de jure or de facto sovereignty, and Atlantic did not meet its burden of showing either. *Id.* at 1160.

[177] *Id.* at 1160.

This holding provides potentially powerful ammunition for plaintiffs seeking to compel insurance providers to cover losses stemming from the actions of foreign governments[178] or non-State actors acting on their behalf.[179] Although the facts surrounding *Universal Cable* are distinct from those in the *Mondelez*, *Merck*, and other cases stemming from the NotPetya attack and other ransomware campaigns, State-sponsored or Sate-condoned cyber attacks targeting U.S. organizations are increasingly common.[180] Moreover, given the historic nature of the act-of-war or terrorism exclusion, its application across myriad contexts over time lends credence to the relevance of this exclusion in the cyber context. Other recent litigation likewise shines a light on the bounds of the "hostile and warlike" acts exclusion, to which we turn next.

---

[178] Relatedly, the Ninth Circuit determined that "the district court erred in failing to address the efficient proximate cause doctrine in holding Israel indirectly contributed to Hamas' conduct." *Id.* at 1161. "[E]ven if Israel countered Hamas' attacks, the district court does not explain how Israel's actions were the proximate cause of Universal's losses in moving the production of Dig. The evidence indicates that, at the least, Universal's decision to relocate production was a result of Hamas firing rockets into Israel (where filming was occurring), and not a result of Israel's retaliatory conduct." *Id.*

[179] *Id.* at 1160 ("A leading insurance treatise notes that 'warlike operations' are 'normally part of an armed conflict between combatants and usually do not include *intentional violence against civilians by political groups*.'" (quoting 10A COUCH ON INSURANCE § 152:3-4 (3d ed. 2017))); *see also* Aylward, *supra* note 173 ("Although the policy expressly included coverage for terrorism losses, it contained a four-part exclusion for war, as follows: [1] War, including undeclared or civil war; or [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 the governmental authority in hindering or defending against any of these. Such loss or damage is excluded regardless of any other cause or event contributed concurrently or in any sequence to the loss; or [4] Any weapon of war including atomic fission or radioactive force, whether in time of peace or war . . . .").

[180] Aylward, *supra* note 173; *Significant Cyber Incidents*, CTR. STRAT. & INT'L STUD., https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents.

D. Other Relevant Litigation

Among the first cases to interpret the meaning and bounds of "warlike" acts was the Second Circuit's *Pan Am Flight 83* case,[181] relied on in *Universal Cable*. In *Pan Am*, a flight was hijacked over London in 1970 by terrorists linked to the Popular Front for the Liberation of Palestine.[182] The terrorists diverted the plane to Cairo, where it was destroyed on the tarmac as purported revenge for the U.S. government's support of Israel.[183] Pan Am sought coverage from its insurer, Aetna, to cover its losses. Aetna claimed the act-of-war exclusion applied.[184] The Ninth Circuit sided with Pan Am,[185] reasoning that the hijackers were not representing a government, but were rather "the agents of a radical political group."[186]

The same year *Pan Am* was decided, a district court considered *Bergara v. Ideal National Life Insurance Co*, a case

---

[181] Pan Am. World Airways, Inc. v. Aetna Cas. & Sur. Co., 505 F.2d 989 (2d Cir. 1974).
[182] *See* Lubin, *supra* note 140, at 41.
[183] *Id.*
[184] *Id.*
[185] *Pan Am.*, 505 F.2d at 1022.
[186] *Id.* at 1015-16 ("There is no warrant in the general understanding of English, in history, or in precedent for reading the phrase 'warlike operations' to encompass (1) the infliction of intentional violence by political groups (neither employed by nor representing governments) (2) upon civilian citizens of non-belligerent powers and their property (3) at places far removed from the locale or the subject of any warfare. (4) This conclusion is merely reinforced when the evident and avowed purpose of the destructive action is not coercion or conquest in any sense, but the striking of spectacular blows for propaganda efforts." (citations omitted)). The Southern District of New York considered a similar case when Holiday Inn sued Aetna over a bombing and other events at its hotel in Beirut, Lebanon from 1975-76. *Holiday Inns, Inc. v. Aetna Ins. Co.*, 571 F. Supp. 1460 (S.D.N.Y. 1983). In this case, Aetna had issued an all-risk policy covering against all risks of direct physical loss or damage to the property from any external cause except as provided. *Id.* at 1463. However, Aetna argued for the applicability of three excluded perils: insurrection, civil war, and war. *Id.* The court determined ultimately that Aetna failed to prove the existence of an insurrection, *id*. at 1487-93, which was equally fatal to its defense based upon "civil war," *id*. at 1493-99. Indeed, the court found that hotel was damaged by a series of factional "civil commotions," of increasing violence. *Id.* at 1503. The requisite intent to overthrow the government had not been proved to the exclusion of other interpretations, and there was no "war" between sovereign or quasi-sovereign states. *Id.*

involving the death of a servicemember in Vietnam.[187] The *Bergara* court reasoned that even though the Vietnam War was an undeclared war, "the greater weight of authority and the better reasoned cases hold that a war in fact is sufficient to exclude coverage where the insured was killed in an undeclared war."[188] As such, the court determined that it was the fact of military confrontation rather than the mere declaration of words that should determine the meaning of the word "war" in the insurance policy, and that the war exclusion properly excluded coverage.[189] This case offers some support to plaintiffs challenging insurance providers to cover losses following an undeclared cyber war involving sovereign military forces.

Other courts have similarly considered the extent to which war exclusions should apply in peacetime. For example, in *International Multifoods Corporation v. Commercial Union Insurance Company,* the Second Circuit grappled with whether an exclusion applied to a peacetime seizure of goods aboard ship by a police authority to enforce a normal police interest in enforcing customs, tax and related criminal laws.[190] The court ultimately found that, because the all-risk insurance policy's war exclusion clause was ambiguous as to whether it applied only to wartime seizures,[191] the district court erred by granting insured summary judgment in action to recover loss of cargo seized by the Russian government.[192] As such, this case may be read to support insurance providers that seek to avoid compensating victims of state-

[187] Bergera v. Ideal Nat'l Life Ins. Co., 524 P.2d 599 (Utah 1974).
[188] *Id.* at 601.
[189] *Id.* at 603.
[190] Int'l Multifoods Corp. v. Commercial Union Ins. Co., 309 F.3d 76 (2d Cir. 2002).
[191] "'All risks' refers to a type of insurance coverage that automatically covers any risk that the contract does not explicitly omit." Investopedia, https://www.investopedia.com/terms/a/all-risks.asp#:~:text=%22All%20risks%22%20refers%20to%20a,the%20event%20of%20flood%20damage (last visited Aug. 11, 2021).
[192] Int'l Multifoods Corp. v. Commercial Union Ins. Co, *supra* note 192, at 85-86.

sponsored cyber attacks that fall below the armed attack threshold. However, the contract-heavy focus of the decision[193] ensures that its overall utility will be limited.

Precedent upon which modern courts, including those in Illinois and New Jersey grappling with the fallout of NotPetya, can rely in determining the bounds of the war exclusion is thus spotty. Already in 2021, though, some courts have referred to NotPetya as an act of war in contrast to the narrower *Pan Am* decision, at least for the sake of argument in finding that defendants did not show that its actions constituted nonperformance.[194]

In an effort to provide more guidance to U.S. courts, the next section considers lessons from Britain. The British example is intriguing because of the relative lack of guiding precedent even as British firms face many of the same challenges of their U.S. counterparts.

E. Insights from Britain

Britain has long been home to an advanced insurance industry. In fact, the first-ever fire, accident, and life insurance firms date back to 1700s-era Britain.[195] Unfortunately, British organizations also have a long track record of dealing with ransomware attacks.[196] As was mentioned in Part I, the NHS "was brought to a standstill for several days" in 2017 due to the WannaCry global ransomware epidemic.[197] Like courts in the United States, British courts seem ripe to face a wave of claims over the bounds of insurance coverage to cover losses due to state-

---

[193] *Id.* at 87.
[194] *Princeton Cmty. Hosp. Ass'n v. Nuance Communs., Inc.*, No. 1:19-00265, 2020 U.S. Dist. LEXIS 60490 *13-14 (S.D. W. Va. Apr. 6, 2020).
[195] *A History of UK Insurance*, SWISS RE 4 (2017), https://www.swissre.com/dam/jcr:e8613a56-8c89-4500-9b1a-34031b904817/150Y_Markt_Broschuere_UK_EN.pdf.
[196] *The Top 5 Ransomware Attacks in the UK and Their Hidden Costs on Business*, ACRONIS, https://www.acronis.com/en-us/articles/ransomware-attacks.
[197] *Id.*

sponsored cyber attacks. But given the expansive data breach liability that is the norm even after Brexit given that the United Kingdom has codified GDPR domestically, there is a chance for a transatlantic divergence to open up with regards to permissible exclusions related to state-sponsored ransomware.

How general insurance coverage should be applied to cyber incidents in British courts has been discussed widely at least since 2016.[198] Back then, though, relatively few British businesses had cyber risk insurance policies.[199] Yet, by 2020 it is estimated that still only 20% of British firms had cyber risk insurance policies.[200] For comparison's sake, many firms have been rated as having immature, reactive approaches to managing cyber risks, and more U.S.-based firms (55%) have insurance coverage as opposed to 30% in Germany.[201] Even those that do have such policies in place are being subject to potentially enormous fines, as seen in EasyJet's data breach involving nine million of its customers that resulted in

---

[198] *See* Ian Birdsey, *Expect UK Court Disputes Over Whether General Insurance Cover Applies to Cyber Incidents, Says Expert*, PINSENT MASONS (May 26, 2016, 12:00 PM), https://www.pinsentmasons.com/out-law/analysis/expect-uk-court-disputes-over-whether-general-insurance-cover-applies-to-cyber-incidents-says-expert (anticipating UK courts having to decide controversies of insurance coverage for cyber attacks in the near future based on recent decisions in the United States).

[199] *Id.*

[200] *See* Phil Muncaster, *Over 80% of UK Firms Don't Have Specialist Cyber Insurance*, INFO SEC. MAG. (Feb. 5, 2020), https://www.infosecurity-magazine.com/news/80-uk-firms-dont-have-specialist (claiming that this is due to a mix of a belief among survey respondents that cyber-attacks are "mainly an issue for bigger organizations" and that the firms' general insurance policies will cover them in the event of a cyber attack, which has been shown to be oftentimes unlikely).

[201] Louie Bacani, *Majority of UK, US Firms Not Ready for Cyberattacks - Study*, INS. BUS. UK (Feb. 8, 2017), https://www.insurancebusinessmag.com/uk/news/cyber/majority-of-uk-us-firms-not-ready-for-cyberattacks--study-59489.aspx.

approximately 10,000 plaintiffs across fifty nations filing suit—leading to a potential total price tag approaching $18 billion.[202]

To date, ransomware losses are typically covered as part of general "extortion coverage" under comprehensive property or specific cyber risk insurance policies.[203] But given mounting losses, this could change.[204] There is thus far relatively little evidence suggesting that British firms are closing the gap with firms in the United States in terms of overall cyber risk insurance coverage, though data remains fragmented and inconsistent.[205] This may be one reason why there is a relative paucity of court decisions on this topic in Britain, despite the extent to which British organizations have fallen victim to cyber attacks in recent years.[206] One of the relatively few cases that discusses the topic, *Axa Corporate Solutions SA v. National Westminster Bank PLC & Marsh Ltd.*, discusses whether and how cyber liability and terrorism exclusions would apply.[207] However, that case centered on evidence of

---

[202] Arthur A. Armstrong, *Navigating Coverage for Losses, Liabilities Triggered by Cyber Attacks*, LEGAL INTELLIGENCER (July 15, 2020, 4:43 PM), https://www.law.com/thelegalintelligencer/2020/07/15/navigating-coverage-for-losses-liabilities-triggered-by-cyber-attacks (primarily discussing American case law but noting that significant data breach liability is imposed in European countries).

[203] *Id*.

[204] There is no reliable, hard data parsing out the proportion of ransomware attacks launched by State versus non-State groups, but there is literature supporting the view that nations are increasingly using cyber-enabled tools to further various national security ends especially given the increasing prevalence of "defend forward" cybersecurity strategies. *See, e.g.*, Danny Palmer, *Hacking and Cyber Espionage: The Countries that are Going to Emerge as Major Threats in the 2020s*, ZDNET (Dec. 12, 2019), https://www.zdnet.com/article/hacking-and-cyber-espionage-the-countries-that-are-going-to-emerge-as-major-threats-in-the-2020s; Paul M. Nakasone & Michael Sulmeyer, *How to Compete in Cyberspace*, FOREIGN AFF. (Aug. 25, 2020), https://www.foreignaffairs.com/articles/united-states/2020-08-25/cybersecurity.

[205] *Cf.* Bacani, *supra* note 201 (noting that 36% of British firms reported having cyber risk insurance coverage, which is nearly double the rate from other surveys).

[206] *See* British-American Insurance (Kenya) Ltd. & Matelec Sal, Thika Power Ltd., [2013] EWHC 3278 (Comm), 2013 Folio 225, 2013 Folio 268 (Eng.) (referencing a "cyber attack exclusion clause," which was ancillary to the core topics at issue).

[207] *See* Axa Corp. Solutions SA v. Nat'l Westminster Bank PLC & Marsh Ltd., [2010] EWHC 1915 (Comm), 2009 Folio 377 (Eng.).

agreement on the exclusions in question, rather than their substance.[208] Still, it does demonstrate that these exclusions have been in play for more than ten years in the British context without common agreement on the key terms at issue.

Going forward, if cyber risk insurance is to mature into a valuable and effective tool for cybersecurity risk management, it is vital to globalize these discussions. After all, the geopolitical trends fueling these attacks largely do not respect national boundaries.

V. POLICY IMPLICATIONS AND PROPOSED STANDARD

As this Article has demonstrated, six trends are shaping the cyber risk insurance market, and in particular how insurance firms are using exclusions to limit their exposure to geopolitical cyber risks. First, the ransomware epidemic—fed by high-profile breaches such as Shadow Brokers and FireEye—is leading to a proliferation of extortion campaigns targeting a wide array of private and public-sector organizations. This is already having implications for insurer participation in the cyber market, which could in time impact the market's solvency.[209] In Britain, for example, the median loss ratio for cybersecurity insurers increased between 2018 and 2019.[210] Second, there is a need for greater transparency as to cyber risk insurance coverage, including what exclusions are being included in policies. This is all the more important during times of public health emergencies when many are working from home given the prevalence of smart home devices that could be targeted. Insurers have been using such exclusions to help cover their losses in times of mounting geopolitical risks, including the mounting prevalence

---

[208] *Id*.

[209] *See infra* Part I.

[210] *U.S. Cyber Market Update*, AON 8 (June 2020), http://thoughtleadership.aon.com/Documents/202006-us-cyber-market-update.pdf (noting thatthe median loss ratio for insurers above $50m did increase by eleven percent over this time period).

of state-sponsored cyber attacks,[211] but as shown in our survey findings, this has resulted in confusion over the types of incidents that are being covered, which in turn is impacting overall cybersecurity readiness and, ultimately, national security.

Third, U.S. courts have been grappling with what constitutes "hostile acts" in cyberspace. Such umbrella terms as the one at issue in *Mondelez* are perhaps intentionally vague, given that they conflate cyber incidents both above and below the armed attack threshold. Absent reform, *Universal Cable* will help plaintiff efforts in limiting the scope of act of war exclusions. *Bergara* will help plaintiffs in situations of undeclared cyber wars involving sovereign military forces, and to an extent, *Multifoods Corporation* will help plaintiffs for cases involving peacetime cyber incidents. Given that the U.S. has arguably the deepest and widest cyber risk insurance market in the world today,[212] the precedents set by the U.S. insurance industry and judicial system will likely be closely followed by other nations – including Britain and Germany – that are seeing similar waves of ransomware and a growing prevalence of insurance coverage.

As Part II analyzed, more nations are developing their offensive cyber capabilities,[213] while at the same time they are following the U.S. example by lowering their use of force thresholds. At the same time, there is a growing prevalence of

---

[211] *See, e.g.*, Robert Lemos, *'Act of War' Clause Could Nix Cyber Insurance Payouts*, DARK READING (Oct. 29, 2020), https://www.darkreading.com/attacks-breaches/act-of-war-clause-could-nix-cyber-insurance-payouts/d/d-id/1339317.

[212] *See, e.g.*, CYBER INSURANCE MARKET BY COMPONENT, TYPE, COVERAGE, ORGANIZATION SIZE, END USER AND REGION - GLOBAL FORECAST TO 2025 (Oct. 2020), https://www.reportlinker.com/p05977659/Cyber-Insurance-Market-by-Component-Type-Coverage-Organization-Size-End-User-And-Region-Global-Forecast-to.html.

[213] *See supra* Part V; *see, e.g.*, Julia Voo et al., *National Cyber Power Index*, BELFER CTR. (Sept. 2020), https://www.belfercenter.org/publication/national-cyber-power-index-2020 (ranking cyber powers based in part of their offensive cyber capabilities).

nations, publicly led by the United States and other Five Eyes nations such as Canada, to rely on "defense forward," which calls for an increasingly assertive and proactive use of offensive cyber power in the name of persistent engagement and active deterrence. This is a recipe for state-sponsored cyber instability and future waves of cyber attacks.

Sixth and finally, the high evidentiary bar baked into the effective control standard, which has been likened to even a higher threshold than a criminal law beyond a reasonable doubt standard,[214] is a far cry from the preponderance of the evidence standard being used in the civil *Mondelez* case. It is unlikely that a U.S. court would rely on this international law evidentiary requirement in determining whether public U.S. government attributions suffice to prove state control or coordination in a contractual dispute, but if they did, then the lower civil threshold would make it more likely that the court would find a linkage between ransomware incidents such as NotPetya and foreign nations, including Russia. However, in seeking additional evidence to attribute these attacks, given the lack of detailed analysis coming from the U.S. intelligence community, courts may rely on equivalent international standards such as the ICJ's effective control stance, which would limit the act of war exclusion.

In short, courts in the United States and around the world are rightly confused about how best to address the mounting cyber risks fed by more nations being more assertive in their offensive cyber operations. There is growing evidence of spillover effects for the wider society. Insurers are getting the message that the act of war exclusion is an at best an imperfect vehicle in their understandable

---

[214] *See* Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosn. & Herz. v. Serb. & Mont.), 2007 I.C.J. 1, 140 para. 391, 422 (Feb. 26) ("The standard laid down was "beyond *any* doubt," not beyond a *reasonable* doubt.").

quest to limit their geopolitical cyber risk exposure. Indeed, more insurers seem to be moving away from broad act of war exclusions to "state motivated" or "directed" exclusions.[215] This move avoids the legally dicey analysis of defining "cyber war," though not the related questions of peacetime cyber attacks operating below the armed attack threshold that may still be actionable.

However, the remaining question around attributing cyber attacks to a nation state is far from simplistic. Exclusions that reference "state motivated" attacks seem to refer to the lower, more flexible "operational control" standard, which constitute a more manageable evidentiary burden to demonstrate the linkage between State and non-State actors.[216] Yet, in some ways, "motivated" is even looser than that envisioned, opening the door for a potentially wide array of cyber actions from non-State groups being attributed back to nations.[217] One potential middle ground could be to adopt the "sliding scale" approach in exclusions, which simply requires that "the graver the charge the more confidence there must be in the evidence relied on."[218] Thus, as is described further below, the more catastrophic the cyber attack, the more evidence there must be in order to prove the attribution and activate the exclusion.

---

[215] *See* Lubin, *supra* note 146, at 45. It is important to note that that the often-broad 'cyber terrorism carveout' in cyber risk insurance policies was added to address analogous situations in which a state-coordinated incident that did not rise to the level of an act of war might still be considered hostile and thus fit the war exclusion, meaning that "[i]n many ways the carveback swallows up the exclusion[,] which is good for insureds." Interview with Stephen Vina, Vice President, Marsh Insurance (Dec. 31, 2020).

[216] *See* Prosecutor v. Tadic, Case No. IT-94–1-I ICTY (Oct. 2, 1995), at 1541.

[217] *See* TALLINN MANUAL, *supra* note 42, at 38 (arguing that state responsibility requires that a state "issued specific instructions or directed or controlled a particular operation," and noting that even the overall control standard still requires that control "go beyond 'the mere financing and equipping of such forces and involv[e] also participation in the planning and supervision of military operations.'") (citing Tadic, at 145).

[218] Oil Platforms (Iran v. U.S.), 2003 I.C.J. 161, 234 (Nov. 6) (separate opinion of Judge Higgins).

In some ways, litigation surrounding the act of war exclusion in cyber risk insurance policies serves as an opportunity for courts to grapple with how to attribute State-sponsored cyber aggression, a topic that has long stymied best efforts at cyber norm development,[219] and one which international courts have so far largely avoided.[220] This is also an opportunity for insurance providers to help shape the conversation about determining an appropriate standard for State-sponsored cyber attacks. For example, insurance providers would seem to benefit from "State motivated" language in such exclusions since it could open up such a broad range of cyber-enabled incidents and activities as discussed above, while the insureds may prefer "State directed."[221] As a compromise, it may be possible to use a standard of "State coordinated" cyber attacks to get to the root of the matter more explicitly, i.e., the extent to which nations were instrumental in organizing and facilitating the cyber attack in question. Absent that approach, there are benefits to policies using language that has been well conceptualized in the international law context, such as by determining attribution "as established by the effective control standard," to help guide jurists, lawyers, and policy holders. It is also possible to use separate exclusions for war-related and other State-sponsored incidents, and even extreme, catastrophic scenarios (such as non-malicious malfunctions caused by natural disasters).[222] Separating exclusions in this manner has the added benefit of

---

[219] For a useful set of resources on cinternational cybersecurity norms, see *International Cybersecurity Norms*, CARNEGIE ENDOWMENT, https://carnegieendowment.org/specialprojects/cybernorms.

[220] Ryan Patterson, *Silencing The Call To Arms: A Shift Away From Cyber Attacks As Warfare*, 48 LOY. L.A. L. REV. 969 (2015) (arguing that existent laws of war are insufficient to govern cyber activities).

[221] Yet there is a balancing act in play here since, as described by Stephen Vina from Marsh Insurance: "If cyber insurers denied NotPetya or WannaCry claims because they were state motivated, coordinated, or directed, companies may lose faith in the product and stop buying it." Vina, *supra* note 215.

[222] Bateman, *supra* note 151.

specificity and transparency for both the insurer and the insured, such as an exclusion for cyber losses stemming from kinetic armed conflicts.[223]

In addition to these targeted reforms that are designed to focus on interpretation challenges involving the act-of-war or hostile acts exclusions in insurance policies, there are also larger potential policy proposals that could address the underlying geopolitical challenges raised by this issue. For example, I have argued for establishing a National Cybersecurity Safety Board (NCSB) loosely modeled after the National Transportation Safety Board.[224] The NCSB could help with the forensic investigation of cyber attacks and, while not assigning blame or establishing attribution, its findings could support other public- and private-sector attribution efforts. To that end, a public-private Attribution Council, or consortium, could be created to pool resources and expertise while insulating any individual organization from the risks of publicly attributing cyber attacks to a potentially hostile nation.[225] A variety of such proposals have been put forward, some run by governments, and others run by the private sector.[226] The extent to which such an organization should have an enforcement role has also varied depending on the proposal in question.[227] Regardless, the politics of such an endeavor are daunting, as is the cyber risk exposure for those organizations involved—a possible reason why it has not yet come to pass. Instead of a single Attribution Council, there are benefits to a network, or regime complex, of attribution organizations, such as

---

[223] *Id*.
[224] *See* Scott J. Shackelford & Austin Brady, *Is It Time for a National Cybersecurity Safety Board? Examining the Policy Implications and Political Pushback*, 28 ALBANY L.J. SCI. & TECH. 56 (2018).
[225] *See* Milton Mueller, *A Global Cyber-Attribution Organization – Thinking it Through*, INTERNET GOVERNANCE PROJ. (June 4, 2017), https://www.internetgovernance.org/2017/06/04/a-global-cyber-attribution-org.
[226] *Id*.
[227] *Id*.

an ecosystem comprised of NCSBs, academic-based initiatives such as Citizen Lab, along with intergovernmental organizations such as NATO.[228] Such a consortium-based, decentralized[229] approach to attribution would likewise have the added benefit of incentivizing robust information sharing, which is vital to the overall cause of cyber peace,[230] and which has come under threat given trends toward cyber sovereignty and data localization.[231] This polycentric system, as envisioned, would likewise permit the "crosschecking or corroboration of the accusations," increasing both the degree of confidence in, and potential buy-in for, attribution conclusions.[232]

Further reforms are also possible, ranging from shifting the burden of proof to the insured to grander plans like extending the Classified Information Procedures Act, creating a National Security Court,[233] establishing a federal backstop for insurance providers similar to what has been done in the terrorism context,[234] or even creating an International Criminal Tribunal for Cyberspace.[235] Similarly, there needs to be frank conversations about related issues, including both the benefits and drawbacks of active defense and

---

[228] *See* Joseph S. Nye, Jr., *The Regime Complex for Managing Global Cyber Activities*, GLOB. COMM'N ON INTERNET GOVERNANCE 6 (May 2014), https://dash.harvard.edu/bitstream/handle/1/12308565/Nye-GlobalCommission.pdf.

[229] *See* Kristen E. Eichensehr, *Decentralized Cyberattack Attribution*, 113 AM. J. INT'L L. UNBOUND 213 (2019).

[230] *See* Scott J. Shackelford, Governing New Frontiers in the Information Age: Toward Cyber Peace (2020).

[231] *See, e.g.*, Trey Herr, *Four Myths About the Cloud: The Geopolitics of Cloud Computing*, ATLANTIC COUNCIL (Aug. 31, 2020), https://www.atlanticcouncil.org/in-depth-research-reports/report/four-myths-about-the-cloud-the-geopolitics-of-cloud-computing (discussing data localization and cyber sovereignty in the context of cloud computing).

[232] Kristen E. Eichensehr, *The Law and Politics of Cyberattack Attribution*, 67 U.C.L.A. L. REV. 520, 520 (2020)

[233] Schniderman, *supra* note 125, at 81.

[234] *See* Klein & Anderson, *supra* note 8.

[235] *See* Judge Stein Schjolberg, *An International Criminal Tribunal for Cyberspace* (EastWest Inst. Working Paper, 2012), https://www.cybercrimelaw.net/documents/ICTC.pdf.

persistent engagement as emerging cyber norms.[236] And, for that matter, more should be done to include cyber risk insurance discussions in ongoing dialogues related to cyber norms and cyber peace building, given the invaluable role that insurance can and should play in mitigating a range of cyber risks.[237]

CONCLUSION

This Article has shown how debates around the scope and meaning of the act of war exclusion in cyber risk insurance policies are bringing to the fore an array of both long-running and more recent cybersecurity trends. U.S. courts—and increasingly, international ones, too—are being thrust into the uncomfortable position of making sense of these policy debates as they grapple with defining and attributing State-sponsored cyber attacks. Reform should happen through polycentric mechanisms: not only from the ground up (in the form of insurance providers revising exclusions to make them more narrowly tailored, transparent, and cyber-focused), but also through state action by insurance commissioners, the federal government, and the international community. Cyber risk insurance is no panacea, but neither is any other cybersecurity risk management tool. Still, its utility will be undermined if this issue is not adequately addressed, and the time to do so is now while the global cyber risk insurance market remains relatively immature. Otherwise, we risk making the same mistakes, and having the same debates, years or even decades hence.

---

[236] *See, e.g.*, Scott J. Shackelford, Danuvasin Charoen, Tristen Waite & Nancy Zhang, *Rethinking Active Defense: A Comparative Analysis of Proactive Cybersecurity Policymaking*, 41 UNIV. PENN. J. INT'L L. 377 (2019).
[237] *See* Hake et al., *supra* note 132.