Cyberattack – Intangible Damages in a Virtual World: Property Insurance Companies Declare War on Cyber-Attack Insurance Claims

ANGAD CHOPRA*

ABSTRACT

Cyber-attacks and the monumental damages they cause are becoming seemingly ubiquitous. Large-scale cyber-attacks have become the norm, as opposed to an anomaly. In fact, cyber-attack has been rated as the number one concern for private entities given the sheer danger each attack poses on entity solvency. Ad-hoc attackers, in combination with state-sponsored cyber-warfare actors, have the capability of wreaking havoc on an entire nation or on an entire private industry. Attacks are conducted with sophistication, while cyber security regimes are lagging in meeting the challenge. The results are catastrophic, leaving private entities to incur massive costs in remediation, or in the case of smaller entitles, collapse under the weight of the attack. No attack better exemplifies this phenomenon than the NotPetya Attack of 2017. The Russian cyber-war attack aimed at the Ukrainian financial sector raced around the world, leaving companies reeling with billions of dollars in damages. The key question then becomes, can companies turn to their all-risk insurance policies to recover the damages? Surely, these very polices were designed and attained to insure against losses incurred due to any substantial risk. Surprisingly, the answer from insurers has been a resounding no. All-risk insurers turn to a rarely-invoked exception in all-risk insurance policies known as a "war-risk" or "hostile-act" exclusionary clause and argue that cyber-attacks, such as the NotPetya attack, fall within such an exception, leaving effected companies without the security blanket they assumed they had.

This Note examines the history of war-risk exclusionary clauses, their invocation, and pertinence to a nuanced type of hostile act: the cyber-attack. It proposes a solution to pending litigation surrounding the NotPetya attack, and advocates for courts to use the doctrine of contra proferentem, an analysis that focuses on the intention of the parties to an insurance policy, to solve currently pending suits surrounding cyber-

* Chief Articles Editor, *Ohio State Law Journal*; Juris Doctor Candidate, The Ohio State University Moritz College of Law, 2021.

This Note is dedicated to my family and friends who have provided endless support throughout the process of this Note's publication and my legal academic career. A special thanks to Professor Bryan Choi, who provided invaluable advice throughout the drafting process. Many thanks to the excellent team at the *Ohio State Law Journal*, led by Editor-in-Chief Meg Burrell. All errors are my own.

attacks. It then proposes a nuanced prophylactic remedy, advocating for the advent of a Federal Cybersecurity Insurance Program, constructed in much the same way as war risk insurance policies created in the aftermath of World War II. This nuanced policy will be specifically tailored to risks arising out of cyber-attacks and provides an added benefit such that governmental involvement can provide national security experts with valuable information about how such attacks are being conducted, spurring innovation in cyber security. With billions of dollars at stake, it is clear that the current foundation upon which insurance in the aftermath of cyber-attack is built, is clearly untenable.

TABLE OF CONTENTS

I. INTRODUCTION

On the morning of June 27, 2017, Ukrainian accountants and financial professionals set off to go to work.[1] The morning was as normal as it could be;

[1] *See* Ellen Nakashima, *Russian Military Was Behind 'NotPetya' Cyberattack in Ukraine, CIA Concludes*, WASH. POST (Jan. 12, 2018), https://www.washingtonpost.com/world/national-security/russian-military-was-behind-notpetya-cyberattack-in-ukraine-cia-concludes/2018/01/12/048d8506-f7ca-11e7-b34a-b85626af34ef_story.html [https://perma.cc/

the country was in the midst of a war with Russia that was seemingly endless, having left more than 10,000 Ukrainians dead.[2] The war had been raging for more than four years, leaving behind not only a bloody battlefield, but also a crippled economy—the result of Ukraine becoming a "scorched-earth testing ground for Russian cyberwar tactics."[3] Russians relentlessly launched a slew of attacks, destroying media outlets, railway firms, and power lines, which left the country voiceless, unable to ambulate, and without electricity.[4] Unbeknownst to the citizens of Ukraine, however, the worst of all of these attacks had yet to come—it laid dormant, waiting for workers to take their chairs that June morning, much like a lioness laying low in the bush, waiting for her prey to come drink at the watering hole.[5]

As Ukrainian financial professionals accessed a common tax and accounting software program, they were met with messages on their screens in red and black lettering.[6] Some read "repairing file system on C:," and others read "oops, your important files are encrypted," which was followed by a demand for a payment of $300 worth of bitcoin to decrypt them.[7] But regardless of whether the ransom was paid, the result was the same: screens turned black and computer systems began to fail.[8] An assessment of the damages would reveal that all data on the crashed systems were left irreversibly corrupted.[9] The insidious NotPetya cyberattack of 2017 had begun.

The hackers behind the NotPetya cyberattack, known collectively as Sandworm,[10] had one true intent: to wreak absolute havoc on the Ukrainian financial sector and leave the country crippled.[11] In order to achieve this end, Sandworm needed to create a vicious cyberweapon, one capable of "spread[ing] automatically, rapidly, and indiscriminately."[12] To say it was successful is a

---

B6JQ-N32P] [hereinafter Nakashima, *NotPetya Strategy*]; David Voreacos, Katherine Chiglinsky & Riley Griffin, *Merck Cyberattack's $1.3 Billion Question: Was It an Act of War?*, BLOOMBERG (Dec. 3, 2019), https://www.bloomberg.com/news/features/2019-12-03/merck-cyberattack-s-1-3-billion-question-was-it-an-act-of-war [https://perma.cc/3ZMB-B2MK] [hereinafter Voreacos et al., *Merck Litigation Summary*].

[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/ [https://perma.cc/GKB7-XR9U] [hereinafter Greenberg, *Effects of NotPetya*].

[3] *Id.*

[4] *Id.*

[5] Russian hackers in the NotPetya attack used a tactic known as the "watering hole" attack. In this attack hackers "infect[] a website to which they kn[o]w their targets [will] navigate—in this case, a Ukrainian site that delivered updates for tax and accounting software programs." Nakashima, *NotPetya Strategy*, *supra* note 1.

[6] Greenberg, *Effects of NotPetya*, *supra* note 2.

[7] *Id.*

[8] *Id.*

[9] *Id.*

[10] *Id.*

[11] Nakashima, *NotPetya Strategy*, *supra* note 1.

[12] Greenberg, *Effects of NotPetya*, *supra* note 2.

complete understatement. One cyberattack expert described the cyberweapon as "simply the fastest-propagating piece of malware [he had] ever seen."[13] Still, the attack was supposedly targeted at the Ukrainian financial sector,[14] so although the cyberweapon was heinous, it would at least be contained. This assumption, however, could not have been more incorrect.

The relentless cyberweapon spread like a plague, far exceeding the expectation of even Sandworm itself.[15] "Within hours of its first appearance, the worm raced beyond Ukraine and out to countless machines around the world, from hospitals in Pennsylvania to a chocolate factory in Tasmania."[16] The worm moved from entity to entity, "crippl[ing] multinational companies including Maersk, pharmaceutical giant Merck, FedEx's European subsidiary TNT Express, French construction company Saint-Gobain, food producer Mondelēz, and manufacturer Reckitt Benckiser."[17] Ironically, the attack made its way back to Russia itself, infecting state oil company Rosneft,[18] an obvious indication that the attack had strayed far from its initial intention.

The effects of the attack, resulting in the systematic destruction of the cyber infrastructure of some of the world's largest companies, were staggering. In total, losses of over $10 billion were reported.[19] Even a year after the attack, companies were still struggling in their efforts to recover.[20] FedEx was forced to spend roughly $400 million in remediation expenses.[21] Merck reported that the NotPetya attack "temporarily disrupted manufacturing, research and sales operations, [which left] the company unable to fulfill orders for certain products," such as vaccinations for the prevention of cancer.[22] Mondelēz International Inc. lost its email services and the ability to invoice its customers'

---

[13] *Id.*

[14] *See* Nakashima, *NotPetya Strategy*, *supra* note 1.

[15] *See* Greenberg, *Effects of NotPetya*, *supra* note 2.

[16] *Id.*

[17] *Id.*

[18] *Id.*

[19] *Id.*

[20] Kim S. Nash, Sara Castellanos & Adam Janofsky, *One Year After NotPetya Cyberattack, Firms Wrestle with Recovery Costs*, WALL ST. J. (June 27, 2018), https://www.wsj.com/articles/one-year-after-notpetya-companies-still-wrestle-with-financial-impacts-1530095906 [https://perma.cc/5FM7-ZHZS] [hereinafter Nash, *Year-After Analysis*].

[21] *Id.* Such staggering recovery rates are to be expected. Companies are saddled with a number of costly recovery steps in the aftermath of an attack—mobilizing incident response teams, enacting creative solutions to ensure continuity of business, conducting an expensive and thorough investigation of the damages, managing public relations and business interruptions, and addressing possible legal and regulatory requirements. Ben Rossi, *Six Critical Steps for Responding to a Cyber Attack*, INFORMATION AGE (June 11, 2015), https://www.information-age.com/6-critical-steps-responding-cyber-attack-123459644/ [https://perma.cc/H5TS-H3ME].

[22] Nash et al., *Year-After Analysis*, *supra* note 20.

orders.[23] Companies not only suffered the direct costs incurred from remedial efforts, but also suffered millions in lost revenue.[24]

Given the monumental losses experienced as a result of the destruction of their cyber infrastructure, companies turned to their all-risk insurance policies and crafted claims in an effort to recover.[25] These companies, however, were met with an unexpected answer: they could not recover.[26] Insurance companies, such as Zurich American Insurance, cited a "common, but rarely used, clause in insurance contracts: the 'war exclusion,' which protects insurers from being saddled with costs related to damage from war."[27] Indeed, "[t]he release of NotPetya was an act of cyberwar by almost any definition . . . ."[28] Affected companies were left wondering if this act of cyberwar, and the damage that arose therefrom, was the type of damage that war exclusion clauses were meant to exclude. This very question has been one of the most contentiously debated and is now the subject of litigation on a global scale.[29] Affected companies demand compensation, having relied on what they believed were robust insurance policies meant to provide coverage for the damages they had suffered from.[30]

There are sound arguments presented on both sides of this issue. Insureds argue, amongst other things, that war exclusion clauses exclude only the physical property damages that arise from physical warfare—damage to tangible property resulting from an act of war between two state actors.[31] Clearly, cyber infrastructure is not tangible, and as such it cannot be excluded under most war exclusion or hostile act clauses.[32] Insurers, on the other hand, argue that war exclusion and hostile acts clauses have evolved over time and no

---

[23] *Id.*

[24] *See id.*

[25] Michael Menapace, *Property Insurance, Cyber Insurance, Coverage and War: Losses from Malware May Not Be Covered Due to Your Policy's Hostile Acts Exclusion*, NAT'L L. REV. (Mar. 10, 2019), https://www.natlawreview.com/article/property-insurance-cyber-insurance-coverage-and-war-losses-malware-may-not-be-0 [https://perma.cc/W2DD-TH3Q] [hereinafter Menapace, *Insurance Overview*].

[26] Adam Satariano & Nicole Perlroth, *Big Companies Thought Insurance Covered a Cyberatack. They May Be Wrong.*, N.Y. TIMES (Apr. 15, 2019), https://www.nytimes.com/2019/04/15/technology/cyberinsurance-notpetya-attack.html [https://perma.cc/BF2T-5VGD] [hereinafter Satariano & Perlroth, *Insurance Companies Reject Claims*].

[27] *Id.*

[28] Greenberg, *Effects of NotPetya*, *supra* note 2.

[29] *See* Jeff Stone, *Demand for Cyber Insurance Grows as Volatility Scares off Some Providers*, CYBERSCOOP (July 29, 2019), https://www.cyberscoop.com/cyber-insurance-demand-cost-2019/ [https://perma.cc/4WWC-HZQU] (noting the increase in cyber insurance claims "driven largely by concerns about data breaches, distributed denial-of-service attacks and, perhaps most notably, ransomware").

[30] Satariano & Perlroth, *Insurance Companies Reject Claims*, *supra* note 26; *see also* Complaint ¶ 1, Mondelēz Int'l, Inc. v. Zurich Am. Ins. Co., No. 2018-L-011008, 2018 WL 4941760 (Ill. Cir. Ct. Oct. 10, 2018) [hereinafter Mondelēz Complaint] (outlining legal claims brought by Mondelēz against Zurich American Insurance).

[31] Menapace, *Insurance Overview*, *supra* note 25.

[32] *Id.*

longer involve only that which is classified as historical *physical* acts of war but also include the damages that are *proximately caused* or *reasonably expected* to ensue from a belligerent act.[33] Which argument is most compelling is left for the courts to decide, but with billions of dollars at stake, the decision to be made is anything but trivial.

This Note will suggest how courts *should* answer this question in the pending litigation and will also offer a solution as to how a new system can be implemented such that companies and other entities can avoid insurance disputes in the aftermath of a cyber-attack. This Note will offer a short-term and a long-term solution to this issue. In the short-term, current litigation will require a fair and equitable solution and this Note will recommend that courts adopt the doctrine of *contra proferentem* to solve ambiguities in insurance policies at the heart of the dispute. In the long-term, a nuanced Federal Cybersecurity Insurance Policy can be adopted by the United States government. This proposed policy would offer insurance *specifically tailored* to cover damages subsequent to a cyber-attack, irrespective of whether the attack is performed by independent rogue operators or by state-sponsored actors. Part II examines the history of property insurance policies and exclusionary clauses and how the interpretation of the same has changed with the ever-evolving nature of modern warfare. This Part will conclude that property insurers tend to try to expand exclusionary clauses as much as possible, given the evolution of hostile or war-like acts, leading to interpretational disputes. Part III provides an in-depth analysis of case law involving war-risk and hostile act exclusionary clauses. Half of the discussion will focus on relevant federal precedent, likely to be of incredible value in the analysis of pending litigation and in providing the necessary background for the short-term solution. The second half will present the two chief cases currently pending in U.S. courts and will analyze arguments made in the complaints from the victims and the responses by insurance providers. Part IV proposes an answer to the pending litigation and introduces a prophylactic strategy with the goal of avoiding these disputes in the future. Part V briefly concludes.

II. HISTORY OF WAR RISK AND HOSTILE ACT EXCLUSIONARY CLAUSES

The insurance industry is based on risk coverage: insurers offer their customers coverage policies wherein the insurer assumes liability for damages

---

[33] *Id.* Cyber-attacks usually involve corruption of an entire systemic network, damaging hardware as well as software. As such, a nexus between cyber-attack and tangible property damage is discernable. In addition, the definition of tangible property, which usually pertains to what individuals can see, touch, and/or use, and thus be able to independently derive value, might need to be expanded to include intangible damages, as surely, in the modern age, intangible property (i.e. data, copyrights, etc.) are fully capable of having independent economic value as well. *See* Charles E. Boyle, *Industry Faces Cyber Risks in Shift from Tangible to Intangible Property*, INS. J. (Sept. 20, 2012), https://www.insurancejournal.com/news/international/2012/09/20/263668.htm [https://perma.cc/N2AP-PRMD].

that an individual or entity would have had to assume on their own without coverage.[34] Insurers "pool[] clients' risks to make payments more affordable for the insured."[35] This business model is an incredibly risky endeavor.[36] Insurers craft their policies to cover damages that vary in size and scope while balancing the objective of remaining solvent and profitable.[37] Often times, the way insurers attempt to maintain this important balance is by crafting exclusionary clauses, including war-risk and hostile act clauses.[38] The modern reasons for war-risk and hostile act exclusionary clauses are grounded in the catastrophic damages that war can cause, which, if covered under an insurance policy, would tip the balance in favor of insurer insolvency.[39]

Modern justifications for insurance exclusionary clauses are also grounded in history. American property insurance policies can be traced back to colonial times.[40] These policies were based on British property insurance schemes.[41] Insurance policies were first created in 1601, when the United Kingdom passed legislation in order to cover damages to merchandise and ships in transit.[42] Sixty-five years later, in what was one of the most important events in the long history of property insurance, the Great Fire of London "demonstrated [the] destructive power of fire in an urban environment, leading [British] entrepreneur Nicholas Barbon to form a business to repair houses damaged by fire."[43] In the

---

[34] Julia Kagan, *Insurance*, INVESTOPEDIA, https://www.investopedia.com/terms/i/insurance.asp [https://perma.cc/XEQ7-VW4X] (last updated July 29, 2020).

[35] *Id.*

[36] *Id.* ("Insurance policies are used to hedge against the risk of financial losses, both big and small, that may result from damage to the insured or her property, or from liability for damage or injury caused to a third party.").

[37] *See, e.g.*, Julia Kagan, *War Exclusion Clause*, INVESTOPEDIA, https://www.investopedia.com/terms/w/war-exclusion-clause.asp [https://perma.cc/T8F3-S7ZD] (last updated June 23, 2020).

[38] *See, e.g.*, *id.* ("Because most insurance companies would be unable to remain solvent, let alone profitable, if an act of war suddenly presented them with thousands or millions of expensive claims, auto, homeowners, renters, commercial property, and life insurance policies often have war exclusion clauses.").

[39] *Id.* ("Insurance companies typically won't cover damages caused by war for clear reasons. If war breaks out in a country, it could cause a catastrophic amount of damage that would likely bankrupt the insurance company if it were on the hook to cover such damages.").

[40] Andre Beattie, *The History of Insurance in America*, INVESTOPEDIA, https://www.investopedia.com/articles/financial-theory/08/american-insurance.asp [https://perma.cc/6LAW-58U5] [hereinafter Beattie, *History of Insurance*] (last updated Dec. 11, 2019).

[41] *Id.*

[42] *Brief History*, INS. INFO. INST., https://www.iii.org/publications/insurance-handbook/brief-history [https://perma.cc/HG7G-4XDK] [hereinafter *Property Insurance History*].

[43] *Id.*

aftermath of this incident, property insurance schemes were born, and later spread to the United States.[44]

In colonial America, as cities, built close in proximity and almost entirely out of wood, began to expand, fears of urban fires, much like the Great Fire of London, became prominent.[45] In 1752, in order to mitigate these concerns, Benjamin Franklin and several other citizens in Philadelphia "founded The Philadelphia Contributionship for the Insurance of Houses from Loss by Fire, modeled after a London firm."[46] From this point, property insurance expanded exponentially, covering homes and businesses both in the United States and abroad.[47] One common ingredient in property insurance policies, which adapted into all-risk insurance coverage, was the relative predictability of the risks that insurers were willing to cover.[48] In fact, insurance coverage specifically excluded risks stemming from unpredictable damages, such as those arising out of war, due to the inability to predict the size and scope of damages that could occur.[49]

"Generally, exclusion clauses protect insurance companies from extraordinarily hazardous risks. War or military exclusion clauses protect insurers against the risk of loss of property or life incident to actual warfare."[50] As such, "[i]f private insurers were to assume the normal risks incident to military service in time of war under ordinary premium rates, they might soon go bankrupt."[51] Historically, courts would "[r]ather [not] penalize the entire nation by causing the bankruptcy of such corporations . . . ."[52] Rather, they would prefer to place the burden on the insured.[53] As is well known, the history of the United States is wrought with war, but, from the very beginning, it was

---

[44] Beattie, *History of Insurance*, *supra* note 40 ("Property insurance was certainly not an unknown concept in the 18th century: England's famed insurer Lloyd's of London had been born in 1688. But it took until the mid-1700s for the American colonies to become prosperous and sophisticated enough to develop the concept.") (citation omitted).

[45] *Id.* ("Much like London in the 1600s, houses at this time were made almost entirely out of wood. Worse yet, the settlements that grew into cities were built close together. This was originally done for security reasons, but as cities grew, developers built homes very close to each other for the same reasons they do today—to fit as many homes as possible on their development plots. Although much of Philadelphia was built with wide streets and brick or stone structures, conflagrations were still a concern.").

[46] *Id.*

[47] *See Property Insurance History*, *supra* note 42.

[48] *See* Sidney I. Simon, *The Dilemma of War and Military Exclusion Clauses in Insurance Contracts*, 19 AM. BUS. L.J. 31, 31 (1981) [hereinafter Simon, *Dilemma of War Exclusion Clause*].

[49] *Id.*

[50] *Id.* "Two important considerations on the part of insurance companies necessitate such exclusions: the inability of insurance companies properly to gauge premiums to cover those risks, and the companies' need to protect against financial disaster which could result from wholesale death or destruction occurring from actual warfare." *Id.*

[51] *Id.*

[52] *Id.*

[53] *Id.*

understood that all-risk insurance policies would not be available to cover damages that took place in the aftermath of war.[54]

"Historically, war exclusions applied only during the interval between the declaration of war and the signing of a peace treaty."[55] Entities that operated in a way which made them prone to war-related injury were still not without recourse.[56] War-risk insurance, a type of coverage specifically tailored to cover damages of the kind that war exclusion clauses did not, provided an alternative option for consumers.[57] These war-risk insurance policies were seen as early as the Civil War when insurance companies wrote life insurance policies given the unique risk to life that war presented.[58] Later, during the Second World War, the United States instituted the War Damage Insurance Corporation: "[a] government financial protection arm created . . . to provide coverage for war risks that were not being covered by existing policies. The coverage was provided by the U.S. government and it compensated American nationals who owned property that was damaged by acts of war."[59] "Prior to World War II, the

---

[54] Michael Sean Quinn, *A Look at Invoking War Exclusions*, INS. J. MAG. (Oct. 8, 2001), https://www.insurancejournal.com/magazines/mag-legalbeat/2001/10/08/18482.htm [https://perma.cc/4DLY-B2WC] [hereinafter Quinn, *War Exclusion Invocation*].

[55] *Id.* As will be discussed shortly, modern versions of war exclusion clauses are not so rigid. In fact, "[m]ost exclusions currently in use exclude otherwise covered injuries resulting from war, whether 'declared or undeclared.'" *Id.*; *see also* discussion *infra* Part III.

[56] *See* Quinn, *War Exclusion Invocation*, *supra* note 54.

[57] Julia Kagan, *War Risk Insurance*, INVESTOPEDIA, https://www.investopedia.com/terms/w/war-risk-insurance.asp [https://perma.cc/X6G3-7JEG] [hereinafter Kagan, *War-Risk Insurance History*] (last updated July 8, 2020). Kagan further explains that:

> War risk insurance is an insurance policy that provides financial protection to the policyholder against losses from events such as invasions, insurrections, riots, strikes, revolutions, military coups, and terrorism. Auto, homeowners, renters, commercial property, fire, and life insurance policies often have *war exclusions*. With these exclusions, *the policy will not pay* for losses from war-related events. Because a standard insurance policy *may specifically exclude* war risk, it is sometimes possible to purchase a separate war risk insurance rider.

Id. (emphasis added).

[58] *See Property Insurance History*, *supra* note 42. "War risk insurance may cover perils such as kidnappings and ransom, sabotage, emergency evacuation, worker injury, long-term disability, and loss or damage of property and cargo." Kagan, *War-Risk Insurance History*, *supra* note 57.

[59] *War Damage Insurance Corporation*, FIN. REFERENCE, https://www.finance reference.com/learn/war-damage-insurance-corporation [https://perma.cc/SW8L-5FW2]; *see also* Jason Fernando, *War Damage Insurance Corporation*, INVESTOPEDIA, https://www.investopedia.com/terms/w/war-damage-insurance-corporation.asp [https://perma.cc/SM8E-575H] [hereinafter Fernando, *War Damage Insurance Corporation*] (last updated Sept. 24, 2020) ("Officially, the War Damage Insurance Corporation was created through the War Damage Insurance Act of 1941. Understandably, many Americans of that time were concerned that the ongoing war could potentially lead to significant physical damage in the United States. In order to protect their personal possessions, citizens sought

U.S. government did not consider individuals automatically entitled to compensation for war-related damage to their private property."[60] This changed, however, after World War II as "governments in the United States and Europe increasingly adopted the view that individuals should be compensated for private property damage caused by war, given that these acts of war are beyond the control of those parties."[61] The United States again, modeled these coverage policies after the U.K.'s.[62]

Modern war-risk insurance policies provide coverage to "[t]hose entities which have risk exposure to the possibility of sudden and violent political upheavals . . . ."[63] These policies, however, are not without caveats themselves.[64] Just like all-risk insurance provides coverage against *predictable* damages through the use of exclusionary clauses, so too did war-risk insurance.[65] With the evolution of warfare, however, ordinary all-risk and war-risk insurance policies came into question, as the traditional definition of warfare had begun to change. As a formal declaration of war between two state actors became increasingly rare, insureds attempted, on a more consistent basis, to recover damages from insurance providers, even if exclusionary clauses would have normally barred recovery.[66]

An example of the evolution of modern warfare was most clearly seen in the aftermath of the attacks on September 11, 2001. The heinous acts committed on that day led to an "insurance catastrophe with . . . insured losses as high as $72 billion."[67] As opposed to the attacks that occurred at Pearl Harbor during the Second World War, the attacks on 9/11 did not take place after a formal declaration of war, nor were they conducted by a state actor.[68] Thus, the attacks

---

to insure against this risk by buying insurance from private providers. However, from the perspective of private insurers at this time, the potential scale of the damage from war could be so vast that they could not offer these sorts of contracts in a profitable manner. In order to make those policies profitable, the premiums they would need to charge would be so high as to be unaffordable to most customers. As a solution to this impasse, the government stepped in to provide this type of insurance to the public at a subsidized rate.").

[60] Fernando, *War Damage Insurance Corporation*, *supra* note 59.

[61] *Id.*

[62] *Id.*

[63] Kagan, *War-Risk Insurance History*, *supra* note 57.

[64] "[M]ost insurance policies include war exclusion clauses which explicitly exempt the insurer from having to cover damages caused by war." Fernando, *War Damage Insurance Corporation*, *supra* note 59.

[65] *See* Kagan, *War-Risk Insurance History*, *supra* note 57.

[66] *Id.* ("The war exclusion clause became a hot issue in the insurance industry following the Sept[ember] 11, 2001, terrorist attacks on New York City and Washington D.C. The attacks caused an estimated $40 billion in insurances losses. The threat of further terrorist attacks or hijackings made the insurance industry leery of issuing war risk policies.").

[67] Quinn, *War Exclusion Invocation*, *supra* note 54.

[68] *Id.* ("The attack on Pearl Harbor was an act which initiated a state of war. There were legal controversies at the time as to whether it constituted war. Then again, the attack on Pearl Harbor is sharply distinguished from the attack on the World Trade Center. The attack

on 9/11, by almost no definition, would qualify as an act of war, especially under the traditional definition of warfare.[69] As such, war-risk or hostile-act exclusionary clauses, as applied in the *insurance* context, did not apply to those attacks.[70]

In a very similar sense, cyber-attacks are conducted by a range of different actors. Many times, attacks are conducted by rogue actors, completely independent of state-sponsorship, targeting non-state entities, and are presented in a way that appears to be the antithesis of traditional warfare.[71] State-sponsored cyber warfare, on the other hand, presents the closest example of a formal act of war against another state.[72] But often times targets of such attacks are non-state actors (similar to the attacks on 9/11).[73] "[A] wide range of states, including the United States, Russia, China, Iran, and Vietnam have offensive and defensive cybersecurity operations and capabilities."[74] As such, certain "[a]ctors will often leverage these threats that, in the very least, support more

---

on Pearl Harbor was an assault on a military installation for an obviously military purpose, whereas the World Trade Center is not a legitimate military target, and there [had] been no military follow-up.").

[69] *Id.*

[70] *Id.* But see generally *In re* September 11 Litig., 751 F.3d 86 (2d Cir. 2014), which noted that, in the *environmental* cleanup context (under CERCLA), the attacks of September 11, 2001 *did*, in fact, constitute an act of war because under the act, the term "act of war" is to be broadly construed. The court explains, "[t]his reading is not at odds with precedent that 'act of war' is construed narrowly in *insurance* contracts." *Id.* at 92 (emphasis added). "The purpose of an all-risk insurance contract is to *protect against any insurable loss not expressly excluded by the insurer or caused by the insured." Id.* at 92–93 (emphasis added). "The experienced all risk insurers should have expected the exclusions drafted by them to be construed *narrowly* against them, and should have calculated their premiums accordingly." *Id.* at 93 (emphasis added) (quoting Pan Am. World Airways, Inc. v. Aetna Cas. & Sur. Co., 505 F.2d 989, 1003–04 (2d Cir. 1974)). "A narrow reading of a contractual 'act of war' exclusion thus achieves the parties' *contractual intent*, insulating the policyholder from loss. *The remedial purpose of CERCLA is both different and unrelated*." *Id.* (emphasis added). This suggests that *context*, in fact, is of imperative importance. All-risk insurance policies are construed narrowly given the nature of contract whereas other legislative acts (e.g. CERCLA) may carry broader scopes. As such, an "act of war," declared both after the attacks on September 11th and after the Not-Petya attack may be *called* an "act of war," but whether an entity becomes liable (such as an insurer), depends upon the context. An all-risk insurance policy tends to show that such attacks would need to be *specifically* excluded and will not be broadly interpreted.

[71] *See* Sarah Rutherford, *Why Do Hackers Commit Cyber-Attacks?*, FICO: BLOG (Mar. 6, 2017), https://www.fico.com/blogs/why-do-hackers-commit-cyber-attacks [https://perma.cc/DX8K-K55Q] (analyzing why ad-hoc hackers conduct cyberattacks and pointing to three over-arching reasons: 1) for financial gain, 2) to make a political or social point, and 3) for the intellectual challenge).

[72] Caleb Townsend, *Cyber Warfare: Modern Front-Lines*, U.S. CYBERSECURITY MAG., https://www.uscybersecurity.net/cyber-warfare/ [https://perma.cc/XG6H-LF4W].

[73] *Id.*

[74] *Id.*

traditional means of warfare."[75] There are notable examples of a state actor using cyber warfare against other entities. For example, the United States used a cyberweapon called Stuxnet as a part of Operation Olympic Game, which was used to infiltrate factory computers and to sabotage Iran's uranium enrichment facility.[76] Still, damages that ensued from attacks such as these do not present the types of traditional damages that occur in the aftermath of warfare (i.e. physical property damage).[77] The active question remains whether even these *cyberwarfare* attacks would fall under war-risk or hostile act exclusionary clauses. As a result, an analysis of judicial precedent, discussing this very question, would be prudent.

III. WAR EXCLUSION LITIGATION

A. *Relevant Precedent Regarding War-Risk and Hostile Act Exclusionary Clauses*

In order to understand how courts should rule on pending litigation involving exclusionary clauses in the aftermath of a cyber-attack, precedent is incredibly valuable. Historically, there is a dearth of litigation involving hostile act and war-risk exclusionary clauses as there is usually little need to invoke them, given the relatively straightforward nature of most property insurance claims. Of importance, however, will be the most relevant precedent decided in various federal courts. Most property insurance policies are held with private insurance providers and resulting litigation from unresolved claims can be brought in state or federal court.[78] Still, with limited precedent available, relevant federal case law will most likely be a helpful barometer for how state courts are likely to rule on the pending litigation.

---

[75] *Id.* This presents an interesting question in the insurance context and especially in the context of the NotPetya attack. Russia, who was actively involved in a "traditional war" with the Ukraine, used the NotPetya attack to topple the Ukrainian *financial* sector. *See supra* notes 1–11 and accompanying text. The target was not the Ukrainian state but rather one financial sector. The target surely was not the vast array of multinational companies that the attack affected. Surely, this cannot fit under the traditional definition of war, just as the attacks on 9/11 did not either.

[76] Townsend, *supra* note 72. State actors can launch cyberwarfare attacks for a myriad of different reasons, including to support general militaristic goals, to attack civilian based targets to take down needed functions of a target state, and finally to practice "hactivisim" (i.e., acts of cyberwarfare that attempt to encourage a political agenda). *Id.*

[77] *See* Boyle, *supra* note 33.

[78] Evan S. Schwartz, *Considerations When Suing an Insurance Company*, SCHWARTZ, CONROY & HACK, PC: BLOG, https://schlawpc.com/blog/considerations-suing-insurance-company/ [https://perma.cc/D5MX-Gcz4] ("If the lawsuit involves more than $75,000 that is owed to your client, you may have the option to bring the case in Federal Court rather than State Court.").

1. *Precedent Upholding Exclusionary Clauses*

In 2002, the Second Circuit heard a case involving Russian operatives who seized a shipment of frozen food that was sent by Multifoods Corporation ("Multifoods").[79] Subsequent to the seizure of the shipment, Multifoods sought to recover the damages incurred via its insurance policy with Commercial Union Insurance Company ("Commercial").[80] Commercial was an all-risk insurance provider, meaning that it covered damage to property that could arise in a multitude of different ways, as long as the damages were fortuitous in nature.[81] The court noted that the damages suffered by Multifoods was easily fortuitous as the attack did not reveal any inherent defect, wear and tear, or intentional misconduct of Multifoods.[82] Multifoods had suffered a fortuitous loss and had thus met its burden in showing sufficient loss, meeting the requirement to trigger its coverage policy with Commercial.[83] The burden then shifted to Commercial to show that, although the losses suffered were sufficient, the insurance policy and the exclusionary clauses therein rendered Multifoods's claim for recovery excluded.[84]

Commercial's insurance policy contained a multitude of different exclusions, including a war-risk exclusion in Clause 6 of the policy:

> In no case shall this insurance cover loss damage or expense caused by
> 6.1 war civil war revolution rebellion insurrection, or civil strife arising therefrom, or any hostile act by or against a belligerent power

---

[79] Int'l Multifoods Corp. v. Commercial Union Ins. Co., 309 F.3d 76, 80 (2d Cir. 2002).

[80] *Id.*

[81] *Id.* at 83 (citations omitted). The court explained the burden, stating:

> "All risk coverage covers all losses which are fortuitous no matter what caused the loss, including the insured's negligence, unless the insured expressly advises otherwise. A loss is fortuitous unless it results from an inherent defect, ordinary wear and tear, or intentional misconduct of the insured. An insured satisfies its burden of proving that its loss resulted from an insured peril if the cargo was damaged while the policy was in force and the loss was fortuitous . . . ."

Id. (citations omitted) (quoting Ingersoll Milling Mach. Co. v. M/V Bodena, 829 F.2d 293, 307–08 (2d Cir. 1987)).

[82] *Id.* at 83. The district court did not thoroughly analyze why Multifoods's losses would be considered "fortuitous;" rather, the court just proclaimed that they were as such. *Id.* at 84. Noting New York's burden-shifting requirement, which places the burden on a plaintiff to *prove* that the losses suffered were fortuitous, the Second Circuit held that had Multifoods been able to recover the seized goods, the losses suffered would not have met the necessary requirements for coverage. *Id.* at 83–84. In this case, however, Multifoods was never able to recover the seized goods even after a good-faith effort to attempt recovery. *Id.* at 84. As such, "Multifoods' dispossession from the property was never remedied, and resulted in considerable financial [i.e. fortuitous] loss." *Id.* (citations omitted).

[83] *Id.* at 84–85.

[84] *Id.* at 85.

> 6.2 capture seizure arrest restraint or detainment (piracy excepted), and the consequences thereof or any attempt thereat
>
> 6.3 derelict mines torpedoes bombs or other derelict weapons of war.[85]

In analyzing this exclusionary clause, the court held that it was clear and unambiguous and that the risks discussed were war-related risks.[86] The Second Circuit further noted that as a result of the risks described being "war-related risks," Multifoods' interpretation of the clause—in that the clause only pertained to acts related to war—was correct.[87] The court, however, noted that although the clause related to acts of war, Multifoods' assertion that the exclusion only applied to wartime acts was at best based on ambiguity and at worst an incorrect interpretation.[88] Multifoods argued that its interpretation of the clause only applied to wartime acts based on the caption preceding the clause, which simply stated "War Exclusion Clause."[89] But the insurance policy had captions before every exclusionary clause and although the subsequent provisions described were related to the caption, they did not provide a contained framework for what was included in each clause; they acted, rather, as an organizational tool.[90] As a result, the court held that the district court was too expeditious in its holding in favor of Multifoods and remanded the case for an analysis of whether the caption and the clause could be analyzed together or if they should be interpreted apart from one another.[91] This holding is of critical importance: if the two clauses could be analyzed separately, Commercial's interpretation of the exclusionary clause could include peacetime acts listed in the provisions of the clause.[92]

---

[85] *Int'l Multifoods Corp.*, 309 F.3d at 85.

[86] *Id.*

[87] *Id.*

[88] *Id.* at 85–87 ("Although the caption and the content of Clauses 6.1 and 6.3 support Multifoods' argument, several other aspects of the language of the War Exclusion Clause bolster [Commercial's] position that Clause 6.2 excludes even peacetime seizures, and at a minimum suggest existence of an ambiguity.").

[89] *See id.* at 86.

[90] For example, the court noted that Clause 7—the "Strikes Exclusion Clause"—pertained to damages caused by terrorist strikes while also pertaining to labor strikes. *Id.* Although the word "strike" was used in the caption, the subsequent provisions involved a variety of different subjects. *Id.*

[91] *Int'l Multifoods Corp.*, 309 F.3d at 86–88.

[92] *See id.* at 90–91. Of critical importance in this case is the additional fact that Multifoods had another insurance provider, Indemnity Insurance Company of North America ("IINA"). Jay M. Levin & Nina Amster, *Recent Developments in Property Insurance Law*, 39 TORT TRIAL & INS. PRAC. L.J. 719, 730 (2004). IINA also refused to cover Multifoods's insurance claims and cited to the policy's "Free-of-capture-or-seizure clause . . . ." *Id.* This clause *specifically* excluded coverage of damages in the event of "capture, seizure, arrest, [or] restraint . . . and the consequences thereof . . . (*whether in time of peace or war and whether lawful or otherwise*) . . . ." *Id.* (emphasis added) (citation omitted). As such, the clause was unambiguous on its face and, as a result, the seizure of

2. *Precedent Questioning the Use of War Risk and Hostile Act Exclusionary Clauses*

In one of the earliest cases analyzing the use of war risk and hostile act exclusionary clauses, the Second Circuit focused its attention on the terms of property insurance policies and the ambiguities contained within such policies.[93] In doing so, the Second Circuit attempted to remain firmly within the four corners of the insurance policy being disputed, in an attempt to retain the original purpose of the insurance policy.[94] Pan American Airlines ("Pan Am" or "Pan American") brought an action to recover against its insurer in the aftermath of a hijacking attack orchestrated by the Popular Front for the Liberation of Palestine ("PFLP") that took place on one of its aircraft while it was flying over London.[95] The attack led to the loss of a Boeing 747 aircraft, as terrorists subsequently destroyed it.[96]

One tier of insurers that offered coverage to Pan American in the event of damage to its aircraft had policies that "indemnified Pan American against 'all physical loss of or damage to the aircraft,' except for any loss 'due to or resulting from' certain specified exclusions."[97] Included in this first tier of insurers ("all-risk insurers") was Aetna,[98] whose policy did not cover any loss or damage resulting from:

> 1. [C]apture, seizure, arrest, restraint or detention or the consequences thereof or of any attempt thereat, or any taking of the property insured or damage to or destruction thereof by any *Government or governmental authority* or agent (whether secret or otherwise) or by any military, naval or usurped power, whether any of the foregoing be done by way of requisition or otherwise and whether in time of peace or war and whether lawful or unlawful (this subdivision 1. shall not apply, however, to any such action by a foreign government or foreign governmental authority follow-the forceful diversion to a foreign country by any person not in lawful possession or custody of such insured aircraft and who is not an agent or representative, secret or otherwise, of any foreign government or government authority) ["Capture Clause"]

Multifoods' goods by Russian actors was expressly excluded. *See id.* IINA's motion for summary judgment was upheld by the Second Circuit given this unambiguity. *Id.*

[93] Pan Am. World Airways, Inc. v. Aetna Cas. & Sur. Co., 505 F.2d 989, 993 (2d Cir. 1974).

[94] *See id.* at 1022.

[95] *Id.* at 993. This case specifically involved war-risk and hostile-acts clauses given the loss of an aircraft to an identified terrorist group. *See id.* at 994. However, Pan Am had protected the aircraft with "'a more or less seamless mosaic' of insurance policies, distributing among three classes of insurers, the risk of loss depending on the proximate cause of the damage." *Id.* at 993 (quoting Pan Am. World Airways, Inc. v. Aetna Cas. & Sur. Co., 368 F. Supp. 1098, 1101 (S.D.N.Y. 1973)).

[96] *Id.* Fortunately, all lives were spared as passengers were evacuated in Cairo, where the plane was diverted. *Id.*

[97] *Id.*

[98] *Id.*

> ;
>
> 2. [W]ar, invasion, civil war, revolution, rebellion, insurrection or warlike operations, whether there be a declaration of war or not ["War Clause"];
>
> 3. [S]trikes, riots, civil commotion ["Civil Clause"].[99]

In response to the insurance claims brought by Pan American given the loss of their aircraft, all insurers denied coverage.[100] Of importance is the position the all-risk insurers took. They stated that the destruction of the aircraft occurred under circumstances that would be excluded by the capture, war, and civil exclusionary clauses.[101] The district court, unimpressed by the arguments made by the insurers, held that the all-risk insurers failed to meet their burden of proving that the cause of the loss "was fairly within the intended scope of any of the exclusions."[102]

Given the fact that the all-risk insurers cited three different exclusionary clauses and multiple phrases within each clause, the district court held, and the Second Circuit affirmed, that the "reliance on so large a number of exclusions" could reasonably lead to the inference that "each of the exclusions [was] ambiguous or [had] only uncertain application to the facts."[103]

---

[99] *Pan Am. World Airways, Inc.*, 505 F.2d, at 994 (emphasis added). Given the number of insurers providing coverage to Pan American, and in an effort to pursue all-encompassing coverage, which included risks emanating from the possibility of war, Pan American sought coverage from multiple sources to plug the holes that the exceptions created. *Id.* at 994–95. In order to bridge the gap, Pan American sought protection from the London market, which was the only market that provided "war risk" coverage as private American insurers absolved themselves of coverage by including exclusionary clauses such as the one used in this case. *Id.* at 994. Additionally, the United States government provided war risk insurance and as a result Pan American opted for a combination of different policies and insurers. *Id.* at 995. The court summarized this combination as follows:

> If the loss was proximately caused by a clause 1 peril [Capture Clause] . . . or a clause 2 peril [War Clause] . . . Pan American [would] recover $24,000,000, approximately $14,200,000 of which will be paid by underwriters in the London war risk market, and approximately $9,800,000 of which will be paid by the United States government. If the loss was proximately caused by one of the risks described in clause 3 of the all risk exclusions [Civil Clause] . . . , Pan American will recover approximately $24,300,000, of which $14,200,000 will be paid by the London war risk market, and approximately $10,000,000 will be paid in two equal shares by members of [the first-tier insurers]. If none of the all risk exclusions describes the proximate cause of the loss, Pan American [would] recover $24,300,000 from the all risk insurers, one-third from [the first-tier insurers], one-sixth from participants in the London all risk market, and one-half from members of the AAU.

Id. at 995.

[100] *Id.* at 996.

[101] *Id.* at 994–96.

[102] *Id.* at 998.

[103] *Id.* at 1005 (citations omitted). The court noted that the "all risk insurers' shotgun approach belies [their] claim that these terms [such as the term "war"] have certain fixed meanings." *Id.*

The Second Circuit noted that the key issue in the case was the proximate cause of the damages that were the *immediate* cause of the damages, or in the court's words the "efficient physical cause of the loss," prohibiting an analysis of the "metaphysical beginnings" that eventually caused the situation in which damages were suffered.[104] The appellate court, relying on different sources of judicial precedent, created a "mechanical test of proximate causation for insurance cases," looking only to the "causes nearest to the loss."[105]

In addition, the court presented the doctrine of *contra proferentem* which became a key component of the court's decision in favor of Pan Am.[106] The doctrine establishes that if terms in an insurance policy are drafted by insurers as between the sophisticated insurance provider and an unsophisticated policyholder, the court must interpret the policy as a reasonable policyholder would.[107] The court noted that the doctrine had "special relevance as a rule of construction when an insurer fails to use apt words to exclude a known risk."[108] In so holding, the court noted that "the risk of a hijacking was well known to the all risk insurers . . . . [In fact,] [t]he specific risk which caused the present loss was known to the all risk insurers at least three months before the inception of the . . . policies."[109] The all-risk insurers failed to update their exclusionary clauses to include threats of hijacking, even after having extensive knowledge of the possibility that such acts could occur, and further failed to use similar terms in their exclusionary clauses that would have covered the act of hijacking.[110] Reading the policy without these terms, the court noted that the "[c]urrent war risk exclusions [did] not appear to be effective against intentional

---

[104] *Id.* at 1006. It continued that:

> [T]he common understanding is that in construing these policies we are not to take broad views but generally are to stop our inquiries with the cause nearest to the loss. This is a settled rule of construction, and if it is understood, does not deserve much criticism, since theoretically at least the parties can shape their contract as they like.

Id. (quoting Queen Ins. Co. v. Globe & Rutgers Fire Ins. Co., 263 U.S. 487, 492 (1924)). This presents an interesting question in the cyber-attack context as, taken literally, *Pan Am.* would suggest the most pertinent cause of damages could be a system malfunction or the spread of worms as opposed to the initiation of the attack and the subsequent proliferation of the attack mechanism. This would almost always preclude insurers from using war exclusionary clauses, as the *cause* of damage may not be hackers sending out a worm but rather would be how the system responded to the attack.

[105] *Pan Am. World Airways, Inc.*, 505 F.2d at 1006–07 (quoting Queen Ins. Co. v. Globe & Rutgers Fire Ins. Co., 263 U.S. 487, 492 (1924)).

[106] *Id.* at 1007.

[107] *See Contra Proferentem*, CORNELL L. SCH. LEGAL INFO. INST., https://www.law.cornell.edu/wex/contra_proferentem [https://perma.cc/JA6N-TJC5] [hereinafter *Contra Proferentem*].

[108] *Pan Am. World Airways, Inc.*, 505 F.2d at 1000.

[109] *Id.*

[110] *Id.* (noting all-risk insurers could have used "hijacking," "act for political or terrorist purposes," "irregular warfare," "intentional damage," "forceful diversion[,]" and "theft" to sufficiently exclude some of the damages incurred as a result of the attack).

damage such as might be caused by hijackings, by bombs placed in aircraft by political activists, by riotous acts, etc."[111]

The court then turned its attention to each of the exclusionary clauses, and specifically, the interpretation of the term "war."[112] Given the court's use of the doctrine of *contra proferentem*, the court adopted a customary definition of war, not one that was technical and would cover the type of attack that Pan Am had suffered from.[113] The court noted that "the loss of the Pan American [plane] was in no sense proximately caused by any 'war' being waged by or between recognized states."[114] Notably, "[t]he PFLP [had] never claimed to be a state."[115] The court concluded:

> The loss of the Pan American [plane] was not caused by any act that is recognized as a warlike act. The hijackers did not wear insignia. They did not openly carry arms. Their acts had criminal rather than military overtones. They were the agents of a radical political group, rather than a sovereign government.[116]

This case is of incredible value, as it may suggest that terms in an insurance contract, especially exclusionary clauses, will be interpreted given the original understanding of both parties[117]—the key analytical question then becomes: what were the actual intentions of the parties when they agreed to the insurance policies? When clear, with sophisticated parties on both ends of the negotiation, *Pan Am.* suggests that the utilization of technical insurance definitions for ambiguous terminology would be the standard procedure.[118] This would mean, in the context of war, that a purposeful action taken by a state actor against another state actor, with little room for any broader interpretation, would be the controlling definition of war, unless the insurer placed specific language in the exclusionary clause that expanded that definition.[119] When exclusionary clauses are ambiguous, or if an unsophisticated party is on one end of the policy negotiation, the ordinary meaning of terminology may be employed.[120] This was the case in *Pan Am.*, given the insurer's failure to carve out a specific

---

[111] *Id.* at 1001.

[112] *Id.* at 1012.

[113] *Id.* The court decided to use the "ancient international law definition [of war]: war refers to and includes only hostilities carried on by entities that constitute governments at least de facto in character." *Id.*

[114] *Pan Am. World Airways, Inc.*, 505 F.2d at 1013.

[115] *Id.*

[116] *Id.* at 1015.

[117] *See id.* at 1004.

[118] *See id.* at 1007, 1015.

[119] *See id.* at 1015 (suggesting a customary meaning of war be utilized for the case as the insurance provider had not provided an exception within their war-risk or hostile-act exclusionary clauses that covered a well-known risk—that of a hijacking attack).

[120] *See Pan Am. World Airways, Inc.*, 505 F.2d at 1015; *Contra Proferentem*, *supra* note 107.

exclusionary clause involving a very well-known risk.[121] This directly correlates to the context of a cyber-attack, given the increasing rate at which these types of attacks occur.[122] Insurers could be tasked with expressly noting cyber-attack in war-risk or hostile-act exclusionary clauses, if the holding in *Pan Am.* is to be closely followed.[123]

More recently, in 2019, the Ninth Circuit heard a case involving the invocation of war-risk and hostile-act clauses in a dispute between Universal Cable Productions, LLC and Atlantic Specialty Insurance Company.[124] The dispute revolved around "plans by a subsidiary of NBC Universal to produce a television show called 'Dig' in Jerusalem in 2014."[125] Suddenly, however,

> [p]roduction on the show was halted, . . . after Hamas began firing rockets into Jerusalem. As a result, Universal Cable had to move its operations outside Jerusalem, at a cost of several hundred thousand dollars. Universal Cable sought reimbursement for these costs under a television production policy issued to it by Atlantic Specialty that provided coverage for first-party losses involving "imminent peril."[126]

---

[121] *See Pan Am. World Airways, Inc.*, 505 F.2d at 1001, 1015.

[122] ACCENTURE SEC. & PONEMON INST., THE COST OF CYBERCRIME: NINTH ANNUAL COST OF CYBERCRIME STUDY 10 (2019), https://www.accenture.com/_acnmedia/PDF-96/Accenture-2019-Cost-of-Cybercrime-Study-Final.pdf#zoom=50 [https://perma.cc/XN9M-UVJV] (noting research has proven that cybersecurity breaches have increased by 67% from 2013 to 2018).

[123] But does this create too heavy a burden on behalf of insurance providers? Are insurers to be tasked with monitoring every possible risk that may occur in the context of a hostile act and carve out express language to protect themselves against these claims? Exclusionary clauses are meant to eliminate coverage for certain types of risk by narrowing the scope of coverage provided by the insuring agreement. Marianne Bonner, *The Purpose of Insurance Exclusions*, BALANCE SMALL BUS., https://www.thebalancesmb.com/Insurance-exclusions-462464 [https://perma.cc/UGA5-D46Q] (last updated Jan. 13, 2019). Outside of the context of war-risk exclusionary clauses, insurance providers that provide other types of exclusionary clauses (i.e. professional service exclusions) are tasked with analyzing inconsistent interpretations that may arise in a dispute initiated by their policyholders, given the fact that courts will provide narrower definitions when exclusionary clauses are taken away, while insurers attempt to craft broad exclusion to maximize the exclusion's cover. *See id.* This would suggest that insurance providers that are not careful in assessing possible misinterpretations in their insurance policies would suffer a penalty of having a court narrow the construction of their exclusionary clauses, favoring the policyholder instead of the provider.

[124] Universal Cable Prods., LLC v. Atl. Specialty Ins. Co., 929 F.3d 1143, 1146–47 (9th Cir. 2019). This case provides an illustration of how courts may question the use of war exclusion clauses and, in particular, begins to question the use of classic definitions of war for incidents involving rogue actors. *Id.* at 1154–55.

[125] Michael F. Aylward, *U.S. Courts Set Their Sights on the War Exclusion*, MORRISON MAHONEY LLP: BLOG (Sept. 10, 2019), https://www.morrisonmahoney.com/blog/470-u-s-courts-set-their-sights-on-the-war-exclusion [https://perma.cc/4863-LQDS] [hereinafter Aylward, *War Exclusion Litigation*].

[126] *Id.*

Upon a showing of a prima facie case of coverage by Atlantic, the burden shifted to the insurer to show that coverage was excluded under a war exclusion clause.[127] Atlantic, in response, noted that the insurance policy included a "four-part exclusion for war," which consisted of the following:

> 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 . . . .[128]

The court dismissed the *contra proferentem* doctrine, rejecting arguments posed by both Atlantic and Universal.[129] Importantly, the court noted that "when

---

[127] *Universal Cable Prods., LLC*, 929 F.3d at 1151.

[128] Aylward, *War Exclusion Litigation*, *supra* note 125. Hamas is not officially recognized by the United States and as such does not come under the classic definition of a nation-state, one of the necessary elements to a declaration of war. *See* Staff, *U.S. State Department Designates Hamas Leader as Terrorist*, REUTERS (Jan. 31, 2018), https://www.reuters.com/article/us-usa-palestinians-hamas/u-s-state-department-designates-hamas-leader-as-terrorist-idUSKBN1FK2IA [https://perma.cc/7LS5-BF6G]. As such, the main issue in the case was whether or not the hostile act of bombing could be considered an act of war or if the attack was carried out by a rogue actor, thus not meeting the requirement of war exclusion clauses. *See* Aylward, *War Exclusion Litigation*, *supra* note 125. Similar to the chief cases discussed in this Note, many cyber-attacks are not conducted by world or state actors. Rather, many hacker groups are directed by state actors to coordinate attacks. *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 [https://perma.cc/SYD7-SHNG] (noting that a U.N. report found that North Korean "cyber actors, many operating under the *direction* of the Reconnaissance General Bureau, raise[d] money for its WMD (weapons of mass destruction) programmes, with total proceeds to date estimated at up to two billion US dollars") (emphasis added). If rogue actors are directed by state officials to carry out a cyber-attack, will that preclude insurance providers from ever using hostile-act or war-risk exclusionary clauses? Will this *require* insurers to draft terrorism or rogue actor clauses as well? This seems to be a daunting task.

[129] *Universal Cable Prods., LLC*, 929 F.3d at 1151–53. Each party argued that the policy should be construed in their favor. Under California law, ambiguities in insurance policies usually favor the insured. *Id.* at 1151 (citing Fireman's Funds Ins. Co. v. Fireboard Corp., 182 Cal. App. 3d 462, 467 (1986)) ("Under the doctrine of contra proferentem, any ambiguity in an exclusion is generally construed against the insurer and in favor of the insured."). If language in the policy was initially proposed by the insured, "language is not construed against the insurer and may even be interpreted against the insured." *Id.* (citing Fireman's Funds Ins. Co. v. Fireboard Corp., 182 Cal. App. 3d 462, 467 (1986)).

two sophisticated parties negotiate the terms of the policy, the insured generally cannot invoke the doctrine of contra proferentem."[130] In this case, Universal had used an insurance broker to aid in negotiating the policy it signed with Atlantic and during negotiation the broker suggested stock language borrowed from other existing insurance policies.[131] Regardless, the broker demonstrated knowledge of the field and as such was not an unsophisticated party, which meant that Universal was aware of the customary usage of terms in the policy, including the term "war" in the policy's war exclusion clause.[132]

In analyzing Atlantic's use of its war exclusion clause, the Ninth Circuit applied a California statute that delineated how terms in insurance contracts must be construed.[133] The statute noted that terms are to be "understood in their ordinary and popular sense, rather than according to their strict legal meaning; unless used by the parties in a technical sense, or unless a special meaning is given to them by usage, in which case the latter must be followed."[134] The Ninth Circuit held that "the district court erred in holding that the war exclusions should be understood in their ordinary and plain sense, instead of applying the special meaning of the terms in the insurance context."[135] As Universal was a sophisticated party that had engaged in business related to the insurance trade, there was no need for the customary use of the term "war" to be applied, rather the technical definition—as it related to the insurance context—would have been the proper application.[136] Universal had provided unrebutted expert evidence that demonstrated "the customary usage of 'war' and 'warlike action by a military force.'"[137] Important to note is the fact that California is not the only state that provides this rule. In fact, most other states and many insurance treatises provide strong support for the overall argument that "popular meanings of these terms do not control in [the insurance] context."[138] Relying on the

---

[130] *Id.* at 1151–52 (citing Garcia v. Truck Ins. Exch., 682 P.2d 1100, 1106 (Cal. 1984)). "Where the policyholder does not suffer from lack of legal sophistication or a relative lack of bargaining power, and where it is clear that an insurance policy was actually negotiated and jointly drafted, we need not go so far in protecting the insured from ambiguous or highly technical drafting." *Id.* at 1152 (quoting AIU Ins. Co. v. Superior Court, 799 P.2d 1253, 1265 (Cal. 1990)).

[131] *Id.* at 1152.

[132] *Id.* at 1153.

[133] *Id.*

[134] CAL. CIV. CODE § 1644 (West 2020).

[135] *Universal Cable Prods., LLC*, 929 F.3d at 1153.

[136] *Id.* at 1153–54. The court noted that "[a]lthough Universal [was] not in the insurance trade, it [was] a sophisticated party that frequently engage[d] in business related to the insurance trade. Moreover, it [was] represented by a broker – who [was] Universal's agent – in the insurance trade." *Id.* at 1153. Further, the court, relying on statutory law, reasoned that even if a party is not engaged in the trade "the party offering customary usage must show the parties had actual or constructive notice of the customary usage." *Id.* at 1153. The court held that, in this regard, Universal had clearly met this burden. *Id.* at 1154.

[137] *Id.* at 1154.

[138] *Id.*

Universal's expert witness and a denial letter written by Atlantic itself, the court applied an insurance customary definition to the term "war."[139]

This term carried a special meaning that required "the existence of hostilities between de jure or de facto governments."[140] "The Ninth Circuit concluded . . . that if Atlantic . . . had wanted to exclude coverage for attacks by terrorist groups, it should have either included a terrorism exclusion in its policy or should have amended the war risk exclusion to encompass terrorist groups."[141] As such, the court held that the damages suffered by Universal were not excluded under the insurance policy. This case, being one of the most recent cases decided in a federal appellate court, will most likely be cited by many insureds in an attempt to narrow the scope of exclusionary clause applicability, focusing on the type of actor that carried out the attack.[142]

B. *Pending Litigation Regarding the Invocation of War-Risk Exclusionary Clauses in the Context of Cyber-Attack*

Two currently pending cases in Illinois and New Jersey state court are of incredible importance. These cases both involve the invocation of war-risk and hostile-act exclusionary clauses in the direct aftermath of the NotPetya attack of 2017.[143] While there are a host of cases pending in the United States and abroad in the aftermath of the NotPetya attack, these two cases directly invoke war-risk and hostile act exclusionary clauses, wherein the main issue is whether such exclusions could be applied in the context of cyber-attack.[144] These cases serve

---

[139] *Id.* Atlantic's denial letter made statements about exclusions for war, which included the meaning of war and other terms. *Id.* War was defined as "'a course of hostility' between '*states or state-like entities*.'" *Id.* (emphasis added). Universal's expert provided further *unrebutted* testimony that Atlantic's insurance policy did not provide a terrorism exclusion, and given insurance customs "if the policy does not contain a terrorism exclusion, there is a reasonable expectation that acts of terrorism by a known terrorist organization, regardless of however else they may be characterized, will be covered." *Id.*

[140] *Id.* As analyzed above, Universal presented a wide range of evidence defining "war" as a hostile act between "sovereign" or "quasi-sovereign states." *Id.* (quoting Holiday Inns Inc. v. Aetna Ins. Co., 571 F. Supp. 1460, 1503 (S.D.N.Y. 1983)).

[141] Aylward, *War Exclusion Litigation*, *supra* note 125.

[142] *See id.* ("The Ninth Circuit's opinion in *Universal Cable* will surely be cited by policyholders as refuting any suggestion that cyber-criminals are state actors whose conduct[] is subject to such exclusions. At the same time, cyber-insurers may push back with respect to whether the industry understanding of 'war' . . . was shared by [the entire industry]. Additionally, the resolution of these issues will be complicated by difficulties of proof with respect to ascertaining the source of these cyber-attacks and the links between the criminals in question and state sponsors.").

[143] *See* Fred Kaplan, *Death, Taxes, and Cyberattacks*, SLATE (Apr. 16, 2019), https://slate.com/news-and-politics/2019/04/cyberinsurance-mondelez-merck-cyberattacks-hacks.html [https://perma.cc/8JL6-9YAV].

[144] *Id.* (noting the key issues presented in the *Mondelēz* and *Merck* cases and suggesting a need for a change in thought to occur wherein cyber-attack is not viewed as a risk that must

as examples of what types of arguments parties to these disputes can make and elucidate the novel issues presented in the context of cyber-warfare, including the possible damages that arise in the aftermath of such attacks.

1. Mondelēz Int'l, Inc. v. Zurich Am. Ins. Co.[145]

In 2017 Mondelēz International, Inc., an American multinational confectionery, food, and beverage holding company,[146] was made a victim to the insidious NotPetya ransomware attack, which resulted in the entity suffering catastrophic losses.[147] Mondelēz's damages were not only reported within the United States, but the entity was also affected in international locations, including at a Cadbury factory in Hobart, Tasmania.[148] In the aftermath of the attack, Mondelēz turned to its IT department for a full assessment of the losses it had suffered.[149] After the assessment was conducted, Mondelēz contacted its all-risk property insurer, Zurich American Insurance Company ("Zurich"), and made a $100 million claim under its policy that was "meant to cover losses incurred from physical loss or damage to electronic data, programs, [or] software caused by the malicious introduction of malicious software code."[150] Zurich eventually denied coverage, citing a war-risk exclusionary clause ("B(2)(a) Exclusion") in its policy.[151] This clause read:

> B. This Policy excludes loss or damage directly or indirectly caused by or resulting from any of the following regardless of any other cause or event, whether or not insured under this Policy, contributing concurrently or in any other sequence to the loss:
>
> . . . .

---

be insured against but rather a reality that needs to be protected against with more sophisticated cybersecurity mechanisms).

[145] Docket, Mondelēz Int'l, Inc. v. Zurich Am. Ins. Co., No. 2018-L-011008 (Ill. Cir. Ct. Oct. 10, 2018).

[146] The company is best known for its development of popular snack brands such as Cadbury, Belvita, Chips Ahoy!, Oreo, Philadelphia, Ritz, Sour Patch Kids, Stride, Trident, Triscuit, and Wheat Thins. *Our Brands*, MONDELĒZ INT'L, https://www.mondelezinternational.com/Our-Brands [https://perma.cc/DH9X-RV73].

[147] The corporation "lost 1,700 servers and 24,000 laptops[,]" leaving WhatsApp as employees' sole method of communication. Satariano & Perlroth, *Insurance Companies Reject Claims*, *supra* note 26. Company leadership was unable to communicate with their staff and was forced to post updates via Yammer, an internal social media platform used by Mondelēz. *Id.* In total, Mondelēz reported over $100 million in damages. *Id.*

[148] *Id.*

[149] Naveen Goud, *Mondelez Files $100M Claim from Zurich Insurance for NotPetya Cyber Attack*, CYBERSECURITY INSIDERS, https://www.cybersecurity-insiders.com/mondelez-files-100m-claim-from-zurich-insurance-for-notpetya-cyber-attack/ [https://perma.cc/L2GH-K9HT].

[150] *Id.*

[151] Mondelēz Complaint, *supra* note 30, ¶ 13.

> 2) a) hostile or warlike action in time of peace or war, including action in hindering, combating or defending against an actual, impending or expected attack by any:
>
> (i) government or sovereign power (de jure or de facto);
>
> (ii) military, naval, or air force; or
>
> (iii) agent or authority of any party specified in i or ii above.[152]

Even though Zurich had the B(2)(a) Exclusion, the policy also expressly covered specific forms of "malicious cyber damage" to electronic and data processing equipment ("Malicious Cyber-Loss Clause") that, to Mondelēz, encompassed the damages that the corporation suffered in the aftermath of the NotPetya attack.[153] In the end, after Zurich had denied coverage, Mondelēz felt the B(2)(a) Exclusion and the Malicious Cyber-Loss Clause were in direct conflict with one another[154] and further, that the B(2)(a) Exclusion did not apply, given its relative vagueness and ambiguity.[155]

---

[152] *Id.*

[153] *See id.* ¶¶ 7–8. Specifically, the insurance policy expressly covered "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 . . . ." *Id.* ¶ 7. Further, the insurance policy covered "'Actual Loss Sustained and EXTRA EXPENSE incurred by the Insured during the *period of interruption directly resulting from the failure of the Insured's electronic data processing equipment or media to operate*' resulting from malicious cyber damage." *Id.* ¶ 8. (emphasis added).

[154] *See id.* ¶ 16 ("[T]he loss and damage for which [Mondelēz] claims coverage under the Policy did not result from a cause or event excluded under Exclusion B.2(a) of the Policy. The two incursions of *malicious* code or instruction into [Mondelēz's] computers did not constitute 'hostile or warlike action' as required by Exclusion B.2(a). Nor was the loss and damage for which [Mondelēz] claims coverage under the Policy directly or indirectly caused by 'hostile or warlike action.'") (emphasis added).

[155] *Id.* ¶ 15 ("Zurich's invocation of 'hostile or warlike action' exclusion to deny coverage for malicious 'cyber' incidents was, on information and belief, unprecedented. Indeed, and also on information and belief, the purported application of this type of exclusion to anything other than conventional armed conflict or hostilities was unprecedented. Accordingly, on this basis alone, Zurich wrongfully denied coverage to [Mondelēz]."). Mondelēz argues that "Exclusion B.2(a) is vague and ambiguous, particularly given Zurich's failure to modify that historical language to specifically address the extent to which it would apply to cyber incidents, and therefore must be interpreted in favor of coverage." *Id.* ¶ 16. This assertion mirrors language provided in *Pan Am.*, perhaps in an attempt to note the lack of specificity and outdated nature of the exclusionary clause, signaling to the court that the doctrine of *contra proferentem* should be available. *See supra* note 110 and accompanying text (noting that, in *Pan Am.*, the all-risk insurer's failure to expressly and specifically identify hijacking as a part of the exclusionary clause provided in the policy, led to the conclusion that such threats had not been excluded from coverage). As noted in *Pan Am.*, this doctrine can be used if an exclusionary clause is far too vague or fails to expressly exclude a threat that already is or will soon become highly prominent, and if used, would normally favor the policyholder's interpretation as opposed to the insurer's interpretation, as common practice would require being as specific as possible in order to exclude coverage. *See supra* notes 121–23 and accompanying text.

Mondelēz asserted that, in accordance with its agreement with Zurich, it provided prompt notice and all required information, fully complying with its insurance policy.[156] It noted that in response, Zurich publicly and privately defined the NotPetya attack as a ransomware attack, and at no time asserted that the attack was an act of war.[157] Importantly, Mondelēz alleged that, in an attempt to continue or assume more business, Zurich had made statements that encouraged new or existing customers to either buy or renew insurance protection to cover risks, the likes of which occurred after the NotPetya attack.[158] In an example of such an announcement, Zurich stated:

> Cybersecurity risks are also growing, both in their prevalence and in their disruptive potential. Attacks against businesses have almost doubled in five years, and incidents that would once have been considered extraordinary are becoming more and more commonplace. The financial impact of cybersecurity breaches is rising, and some of the largest costs in 2017 related to ransomware attacks, which accounted for 64% of all malicious emails. Notable examples include the WannaCry attack—which affected 300,000 computers across 150 countries—and NotPetya, which caused quarterly losses of USD 300 million for a number of affected businesses.[159]

Mondelēz, dissatisfied with the denial of coverage, asserted that Zurich allegedly "recognized . . . [that] coverage denial was wrongful and improper, and further recognized the potential for [Mondelēz] to initiate immediate litigation that would publicize Zurich's ill-advised coverage denial in a manner that would adversely impact its dealings with actual and prospective policyholders," and proceeded to rescind its denial to avoid litigation publicity.[160] Zurich then offered a $10,000,000 "partial payment" toward Mondelēz's claim, to which Mondelēz refused, and instead sought a meeting to discuss the claim.[161] Mondelēz asserted that Zurich continued to avoid the full

---

[156] Among other information, Mondelēz provided Zurich with "(i) . . . information quantifying and substantiating the extent of [Mondelēz's] losses; and (ii) access to [Mondelēz] employees as well as consultants retained by [Mondelēz] to provide explanations pertinent to [the] claim." Mondelēz Complaint, *supra* note 30, ¶ 11.

[157] *Id.* ¶ 12 ("Zurich publicly and, on information and belief, in its non-public dealings with actual and prospective policyholders who were considering the purchase or renewal of insurance coverage from Zurich, portrayed the NotPetya malware as a form of 'ransomware' that merited the continued (if not increased) purchase of coverage from Zurich.").

[158] This, again, may be a signal from Mondelēz counsel for the court to follow precedent—this time focusing on *Universal Cable Prods., LLC*, because, in that case, the court noted that the policyholder had made statements in its own writing that contradicted an interpretational expansion on the term "war." *See supra* note 140 and accompanying text (noting Atlantic's (i.e. the insurer's) denial letter that contained statements referring to the "traditional" definition of war, suggesting the interpretation be limited to the traditional usage of the term).

[159] Mondelēz Complaint, *supra* note 30, ¶ 12.

[160] *Id.* ¶¶ 17–18.

[161] *Id.* ¶¶ 19–20.

insurance claim, and in reliance on the formal rescission of denial, did not pursue litigation when it had the full capability of doing.[162] After a prolonged back-and-forth, with no consensus on the insurance claim, Mondelēz alleged that Zurich reasserted their declination of coverage, based solely on the B(2)(a) Exclusion, even though Zurich's initial denial—grounded in this exclusionary clause—had been formally rescinded.[163] This resulted in Mondelēz bringing four claims against Zurich, asserting two breaches of contract,[164] promissory estoppel,[165] and vexatious and unreasonable conduct.[166]

In response, Zurich broadly rejected the allegations made by Mondelēz and reaffirmed its reliance on the B(2)(a) Exclusion.[167] Further, Zurich stated that certain exclusionary clauses, including a "Terrorism Exclusion" ("B(2)(f) Exclusion")[168] were left out of the complaint, and that in fact, the NotPetya

---

[162] *Id.* ¶¶ 20–21. Mondelēz claims that,

> [i]n reliance upon Zurich's representations concerning (i) the recession of its denial of coverage based upon Exclusion B.2(a); and (ii) the resumption of its adjustment of [Mondelēz's] insurance claim, including the advance of an unconditional $10,000,000 partial payment, [Mondelēz] refrained *to its detriment* from instituting immediate litigation challenging the June 1, 2018 denial letter. [Mondelēz] instead agreed to meet with Zurich representatives regarding adjustment and payment of its insurance claim. [Mondelēz] would not have done so *were it not for these explicit representations and promises* from Zurich.

Id. ¶ 20 (emphasis added).

[163] *Id.* ¶ 21.

[164] *Id.* ¶¶ 23–32. The first breach of contract claim asserted that Zurich had an insufficient basis for declining coverage under the B(2)(a) Exclusion and further asserted that the reassertion of denial, after rescinding its initial denial was a breach of the policy. *Id.* ¶¶ 23–28. The second breach of contract claim asserted that the formal rescission of denial and the $10,000,000 offer were contractually binding decisions that Zurich then reneged on, breaching the insurance policy. *Id.* ¶¶ 29–32.

[165] Mondelēz Complaint, *supra* note 30, ¶¶ 33–38. This claim asserted that Mondelēz had relied upon Zurich's promises regarding the rescission of denial and initial offer for coverage and that Mondelēz had foregone litigation in reliance on these promises. *Id.* ¶¶ 34–35.

[166] *Id.* ¶¶ 39–41. Mondelēz asserted that Zurich had been unreasonable and vexatious in refusing to honor its promises and then reasserting its denial of coverage, which led to Mondelēz being forced to incur burden, expense, and disruption. *Id.*

[167] Defendant's Answer and Additional Defenses ¶¶ 1, 46, Mondelēz Int'l, Inc. v. Zurich Am. Ins. Co., No. 2018-L-011008, 2018 WL 8951011 (Ill. Cir. Ct. Oct. 10, 2018) [hereinafter Zurich Answer].

[168] *Id.* ¶ 47. This Exclusion states that the policy:

> excludes loss or damage directly or indirectly caused by or resulting from any of the following *regardless of any other cause or event,* whether or not insured under this Policy, contributing concurrently or in any other sequence to the loss: . . . (i) direct loss or damage by fire which results from any other applicable exclusion in the Policy, including the discharge, explosion or use of any nuclear device, weapon or material employing or involving nuclear fission, fusion or radioactive force, whether in time of

attack was a form of terrorism.[169] With regard to Mondelēz's allegation that Zurich had made a statement to encourage existing policyholders to renew policies and for new customers to attain insurance coverage, Zurich claimed that it was not the author of the statement, and that it had appeared in a General Global Risk Report in 2018.[170] In its response, Zurich also admitted to many assertions made by Mondelēz, including that: the attack was a form of malware machine code or intrusion, that Mondelēz had given Zurich notice of the attack's damage on its property, that it had offered Mondelēz $10,000,000 (subject to certain terms that Mondelēz had not agreed to), and that the rescission of its primary denial of coverage was done in good faith, in order to promote negotiation.[171]

This case casts light onto incredibly important issues that may set the stage for future litigation regarding insurance coverage of damages incurred in the aftermath of a cyber-attack. Likely to be at issue is the doctrine of *contra proferentem* given Zurich's reliance on what seems to be broad, ambiguous clauses in both the B(2)(a) and B(2)(f) Exclusions. Relying on precedent, this doctrine may also be invoked given what seems to be a conflict in the policy between the Exclusionary Clauses and the Malicious Cyber-Loss Clause, which Zurich did not address in its Answer. If the court concludes that the clauses were far too ambiguous, this may cause a domino effect to ensue, wherein insurers would be required to be much more specific in their insurance policies in order to try to exclude losses incurred in the aftermath of cyber-attack.[172] Further, if

---

> peace or war and regardless of who commits the act [or;] (ii) any coverage provided in the TIME ELEMENT section of this Policy or to any other coverages provided in this Policy.

Id. (emphasis added). The Exclusion further noted that "any act which satisfies the definition of *terrorism* shall not be considered to be vandalism, malicious mischief, riot, civil commotion, or any other risk of physical loss or damage covered elsewhere in [the] Policy." *Id.*

[169] *Id.* ¶ 47.

[170] *Id.* ¶ 12.

[171] *See generally id.*

[172] *See infra* Part IV.A. (suggesting that if the doctrine of *contra proferentem* is to be used in these cases, insurance providers would have to draft insurance policies with an incredible specificity in order to mitigate possible misinterpretations on behalf of policyholders). This may seem like an inequitable solution as policyholders can quite possibly hide behind the veil of misinterpretation and then use such factors to initiate litigation against their insurance providers in the event of a dispute involving an ambiguous Exclusionary Clause. But courts have generally been reluctant to use the doctrine of *contra proferentem*, unless it is deemed *absolutely necessary*. *See* Schering Corp. v. Home Ins. Co., 712 F.2d 4, 10 n.2 (2d Cir. 1983) ("The trial court erroneously invoked this doctrine because *contra proferentem* is used only *as a matter of last resort, after all aids to construction have been employed but have failed* to resolve the ambiguities in the written instrument.") (emphasis added). This would force parties like Mondelēz to show that even after all extrinsic evidence has been analyzed, there is no common understanding with respect to the Exclusionary Clauses or to the apparent conflict between the Exclusionary Clauses and the Malicious Cyber-Loss Clause.

the court is to conclude that, in the event there are two conflicting clauses, the interpretation of the policyholder is to be followed, insurers would need to change their policies in a way that would almost have to predict what a reasonable policyholder would assume when first attaining insurance coverage.

2. Merck & Co., Inc. v. ACE Am. Ins. Co.[173]

Pharmaceutical giant Merck was also made a victim to the vicious NotPetya attack of 2017.[174] On the day of the attack, employees who arrived at work at Merck's enormous campus just north of Philadelphia were met with widespread systemic failure.[175] Operations were halted for a period of two weeks, leading to catastrophically large damages.[176] At the end of 2017, Merck estimated that the attack caused $870 million in damages.[177] Merck turned to its all-risk property insurers for relief.[178] "[T]he company was covered—after a $150 million deductible—to the tune of $1.75 billion for catastrophic risks including the destruction of computer data, coding, and software."[179] Unlike Mondelēz, Merck had an army of over thirty insurers, each one denying coverage, citing war-risk and hostile action exclusionary clauses.[180]

Merck asserted that each of the defendant insurance providers offered all-risk policies that covered any and all risks to physical property, not otherwise excluded.[181] Merck argued that coverage under the insurance policies included:

> (a) physical loss or damage to property, including destruction, distortion, or corruption of *computer data, coding, program, or software*; (b) business interruption; (c) extra expenses; (d) expenses to reduce loss; (e) research and

---

[173] Docket, Merck & Co., Inc. v. Ace Am. Ins. Co., No. UNN-L-002682-18 (N.J. Super. Ct. Law Div. Aug. 2, 2018).

[174] Voreacos et al., *Merck Litigation Summary*, *supra* note 1.

[175] *Id.*

[176] *Id.* ("In all, the attack crippled more than 30,000 laptop and desktop computers at the global drugmaker, as well as 7,500 servers, according to a person familiar with the matter. Sales, manufacturing, and research units were all hit. One researcher told a colleague she'd lost 15 years of work.").

[177] *Id.* The damages because:

> Among other things, NotPetya so crippled Merck's production facilities that it couldn't meet demand that year for Gardasil 9, the leading vaccine against the human papillomavirus, or HPV, which can cause cervical cancer. Merck had to borrow 1.8 million doses—the entire U.S. emergency supply—from the Pediatric National Stockpile. It took Merck 18 months to replenish the cache, valued at $240 million.

Id.

[178] *Id.*

[179] *Id.*

[180] Voreacos et al., *Merck Litigation Summary*, *supra* note 1.

[181] Complaint for Declaratory Relief and Compensatory Damages ¶ 32, Merck & Co., Inc. v. ACE Am. Ins. Co., No. UNN-L-002682-18, 2018 WL 8415885 (N.J. Super. Ct. Law Div. Aug. 2, 2018) [hereinafter Merck Complaint].

> development expenses; (f) finished stock and merchandise for sale; (g) extra costs to temporarily continue the movement of goods and materials; and (h) loss adjustment expenses.[182]

All Merck insurers, including reinsurers, denied coverage after Merck had notified them of the attack.[183] Merck utilized reinsurers as a supplementary insurance provider in addition to their all-risk insurance providers.[184] These reinsurers were tasked with covering risks associated with "physical loss or damage to property through its captive insurance company, International Indemnity . . . ."[185] The reinsurance policies provided materially the same coverage as the all-risk insurance policies.[186] The reinsurers defended their denial of these claims using the same theory as the all-risk insurers: that the attack was excluded as a result of it being an act of war or terrorism.[187]

As a result of both the all-risk insurers and reinsurers rejecting Merck's claim, this litigation was initiated. Merck asserted that the NotPetya attack caused a widespread disruption that led to the damages that were expressly covered by the all-risk insurance policies it held with various insurance providers.[188] Merck further argued that no exclusionary clause, war-risk, or terrorism applied to the attack and brought a claim for declaratory relief, asserting that the court should acknowledge that the exclusionary clauses did

---

[182] *Id.* ¶ 34 (emphasis added).

[183] *Id.* ¶¶ 45–47 (" . . . on or about March 30, 2018, certain, but not all, of the Insurers and Reinsurers reserved the purported right to deny coverage on the purported ground that the [NotPetya attack] was an act of war or terrorism purportedly excluded from coverage under the Policies").

[184] *Id.* ¶ 39.

[185] *Id.* ¶ 37. "Reinsurance is a form of insurance purchased by insurance companies in order to mitigate risk. Essentially, reinsurance can limit the amount of loss an insurer can potentially suffer. In other words, it protects insurance companies from financial ruin, thereby protecting the companies' customers from uncovered losses." Staff, *What Is Reinsurance?*, MOTLEY FOOL (May 29, 2017), https://www.fool.com/knowledge-center/what-is-reinsurance.aspx [https://perma.cc/5SMQ-U8GU]. Simply, reinsurance is insurance for insurance providers. *Id.* "If an insurer has too much exposure to a potentially costly event, then that event could cause the company to go bankrupt or even shut down if it's unable to cover the loss." *Id.*

[186] Merck Complaint, *supra* note 181, ¶ 39.

[187] *Id.* ¶¶ 46–47.

[188] *Id.* ¶ 41. ("On or about June 27, 2017, Merck experienced a network interruption event (the 'Event'), resulting from a malware infection, which involved the destruction, distortion, or corruption of its computer data, coding, program, or software resulting from malware presented as ransomware.").

not apply.[189] Further, Merck brought an additional claim for declaratory relief,[190] accompanying a claim for breach of contract.[191]

As there are over thirty insurance and reinsurance providers in this case, Ace American Insurance's ("Ace") response will serve as an example for each of the all-risk insurance providers' responses to Merck's claims, given that it covers many of the defenses that each of the insurance providers provided in response to Merck's complaint.[192] Similar to Zurich's response in *Mondelēz*, Ace also relied on its exclusionary clauses as an affirmative defense to the claims made by Merck.[193] Ace asserted that the NotPetya attack was not covered under the policy because it was either an act of war or an act of terrorism.[194] Ace's policy with Merck contained both war-risk and terrorism exclusionary clauses.[195] The war-risk exclusionary clause stated:

> This Policy does not insure the following:
>
> **A.** 1. Loss or damage caused by hostile or warlike action in time of peace or war, including action in hindering, combating, or defending against an actual, impending or expected attack:
>
> (a) by any government or sovereign power (de jure or de facto) or by any authority maintaining or using military, naval, or air forces;
>
> (b) or by military, naval, or air forces;
>
> (c) or by an agent of such government, power, authority, or forces;
>
> . . . .
>
> 3. Loss or damage caused by rebellion, revolution, civil war, usurped power; or action taken by governmental authority in hindering, combating, or defending against such **occurrence.**[196]

---

[189] *Id.* ¶ 55. (asking for the court to declare "that no exclusion from coverage under Insurance Policies—including, without limitation, any exclusion for war or terrorism—applies to the Event [(NotPetya Attack)] and/or the resulting loss or damage").

[190] *Id.* Additionally, Merck sought a declaration that the insurers, "under the Insurance Policies, are liable, subject to applicable policy limits, to pay their respective shares of Merck's losses and damages in connection with the [NotPetya Attack]." *Id.*

[191] *See id.* ¶¶ 56–61, 69–74 (outlining breach of contract claims against the all-risk insurance providers and reinsurance providers). Unlike the claims brought in *Mondelēz*, this case only focuses on the ambiguity of the exclusionary clauses written into the insurance policies of both the all-risk insurance providers and the reinsurance providers. *Id.* There are no contradicting clauses and the insurance providers never offered to pay any part of Merck's claims. *See generally id.*

[192] *See* Merck Complaint, *supra* note 181, ¶¶ 5–31.

[193] Answer and Affirmative Defenses of Ace American Insurance Company at 12, Merck & Co., Inc. v. ACE Am. Ins. Co., No. UNN-L-002682-18 (N.J. Super. Ct. Law Div. Aug. 2, 2018) [hereinafter Ace Answer].

[194] *Id.* at 12–13.

[195] *Id.* at 13–15.

[196] *Id.* at 13.

Ace's terrorism exclusionary clause relied on a broad definition of terms related to terrorism[197] and provided a sweeping exclusion.[198]

As in *Mondelēz*, this case presents incredibly important issues regarding insurance coverage in the aftermath of a cyber-attack. Because it does not present the same nuance as was the case in *Mondelēz* (e.g. conflicting clauses, statements made by company leadership, initial offer for coverage that was subsequently rescinded), the court will be more likely to restrict its analysis to the four corners of the policy itself because Merck has only asserted that it relied on the policy and not on any other promises made by its insurance providers. In analyzing the policy, if the court uses the doctrine of *contra proferentem*, the analysis would be focused on whether the exclusionary clauses provided by the all-risk insurers and reinsurers were specific enough to exclude cyber-attacks from coverage.[199] Like in *Mondelēz*, the war-risk and terrorism clauses provided in the *Merck* litigation are broad and non-specific. Interpretation is going to be the key issue and the court's conclusion is likely to shape the American insurance landscape for years to come.[200]

---

[197] The insurance policy contained a definition for an "act of terrorism" which meant

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

Id. at 14. This clause presents a unique question as to whether the NotPetya attack was taken out by a "group of persons acting on behalf of government" for "political purposes" to "influence another government." The court may hold that the NotPetya attack, taken out by Russian operatives, and meant to influence Ukraine, is included in the scope of this exclusion. The clause, however, does not expressly state the risk of cyber-attack and customarily, terrorism is not understood to include cyber-attack. If the court is to use the doctrine of *contra proferentem*, used in the event of ambiguity in an insurance policy, it's most likely that Merck's interpretation would rule the dispute given this relative ambiguity.

[198] The clause excluded "loss, damage, cost, or expense of whatsoever nature directly or indirectly caused by, resulting from, or in connection with any action taken in controlling, preventing, suppressing, or in any way relating to any act of terrorism." *Id.*

[199] This would have the same impact in this case as it would potentially have in *Mondelēz*. *See supra* note 172.

[200] Counsel for Merck, who wrote the complaint, noted that the exclusionary clauses did "not mention cyber events, networks, computers, data, coding, or software; nor do they contain any other language suggesting an intention to exclude coverage for cyber events." Voreacos et al., *Merck Litigation Summary*, *supra* note 1. This statement may signal what is to come. It is entirely plausible that Merck will attempt to assert that, without express specificity, these exclusionary clauses cannot apply. This would be an argument invoking the doctrine of *contra proferentem*. Regardless of how the court rules,

> the NotPetya attack will catapult the U.S. legal system into [murky terrain]. Nation-states for years have been developing digital tools to create chaos in time of war: computer code that can shut down ports, tangle land transportation networks, and bring

IV. THE FUTURE OF CYBERATTACK AND INSURANCE COVERAGE

Having analyzed the history of war-risk and hostile-act exclusionary clauses, and both precedent related to exclusionary clause litigation and pending litigation as a result of the NotPetya attack, the question of how courts should rule and what prophylactic strategies can be adopted to prevent future litigation is of paramount importance. With the rapid development of newer technology, cyber threats are poised to become ever more frequent and sophisticated.[201] As such, crippling damage, the likes of which were seen in the NotPetya attack, can certainly occur again, concerningly at even larger and more destructive levels.[202] Unfortunately, advancements in cybersecurity protocols are still developing and are incredibly expensive.[203] Still, corporate entities have now

---

> down the electrical grid. But increasingly those tools are being used in forms of conflict that defy categorization.

Id.

[201] For an overview of the most recent cyber incidents, the Center for Strategic & International Studies created a tracker that it routinely updates. The Center focuses on "cyber attacks on government agencies, defense and high tech companies, or economic crimes with losses of more than a million dollars." *Significant Cyber Incidents*, CTR. FOR STRATEGIC & INT'L STUD., https://www.csis.org/programs/technology-policy-program/significant-cyber-incidents [https://perma.cc/X2BF-H5Q5] (last updated Jan. 2021). As of the time of this writing, the Center reported over one hundred cyber incidents in 2019 alone, with Microsoft having reported "almost 800 cyberattacks . . . targeting think tanks, NGOs, and other political organizations around the world, with the majority of attacks originating in Iran, North Korea, and Russia." *Id.*; *see also Significant Cyber Incidents Since 2006*, CTR. FOR STRATEGIC & INT'L STUD., https://csis-website-prod.s3.amazonaws.com/s3fs-public/201218_Significant_Cyber_Events.pdf [https://perma.cc/N6N6-24RR] (last updated Jan. 2021). Worthy of note, new cyber-attacks have utilized new innovation in order to counter two-step security protocols, previously considered a safe way to shield a possible attack. *See Significant Cyber Incidents Since 2006*, *supra* note 201.

[202] Although the NotPetya Attack of 2017 is the chief focus of this Note, given its connection with extensive insurance litigation, similar attacks have caused massive damage at a world-wide scale. One of the most potent and prominent attacks has been through the use of ransomware called WanaCrypt0r 2.0 ("WannaCry"). Julia Carrie Wong & Olivia Solon, *Massive Ransomware Cyber-Attack Hits Nearly 100 Countries Around the World*, GUARDIAN (May 12, 2017), https://www.theguardian.com/technology/2017/may/12/global-cyber-attack-ransomware-nsa-uk-nhs [https://perma.cc/6G9C-53AV]. The Kaspersky Lab, a leading cybersecurity research institution, "recorded more than 45,000 attacks in 99 countries, including the UK, Russia, Ukraine, India, China, Italy, and Egypt." *Id.* In general, Ransomware attacks have been steadily rising, targeting vulnerable systems on a global scale. *Id.* "A Los Angeles hospital paid $17,000 in bitcoin to ransomware hackers . . . after a cyber-attack locked doctors and nurses out of their computer system for days." *Id.* Evidence of such attacks makes it clear that cyber-attack has the potential of becoming increasingly frequent, leaving entities vulnerable to catastrophic damage.

[203] *See generally* Gaurav Banga, *How Three Waves of Cybersecurity Innovation Led Us Here*, FORBES (Oct. 10, 2018), https://www.forbes.com/sites/forbestechcouncil/2018/10/10/how-three-waves-of-cyber-security-innovation-led-us-here/ (on file with the *Ohio State Law*

become aware that "cybersecurity is no longer a human-scale problem [but rather a problem that] will require a collaboration between humans and innovative machine learning techniques to meet the challenge of the latest cyber threats."[204]

In the interim, as cybersecurity develops, and as more corporate entities realize the importance of cybersecurity,[205] it seems the most cost-effective solution is to find insurance policies that provide protection in the event of an attack. Although this solution may seem like a reasonable approach to protection from the corporate perspective, it fails to view cyber-attack from a risk-prevention standpoint and shifts the burden of possible attack and subsequent loss to insurance providers that are not generally knowledgeable of the risks they face. If courts hold that *property* insurers, offering robust property policies to corporations in the event of catastrophic property damage, are also to cover loss from cyber-attacks, the incentive for property insurers to provide such robust policies may dwindle. Of importance will be how courts utilize relevant precedent in their war exclusion clause analysis and, in the event of a cyber-attack, if courts should enforce policies while holding war exclusion clauses unenforceable in the context of cyber-attack. Conversely, courts can hold war-risk or hostile-act exclusionary clauses enforceable, preventing the burden being placed on property insurers to cover cyber-attacks. In either event, however, there is a clear loser.

In the event that war exclusion clauses are held unenforceable, all-risk property insurance providers, classically involved in protecting "physical damages to tangible property,"[206] will be made to measure the nexus between the cyber loss suffered by the companies they cover, and the resulting damage

---

Journal) (overviewing the history of changes in cybersecurity innovation, noting new trends and the need for new innovation in fast-developing, tech-focused future).

[204] *Id.* "We live in a world where it appears to be a matter of when, not if, an enterprise is breached. Billions of dollars have been spent on beefing up cybersecurity, but the bad guys keep winning. Securing even a small organization seems quite hard." *Id.*

[205] Of importance will be when and how insureds begin to prioritize cybersecurity, so as to lessen possible cyber risks and reduce the possibility of internal system deficiencies or ignorance being the most important factor in potential vulnerability to breach. For an analysis of internal corporate responsibility and a need to introduce a system of corporate accountability in the context of data breach. *See generally* Lauren Miller, *Cyber Insurance: An Incentive Alignment Solution to Corporate Cyber-Insecurity*, 7 J.L. & CYBER WARFARE 147 (2019). Miller proposes a compulsory, nation-wide adoption of cyber insurance, as a means to "encourage corporations to be proactive about cybersecurity practices through monetary incentives and pressure from insurance carriers to prevent future breaches, and therefore, litigation." *Id.* at 148.

[206] Angela Yu, Note, *Let's Get Physical: Loss of Use of Tangible Property as Coverage in Cyber Insurance*, 40 RUTGERS COMPUTER & TECH. L.J. 229, 230 (2014) [hereinafter Yu, *Cyber Loss as Property Loss*].

to tangible property, as defined by relevant judicial precedent.[207] This measurement will be added to the calculus of understanding what actions are classified as acts of war,[208] and who exactly carried out the attack,[209] two incredibly difficult tasks. This measurement may prove to be exceedingly difficult and also create an opening for insureds to claim damages of small property value but incredibly large systemic or data value—damages being largely intangible in nature.[210]

On the other hand, holding war exclusion clauses unenforceable will leave insureds without recourse while cybersecurity systems are still being developed. Catastrophic damages may cost large corporate entities millions of dollars, while small corporations could cease operations altogether. Additionally, war-risk and hostile-act exclusionary clauses, in a fast-adapting, technological world, may be used indiscriminately to limit coverage to the very type of attack that is becoming one of the most prominent concerns of corporate entities.[211]

---

[207] Insureds, in the aftermath of cyber-attack, can attempt to allege a minimum nexus to tangible property, although most of the losses incurred are due to internal data systems, not just the hardware. By way of example, counsel may suggest "future claimants . . . allege a loss of the computer, particularly when the claimant has an eye toward triggering a defendant's insurance coverage." *Id.* at 247 (quoting William P. Shelley, Richard Bortnick & Samantha Evans, *'Tangible Property' Defined in the Computer Age*, L.J. NEWSL. (Apr. 28, 2011), https://www.lawjournalnewsletters.com/sites/lawjournalnewsletters/2011/04/28/tangible-property-defined-in-the-computer-age/ (on file with the *Ohio State Law Journal*)).

[208] *See supra* Part II.

[209] Adam Shniderman discusses the increasingly problematic task of identifying who is responsible for cyber-attacks and notes that "hostile-or-warlike-action exclusion hinges in part on the perpetrator's identity." Adam B. Shniderman, *Prove It! Judging the Hostile-or-Warlike-Action Exclusion in Cyber-Insurance Policies*, 129 YALE L.J.F. 64, 68–73 (2019) [hereinafter Shniderman, *Issues with Hostile Act or War Exclusion Clauses*].

[210] Travis Toemoe, Peter Yeldham & Alexa Milosevic, *Touch the Edge—is Data "Tangible Property" for the Purpose of Your Insurance Policy?*, KING & WOOD MALLESONS (Mar. 27, 2017), https://www.kwm.com/en/us/knowledge/insights/data-tangible-property-insurance-policy-damage-loss-cover-20170327 [https://perma.cc/M6RM-EGLW]. The authors discuss the difficulties presented in including data and damages that occur as a result of systemic breach, into the accepted definition of tangible property *Id.* There is a case to expand this definition to include data and other cyber property given the ever-increasing prevalence of cyber-crime, even though it is classically regarded as "intangible." *Id.* Intangible property has been defined as "property that has no intrinsic and marketable value, but is merely the representative or evidence of value, such as certificates of deposit, bonds, promissory notes, copyrights and franchises." *Id.* In the modern "big data" age, "[i]t is difficult to see how . . . data has no intrinsic value." *Id.*; *see also* Yu, *Cyber Loss as Property Loss*, *supra* note 206, at 245–47 (discussing strategies for initiating insurance claims for cyber-attack related damages).

[211] *Cyber Ranks as Top Peril for Companies Globally for 1st Time: Allianz Survey*, INS. J. (Jan. 15, 2020), https://www.insurancejournal.com/news/international/2020/01/15/554802.htm [https://perma.cc/5VMQ-5VY4] (reporting that for the first time ever, business have ranked cyber incidents as the number peril to potentially befall a company). Amongst the greatest concerns were cybercrime, causing IT failure, data breach, and business interruption. *Id.*

War exclusion clauses, developed in the event of nation-state against nation-state warfare,[212] wherein the possibility of catastrophic property damage is very real, could be invoked for purposes far too attenuated from their initial purpose.

Still, pending litigation cannot go unanswered and courts will need to find a solution to decide these cases in fair and equitable ways. It is relatively clear, however, that litigation stemming from the invocation of hostile-act or war-risk exclusionary clauses is not a sustainable way for corporations and insurance providers to continue relations. As such, a scrutinization of current insurance policies and the utilization of property insurance to cover cyber-attack risks should be conducted—using a forward-looking perspective—in order to analyze whether newer, more specialized insurance policies would be better for corporate entities to attain. Therefore, in the short-term, as pending litigation will require a decisive outcome, courts should use tools of interpretation[213] that are *uniquely* suited to combat contradicting or ambiguous clauses in insurance policies. Further, the availability of a new federal insurance policy, designed to cover damages that occur in the event of a cyber-attack, can provide a sound solution for the current issues with insurance policies, including the difficulties with valuing insurance claims and discerning responsibility of the exact entity that carried out the attack. This would provide easier answers for both insureds and insurers, reducing litigation costs, while clarifying how corporations should prioritize their cybersecurity needs in a new tech-centered society.

A. *Courts Should Use the Doctrine of* Contra Proferentem *in Deciding Current Cyber-Attack Insurance Litigation.*

As noted in the analysis of the relevant precedent involving the use of war-risk or hostile-act exclusionary clauses, courts will most likely rule on insurance disputes depending on the type of coverage offered, the language in the insurance policy, and the interpretation of this language.[214] Such considerations are difficult, especially in insurance policies that have contradicting provisions or provisions that are expressly ambiguous. Normally, insurance policies are viewed as a contractual obligation between both parties.[215] Large corporations engage in bargaining and use insurance brokers while negotiating the

---

[212] *See supra* Part II.

[213] *See infra* Part IV.A (discussing the doctrine of *contra proferentem* in relevant precedent). This tool seems to be uniquely suited to answer questions when parties to an insurance dispute are uncertain of the exact answer to clausal discrepancy or ambiguity. The following discussion will recommend the use of this doctrine, invoked by the court itself, in order to solve the current disputes now pending.

[214] *See generally supra* Part III.A.

[215] Pan Am. World Airways, Inc. v. Aetna Cas. & Sur. Co., 505 F.2d 989, 1006 (2d Cir. 1974) (quoting Queen Ins. Co. v. Globe & Rutgers Fire Ins. Co., 263 U.S. 487, 492 (1924)) (discussing insurance policies in terms of a contract between two parties).

policies.[216] Other corporations that are incapable of hiring brokers and are unsophisticated parties are, at times, unable to negotiate insurance policies with sophistication.[217] The doctrine of *contra proferentem* aids these parties by allowing the insured's interpretation of the policy to control the dispute. This doctrine seems to be a perfect starting point for a court in order to resolve a dispute between parties involving the language of exclusionary clauses. Additionally, when exclusionary clauses are paired with coverage clauses that seem to be in direct conflict with one another, the doctrine seems to be uniquely suited to provide a decisive interpretation to follow. As noted in the analysis of the pending litigation regarding the NotPetya cyber-attack, both of these situations are currently in dispute.[218]

This is not to say that *contra proferentem* should be used to the advantage of insured parties in every dispute involving insurance claims in the aftermath of a cyber-attack, especially if policies have been negotiated with relatively equal bargaining power on behalf of both parties. But in a vast majority of litigation involving the use of war-risk or hostile-act exclusionary clauses, language is broad and ambiguous, and as shown in *Universal Cable*, this can lead to a dispute regarding customary or technical usage of such terms in how exactly they should be interpreted, even if the dispute is not privy to the doctrine of *contra proferentem*.[219] Specificity is incredibly important, and in insurance policies that do not define terms such as "war" to mean anything other than its customary or traditional meaning, insurers would have an uphill battle in the context of most cyber-attacks.[220] Still, if all-risk insurers provided specified definitions within their policies, they may be able to successfully exclude

---

[216] *See supra* Part IV.A. In *Universal Cable Prods., LLC*, an insurance broker was used, which made both parties sophisticated. 929 F.3d 1143, 1153 (9th Cir. 2019).

[217] *See, e.g.*, Lamps Plus, Inc. v. Varela, 139 S. Ct. 1407, 1417 (2019) (noting the doctrine of *contra proferentem* applies "after exhausting the ordinary methods of interpretation . . . [to resolve] the ambiguity against the drafter based on . . . equitable considerations about the parties' relative bargaining strength"); Aleynikov v. Goldman Sachs Grp., Inc., 765 F.3d 350, 366 (3d Cir. 2014) ("When one side of a contract [is] unilaterally responsible for the drafting, courts apply *contra proferentem* and construe ambiguous terms against the drafter."); Morgan Stanley Grp. Inc. v. New England Ins. Co., 225 F.3d 270, 272, 279–80 (2d Cir. 2000) ("*[C]ontra proferentem* . . . [can be] applied to resolve any remaining ambiguity . . . where the insured had not negotiated coverage terms."); Phillips v. Lincoln Nat'l Life Ins. Co., 978 F.2d 302, 312 (7th Cir. 1992) ("*contra proferentem* does not apply to insurance contracts resulting from arms-length bargaining power between parties of *equal* power") (emphasis added) (citing Eley v. Boeing Inc., 945 F.2d 276, 279–80 (9th Cir. 1991)).

[218] *See supra* Part III.B.

[219] *See Universal Cable Prods., LLC*, 929 F.3d at 1153.

[220] As discussed throughout this Note, cyber-attacks are often conducted by independent cyber-criminals and in only few situations are state actors ever directly involved. As such, the common judicial interpretation of the term "war" would almost never be covered by insurance policies. Examples of how courts have defined war is shown in any of the cases presented in Part III above. *See generally supra* Part III. Normally, a prerequisite to war or warlike operations is aggression on behalf of a state or quasi-state actor directed at another state. *Id.*

policyholders from recovering on claims, regardless of whether or not the policy was negotiated with unequal bargaining power, as was the case in *International Multifoods Corp. v. Commercial Union Ins. Co.*[221]

In addition, courts have noted that the proximate cause of damages are of imperative importance in the analysis of whether an insurance claim and recovery subsequent to damages suffered is possible.[222] In the context of the NotPetya attack, where the worm was initially designed by a state actor to take down the financial sector of another state, the cyberweapon proliferated far beyond the original intent of Sandworm itself.[223] Given the unintended and incidental nature of the proliferation of the attack, the proximate cause of damages suffered by entities worldwide is difficult to surmise.[224] It seems unduly burdensome to require courts to conduct a calculus of the proximate cause of attacks that are intangible in nature and can be the result of vulnerabilities in cybersecurity measures taken by multiple effected entities. In effect, any previous victims from which the attack spread could be the proximate cause of the "fortuitous damages" suffered by the entity seeking coverage by their insurance policy.[225] To avoid this calculus, courts can simply use the doctrine of *contra proferentem* to hear the interpretation of both parties and avoid analyzing the proximate cause analysis. Parties would state their case as to why or why not exclusionary clauses included damages resulting from cyber-attacks and the proliferation of the same, and the court would be able to decide which interpretation to follow without attempting to track the real proximate cause of the damages suffered. This would encourage policyholders and insurers to add as much specificity as possible to the provisions within policies to make abundantly clear that damages are either excluded or covered.

Another important aspect to the current pending litigation regarding cyber-attack insurance disputes is the existence of conflicting clauses in existing insurance policies. A good example of such a conflict can be viewed in the

---

[221] IINA had provided an incredibly specific exclusion in the insurance policy and as such the seizure of Multifoods' goods constituted damages that were excluded from coverage. *See* Int'l Multifoods Corp. v. Commercial Union Ins. Co., 309 F.3d 76, 90–91 (2d Cir. 2002).

[222] *See, e.g.*, Pan Am. World Airways, Inc. v. Aetna Cas. & Sur. Co., 505 F.2d 989, 1006 (2d Cir. 1974).

[223] *See* Greenberg, *Effects of NotPetya*, *supra* note 2.

[224] *See id.*

[225] The NotPetya ransomware attack was caused by a worm that spread from entity to entity in an insidious and indiscriminate manner. As a result of this, would companies like Mondelēz be able to allege that the real proximate cause of the damages they suffered was not the initial introduction of the worm itself but rather the spread of the worm from other entities that were not able to shield themselves from the reach of the attack? Cases like *Pan Am.* would suggest that this is possible and as a result insurance providers would almost never be able to evoke war exclusionary clauses as, even though the attack was directed by a state actor against another state actor, the proximate cause of damages to entities worldwide would be the systemic spread of the worm due to a lack of cybersecurity measures in force. *See Pan Am. World Airways, Inc.*, 505 F.2d at 1006.

Mondelēz case, wherein the insurance policy expressly stated that a failure of Mondelēz's electronic data processing equipment resulting from malicious cyber damage was covered but also stated that hostile or warlike actions were expressly excluded.[226] How are courts to reconcile these conflicting clauses? The court in *International Multifoods Corp.* would suggest that an analysis of the conflicting parts of the policy can and should be done,[227] and the doctrine of *contra proferentem* seems well-suited for this analysis. If the policy had been drafted by the insurer, without negotiation by the insured or a clear statement including cyber-attack in the war exclusionary provision, the court should adopt the interpretation of policyholders (i.e., that cyber-attacks are not covered) to signal to insurers that negotiation must either be complete or an express exclusionary clause delineated, so as to remove any chance of confusion.

B. *The Introduction of a Federal Cybersecurity Insurance Policy*

War-risk and hostile-act exclusionary clauses are not a nuanced idea; they have a rich history and were necessary additions in order to keep risk coverage predictable and to prevent insureds from abusing insurance policies in the event of high-value damages pursuant to the destruction that war elicits.[228] But cybersecurity is changing and technology will bring new threats that modern day exclusionary clauses will be unable to predict.[229] Courts may reward

---

[226] *See* Mondelēz Complaint, *supra* note 30, ¶¶ 8, 15.

[227] *See* Int'l Multifoods Corp. v. Commercial Union Ins. Co., 309 F.3d 76, 85–87 (2d Cir. 2002).

[228] *See supra* Part II.

[229] *See* Anthony Ferrante, *2020 Cybersecurity Predictions: Evolving Vulnerabilities on the Horizon*, HILL (Jan. 22, 2020), https://thehill.com/opinion/cybersecurity/479316-2020-cybersecurity-predictions-evolving-vulnerabilities-on-the-horizon (on file with the *Ohio State Law Journal*) (suggesting, amongst other predictions, that "local governments will continue to be hit by crippling ransomware attacks"). This presents more concerning information even outside the context of commercial cyber-attack. "Given that local governments and municipalities often have limited resources to implement robust cybersecurity measures, cannot afford to cease operations when they are attacked, and the relative ease in which these ransomware attacks can be executed, [the expectation is that] hackers [will] continue to target these entities in 2020." *Id.* In addition to local municipalities being the target of cyber-attacks, these attacks are destined to become more sophisticated, employing readily available hacking toolkits, biometric data, mobile device security deficiencies, and artificial intelligence to widen the scope of attacks. *Id.* Of pertinence to this Note, this means that cyber-attacks on critical infrastructure, from a state perspective, are also most likely going to rise. Specifically:

> Nation states have increasingly launched cyber operations to steal intellectual property and target critical infrastructure [(i.e., transportation systems, nuclear reactors, healthcare, financial services, energy, and communications)] to gain leverage over another state . . . [this will likely] continue, as hackers seek to lay the groundwork for a future attack or a retaliatory measure against a target state.

Id.

specificity in policies, but this is an arduous task in the context of cyber-attacks given the continually evolving nature of the same. What may ensue, is a broadening of insurance exclusionary clauses, which poses a very specific danger: if courts were to implement *contra proferentem* in a way that demanded insurers to be more specific with both their coverage and exclusionary clauses, the expansive protections offered by all-risk insurers may begin to dwindle. All-risk insurers may begin to draft as many exclusions as possible, with increasing amounts of specificity, slowing the negotiation process and complicating policies even further, adding to the confusion already present in detailed insurance contracts. As was analyzed above, all-risk property insurance policies were never meant to cover damages that arise out of war, let alone cyber-attacks that are used in a hostile fashion by state/rogue actors.[230] The insurance industry is meant to be *predictable*, so that insurers do not risk insolvency by covering risks they had not predicted.[231] Insurance policies are also specified, providing risk coverage to a very specific set of risks, ensuring a certain level of expertise in the brokering of each policy.[232] It is true that cybersecurity insurance is now readily available, however, coverage is sometimes limited to breaches in data security and other software-related harms; hardware and property damage would be difficult to have covered.[233] These policies also include exclusionary clauses, which may once again resurface the exact same issue.[234] It seems cyber-attacks are far too attenuated from all-risk property insurance coverage and other

---

[230] *See supra* Part II.

[231] *See supra* note 48 and accompanying text. With billions of dollars at stake, insurers very well could become insolvent if they had to cover all damages arising out of cyber-attack *in addition to* the predictable damages that the policy had originally been negotiated for. In the context of a state actor using a cyber-attack against another state that then proliferates and leaves other entities, unassociated with the state v. state conflict as victims, the predictability of such attacks would be incredibly difficult. As was the policy in history, the United States should elect to attempt to keep insurance companies solvent, in the interest of the entire nation, and shift the burden to the insured to attain more specified coverage. *See supra* note 48 and accompanying text.

[232] For a list and explanation of different types of insurance see Christy Bieber, *What Types of Insurance Do You Need?*, MOTLEY FOOL (Aug. 5, 2019), https://www.fool.com/investing/what-types-of-insurance-do-you-need.aspx [https://perma.cc/4ERF-A4AT]. Individuals needing insurance usually seek a specific *type* of policy, such as health insurance, dental insurance, disability insurance, life insurance, pet insurance, homeowners or renters insurance, flood insurance, car insurance, umbrella insurance, business insurance, cybersecurity insurance, all-risk property insurance, and more. *Id.*

[233] *Cybersecurity Insurance*, CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY (Mar. 15, 2020), https://www.cisa.gov/cybersecurity-insurance [https://perma.cc/5W9F-5F5B] [hereinafter *CISA Cybersecurity Insurance Overview*]. CISA provides incredibly valuable guidance with regard to cyber-attack risk mitigation. It encourages proactive cybersecurity measures but also discusses the need for insurance for risks that are unpredictable, regarding data loss *and* property damage. *Id.* With such research and guidance already available, a federal cybersecurity insurance entity would seem relatively simple to institute.

[234] *See id.*

insurance policies do not go far enough. It thus becomes clear that another mechanism may be needed.

Given the untenability of the continued use of exclusionary clauses, a new, more specialized insurance policy would most likely be incredibly helpful, in order to slow litigation and prevent disputes from occurring in the first case. The federal government once anticipated this result in the aftermath of the attacks on Pearl Harbor in the Second World War through the creation of the War Damage Insurance Corporation.[235] Insurance policies included exclusionary provisions that were meant to prevent massive insurance claims in a world tightly grasped in turmoil.[236] But still, the United Kingdom and other countries in Europe provided national insurance policies *specifically tailored* to cover the types of risks that were commonly exempted under exclusionary provisions, and the United States then followed suit.[237] These policies were offered at a premium price and acted as a source of income for the United States government while providing necessary protection to companies running services in war-torn areas.[238]

Similar to a federal war-risk insurance policy, a specialized form of insurance, provided by the federal government, and at premium prices, may be better suited to combat the ever-evolving nature of cyber warfare. This should be available to entities at a premium cost, in the same way that war risk insurance was offered, in order to provide all-encompassing protection in the event of cyber-attack. Attacks that are expressly excluded by all-risk policies

---

[235] *See supra* note 59 and accompanying text. Congress specifically ratified this corporation which "pledged to pay for any losses or damage to property in the United States as a result of an enemy attack. To get coverage, American property owners had to pay insurance premiums to the War Damage Insurance Corporation. This program ended after World War II." *War Damage Insurance Corporation*, INSURANCEOPEDIA (Apr. 27, 2015), https://www.insuranceopedia.com/definition/4840/war-damage-insurance-corporation [https://perma.cc/S5PL-VSR2].

[236] *See generally* Comment, *War Damage Insurance*, 51 YALE L.J. 1160 (1942) [hereinafter *War Damage Insurance History*] (overviewing the need for a federal insurance program in the wake of the Second World War given the potentially catastrophic damages that newly created aerial had on the United States). Much like the advent of aerial warfare, cyber-attack presents an incredibly nuanced form of warfare where there is great informational asymmetry between insurers and insureds. As the federal government is privy to more information than private insurance companies, it would seem most prudent for the federal government to create a Federal Cybersecurity Insurance entity. *See* Shniderman, *Issues with Hostile Act or War Exclusion Clauses*, *supra* note 209, at 70–76. The federal government would be in the best position to assess damages and cover the exact type of risks associated with cyber-attack.

[237] *War Damage Insurance History*, *supra* note 236, at 1161 ("In the last year Britain made use of a war damage insurance scheme in which indemnity was to be given by the Government only when the individual had taken insurance with the Government. This plan did not lead to comprehensive coverage in the face of an almost universal belief by the people in one district that the damage would be visited upon some other sector of the nation.") (citations omitted).

[238] *See generally id.*

can be circumvented by attaining this specialized form of insurance offered by the federal government. This would provide relief for all-risk property insurers by negating the potential requirement of having to rewrite insurance policies, thus making them more complex and amorphous, in order to exclude risks associated with cyber-attack. The burden would be shifted to the insured to attain specialized insurance coverage provided by the federal government, but surely this does not seem to be much of a burden to bear, especially in the face of the sheer amount of damage an entity can face due to a cyber-attack.

The United States government is also better suited to investigate cyber-attacks carefully to ensure that insurance claims are legitimate and are in no way attributed to the negligence of an individual entity.[239] Oftentimes, and especially in the context of cyber-attacks, substantial informational asymmetry is present where insureds have a lot of information that insurance companies will never be able to get, especially if there are matters of national security at play.[240] Rather than working *ex post*, when insurers and insureds are *disputing* whether or not exclusionary clauses in all-risk *property* insurance schemes apply to a cyber-attack, a nuanced federal cybersecurity insurance program would work *ex ante* and provide a prophylactic method to prevent litigation. The federal government could mitigate the vast information asymmetry, as the same privilege issues would not be present given the federal government's involvement at the earliest stages and given its ability to be automatically privy to information regarding national security. This is a positive factor for many reasons. Not only is the cost of litigation mitigated through an insurance policy *specifically tailored* to cover risks associated with cyber-attack, but it also necessitates an amount of care by insureds to take proactive measures in maintaining robust cybersecurity protocols. It also provides a source of income for the United States federal government, and it would allow for entities around the United States to learn more about malicious cyber-attacks, enabling better research and development methods, with the eventual goal of being more prepared for insidious attacks. This worked incredibly well in past instances of armed conflict, and as the battlefield evolves into the digital arena, it seems to be a prudent strategy for government entities to assume.

---

[239] *See* Shniderman, *Issues with Hostile Act or War Exclusion Clauses*, *supra* note 209, at 76–83. Shniderman analyzes informational asymmetry present in insurance claims and notes the very important fact that during trial, certain information, especially during war is privileged, as they may include sensitive intelligence information. *Id.* Shniderman suggests, amongst other things, to shift the burden of proving a cyber-attack to the insured as opposed to the insurer but also suggests the creation of a National Security Court to address concerns arising out of cyberbreaches. *Id.* at 81. Doing this would help to "avoid burdening ordinary civilian courts with extraordinary measures necessary to litigate terrorism cases." *Id.* at 82. Shniderman notes that the "NSC's jurisdiction could extend to critical questions in cyber-insurance coverage disputes given their nexus to national security. This would be particularly useful in cases involving allegations that state-sponsored or nation-state actors are responsible, for instance those to whom the hostile-or-warlike-action exclusion might apply." *Id.*

[240] *Id.* at 76–80.

V. CONCLUSION

Cyber-attacks are becoming incredibly prominent. The attacks are instigated by a variety of different actors, from state actors, to quasi-state actors, to rogue operators. The bottom line is that attacks like the insidious NotPetya attack of 2017 will continue, quite possibly, and even more concerningly, at more sophisticated and damaging levels. As such, entities around the United States, and the world more generally, are in a position to face devastating damages, measured in the hundreds of millions of dollars. Entities are now relying on all-risk property insurers to recover from these attacks, but disputes have ensued with meritorious claims made on behalf of the insured and the insurers. The insured argue that all-risk insurance policies are *meant* to cover damages in the aftermath of cyber-attack and that the millions of dollars of loss they suffered cannot go uncovered given exclusionary clauses that were meant to exclude traditional state v. state warfare. Insurers, on the other hand, argue that all-risk *property* insurance policies cannot cover hostile/aggressive acts of cyber warfare and specifically that such policies were never meant to cover such unpredictable damages. They argue that even if such damages could be covered under all-risk policies, war-risk and hostile-act exclusionary clauses would exclude coverage. As a result of this conflict, a short-term solution to current disputes and a long-term solution that prophylactically combats disputes are necessary.

In the short-term, courts should use the doctrine of *contra proferentem* in analyzing whether the interpretation of a specific all-risk property insurance policy should favor the insured or the insurer. In analyzing the specificity of the language in insurance policies and the bargaining power of each party, courts will be most able to come to a fair and equitable decision using the doctrine. But this short-term solution would be a temporary fix to what could turn out to be an overwhelming problem. If courts favor insurers, insureds will have to sustain massive losses with limited to no recourse. If courts favor insureds, insurers may be liable for extraordinarily high claims, risking their own solvency. As such, it seems prudent that a new federally supported cybersecurity insurance program, *specifically tailored* to cover losses that can arise from cyber-attacks, would be a welcome addition to the insurance landscape. Such a solution would provide an alternative for entities seeking insurance coverage in the event of a cyber-attack and would also prevent insurers from fearing insolvency given the extent of damages that can ensue. It is abundantly clear that current insurance schemes in response to malicious cyber-attack are, at best, unsubstantial. Without course correction, massive damages are likely to continue and, even worse, litigation costs are set to sky-rocket. It is now time for the world to get ready for the new battlefield: the cyber battlefield.