"CYBERWAR BY ALMOST ANY DEFINITION"[1]: NOTPETYA, THE EVOLUTION OF INSURANCE WAR EXCLUSIONS, AND THEIR APPLICATION TO CYBERATTACKS

JOSEPHINE WOLFF[*]

TABLE OF CONTENTS

INTRODUCTION

In June 2017, the multinational food company Mondelez International Inc. ("Mondelez") was hit by the NotPetya ransomware virus.[2] NotPetya exploited a vulnerability in the Microsoft Windows operating system to encrypt the contents of infected computers' hard drives[3] and demanded a ransom payment of roughly $300 worth of bitcoins before it would turn the contents of the computers back over to their owners.[4]

---

[1] Andy Greenberg, *The Untold Story of NotPetya, the Most Devastating Cyberattack in History*, WIRED (Aug. 22, 2018, 5:00 AM), https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world.

[*] Associate Professor of Cybersecurity Policy, Tufts University Fletcher School of Law and Diplomacy. I am grateful to Daniel Schwarcz, Daniel Woods, and participants in the symposium on The Role of Law and Government in Cyber Insurance Markets co-hosted by the University of Connecticut School of Law and University of Minnesota Law School for their helpful comments and suggestions.

[2] Complaint & Demand for Jury Trial at 2, Mondelez Int'l, Inc. v. Zurich Am. Ins. Co., No. 2018L011008 (Ill. Cir. Ct. Oct. 10, 2018) [hereinafter Mondelez Complaint].

[3] CITI GPS, MANAGING CYBER RISK WITH HUMAN INTELLIGENCE: A PRACTICAL APPROACH 24, 28 (Global Perspective & Solutions May 2019 ed., 2019).

[4] Matt Burgess, *What Is the Petya Ransomware Spreading Across Europe? WIRED Explains*, WIRED (Mar. 7, 2017, 10:35 AM), https://www.wired.co.uk/article/petya-malware-ransomware-attack-outbreak-june-2017.

NotPetya infiltrated more than 2,000 organizations worldwide during the summer of 2017,[5] including Mondelez, which had to shut down 1,700 servers and 24,000 laptops due to NotPetya infections.[6] In the aftermath of the incident, Mondelez filed a claim with its insurer, Zurich American Insurance Co. ("Zurich"), under its global property insurance policy, which 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 . . . ."[7] Zurich initially agreed to pay out $10 million to Mondelez to cover its losses but then changed its mind and refused to cover any of the costs on the grounds that NotPetya was a "hostile or warlike action" perpetrated by a "government or sovereign power" and thereby excluded from coverage.[8]

Mondelez filed a $100 million lawsuit against Zurich in October 2018[9] and the case (unresolved at the time of writing) raises difficult questions about what constitutes war (or "warlike" actions) in the online domain. Since the lines between online espionage, sabotage, and warlike attacks are often blurrier online than in the physical domain, classifying an incident like NotPetya as "warlike" is far from straightforward. While war is typically not a regular occurrence or routine concern for insurance holders, cyberattacks perpetrated by nation states are not uncommon,[10] and excluding them from coverage could place a significant burden on policyholders.[11] Moreover, the lengthy and sometimes contentious process of determining

---

[5] CITI GPS, *supra* note 3, at 23.

[6] Mondelez Complaint, *supra* note 2, at 2–3.

[7] *Id.* at 2.

[8] *Id.* at 4–6.

[9] *Id.* at 1, 10.

[10] MICHAEL GROSKOP, NISSIM PARIENTE, LOUIS SCIALABBA, EYAL ARAZI, & DANIEL SMITH, RADWARE, PROTECTING WHAT YOU CAN'T SEE: ELIMINATING SECURITY BLIND SPOTS IN AN AGE OF TECHNOLOGICAL CHANGE 5 (Deborah Szajngarten & Ben Zilberman eds., Global Application & Network Security Report 2019-2020 ed., 2020) ("Nation-state attacks were an issue as respondents indicated a substantial increase in the percentage of cyberattacks attributed to cyberwar, up from 19% in 2018 to 27% in 2019."). *See also* CITI GPS, *supra* note 3, at 16 ("Nation state actors conduct espionage to steal intellectual property and collect intelligence considered vital to advancing national interests. Challenging to detect and mitigate, these actors have substantial resources allocated to developing and sustaining sophisticated capabilities.").

[11] *See generally* Kenneth S. Abraham & Daniel Schwarcz, *Courting Disaster: The Underappreciated Risk of a Cyber Insurance Catastrophe*, 27 CONN. INS. L.J. 1, 48 (2021) (discussing the lack of clarity of nation-state exclusions for policyholders).

who is behind a cyberattack and whether it can be definitively attributed to a nation state, adds to the challenges of interpreting this exception and applying it to online threats.[12] Additionally, since a single piece of malware like NotPetya may not only be used for a warlike purpose (e.g., shutting down the Ukrainian electric grid)[13] but can also cause significant collateral damage to unintended victims, such as Mondelez and other private entities,[14] it is not clear whether a war exclusion should apply to every incident caused by the same piece of malware or only to specific warlike components or impacts of that malware's effects.

Because NotPetya was the first public case of a cyberattack being deemed an act of war by insurers as grounds for denying a claim,[15] both insurers and policyholders have few directly analogous precedents to rely on in order to understand what these war exclusions do and do not apply to in the cyber domain.[16] However, while it may be the first cyberattack to land in court over its disputed warlikeness, NotPetya is not the first time that ambiguous incidents categorized by insurers as "war" or "warlike" have been challenged in court by policyholders.[17] In fact, the language of war exclusions in insurance policies, like that purchased by Mondelez, has been shaped by a series of historical inflection points when claims activity and subsequent lawsuits forced insurers to realize they needed to broaden or otherwise clarify what types of activities these exceptions applied to.[18] As buyers and sellers of cyber-insurance seek to better understand how these exclusions may apply to online attacks and intrusions, it may be helpful to

---

[12] *Id.* at 44–50.

[13] Thomas Brewster, *NotPetya Ransomware Hackers 'Took Down Ukraine Power Grid'*, FORBES (July 3, 2017, 7:45 AM), https://www.forbes.com/sites/thomasbrewster/2017/07/03/russia-suspect-in-ransomware-attacks-says-ukraine/.

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

[15] Dominic T. Clarke, *Cyber Warfare and the Act of War Exclusion, in* GLOBAL LEGAL GROUP LTD., INTERNATIONAL COMPARATIVE LEGAL GUIDE: INSURANCE & REINSURANCE 2020 11, 12 (9th ed. 2020).

[16] Abraham & Schwarcz, *supra* note 11, at 48.

[17] *See, e.g.*, Pan Am. World Airways v. Aetna Cas. & Sur. Co., 505 F.2d 989 (2d Cir. 1974); Holiday Inns Inc. v. Aetna Ins. Co., 571 F. Supp. 1460 (S.D.N.Y. 1983); Sherwin-Williams Co. v. Ins. Co. of Pa., 863 F. Supp. 542 (N.D. Ohio 1994).

[18] *See generally* Josephine Wolff, Cyberinsurance Policy: Rethinking Risk in an Age of Ransomware, Computer Fraud, Data Breaches, and Cyberattacks (Jan. 8, 2022) (unpublished manuscript) (on file with author).

consider the development and legal history of insurance war exclusions and what lessons that history offers about how such exclusions may be applied to cyberattacks in their current form or further refined to more directly address emerging online threats.

This article describes some of the stages of the evolution of war exclusions in insurance policies since the mid-twentieth century. It also considers what we can learn from the history of legal challenges to claims denied under these exclusions and about how courts and insurers are likely to interpret their relevance and application to cyberattacks like NotPetya. Specifically, this article looks at lawsuits resulting from the aftermath of Pearl Harbor, the 1970 hijacking of Pan American Flight 093, the destruction in 1975 of the Holiday Inn hotel in Beirut during a civil war, and explores how each incident changed the language used by insurers in drafting war exclusions to encompass increasingly broader categories of activity that could, conceivably, be interpreted as applying to many forms of cyberattacks and online intrusions, including NotPetya. Finally, this article argues that given the challenges of attribution, risk correlation, and determining the precise purpose of malware, war exclusions that apply to cyberattacks should not be predicated on being able to identify the perpetrator or motive of such attacks, but rather on their victims, impacts, and scale. However, this framing of war exclusions is, in many ways, directly contradictory to their evolution over the past century and may therefore be difficult to reconcile with existing language governing these exclusions.

I. ORIGINS OF WAR EXCLUSIONS & PEARL HARBOR

The exclusion Zurich pointed to in Mondelez's property insurance policy excluded losses or damage directly or indirectly caused by "hostile or warlike action in time of peace or war . . . ."[19] The practice of excluding war risks from all-risk insurance policies dates back more than one hundred years before NotPetya. Originally, in the nineteenth century maritime insurance policies had included coverage for losses at sea caused by wars—an issue of particular concern to ship owners since wars often affected marine voyages.[20] However, in 1898, Lloyd's Insurance Exchange ("Lloyds") added a Free of Capture & Seizure Clause ("FC&S") to its general marine cargo clause that excluded coverage for any losses caused by war. [21] As FC&S

---

[19] Mondelez Complaint, *supra* note 2, at 4.

[20] Helen M. Benzie, *War and Terrorism Risk Insurance*, 18 J.C.R. & ECON. DEV. 427, 428 (2004).

[21] *Id.* at 428–29.

clauses became standard practice, some insurers, including Lloyd's, also started offering coverage specifically for war risks, but the scale and unpredictability of losses caused by wars made it difficult for insurers to reliably model such policies or be certain they could cover the resulting claims.[22] In particular, the potential for wars to result in highly correlated risks posed significant challenges to insurers and continues to make these risks difficult for insurers to model and cover today. Accordingly, in 1913, a committee established by the British government determined that private insurers could not meet the demand for war insurance, and the government subsequently agreed to reinsure eighty percent of the war risks insurers underwrote.[23] Similarly, in the United States, Congress passed the War Risk Insurance Act in 1914, establishing the Bureau of War Risk Insurance in the Treasury Department to provide war risk coverage for marine commerce.[24] Thus, by the early twentieth century, war risks were already being excluded from standard forms of all-risk insurance and were understood to be uninsurable by the private market without support from policymakers.

War exclusions have evolved from their roots in marine insurance to become a common feature in other types of coverage, including property insurance and life insurance. Following the attack on Pearl Harbor in 1941, a series of lawsuits—mostly brought by the beneficiaries of life insurance policies for people killed during the attack—tested the meaning and limitations of this type of exclusion.[25] In particular, the fact that the attack on the morning of December 7, 1941, occurred one day prior to the United States' declaration of war against Japan, complicated the question of whether Pearl Harbor could be considered an act of war for insurance purposes.[26] For instance, when Navy seaman Howard A. Rosenau died at Pearl Harbor, his parents, Arthur and Freda Rosenau, filed a claim with Idaho Mutual Benefit Association ("Idaho Mutual"), where their son had purchased a $1,000 life insurance policy prior to his death and named them as beneficiaries.[27] Idaho Mutual denied the claim because Rosenau's policy included an exclusion for

---

[22] *See generally id.*

[23] *Id.* at 429.

[24] War Risk Insurance Act of 1914, Pub. L. No. 63-193, 38 Stat. 711 (1914) (repealed 1933).

[25] *See, e.g.,* Stankus v. N.Y. Life Ins. Co., 44 N.E.2d 687 (Mass. 1942); Rosenau v. Idaho Mut. Benefit Ass'n, 145 P.2d 227 (Idaho 1944); Cladys Ching Pang v. Sun Life Assurance Co. of Can., 37 Haw. 208 (1945); N.Y. Life Ins. Co. v. Bennion, 158 F.2d 260 (10th Cir. 1946).

[26] *Rosenau*, 145 P.2d at 228.

[27] *Id.* at 227–28.

"death, disability or other loss sustained while in military, naval, or air service of any country at war."[28]

Because the United States was not yet at war with Japan at the time of the Pearl Harbor attack, an Idaho court ruled in favor of Rosenau's parents, ordering Idaho Mutual to pay them the full amount due under their son's policy.[29] The insurer appealed this decision to the Idaho Supreme Court, arguing that the United States was already at war when Rosenau died at Pearl Harbor, and his death was therefore excluded from coverage.[30] To support this argument, Idaho Mutual cited the preamble of the resolution Congress adopted the day after Pearl Harbor, on December 8, 1941, titled *Joint Resolution declaring that a state of war exists between the Imperial Government of Japan and the Government and People of the United States*.[31] The preamble stated, "[w]hereas, the Imperial Government of Japan has committed unprovoked acts of war . . . . That the state of war between the United States and the Imperial Government of Japan, which has thus been thrust upon the United States is hereby formally declared . . . ."[32] Idaho Mutual argued that these references to the Pearl Harbor attack as an "unprovoked act of war" and a pre-existing "state of war" between the United States and Japan that was merely codified, not initiated, by Congress on December 8th, meant that the Pearl Harbor attack occurred in a "country at war."[33]

Arthur and Freda Rosenau disputed this broad interpretation of "war" that allowed for a country to be considered "at war" even prior to a formal declaration by its government.[34] They argued that if the court accepted the insurer's interpretation of what it meant to be "at war" then:

> [I]t would mean that the United States has been constantly at 'war' with Japan since the sinking of the gunboat Panay in China in the early 1930's, and it would mean that Russia and Japan are now at 'war' by virtue of the fact that within recent years there have been border patrol clashes and

---

[28] *Id.*
[29] *Id.* at 228.
[30] *Id.* at 228–29.
[31] *Id.* at 229. *See* S.J. Res. 116, 77th Cong. (1941).
[32] S.J. Res. 116.
[33] *Rosenau*, 145 P.2d at 229.
[34] *Id.* at 232.

> hostilities in some force along the border between Manchuria and Russian Siberia.[35]

Their point—a particularly poignant one for considerations of online warlike acts—was that a broad interpretation of what it meant to be "at war" could quickly expand to apply to many hostile attacks, not all of which would necessarily lead to actual wars that were officially declared as such by the nations involved.[36] They further argued,

> The Panay incident was a hostile attack, but it was atoned for. The border clashes between Russian and Japanese territory were unquestionably armed invasions of the other's territory. Yet they were atoned for and 'war' did not ensue. It was possible, no matter how improbable, that the Pearl Harbor attack could have been atoned for and adjusted without 'war' necessarily ensuing.[37]

The majority ruling of the Idaho Supreme Court was sympathetic to this line of reasoning, citing an international law textbook by John Bassett Moore that emphasized war as a "legal condition" such that "if two nations declare war one against the other, war exists, though no force whatever may as yet have been employed. On the other hand, force may be employed by one nation against another, as in the case of reprisals, and yet no state of war may arise."[38] The court majority was unwilling to deviate from this strict, legal definition of war in interpreting Rosenau's life insurance policy, writing in its 1944 ruling:

> It is true, as pointed out by appellant, that the word war, in a broad sense, is used to connote a state or condition of war, warlike activities, fighting with arms between troops, etc., but we are here concerned with the meaning and intent of the word as contained in a formal, legal contract of insurance, a class of contracts which the courts are very frequently called upon to consider and construe, and it

---

[35] *Id.*

[36] *Id.*

[37] *Id.*

[38] *Id.* at 229–30 (quoting 7 JOHN BASSET MOORE, A DIGEST OF INTERNATIONAL LAW 153 (1906)).

> seems quite obvious that words and phrases in a contract of this nature, are used and intended to be used in the legal sense.[39]

The Idaho Supreme Court determined that a ruling in favor of Idaho Mutual would mean interpreting the language in the life insurance policy not "in its accepted legal sense" but rather, as applying to "cases where conditions of war, or conditions which might lead to war, existed."[40] If it did that, the majority opinion pointed out, "the court would . . . be making a new contract for the parties, by adding to the contract phrases, terms and conditions, which it does not contain. This, of course, is not one of the functions of a court."[41]

Two justices on the Idaho Supreme Court dissented, arguing that the Pearl Harbor attack had, for all intents and purposes, been an act of war.[42] Justice James F. Ailshie wrote, "[w]here the armed forces of two sovereign nations strike blows at each other, as occurred at Pearl Harbor on December 7, 1941, and do so under the direction and authority of their respective governments, it is difficult for me to understand why that is not *war*."[43] Ailshie's rationale was based on the idea that Pearl Harbor looked like an act of war—not just to him, but also to "the average citizen, who might apply for and procure a life insurance policy [sic] . . . ."[44] To him, what determined whether a country was at war was not the legal status of that war but rather, whether a person witnessing a violent or hostile act would recognize it as such. Broadening the definition of war in this way was essential, Ailshie argued, because "[o]ur political history demonstrates that most wars have been commenced and prosecuted without any formal declaration of war; and that war dates from its inception rather than from the time on which some formal declaration to that effect is made."[45]

While the Rosenaus were ultimately successful in forcing their son's insurer to pay out his policy, other beneficiaries met with more mixed results. In 1942, two years before the final ruling in *Rosenau*, the Supreme Court of Massachusetts ruled against Marcella Stankus, who sought a life insurance payout from New York Life Insurance Co. ("New York Life Insurance")

---

[39] *Id.* at 230.

[40] *Id.*

[41] *Id.*

[42] *Id.* at 232–36 (Ailshie, J., dissenting) (with Justice Budge concurring with Justice Ailshie's dissent).

[43] *Id.* at 236.

[44] *Id.*

[45] *Id.*

following the death of her son, Anthony Stankus in 1941.[46] Anthony, like Howard Rosenau, was a Navy seaman, but he did not die at Pearl Harbor—instead, he died two months earlier on October 30, 1941, when his ship, the U.S.S. Reuben James, was sunk by a torpedo in the Atlantic Ocean.[47] The war exclusion in Stankus's life insurance policy, worded slightly more broadly than the one in Rosenau's policy, ruled out coverage for death resulting "directly or indirectly from . . . war or any act incident thereto."[48] Marcella Stankus, like Rosenau's parents, argued that since the United States had not declared war on October 30, 1941, at the time of Anthony's death, it could not be considered a death resulting from war.[49]

An early judgment by a lower court had agreed with that argument, holding that the insurer must pay out the full claim to Marcella Stankus, but when New York Life Insurance appealed that decision, the Supreme Judicial Court of Massachusetts sided with them, reversing the initial decision.[50] Justice James J. Ronan authored the 1942 opinion, writing, "the existence of a war is not dependent upon a formal declaration of war. Wars are being waged today that began without any declaration of war. The attack by the Japanese on Pearl Harbor on December 7, 1941, is the latest illustration."[51] Two years later, in his dissent in *Rosenau*, Ailshie seized on that line as evidence that the attack on Pearl Harbor should also count as an act of war because the Massachusetts court had already deemed it so when deciding *Stankus*.[52] Ultimately, the Massachusetts Court reached exactly the opposite conclusion of the Idaho Court, deciding, "the clause exempting the defendant from liability where death is caused by war is not restricted in its operation to a death that has resulted from a war being prosecuted by the United States."[53] Ailshie, in his *Rosenau* dissent, alluded to the fact that war was ongoing in Europe well before the United States' official declaration, raising the question of whether an officially declared conflict between some countries would suffice to satisfy the war exclusion, even if the resulting damage occurred in a different country.[54] This line of reasoning could be relevant for NotPetya as well since the malware was designed for the

---

[46] Stankus v. N.Y. Life Ins. Co., 44 N.E.2d 687 (Mass. 1942).
[47] *Id.* at 688.
[48] *Id.* at 687–88.
[49] *Id.* at 688.
[50] *Id.* at 688, 689–90.
[51] *Id.* at 688.
[52] Rosenau v. Idaho Mut. Benefit Ass'n, 145 P.2d 227, 236 (Idaho 1944).
[53] *Stankus*, 44 N.E.2d at 689.
[54] *Rosenau*, 145 P.2d at 235–36.

ongoing conflict between Russia and Ukraine, but the damage inflicted by it spread well beyond the borders of those two countries.[55] This is not unique to NotPetya—many pieces of malware that have been designed for particular cyberattacks, such as the Stuxnet worm used to compromise Iranian nuclear enrichment tubes,[56] but spread far beyond their specific targets and infected computers belonging to victims who were in no way involved in the central conflict that motivated the attack.[57]

The disagreement among courts about the meaning of war continued in the years following the contradictory *Stankus* and *Rosenau* rulings. In 1945, the year after the *Rosenau* decision, the Supreme Court of Hawaii came to a similar decision as the Idaho court, ruling in favor of Gladys Ching Pang, who sued Sun Life Assurance Co. of Canada ("Sun Life") for refusing to pay out the life insurance policy of her husband, Tuck Lee Pang, a Honolulu Fire Department employee who died at Pearl Harbor.[58]

> On December 7, 1941, we not only were maintaining diplomatic relations with Japan but a special Japanese envoy was then in Washington ostensibly for the purpose of patching up the strained relations then existing between his country and ours, and not until December 8, 1941, did the political department of our Government or the Japanese Government do any act of which judicial notice can be taken creating "a state of war" between the two countries.[59]

The Supreme Court of Hawaii concluded that the Pearl Harbor attack did not fall within the war exclusion in Pang's life insurance policy and Sun Life was therefore required to pay his wife.[60]

The following year, in 1946, the Tenth Circuit Court of Appeals came to the opposite conclusion, following the model of the Supreme Court of Massachusetts in *Stankus*, by reversing a judgment for the beneficiaries of the life insurance policy belonging to Captain Mervyn S. Bennion, a naval officer who died at Pearl Harbor on the Battleship West Virginia.[61] Bennion's life insurance policy, also issued by New York Life Insurance,

---

[55] Satariano & Perlroth, *supra* note 14.

[56] Abraham & Schwarcz, *supra* note 11, at 13.

[57] CITI GPS, *supra* note 3, at 15.

[58] Cladys Ching Pang v. Sun Life Assurance Co. of Can., 37 Haw. 208, 208–09 (1945).

[59] *Id.* at 215–16.

[60] *Id.* at 222.

[61] N.Y. Life Ins. Co. v. Bennion, 158 F.2d 260, 261, 265–66 (10th Cir. 1946).

contained exactly the same exception as Stankus's—word-for-word—and the Tenth Circuit determined that the exception applied to "any type or kind of war in which the hazard of human life was involved," including Pearl Harbor.[62] This, too, is a rationale that has significant implications for cyberattacks given how rarely even the most significant and devastating of them threaten human lives. Indeed, the fact that existing cases of cyberattacks have so rarely led to the loss of lives has been used to argue that these incidents do not constitute acts of war and that "cyber war" itself is unlikely to occur.[63]

The difference between the outcomes in favor of the insurers in *Stankus* and *Bennion* and the rulings for the insurance beneficiaries in *Rosenau* and *Pang* stems from a fundamental disagreement between the deciding courts about how narrowly and colloquially the language of an insurance policy should be interpreted—particularly, the term "war." The Supreme Courts of Idaho and Hawaii in *Rosenau* and *Pang*, respectively, were in favor of a very narrow legal interpretation of "war."[64] Meanwhile, the Tenth Circuit and Supreme Court of Massachusetts were instead focused on how people commonly understood war and the idea that, to many people, Pearl Harbor would *look* like an act of war, even if war between the United States and Japan had not yet been officially declared at the time of the attack.[65] The Tenth Circuit insisted that "[m]ankind goes no further in his definitive search [to understand what war is]- he does not stand on ceremony or wait for technical niceties."[66] In a similar vein, the Supreme Court of Massachusetts argued, "the words of an insurance policy . . . must be given their usual and ordinary meaning."[67] That "ordinary meaning," the Supreme Court of Massachusetts held, was determined by "ordinary people" and what they would consider to be war.[68] Justice Ronan explained, "[t]he term 'war' is not limited, restricted or modified by anything appearing in the policy. It refers to no particular type or kind of war, but applies in general to every situation that ordinary people would commonly regard as war."[69] While this

---

[62] *Id.* at 265.

[63] *See* THOMAS RID, CYBER WAR WILL NOT TAKE PLACE ch. 2 (2013).

[64] Rosenau v. Idaho Mut. Benefit Ass'n, 145 P.2d 227, 230 (Idaho 1944); *Cladys Ching Pang*, 37 Haw. at 216–15.

[65] *Bennion*, 158 F.2d at 264; Stankus v. N.Y. Life Ins. Co., 44 N.E.2d 687, 688–89 (Mass. 1942).

[66] *Bennion*, 158 F.2d at 264.

[67] *Stankus*, 44 N.E.2d at 688.

[68] *Id.*

[69] *Id.*

"ordinary person" test may be common in insurance policy interpretation, it presents significant challenges when applied to emerging notions of cyber war, where there is little common consensus or understanding of when an online threat crosses the threshold of a warlike act even among experts, much less among ordinary people.

The evidence provided by the Massachusetts Court in *Stankus* relied heavily on the historical context of the moment when Stankus died—the hints that the United States was gearing up for military conflict in 1941, if not yet directly engaged in war.[70] Justice Ronan cited a September 11, 1941, address by President Roosevelt in which he declared, "[f]rom now on, if German or Italian vessels of war enter the waters the protection of which is necessary for American defense [sic], they do so at their own peril."[71] Ronan also cited the Lease-Lend Act in March 1941 as an indicator that the United States was already effectively engaging in war-related activities at the time of Stankus's death.[72]

> The President . . . had stated that German or Italian vessels of war entered these waters at their peril. The sinking by German or Italian submarines of ships belonging to a belligerent nation, or of ships of another nation convoying war materials and supplies to a belligerent nation, is the usual result of waging war by one nation against another, and the torpedoing of the Reuben James while convoying vessels engaged in such traffic was an act that arose out of the prosecution of such a war.[73]

It is striking that the President's statements carried so much weight with the Supreme Court of Massachusetts and hints at just how significant the public-facing language and political context of conflicts can be for determining when an event does or does not qualify for an insurance policy's war exception. After all, much stronger statements made by both the President and Congress following Pearl Harbor were quickly dismissed by the Idaho Supreme Court in the *Rosenau* case, which dealt with an incident that occurred much closer to the official declaration of war in the United

---

[70] *Id.* at 689.

[71] *Id.* at 688 (quoting *Fireside Chat 18: On the Greer Incident* (radio broadcast Sept. 11, 1941).

[72] *Id.* at 689. *See* H.R. 1776, 77th Cong. (1941).

[73] *Id.* (citations omitted).

States.[74] This uncertainty around the weight of public statements about the war-like nature of certain events also has important implications for cybersecurity incidents, particularly since terms like "cyber war" are thrown around freely for political purposes with relatively little consistency or clarity about what they actually mean.

The very different rulings in *Stankus* and *Bennion*, as compared to *Rosenau* and *Pang*, also make clear just how important the specific language of the actual exclusion written into an insurance policy can be. In *Rosenau*, for instance, the majority justified its decision to diverge from the rationale used to decide *Stankus* by stating that the war-related provisions in Stankus's life insurance coverage were "quite different" from those included in Rosenau's policy.[75] Unlike the *Stankus* and *Bennion* policies, which excluded deaths that resulted from "war or any act incident thereto,"[76] the *Rosenau* policy specifically excluded injuries "sustained while in military, naval, or air service of any country at war . . . ."[77] The Idaho Supreme Court focused particularly on the phrase "at war," arguing that it "very clearly" meant the exclusion only applied during a time when war had been legally declared.[78] Similarly, they distinguished the *Rosenau* case from an even earlier life insurance dispute brought after Alfred G. Vanderbilt died on May 7, 1915, aboard the British steamer Lusitania, when it was sunk by German submarines.[79] In that case—where the beneficiaries of Vanderbilt's life insurance lost against his insurer, Travelers' Insurance Co. ("Travelers")—the war exclusion had ruled out coverage for deaths "resulting, directly or indirectly, wholly or partly, from war [or riot]."[80] The absence of that crucial reference to a "time of war" differentiated the *Vanderbilt* policy from the *Rosenau* policy. Accordingly, the Idaho Supreme Court reasoned Travelers had more leeway to interpret the sinking of the British steamer Lusitania as an excluded act than Idaho Mutual had to interpret Pearl Harbor as occurring "in time of war."[81]

---

[74] Rosenau v. Idaho Mut. Benefit Ass'n, 145 P.2d 227, 229–30 (Idaho 1944).

[75] *Id.* at 231.

[76] *Stankus*, 44 N.E.2d at 687–88; N.Y. Life Ins. Co. v. Bennion, 158 F.2d 260, 261 (10th Cir. 1946).

[77] *Rosenau*, 145 P.2d at 227.

[78] *Id.* at 231.

[79] *Id. See* Vanderbilt v. Travelers' Ins. Co., 184 N.Y.S. 54 (Sup. Ct. 1920), *aff'd*, 194 N.Y.S. 986 (App. Div. 1922), *aff'd*, 139 N.E. 715 (N.Y. 1923).

[80] *Rosenau*, 145 P.2d at 227 (quoting *Vanderbilt*, 184 N.Y.S. at 54).

[81] *Id.*

In other words, the majority in *Rosenau* did not hold that Pearl Harbor was any less an act of war than the torpedoing of the British steamer Lusitania or the U.S.S. Reuben James, but rather, they found that Idaho Mutual had crafted the language of their war exclusion more narrowly to apply only to deaths that occurred "in time of war." Indeed, one of the lessons for insurers following Pearl Harbor was that they should rewrite their war exclusions more broadly. Sun Life, for instance, changed the wording of its policies after Pearl Harbor. The life insurance policy in *Pang* issued by the company had excluded "death resulting from riot, insurrection, or war, or any act incident thereto," but shortly after Pearl Harbor the company modified that exclusion in new policies by inserting the words "whether declared or not" after the word "war."[82]

These early war exclusion disputes shaped the language of those exclusions for years to come, pushing insurers to broaden their descriptions of war to include undeclared war or warlike acts. This broadening of the terms of war exclusions to hedge what kinds of losses they could be applied to was not unique to life insurance; it spread into other insurance products, including property insurance. For instance, the policy Mondelez had purchased from Zurich at the time of the NotPetya ransomware attacks excluded property loss and damage "directly or indirectly caused by or resulting from . . . hostile or warlike action in time of peace or war . . . ."[83] This language had been deliberately crafted to apply to a much broader swath of circumstances than the narrower war exclusions that had appeared in the life insurance policies belonging to *Vanderbilt*, *Rosenau*, *Bennion*, *Stankus*, and *Pang* many decades earlier.

Almost a century before the NotPetya attacks, in June 1920, the Supreme Court of New York ruled in favor of Travelers in the *Vanderbilt* life insurance dispute.[84] The foundation of that ruling, disqualifying the claim on Vanderbilt's life insurance, was an assumption that any conflict between the governments of two countries constituted war, whether or not it had been officially and legally declared.[85] The Supreme Court of New York cited an even older maritime law case, decided in 1800, in which the United States Supreme Court had ruled that "every contention by force, between two nations, in external matters, under authority of their respective governments,

---

[82] Cladys Ching Pang v. Sun Life Assurance Co. of Can., 37 Haw. 208, 208, 211 (1945).

[83] Mondelez Complaint, *supra* note 2, at 4.

[84] *Vanderbilt*, 184 N.Y.S. at 56.

[85] *Id.*

is not only war, but public war."[86] Going by that logic, the Supreme Court of New York determined in the *Vanderbilt* life insurance case:

> The concessions of the parties that the Lusitania was sunk in accordance with instructions of a sovereign government, by the act of a vessel commanded by a commissioned officer of that sovereign government, being then operated by that said officer and its crew, all of whom were part of the naval forces of the said sovereign government, and that war was then being waged by and between Great Britain, the sovereign controlling the Lusitania, and Germany, the sovereign controlling the submarine vessel, control the conclusion which must be reached that the casualty resulted from war and that the consequences of the casualty come within the excepted portions of the policy.[87]

Twenty-six years later, the Tenth Circuit would use a similar rationale in deciding *Bennion*, where it determined that Pearl Harbor was an act of war.

> When one sovereign nation attacks another with premeditated and deliberate intent to wage war against it, and that nation resists the attacks with all the force at its command, we have war in the grim sense of reality. It is war in the only sense that men know and understand it.[88]

This, too, is a line of reasoning with significant implications for cyberattacks which are regularly directed by one sovereign government against another. Indeed, it was, in many ways, the crux of Zurich's argument that the NotPetya attacks were not covered under Mondelez's property insurance policy.[89] The ransomware attacks were not violent. It was not obvious that they looked like what an ordinary person might consider to be war. They did not occur at a time when the United States had officially declared war on the perpetrator, but that perpetrator was credibly believed

---

[86] *Id.* at 56 (quoting Bas v. Tingy, 4 U.S. (4 Dall.) 37, 40 (1800)).
[87] *Id.*
[88] N.Y. Life Ins. Co. v. Bennion, 158 F.2d 260, 264 (10th Cir. 1946).
[89] *See* Mondelez Complaint, *supra* note 2, at 4.

by many to be Russia—a sovereign government.[90] Russia had not even formally declared war on Ukraine, the intended target of the NotPetya malware, though in 2014 the Ukrainian interim Prime Minister Arseniy Yatsenyuk referred to Russia's annexation of the Crimean Peninsula as "a declaration of war to my country."[91] However, while the malware targeted Ukrainian infrastructure, many of the victims of NotPetya, including Mondelez, were also private entities and organizations outside Ukraine,[92] so NotPetya was not exactly a "contention by force between two nations."[93] This was yet another way in which cyberattacks complicated traditional interpretations of war and war exclusions—the entanglement of public and private actors and the challenges of targeting cyberattacks so as not to cause widespread collateral damage under circumstances that insurers and earlier insurance disputes had not anticipated and for which insurers had not devised clear rules.

II. PAN AM FLIGHT 093 & EXPANSION OF WAR EXCLUSIONS TO TERRORISM

Pearl Harbor and the sinking of the British steamer Lusitania may not have been unambiguous acts of war, but they both certainly came much closer to situations "that ordinary people would commonly regard as war"[94] than NotPetya—a computer virus of ambiguous origin, at the time of its spread, that caused no direct casualties or violence and targeted mostly private companies.[95] More recent insurance disputes dealing with circumstances further removed from war than the British steamer Lusitania or Pearl Harbor, sheds some light on how war exclusions might apply to situations like NotPetya and other cyberattacks, as well as the role of these exclusions in property insurance policies, like the one Mondelez had purchased from Zurich. Ultimately, what these cases reveal is how much remains uncertain and unclear in the interpretation of insurance policy war

---

[90] *See* Satariano & Perloth, *supra* note 14 (noting the United States government blamed Russia in 2018); Brewster, *supra* note 13 (noting Ukraine blamed Russia in 2017).

[91] Marie-Louise Gumuchian, Ben Wedeman & Ian Lee, *Ukraine Mobilizes Troops After Russia's 'Declaration of War'*, CNN: WORLD (Mar. 3, 2014, 8:26 AM), https://www.cnn.com/2014/03/02/world/europe/ukraine-politics/index.html.

[92] Satariano & Perloth, *supra* note 14.

[93] Bas v. Tingy, 4 U.S. (4 Dall.) 37, 40 (1800).

[94] Stankus v. N.Y. Life Ins. Co., 44 N.E.2d 687, 688 (Mass. 1942).

[95] *See* CITI GPS, *supra* note 3, at 23–24.

exclusions, particularly when it comes to distinguishing between acts of war and acts of terrorism.

On September 6, 1970, Pan American World Airways Inc.'s ("Pam Am") Flight 093 was hijacked by two passengers, forty-five minutes after the Boeing 747 had departed from Amsterdam, heading to New York.[96] The two hijackers, armed with guns and grenades, ordered the pilot to fly to Beirut, Lebanon, and announced to the passengers and crew that they were working on behalf of the Popular Front for the Liberation of Palestine ("PFLP").[97] After the hijackers threatened to blow up the plane in mid-air, Lebanese officials permitted the flight to land in Beirut on the condition that it refuel and then leave.[98] On the ground in Lebanon, more PFLP members boarded the plane with explosives, and one—a demolition expert—stayed on the plane when it took off again, this time bound for Cairo.[99] Egyptian officials permitted the plane to land after the hijackers lit the fuses of the explosives while the plane was still in the air.[100] The hijackers informed the crew that they would have only eight minutes after the plane landed to evacuate everyone before the plane blew up, and the passengers were all successfully evacuated in Cairo.[101] The explosives detonated on schedule and the plane was subsequently destroyed.[102] Pan Am filed a claim with its insurers for the value of the aircraft, totaling $24,288,759.[103]

Pan Am had purchased comprehensive insurance coverage from several different insurers.[104] From Aetna Casualty and Surety Co. ("Aetna"), as well as other insurers, the airline had purchased all-risk insurance that covered one-third of the value of their fleet in the event of "all physical loss of or damage to the aircraft."[105] That policy excluded any losses or damage resulting from:

> 1. capture, seizure, arrest, restraint or detention or the consequences thereof or of any attempt thereat, or any

---

[96] Pan Am. World Airways, Inc. v. Aetna Cas. & Sur. Co., 368 F. Supp 1098, 1100, 1104 (S.D.N.Y. 1973), *aff'd*, 505 F.2d 989 (2d Cir. 1974).

[97] *Id.* at 1100–01, 1114.

[98] *Id.* at 1114.

[99] *Id.*

[100] *Id.* at 1115.

[101] *Id.* at 1101, 1115.

[102] *Id.* at 1102.

[103] *Id.*

[104] *Id.*

[105] *Id.*

> 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 . . . [hereinafter "Clause 1"];
> 2. war, invasion, civil war, revolution, rebellion, insurrection or warlike operations, whether there be a declaration of war or not [hereinafter "Clause 2"];
> 3. strikes, riots, civil commotion [hereinafter "Clause 3"].[106]

In order to ensure they would still be covered in the event of these excluded circumstances, Pan Am also purchased war risk insurance from Lloyd's, which had an upper limit of $14,226,290.47 in coverage and covered the three clauses of excluded risks in the all-risks policy, verbatim.[107] Since American underwriters did not offer war risk coverage, Pan Am obtained the rest of its war risk coverage, beyond what Lloyd's was willing to insure, from the United States government for an additional $9,763,709.53 of coverage that only applied to damage caused by the perils in the Clause 1 and Clause 2 of the Aetna policy exclusions.[108] This coverage was issued by United States Secretary of Commerce as authorized under the Federal Aviation Act of 1958, which allowed the government to provide insurance for risks that are excluded from commercial policies under "free of capture and seizure" clauses, like the Clause 1 and Clause 2 in Pan Am's all-risk policies exclusions.[109] Because the United States government was only authorized to cover risks excluded under "free of capture and seizure" clauses, this insurance could not apply to the Clause 3 exclusions—strikes, riots, and civil commotions—in Pan Am's all-risk insurance. So, in July 1970, just a few months before the hijacking, Pan Am came to an agreement with Aetna and its other insurers to make an additional premium payment of $29,935 in order to delete the Clause 3, which had previously ruled out

---

[106] *Id.*

[107] *Id.* at 1103–04.

[108] *Id.* at 1103.

[109] Federal Aviation Act of 1958, Pub. L. No. 85-726, §1301, 72 Stat. 731, 800–01 (1958) (current version at 49 U.S.C.A. §40101).

coverage for "strikes, riots, [and] civil commotion" and cover damage caused by those risks up to $10,062,393.[110]

Unsurprisingly, all of the insurers claimed that the hijacking was a type of risk covered by someone else's policy, leading to an extended legal battle. Aetna and the other all-risk insurers argued in court that the hijacking fell under the exclusions of Clause 1 and Clause 2—the ones it had no responsibility to cover—because it was perpetrated by a "'taking . . . by [a] military . . . or usurped power'" and was an example of "'insurrection,' 'rebellion,' 'civil war' . . . 'warlike operations,' 'war,' 'riot' and 'civil commotion.'"[111] Lloyd's and the United States government argued that the hijacking did not fall under any of the exception clauses and was therefore entirely the responsibility of the all-risk insurers.[112] Pan Am itself took this position as well, arguing that the hijacking was not an excluded risk; but further argued that, if the hijacking was an excluded risk, then it fell under the Clause 3 exclusion as a "riot" or "civil commotion."[113] Perhaps not coincidentally, these were the two interpretations—that the hijacking was not excluded or that it was an excluded Clause 3 peril—that would lead to the largest payouts for the company given the complicated coverage situation.[114]

New York District Judge Marvin Frankel ruled in 1973 that the Pan Am hijacking did not fall under any of the exclusion clauses, in a decision that discussed the political circumstances surrounding the Middle East and the PFLP at some length.[115] Aetna had argued that "the Arab-Israeli Conflict was the efficient cause of the hijacking operation" and that the hijacking should therefore be considered a war risk.[116] They also noted the hijackers' attempt to use the plane loudspeaker system to read a handwritten note to the passengers explaining that they were hijacking the plane "because the government of America helps Israel daily. The government of America gives Israel fantom airoplanes [sic] which attack our camps and burn our village."[117] Aetna argued that because the "seizure and destruction of the aircraft were announced by the group as a blow and as retaliation against the

---

[110] *Pan Am. World Airways, Inc.*, 368 F. Supp at 1102–03.

[111] *Id.* at 1117.

[112] *Id.* at 1103–04.

[113] Pan Am. World Airways, Inc. v. Aetna Cas. & Sur. Co., 505 F.2d 989, 996 (2d Cir. 1974).

[114] *Id.* at 1022.

[115] *Pan Am. World Airways, Inc.*, 368 F. Supp. at 1139.

[116] *Id.* at 1123.

[117] *Id.* at 1115.

United States. . . . [T]hese facts alone would be sufficient to place the loss under the broadly drawn war risk language."[118] Frankel rejected these arguments for relying on an overbroad definition of war; finding error in Aetna's justification for why the hijacking of the Pan Am plane qualified for the war risk exclusion because it "would apply equally to the bombing of stores in Europe, by children or adults, the killing of Olympic athletes, the killing of an American military attaché in Amman . . . or other individual acts of organization-sponsored violence in the United States or any other place."[119] Nor did he find that the larger Arab-Israeli conflict was to blame for the hijacking, or could be said to have "proximately caused" the incident.[120]

Several courts' rulings on computer fraud insurance cases in later years would focus on the question of whether a computer had directly or immediately caused an act of fraud, determining in many of those cases that the computer-based stages were too far removed from the actual theft for it to be considered an act of computer fraud.[121] Similarly, Frankel felt there was too much distance—both literally and metaphorically—between the conflict in the Middle East and the Pan Am hijacking for the latter to be viewed as an act of war, or even a direct consequence of war. Specifically, Frankel found "[i]t would take a most unusual and explicit contract to make the self-determined depredations of a terrorist group, thousands of miles from the area of the '[Arab-Israeli] Conflict,' acts of 'war' for insurance purposes."[122] And Aetna had not, in Frankel's view, authored a sufficiently explicit (or unusual) contract for this purpose.[123] In fact, Frankel noted that,

---

[118] *Id.* at 1123.

[119] *Id.*

[120] *Id.*

[121] *Compare* Brightpoint, Inc. v. Zurich Am. Ins. Co., No. 1:04-CV-2085, 2006 WL 693377 (S.D. Ind. Mar. 10, 2006) (reasoning that the fax of unauthorized checks and bank guarantees in payment for goods–here phone cards–did not meet Zurich policy's Computer Fraud requirement that the insured's loss be directly related to the use of a computer), *and* Pestmaster Servs., Inc. v. Travelers Cas. & Sur. Co. of Am., 656 F. App'x 332, 333 (9th Cir. 2016) (affirming the district court's decision that the Computer Fraud provision "does not cover authorized or valid electronic transactions . . . even though they are, or may be, associated with a fraudulent scheme."), *with* Am. Tooling Ctr., Inc. v. Travelers Cas. & Sur. Co. of Am., 895 F.3d 455, 462–63 (6th Cir. 2018) (finding that the plaintiff's loss in this case was "directly caused" by the computer fraud when the plaintiff's employees conducted a series of actions, all induced by a fraudulent email).

[122] *Pan Am. World Airways, Inc.*, 368 F. Supp. at 1123.

[123] *Id.*

as in the case of the Pearl Harbor disputes, Aetna and the other all-risk insurers had changed the language of their exclusion clauses to respond to the hijacking, adopting "new exclusion clauses applying in adequate and unambiguous terms to operations like the PFLP hijackings."[124] In doing so, Frankel noted, they seemed to concede that "the former clauses lacked the clarity necessary to vindicate" their position in the Pan Am case that the previous language already unambiguously applied to hijackings.[125]

In 1974, the Second Circuit Court of Appeals upheld Frankel's ruling in finding that "war refers to and includes only hostilities carried on by entities that constitute governments at least de facto in character," and that the hijacking could not be considered a "'warlike operation' because that term does not include the inflicting of damage on the civilian property of non-belligerents by political groups far from the site of warfare . . . ."[126] While NotPetya is believed to have been developed and distributed by a government, there are echoes of what happened to Mondelez in this description of the Flight 093 hijacking. After all, Mondelez, and several other victims of the NotPetya malware, were caught up in the conflict between Russia and Ukraine despite being civilian victims located far from the Crimean Peninsula. Physical proximity to conflict is a more complicated and problematic consideration in cyberattacks than physical ones, since malware can so easily and quickly spread across geographic distance.[127] However, it is notable that this geographic distance from conflict was so central to the *Pan Am* ruling given how far-flung victims of cyberattacks often are from each other and the intended target of those attacks. This lack of geographic containment also contributes to the potential for even more highly correlated risks resulting from these incidents, causing even greater challenges for insurers.[128]

In the *Pan Am* case, the insurers tried to get around the fact that the PFLP was not a government by arguing that it was a "military . . . or usurped power" in Jordan and therefore still covered under the exceptions listed in Clause 1.[129] But the Second Circuit held "in order to constitute a military or usurped power the power must be at least that of a de facto government. On

---

[124] *Id.* at 1120.

[125] *Id.*

[126] Pan Am. World Airways, Inc. v. Aetna Cas. & Sur. Co., 505 F.2d 989, 997, 1012 (2d Cir. 1974).

[127] *See* CITI GPS, *supra* note 3, at 14, 83.

[128] Abraham & Schwarcz, *supra* note 11, at 50–52.

[129] *Pan Am. World Airways, Inc.*, 368 F. Supp. at 1129.

the facts of this case, the PFLP was not a de facto government in the sky over London when the 747 was taken."[130] Going clause by clause, the Second Circuit went on to eliminate each possible category of exception that the incident might have fallen under. The hijacking could not be considered a "warlike act" because "[t]he 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."[131] It was not an "insurrection" because "the PFLP did not intend to overthrow King Hussein when it hijacked the Pan American 747."[132] It was not a "civil commotion" because "[f]or there to be a civil commotion, the agents causing the disorder must gather together and cause a disturbance and tumult."[133] It was not a "riot" because "the hijacking was accomplished by only two persons."[134]

If Aetna and Pan Am's other property insurers had intended for their policies to exclude hijackings then they should have used clearer, more specific language, the Second Circuit ruled.[135] In this regard, the Second Circuit suggested, the history of property insurance and its roots in early marine policies had not served the insurers well. The Second Circuit, in agreement with the District Court, dismissed the language of the Pan Am policy exclusions as being based on "ancient marine insurance terms selected by the all risk insurers simply do not describe a violent and senseless intercontinental hijacking carried out by an isolated band of political terrorists."[136]

III. HOLIDAY INN AND CIVIL COMMOTIONS

The *Pan Am* ruling that terrorist acts were not excluded from property insurance policies under war exclusions was highly influential in later legal disputes about what did or did not constitute an act of war under property insurance policies. In 1974, the same year that the Second Circuit issued its decision in the *Pan Am* case, a twenty-six floor Holiday Inn hotel

---

[130] *Pan Am. World Airways, Inc.*, 505 F.2d at 1009.

[131] *Id.* at 1015.

[132] *Id.* at 1018–19.

[133] *Id.* at 1020.

[134] *Id.* at 1021.

[135] *Id.* at 1009 ("[T]he all risk insurers were quite capable of resolving known ambiguities in concrete terms descriptive of today's events.").

[136] *Id.* at 998.

opened in Beirut, Lebanon.[137] In October 1975, conflict broke out in the neighborhood in West Beirut where the hotel was located between the Muslim Nasserist political party (called the "Mourabitoun") and the Christian right-wing party (called the "Phalange").[138] As the fighting continued in late 1975, members of the Phalangist militia occupied the Holiday Inn and the conflict caused considerable damage to the building—windows were shot out, fifteen rooms were damaged by fire, and another thirty-five had burned curtains and broken glass—forcing Holiday Inn to close the hotel to guests in November 1975.[139]

On "Black Saturday," December 6, 1975, the fighting in Beirut escalated significantly and the Holiday Inn became a focal point for the combatants.[140] All of the remaining staff were evacuated as the Phalangists claimed the hotel for themselves, and the building changed hands between the two sides several times over the course of the next few months as the fighting continued.[141] George McMurtrie Godley, who was serving as the American ambassador to Lebanon at the time, described the scene around the hotel:

> [You had] Christians occupying Holiday Inn. You had Moslems wanting to take it. Holiday Inn was right, you might say, on the borderline between the predominantly Christian areas and the predominantly Moslem areas. There you had rather well-organized military factions where men were holding an area and other men were attacking it.[142]

Holiday Inn had insured its foreign properties through Aetna under an all-risk policy similar to the one that covered Pan Am's fleet that provided coverage for "all risks . . . of direct physical loss or damage . . . from any external cause except as hereinafter provided."[143] Unlike Pan Am's policy, the Holiday Inn policy specifically included damage "directly caused by persons taking part in riots or civil commotion or by strikers or locked-out workers or by persons of malicious intent acting in behalf of or in connection

---

[137] Holiday Inns Inc. v. Aetna Ins. Co., 571 F. Supp. 1460, 1467 (S.D.N.Y. 1983).

[138] *Id.* at 1468.

[139] *Id.* at 1469–70.

[140] *Id.* at 1470–71.

[141] *Id.* at 1471.

[142] *Id.* at 1479 n.73.

[143] *Id.* at 1463.

with any political organization . . . ."[144] In fact, Holiday Inn had agreed to higher premiums so that Aetna would include civil commotion coverage for their Beirut property.[145] But, the Holiday Inn policy still excluded any losses or damage caused "directly or indirectly, proximately or remotely . . . [by] [w]ar, invasion, act of foreign enemy, hostilities or warlike operations (whether war be declared or not), civil war, mutiny, insurrection, revolution, conspiracy, military or usurped power."[146] Unsurprisingly, when Holiday Inn filed a claim for nearly $11 million to cover the damage to their Beirut hotel, Aetna contended that the conflict between the Mourabitoun and the Phalangists had been a civil war or insurrection, and insurrection was therefore excluded from Holiday Inn's coverage.[147] Holiday Inn—like Pan Am—sued Aetna, insisting that the conflict was instead a form of "civil commotion" and therefore covered according to the terms for which it had specifically negotiated and paid extra.[148]

District Judge Charles S. Haight Jr., who decided *Holiday Inn* in 1983 in favor of the hotel chain, relied heavily on the *Pan Am* precedent in his ruling. Although Aetna had called various journalists to testify that the events in Beirut were widely regarded as a civil war, Haight rejected the testimony in favor of the assertion made by the Second Circuit in *Pan Am* that, "'the specific purpose of overthrowing the constituted government and seizing its powers' is a necessary element of both 'insurrection' and 'civil war.'"[149] Based on that definition, Haight found the events in Beirut could not be considered an insurrection because "the Mourabitoun, in seeking to dislodge the Phalange from the Holiday Inn, were not acting for the specific purpose of overthrowing the Lebanese government. They did not proclaim a casting off of allegiance to that government; they did not proclaim or seek to establish a government of their own."[150] It was not a civil war, according to Haight, because none of "the factions involved in any way with the damage to the Holiday Inn embraced partition of Lebanon as a specific objective."[151] Instead, Haight ruled:

---

[144] *Id.*
[145] *Id.*
[146] *Id.*
[147] *Id.*
[148] *Id.*
[149] *Id.* at 1497 (quoting Pan Am. World Airways, Inc. v. Aetna Cas. & Sur. Co., 368 F. Supp 1098, 1124 (S.D.N.Y. 1973), *aff'd*, 505 F.2d 989 (2d Cir. 1974)).
[150] *Id.*
[151] *Id.* at 1498.

> The Holiday Inn was damaged by a series of factional "civil commotions," of increasing violence. The Lebanese government could not deal effectively with these commotions. The country came close to anarchy. But the constitutional government existed throughout; the requisite intent to overthrow it has not been proved to the exclusion of other interpretations; and there was no "war" in Lebanon between sovereign or quasi-sovereign states.[152]

Thanks to its foresight in negotiating special "civil commotion" coverage for an additional premium, Holiday Inn was therefore covered under its Aetna property insurance policy, and Aetna was ordered by the court to pay the claim.[153]

"Journalists and politicians invariably referred to these events in Lebanon as a 'civil war.' They do so today," Haight wrote towards the end of his ruling.[154] He went on to explain that regardless of how people commonly used those terms, his job was "to give the words at issue their insurance meaning . . . ."[155] Haight's willingness to dismiss the terms that people commonly used to describe the conflict is striking, as is his insistence that terms like "civil war" and "insurrection" could—and did—have a specific "insurance meaning," which is quite different from how they might be used and understood by the general public. Following Pearl Harbor, courts insisted that any event that looked to an ordinary person like war, should be considered as such for insurance purposes.[156] However, Haight (following in the footsteps of Frankel and the Second Circuit) was advocating for very narrow interpretations of the war exceptions written into property insurance policies.[157] This approach was in line with interpreting ambiguities in the coverage in favor of the policyholder, rather than the insurer.[158] In *Stankus*, the Massachusetts Supreme Court advocated for interpreting war under its

---

[152] *Id.* at 1503.

[153] *Id.*

[154] *Id.*

[155] *Id.*

[156] *See* Universal Cable Prods., LLC v. Atlantic Specialty Ins. Co., 929 F.3d 1143, 1157 (9th Cir. 2019) (holding that the lower court's application of the plain and ordinary meaning of 'war' was incorrect and instead affirming that for purposes of insurance, a special meaning should be applied).

[157] *Holiday Inns*, 571 F. Supp at 1464.

[158] *Id.*

"ordinary meaning,"[159] but Haight had no interest in the ordinary meaning of all-risk policy exclusions; he cared only about their insurance meaning.[160]

The idea that war has a very particular meaning and definition in the context of insurance contracts continued to gain traction in courts following the *Pan Am* and *Holiday Inn* rulings. In 2019, the Ninth Circuit Court of Appeals reversed a ruling in favor of the insurer, and an entire section of the opinion authored by Judge A. Wallace Tashima was captioned: "[*t*]*he special meaning of 'war' in the insurance context*."[161] The case was brought by Universal Cable Productions ("Universal"), which had been filming a television series called "Dig" in Jerusalem during the summer of 2014 when Hamas launched rockets at Israeli targets from Gaza, forcing the studio to shut down production and move filming to a new location.[162] Universal filed a claim with its insurer, Atlantic Specialty Insurance Co. ("Atlantic"), under their television production insurance policy to cover the costs of interrupting and moving production.[163] Atlantic denied the claim citing the four war exclusions in Universal's policy, which excluded coverage for losses caused by: (1) "[w]ar, including undeclared or civil war"; (2) "[w]arlike action by a military force;" (3) "[i]nsurrection, rebellion, [and] revolution;" and (4) "[a]ny weapon of war including atomic fission or radioactive force, whether in time of peace or war."[164]

In 2017, a district court in California concluded that Atlantic was correct in its assessment, and the Hamas attacks fell under the first two exclusion categories of war and warlike action because "[s]uch a conflict easily would be considered a 'war' by a layperson."[165] The district court based its analysis on California state law which dictated that the terms of an insurance policy must be "understood in their ordinary and popular sense, rather than according to their strict legal meaning . . . ."[166] The Ninth Circuit reversed the district court's decision, noting that, in fact, California law actually made an exception to its "ordinary and popular" rule on the interpretation of insurance policies if "a special meaning is given to them by

---

[159] Stankus v. N.Y Life Ins. Co., 44 N.E.2d 687, 688 (Mass. 1942).

[160] *Holiday Inns*, 571 F. Supp at 1503.

[161] *Universal Cable Prods., LLC*, 929 F.3d at 1154.

[162] *Id.* at 1146.

[163] *Id.* at 1146–47.

[164] *Id.* at 1149.

[165] Universal Cable Prods., LLC v. Atlantic Specialty Ins. Co., 278 F. Supp. 3d 1165, 1173–74 (C.D. Cal. 2017), *rev'd in part*, *vacated in part*, 929 F.3d 1143 (9th Cir. 2019).

[166] *Id.* at 1172–73 (quoting CAL. CIV. CODE § 1644 (West 1872).

usage . . . ."[167] Citing both *Pan Am* and *Holiday Inn*, the Ninth Circuit determined that this exception applied to war on the grounds that "in the insurance context, the term 'war' has a special meaning that requires the existence of hostilities between de jure or de facto governments."[168] Since Hamas was not, in the Ninth Circuit's view, a de jure or de facto sovereign, its "conduct in the summer of 2014 cannot be defined as 'war' for the purposes of interpreting this policy."[169] Nor could the firing of those rockets be considered a warlike action, the Ninth Circuit ruled, because such a determination would conflate war with terrorism.[170] Tashima noted in the ruling that Hamas launched unguided missiles that were "likely used to injure and kill civilians because of their indiscriminate nature."[171] Therefore Tashima concluded, "Hamas' conduct consisted of intentional violence against civilians—conduct which is far closer to acts of terror than 'warlike action by a military force.'"[172]

A very narrow and particular meaning of war in the context of insurance policies, as well as a sharp distinction between warlike acts and terrorism, emerged from *Pan Am* and the cases that followed it like *Holiday Inn* and *Universal*. Both of those legacies—the narrow definition of war and the separation from terrorism—have significant implications for cybersecurity incidents like NotPetya, that appear to originate from government actors but that affect civilians.[173] Attribution of cyberattacks can be a slow and tricky endeavor,[174] but at least in the case of NotPetya, that process seemed to point unequivocally to the Russian government as the responsible party.[175] Moreover, the distribution of NotPetya in 2017 occurred in the midst of ongoing hostilities and armed conflict between two

---

[167] *Universal Cable Prods., LLC*, 929 F.3d at 1153 (quoting CAL. CIV. CODE § 1644 (West 1872).

[168] *Id.* at 1154.

[169] *Id.* at 1159.

[170] *Id.* at 1160.

[171] *Id.* at 1161.

[172] *Id.*

[173] *See* Satariano & Perloth, *supra* note 14.

[174] 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.

[175] *Id.*

governments: Ukraine and Russia.[176] In this sense, an attack like NotPetya might seem to come closer to meeting the criteria for the insurance definition of war as "hostilities between de jure or de facto governments"[177] than an attack launched by a non-sovereign group like Hamas, Mourabitoun, or PFLP.[178]

On the other hand, while the perpetrator of NotPetya may have been a government actor, the victims were largely civilian and only those that were clearly elements of Ukraine's critical infrastructure—including Ukrainian power companies, transportation organizations, and banks—were clearly the intended targets due to their close ties to the ongoing Russia-Ukraine conflict.[179] Many other firms, both Ukrainian and non-Ukrainian, were affected indiscriminately by the malware, including Mondelez, and in those cases, Russia's use of a far-reaching, untargeted ransomware program suggests something closer to the Ninth Circuit's definition of terrorism as "intentional violence against civilians by political groups."[180] Perhaps most important, for all the extensive damage NotPetya caused, it was not a violent attack.[181] Unlike almost every other incident that has raised legal disputes on the meaning of war exclusions in insurance—the sinking of the British steamer Lusitania, the attack on Pearl Harbor to the hijacking of Pan Am Flight 093, and the attacks on Israel by Hamas—NotPetya did not directly put anyone's life in danger.[182] To call a piece of computer code, no matter how destructive, an act of war that resulted in no physical destruction or loss of lives would be to go against most people's common conceptions of what resembles war. In 2014, following the breach of Sony Pictures by the North Korean government, President Obama referred to the breach as "an act of cyber-vandalism that was very costly, very expensive" during an interview

---

[176] Sam Jones, *Finger Points at Russian State Over Petya Hack Attack*, FIN. TIMES (June 30, 2017), https://www.ft.com/content/f300ad84-5d9d-11e7-b553-e2df1b0c3220.

[177] *Universal Cable Prods., LLC*, 929 F.3d at 1154.

[178] *Id.* at 1147; Holiday Inns Inc. v. Aetna Ins. Co, 571 F. Supp. 1460, 1465 (S.D.N.Y. 1983); Pan Am. World Airways, Inc. v. Aetna Cas. & Sur. Co., 505 F.2d 989, 1013 (2d Cir. 1974).

[179] Andy Greenberg, *Petya Ransomware Epidemic May Be Spillover from Cyberwar*, WIRED (June 28, 2017, 1:02 PM), https://www.wired.com/story/petya-ransomware-ukraine.

[180] *Universal Cable Prods., LLC*, 929 F.3d at 1160.

[181] Greenberg, *supra* note 1 (estimating that damages stemming from the NotPetya attack totaled roughly $10 billion).

[182] Mondelez Complaint, *supra* note 2, at 2–3.

on CNN but said, explicitly, "I don't think it was an act of war."[183] NotPetya exhibited more elements of warlike activity than the Sony Pictures breach, including more immediate armed conflict between the central two nations involved, and targeting of critical infrastructure. But, for most of its non-critical infrastructure victims, NotPeya fundamentally shut down computers and deleted data (much like the Sony Pictures breach) rather than causing physical damages, [184] suggesting it still retained many more elements of an act of cyber-sabotage than a violent or warlike act. The key exception to this is the critical infrastructure targets of NotPetya, including the Ukrainian power grid—which resulted in some clear kinetic consequences[185]—raising the question of whether all victims and consequences of NotPetya should be lumped together for the purposes of classification, or whether the attacks on Mondelez might be categorized differently from those on Ukraine's power infrastructure, despite being executed by the same lines of code.

IV. MONDELEZ, NOTPETYA, AND THE MEANING OF CYBER WAR

When Mondelez was hit by the NotPetya ransomware in 2017, it had a comprehensive property insurance policy from Zurich that appeared to be explicitly designed to cover any digital disruptions to the company's business.[186] Specifically, the policy covered expenses "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."[187] Following the attack, Mondelez promptly filed a claim with Zurich and provided documentation of the malware and its impacts.[188] On June 1, 2018, Mondelez received a letter from Zurich denying the claim on

---

[183] Sean Sullivan, *Obama: North Korea Hack 'Cyber-Vandalism,' Not 'Act of War',* WASH. POST (Dec. 21, 2014), https://www.washingtonpost.com/news/post-politics/wp/2014/12/21/obama-north-korea-hack-cyber-vandalism-not-act-of-war/.

[184] *See, e.g.,* Mondelez Complaint, *supra* note 2, at 2–3. *See also* Greenberg, *supra* note 179.

[185] *See* Satariano & Perloth, *supra* note 14 ("In just 24 hours, NotPetya wiped clean 10 percent of all computers in Ukraine, paralyzing networks at banks, gas stations, hospitals, airports, power companies and nearly every government agency, and shutting down the radiation monitors at the old Chernobyl nuclear power plant.").

[186] Mondelez Complaint, *supra* note 2, at 2.

[187] *Id.*

[188] *Id.* at 3.

the grounds that NotPetya was excluded from their policy based on Exclusion B.2(a):

> 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:
> . . .
> 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.[189]

The war exclusion in Mondelez's policy bore many of the marks of insurers' efforts to broaden the language of their exclusions in light of previous court losses. The reference to warlike actions "in time of peace or war" codified the lesson of the Rosenau family's life insurance dispute about Pearl Harbor.[190] In that case, the insurance exclusion phrasing about policyholders "engaged in military or naval service in time of war" had been the insurer's downfall,[191] so insurers like Zurich now made sure to clarify that the war exclusions also applied at times when war had not been officially declared. The use of the term "warlike" was also an attempt to broaden the boundaries of a strict definition of war, just as it had been when used in the insurance policies disputed in *Pan Am*, *Holiday Inn*, and *Universal*. Further, the inclusion of any "agents or authority" of governments or sovereign powers in the scope of whose actions could be considered warlike hinted at yet another way in which Zurich was aiming to broaden the exclusion.

In the life insurance disputes following Pearl Harbor, the central question for the courts to decide was whether one country's attack on another's military could be considered war even absent a formal, legal

---

[189] *Id.* at 4.
[190] Rosenau v. Idaho Mut. Ben. Ass'n, 145 P.2d 227 (Idaho 1944).
[191] *Id.* at 231–32.

declaration.[192] In the more recent property insurance disputes about war exceptions in *Pan Am*, *Holiday Inn*, and *Universal*, the disagreements hinged chiefly on whether those exclusions encompassed violence directed at civilians by groups that were not governments.[193] NotPetya combined elements of both of these issues. Like the attack on Pearl Harbor, NotPetya emerged in the midst of ongoing, escalating conflict between two countries (in this case, Russia and Ukraine), and it appeared to have been developed and launched by a sovereign government, though the attribution to Russia took some months and was strenuously denied by the Russian government.[194] However, as in the *Pan Am*, *Holiday Inn*, and *Universal* cases, NotPetya primarily affected civilian victims rather than military ones, and many of those targets—including Mondelez—were outside Ukraine and fairly far removed from the political conflict between the two governments.[195] And unlike *Pan Am*, *Holiday Inn*, and *Universal*, NotPetya caused no direct physical damage to the Mondelez's property.[196] However, that did not invalidate the insurance coverage since Mondelez's policy from Zurich explicitly included coverage for business interruptions and the associated losses that were caused by the failure of computers.[197] But it did make the incident seem, on the whole, slightly less "warlike" than an airplane hijacking or a missile attack.

The strongest evidence in favor of Zurich's assertion that NotPetya was a "hostile or warlike action" lay in the attack being attributed to the Russian government.[198] That process of attribution lasted months and took

---

[192] *Id.* (noting the war exclusion did not apply because "no act or recognition had taken place by any department of our government with regard to the existence of war, or warlike activities, at the time of the death of the insured.").

[193] Universal Cable Prods., LLC, v. Atlantic Specialty Ins. Co., 929 F.3d 1143, 1154 (9th Cir. 2019); Holiday Inns Inc. v. Aetna Ins. Co, 571 F. Supp. 1460 (S.D.N.Y. 1983); Pan Am. World Airways, Inc. v. Aetna Cas. & Sur. Co., 505 F.2d 989 (2d Cir. 1974).

[194] Denis Pinchuk, *Russia Denies British Allegations That Moscow Was Behind Cyber-Attack*, REUTERS (Feb. 15, 2018, 4:50 AM), https://www.reuters.com/article/us-britain-russia-cyber-kremlin/russia-denies-british-allegations-that-moscow-was-behind-cyber-attack-idUSKCN1FZ102.

[195] Mondelez Complaint, *supra* note 2, at 2. *See also* Greenberg, *supra* note 179 ("Hackers may instead have been continuing a long-running assault against Ukraine. But this time, the rest of the world feels their pain too.").

[196] Mondelez Complaint, *supra* note 2, at 2–3.

[197] *Id*. at 2.

[198] Jones, *supra* note 176.

place during the nearly year-long period between Mondelez's initial filing of an insurance claim and Zurich's denial of that claim.[199] Beginning immediately after the NotPetya attacks in June 2017, Ukrainian officials and cybersecurity researchers were quick to cast blame for the attack on Russia.[200] That same month, Roman Boyarchuk, who ran Ukraine's Center for Cyber Protection, told *Wired* that the attack was "likely state-sponsored" and that it was "difficult to imagine anyone else," besides Russia, who "would want to do this."[201] Ukrainian cybersecurity firm, Information Systems Security Partners, was also among the first to claim that the NotPetya code closely resembled previous Russian cyberattacks in its design and technical "fingerprints."[202] Later that month, United States cybersecurity company, FireEye, made a similar claim, when its head of global cyber intelligence, John Watters, told *The Financial Times*, "we are reasonably confident towards it being Russia" that was responsible for NotPetya, based on analysis of the targets, code, and malware infection vectors.[203] "The best you can get is high confidence," Watters said of the attribution effort, emphasizing that it was not definite Russia was behind the attack even though "there are a lot of things that point to Russia."[204]

On February 14, 2018, the UK National Cyber Security Centre published a statement saying the Russian military was "almost certainly responsible" for NotPetya.[205] The next day, February 15, 2018, the Australian Minister for Law Enforcement and Cyber Security, Angus Taylor, issued a similar statement that "the Australian Government has judged that Russian state sponsored actors were responsible" for NotPetya,[206] as did White House press secretary, Sarah Huckabee Sanders. Sanders' brief statement read, in its entirety:

---

[199] *Id.*

[200] Greenberg, *supra* note 179.

[201] *Id.*

[202] *Id.*

[203] Jones, *supra* note 176.

[204] *Id.*

[205] *Russian Military 'Almost Certainly' Responsible for Destructive 2017 Cyber Attack*, NAT'L CYBER SEC. CTR. (Feb. 14, 2018), https://www.ncsc.gov.uk/news/russian-military-almost-certainly-responsible-destructive-2017-cyber-attack.

[206] Asha Barbaschow, *Australia Also Points Finger at Russia for NotPetya*, ZDNET (Feb. 15, 2018), https://www.zdnet.com/article/australia-also-points-finger-at-russia-for-notpetya/.

> In June 2017, the Russian military launched the most destructive and costly cyber-attack in history.
>
> The attack, dubbed "NotPetya," quickly spread worldwide, causing billions of dollars in damage across Europe, Asia, and the Americas. It was part of the Kremlin's ongoing effort to destabilize Ukraine and demonstrates ever more clearly Russia's involvement in the ongoing conflict. This was also a reckless and indiscriminate cyber-attack that will be met with international consequences.[207]

Four more countries—Canada, Denmark, Lithuania, and Estonia—quickly followed suit, issuing official statements blaming Russia for the attack within the week in what Australia's Ambassador for Cyber Affairs, Tobias Feakin, later referred to as "the largest coordinated attribution of its kind to date."[208] A spokesman for the Russian government, Dmitry Peskov, denied the coordinated allegations and denounced them as "Russophobic."[209]

It is, of course, difficult to say definitively whether the Russian government was behind the NotPetya malware, but Zurich's case for claiming the incident was the act of a "government or sovereign power" is about as persuasive as it is possible for a cyberattack attribution to be.[210] The evidence pointing to Russia includes similarities between the NotPetya code and previous strains of malware attributed to Russia.[211] While most ransomware encrypts the contents of infected computers and then provides a way for victims to decrypt their files so long as they make a cryptocurrency ransom payment, NotPetya did not only encrypt the hard drives of computers it infected.[212] It also overwrote the master boot records of those computers, making it nearly impossible for the files to be restored.[213] Additionally, while NotPetya did appear to demand a (relatively small) ransom payment from victims of roughly $300 in bitcoin, the ransom demand was unusual in that

---

[207] WHITE HOUSE, Statement from the Press Sec'y (Feb. 15, 2018), https://trumpwhitehouse.archives.gov/briefings-statements/statement-press-secretary-25/.

[208] Stilgherrian, *Blaming Russia for NotPetya was Coordinated Diplomatic Action*, ZDNET (Apr. 11, 2018), https://www.zdnet.com/article/blaming-russia-for-notpetya-was-coordinated-diplomatic-action/.

[209] Pinchuk, *supra* note 194.

[210] Mondelez Complaint, *supra* note 2, at 4.

[211] Greenberg, *supra* note 179.

[212] Jones, *supra* note 176.

[213] *Id.*

it required victims to send confirmation of their payments to a particular, fixed email address.[214] That address was quickly blocked by the email service provider after the attack began—making it difficult for anyone to prove they had actually paid the demanded ransom according to the attackers' terms.[215]

The signs that the attackers did not actually aim to restore their victims' files and had no real interest in collecting ransom payments, hinted that the perpetrators were not financially motivated criminals, but instead had some other agenda.[216] That agenda was clarified somewhat by the fact that the perpetrators initially spread NotPetya by embedding it inside a software update from a Ukrainian accounting software company called MeDoc.[217] Because a Ukrainian firm was used as the initial conduit, most of the victims of NotPetya were Ukrainian. In fact, early estimates suggested that more than three-quarters of the affected organizations were based in Ukraine—though the malware quickly spread to other companies outside Ukraine, at least in part through their infected Ukrainian subsidiaries.[218] This focus on Ukraine aligned with earlier Russian cyberattacks focused on Ukrainian infrastructure, as well as the ongoing military conflict between the two countries dating from Russia's annexation of Crimea in February 2014—a conflict sometimes referred to as the "Russo-Ukrainian War."[219]

This political context—and even the language used to describe it—is relevant to Zurich's argument that NotPetya was a "warlike action."[220] In July 2019, six months after Mondelez filed its lawsuit against Zurich, the Ninth Circuit issued its *Universal* ruling stating, "in the insurance context, the term 'war' has a special meaning that requires the existence of hostilities between de jure or de facto governments."[221] The conflict between Russia and Ukraine certainly appeared to meet that bar of hostilities between governments, and the coordinated attribution of NotPetya to Russia by several countries in February 2018, three and a half months before Zurich denied the Mondelez claim, gave Zurich a strong basis for arguing that NotPetya had been perpetrated by a government party to those hostilities.

---

[214] *Id.*

[215] *Id.*

[216] Greenberg, *supra* note 179.

[217] Jones, *supra* note 176.

[218] *Id.*

[219] Joshua P. Mulford, *Non-State Actors in the Russo-Ukrainian War*, 15 CONNECTIONS: Q.J. 89, 89–106 (2016).

[220] Mondelez Complaint, *supra* note 2, at 4.

[221] Universal Cable Prods., LLC v. Atlantic Specialty Ins. Co., 929 F.3d 1143, 1154 (9th Cir. 2019).

What was less clear was whether NotPetya itself—or any computer-based attack, for that matter—could legitimately be considered "warlike."

Mondelez thought not. In its lawsuit against Zurich, the company referred to "Zurich's invocation of a 'hostile or warlike action' exclusion to deny coverage for malicious 'cyber' incidents" as "unprecedented."[222] Indeed, no previous legal conflicts that centered on interpretation of insurance war exclusions had dealt with cyberattacks, nor was there any reason to believe that the exclusions had been crafted to apply to computer-based attacks. This supported Mondelez's claim that "the purported application of this type of exclusion to anything other than conventional armed conflict or hostilities was unprecedented."[223] But just because Zurich's interpretation of the war exclusion was unprecedented did not necessarily mean it was wrong. In fact, much of Mondelez's argument seemed to lie in simply asserting that "incursions of malicious code or instruction into MDLZ's [Mondelez's] computers did not constitute 'hostile or warlike action,' as required by Exclusion B.2(a)."[224] In framing its argument this way, Mondelez implied that malware directed at a private company, that plays no role in a country's critical infrastructure, cannot constitute "hostile or warlike action" rather than asserting that every victim or impact of NotPetya should necessarily be considered un-warlike.[225]

By the time Mondelez filed its lawsuit, there was already a growing trend of nations and international organizations recognizing that cyberattacks were rapidly becoming an integral part of warfare and that "incursions into computers" had the potential to cause serious damage, on par with the destruction of kinetic attacks. For instance, in June 2016, a year before NotPetya, NATO Secretary-General Jens Stoltenberg told the German newspaper, *Bild*, that the alliance had classified cyberspace as an "official domain of warfare" and confirmed that a sufficiently severe cyberattack on any of its members would be considered an act of war, triggering a military response.[226] At the time, Stoltenberg did not point to any specific examples of known cyberattacks that had reached that level, but

---

[222] Mondelez Complaint, *supra* note 2, at 4.

[223] *Id.*

[224] *Id.* at 4–5.

[225] *Id.*

[226] Andrea Shalal, *Massive Cyber Attack Could Trigger NATO Response: Stoltenberg*, REUTERS (June 15, 2016, 5:38 PM), https://www.reuters.com/article/us-cyber-nato/massive-cyber-attack-could-trigger-nato-response-stoltenberg-idUSKCN0Z12NE.

some experts later indicated that the use of cyber capabilities by Russia against Ukraine was a prime example of what such warlike actions in cyberspace might look like.[227]

On March 29, 2017, just a few months before NotPetya hit Mondelez, Center for Strategic and International Studies adviser Olga Oliker testified before the Senate Armed Services Subcommittee on Emerging Threats and Capabilities that if an earlier attack on the Ukrainian electric grid had been perpetrated by Russia, then it was "an example of precisely the type of cyber operation that could be seen as warfare."[228] But whether the collateral damage of that operation and the malware designed for it, including the impacts of NotPetya on companies like Mondelez, could also be seen as warfare was less clear from Oliker's testimony.[229] Looking back at earlier lawsuits over the application of insurance war exclusions, many of which prominently feature public statements from political figures, journalists, and experts about whether the relevant events were akin to war, it is not hard to imagine Zurich building its case on statements like this one by Oliker. For instance, *Wired* reporter Andy Greenberg, who did extensive reporting on NotPetya and in 2020 published a book about it titled *Sandworm*, wrote in one of his widely read articles about the attack, "[t]he release of NotPetya was an act of cyberwar by almost any definition."[230]

Some courts—for instance, the Massachusetts Supreme Court in *Stankus* looking at President Roosevelt's address—have been swayed by public statements and popular coverage of the events at issue in insurance cases.[231] But this is typically only the case for courts that believe that the meaning of war in an insurance context is the same as its common meaning in everyday parlance. The more recent trend of war exception cases, since the *Pan Am* ruling, has been to insist on a narrower, insurance-specific definition of war that operates independently of the language and terms used by the broader public. In the *Holiday Inn* ruling, for instance, the deciding judge was quite ready to dismiss the fact that "[j]ournalists and politicians invariably referred to these events in Lebanon as a 'civil war'" on the

---

[227] *See, e.g.*, Greenberg, *supra* note 1; *Russian Influence and Unconventional Warfare Operations in the 'Grey Zone:' Lessons from Ukraine*: *Statement before the S. Armed Servs. Comm., Subcomm. on Emerging Threats and Capabilities,* 115th Con. (2017) (statement by Dr. Olga Oliker, Senior Adviser & Dir, Russ. and Eurasia Program, Ctr. for Strategic & Int'l Stud.), https://www.armed-services.senate.gov/imo/media/doc/Oliker_03-29-17.pdf [hereinafter *Statement by Dr. Olga Oliker*].

[228] *Statement by Dr. Olga Oliker*, *supra* note 227, at 5.

[229] *Id.*

[230] Greenberg, *supra* note 1.

[231] Stankus v. N.Y Life Ins. Co., 44 N.E.2d 687, 688–89 (Mass. 1942).

grounds that it was irrelevant to determining whether the conflict was a civil war in the "insurance meaning" of the words.[232] It seems plausible that a court could similarly dismiss references to NotPetya as an act of cyber war as irrelevant to the question of whether the cyberattack qualified as warlike in an insurance context.

One insurance broker, Marsh & McLennan ("Marsh"), took a strong stand to this effect in August 2018, shortly after Zurich denied Mondelez's claim, but before Mondelez filed its lawsuit. In a short article titled *NotPetya Was Not Cyber 'War'*, Matthew McCabe, Marsh's assistant general counsel for cyber policy, made the case that NotPetya was not a warlike action and should therefore not be excluded from insurance coverage under war exceptions.[233] "For a cyber-attack to reach the level of warlike activity, its consequences must go beyond economic losses, even large ones," McCabe wrote.[234] Furthermore, he pointed out, "[t]he most prominent victims of NotPetya operated far from any field of conflict and worked at purely civilian tasks like delivering packages, producing pharmaceuticals, and making disinfectants and cookies."[235] As the representative of an insurance broker, an organization that assists customers purchase insurance policies, McCabe clearly had an interest in representing his clients' interests and persuading them that continuing to purchase these types of policies was worthwhile and not a waste of money. But even if his motives may have been influenced by his employer's business interests, McCabe's concluding call for greater clarity in war exclusions is an important one. "[I]f insurers are going to continue including the war exclusion on cyber insurance policies, the wording should be reformed to make clear the circumstances required to trigger it."[236]

Perhaps the strongest piece of Mondelez's argument is that the language of Exclusion B.2(a) is "vague and ambiguous" and that "Zurich's failure to modify that historical language to specifically address the extent to which it would apply to cyber incidents" means it "therefore must be

---

[232] Holiday Inns Inc. v. Aetna Ins. Co., 571 F. Supp.1460, 1503 (S.D.N.Y. 1983).

[233] Thomas Reagan & Matthew McCabe, *NotPetya Was Not Cyber "War", in* MMC CYBER HANDBOOK 2019: PERSPECTIVES ON CYBER RISK IN THE DIGITAL ERA 18 (2019), https://www.marshmclennan.com/content/dam/mmc-web/insights/publications/2019/mar/OWY22801-076_Cyber-Handbook-2019-Digital.pdf.

[234] *Id.* at 18.

[235] *Id.*

[236] *Id.*

interpreted in favor of coverage."[237] The courts in *Pan Am*, *Holiday Inn*, and *Universal* ruled in favor of policyholders rather than their insurers in large part based on this rationale—that absent specific language excluding a certain scenario, courts were generally inclined to interpret the exclusions fairly narrowly.[238] On the other hand, in a certain light, NotPetya could be viewed as fitting even that narrow definition because, unlike the incidents in *Pan Am*, *Holiday Inn*, and *Universal*, the perpetrator appeared to be a sovereign government engaged in hostilities with another country. When the Second Circuit determined that the hijacking of Pan Am Flight 093 was not a warlike act, it based that decision largely on the fact that the hijackers' "acts had criminal rather than military overtones. They were the agents of a radical political group, rather than a sovereign government."[239] Similarly, the *Holiday Inn* ruling rested in part on the fact that "there was no 'war' in Lebanon between sovereign or quasi-sovereign states."[240] Neither of those rationales quite fit the NotPetya case, assuming one accepts the attribution of the attack to Russia and the extensive documentation that it was part of the conflict with Ukraine.

The *Universal* ruling offers perhaps the most support for Mondelez's contention that NotPetya was not a warlike action. In that case, the Ninth Circuit highlighted the "indiscriminate nature" of the unguided missiles used by Hamas as evidence that they were trying to injure and kill civilians, conduct that the court ruled was "far closer to acts of terror" than "warlike action."[241] NotPetya could also be viewed as an indiscriminate or unguided weapon, one that caused significant damage to civilian targets—including Mondelez. Indeed, Mondelez's distance from the Russia-Ukraine conflict could work in its favor. Just as the Second Circuit ruled that the Pan Am hijacking could not be considered a "warlike operation" because "that term does not include the inflicting of damage on the civilian property of non-belligerents by political groups far from the site of warfare,"[242] so, too, a court could conceivably determine that it was a stretch to deem "warlike" the

---

[237] Mondelez Complaint, *supra* note 2, at 16.

[238] Pan Am. World Airways, Inc. v. Aetna Cas. & Sur. Co., 505 F.2d 989, 1022 (2d Cir. 1974); Holiday Inns Inc. v. Aetna Ins. Co., 571 F. Supp.1460, 1503 (S.D.N.Y. 1983); Universal Cable Prods., LLC v. Atlantic Specialty Ins. Co., 929 F.3d 1143, 1162 (9th Cir. 2019).

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

[240] *Holiday Inns Inc.*, 571 F. Supp. at 1503.

[241] *Universal Cable Prods., LLC*, 929 F.3d at 1161.

[242] *Pan Am. World Airways, Inc.,* 505 F.2d at 997.

inflicting of damage on the civilian property of a multinational food company headquartered in Chicago, Illinois, far from Russia and Ukraine.[243]

V. CRAFTING WAR EXCLUSIONS FOR CYBERATTACKS

One of the more fascinating elements of Mondelez's lawsuit is its description of Zurich's behavior in the aftermath of issuing its formal coverage denial letter on June 1, 2018.[244] According to Mondelez, soon after sending that letter, Zurich appeared to change its mind and told the firm that it would rescind the declination of coverage and resume adjustment of Mondelez's claim.[245] On July 18, 2018, Zurich sent Mondelez an email "formally rescind[ing]" its previous coverage denial and promising to resume work on the claim.[246] Then, in another email sent less than a week later on July 24, Zurich offered Mondelez a $10 million partial payment towards the company's insurance claim.[247] However, that payment never materialized—nor did Zurich ever appear to resume work on the claim.[248]

Mondelez, in its complaint against Zurich, is quick to assert that these prevarications on Zurich's part stemmed from the insurer's fears that denying Mondelez's claim might lead to bad publicity.[249] The July 2018 emails, promising a $10 million advance payment and a continued claim adjustment process, were aimed at convincing Mondelez "to refrain from filing immediate litigation," the company alleges in its lawsuit.[250] If that was in fact the intention of those emails, then they seem to have worked since Mondelez waited until January 2019 to file its lawsuit, more than six months after its initial claim was denied by Zurich because of the "explicit representations and promises from Zurich" made in the July 2018 emails.[251]

Zurich was hoping to prevent, or at the very least delay, a lawsuit, Mondelez contended, because the insurer feared the publicity surrounding such a suit would draw attention to all the ways that Zurich policies might not actually cover cyberattacks.[252] Mondelez goes so far as to claim in its

---

[243] Mondelez Complaint, *supra* note 2, at 5.
[244] *Id*.
[245] *Id.*
[246] *Id.*
[247] *Id.*
[248] *Id.* at 6.
[249] *Id.* at 5.
[250] *Id.*
[251] *Id.*
[252] *Id.* at 8.

lawsuit that Zurich feared the publicity would "adversely impact its dealings with actual and prospective policyholders who were considering the purchase or renewal of insurance coverage from Zurich."[253] Whether or not this was actually the line of reasoning behind the mixed signals Zurich sent Mondelez in the summer of 2018, it is clear that the insurer was undecided, or at the very least uncertain, about how to handle the NotPetya claim. For one thing, it was an extraordinarily expensive cyberattack—the United States government dubbed it "the most destructive and costly cyber-attack in history" in February 2018, and later reports estimated that the damages totaled roughly $10 billion.[254]

For Zurich, and other insurers, the issues raised by the Mondelez claim were much larger than just coverage for the losses borne by one company—they spoke to the question of who would bear the costs NotPetya inflicted on hundreds of companies across the world. For instance, pharmaceutical firm Merck estimated that it had suffered $870 million in damages from NotPetya, ranging from its 30,000 infected laptop and desktop computers to its inability to meet demand for the Gardasil 9 vaccine used to prevent HPV.[255] Merck, like Mondelez, had extensive insurance coverage for property damage and catastrophic risks—a total of $1.75 billion in coverage, in Merck's case, less a $150 million deductible.[256] But most of Merck's thirty insurers and reinsurers, like Zurich, denied the pharmaceutical company's claims citing war exclusions. Merck, like Mondelez, subsequently sued those insurers—a group that included several prominent cyber-insurance providers such as Allianz and AIG—for $1.3 billion under its property insurance policies.[257] Merck's arguments for why the war exclusions do not apply to NotPetya closely mirrored Mondelez's, and primarily center on the claim that those exclusions were never intended to address cybersecurity incidents or tailored to that purpose. Merck argued:

> The "war" and "terrorism" exclusions do not, on their face, apply to losses caused by network interruption events such

---

[253] *Id.* at 17.

[254] Andy Greenberg, *The White House Blames Russia for NotPetya, the 'Most Costly Cyberattack in History',* WIRED (Feb. 15, 2018, 6:20 PM), https://www.wired.com/story/white-house-russia-notpetya-attribution.

[255] David Voreacos, Katherine Chiglinsky & Riley Griffin, *Merck Cyberattack's $1.3 Billion Question: Was It an Act of War?*, BLOOMBERG L. (Dec. 3, 2019, 12:01 AM), https://www.bloomberg.com/news/features/2019-12-03/merck-cyberattack-s-1-3-billion-question-was-it-an-act-of-war.

[256] *Id.*

[257] *Id.*

> as NotPetya, . . . [t]hey do 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.[258]

In an opinion in the Merck case issued on December 6, 2021, Judge Thomas J. Walsh sided with Merck, ruling that the war exclusion in its property insurance did not apply to NotPetya because Merck's "reasonable understanding of this exclusion involved the use of armed forces, and all of the caselaw on the war exclusion supports this interpretation."[259] Walsh particularly called out the insurance companies for failing to update the language of the exclusion if they intended for it to cover state-sponsored cyberattacks, pointing out that "the language used in these policies has been virtually the same for many years."[260] He continued, "both parties to this contract are aware that cyber attacks of various forms, sometimes from private sources and sometimes from nation-states have become more common. Despite this, Insurers did nothing to change the language of the exemption to reasonably put this insured on notice that it intended to exclude cyber attacks. Certainly they had the ability to do so."[261] This portion of the ruling strongly suggests that insurers will now hasten to change those exceptions to more explicitly rule out coverage for large-scale cyberattacks—if they have not done so already.

Undoubtedly, property and other types of insurance policies dealing with cyber risks will contain exactly that sort of language in the future, due in no small part to NotPetya and the resulting, as-yet-unresolved disputes initiated by companies like Mondelez and Merck. On November 13, 2019, the Lloyd's Market Association introduced new cyber exclusions, the Property D&F Cyber Endorsement, or LMA5400, and the Property Cyber and Data Exclusion, LMA5401, both of which would exclude from coverage any losses resulting from malicious cyber acts as well as non-malicious cyber incidents resulting from errors or omissions in the operation of computer

---

[258] *Id.* (quoting Plaintiff's Requests to Produce Documents, Merck & Co. v. Ace Am. Ins. Co., No. UUN-L-2682 (N.J. Super. Ct. Law Div. Aug. 1, 2019)

[259] Merck & Co. v. Ace Am. Ins. Co., No. UUN-L-2682 at 8 (N.J. Super. Ct. Law Div. Dec. 6, 2021) (Bloomberg Law, Court Dockets).

[260] *Id.* at 10.

[261] *Id.* at 10–11.

systems or any outages or malfunctions of those systems.[262] NotPetya and the resulting claims activity did not just reshape the cyber exclusions in property policies, it also had a profound influence on the exclusions written into stand-alone cyber policies as well. In this case, however, insurers were more concerned about assuaging customers' concerns that war exclusions would prevent them from being able to exercise such policies. Kenneth Abraham and Daniel Schwarcz point out that construing war exclusions to apply broadly to cyberattacks initiated by nation states could lead to exclusion of many types of online threats that policyholders would expect to have covered by cyber-insurance policies.[263] They note that, "unlike in traditional insurance settings, it is often difficult or impossible for cyber insurers to identify and exclude from coverage the casual mechanisms of potentially catastrophic cyber risks without eviscerating coverage for ordinary cyberattacks that policyholders demand."[264]

In order to reassure policyholders that stand-alone cyber policies would still be useful in the wake of NotPetya claim denials, cyber-insurers began to explicitly include coverage for "cyberterrorism" in those products, without ever quite clarifying how cyberterrorism differed from warlike acts. For instance, Zurich's stand-alone cyber-insurance policy template, covering first- and third-party losses related to breaches, extortion, privacy incidents, and social engineering, included a "War or Civil Unrest" exclusion for costs incurred by:

> 1. war, including undeclared or civil war;
> 2. warlike action by a military force, including action in hindering or defending against an actual or expected attack, by any government, sovereign, or other authority using military personnel or other agents; or
> 3. insurrection, rebellion, revolution, riot, usurped power, or action taken by governmental authority in hindering or defending against any of these.[265]

---

[262] Andrew Hill, *Cyber Risk Poses Ongoing Challenge for First-Party Property Damage Lines of Business,* WILLIS TOWERS WATSON (Jan. 28, 2020), https://www.willistowerswatson.com/en-US/Insights/2020/01/cyber-risk-poses-ongoing-challenge-for-first-party-property-damage-lines-of-business.

[263] Abraham & Schwarcz, *supra* note 11, at 37.

[264] *Id.*

[265] ZURICH CYBER INSURANCE POLICY U-SPR-200-A CW (09/18) 23 (2018) (on file with author).

However, perhaps in recognition of the concerns policyholders might have about this exclusion following the Merck and Mondelez claim denials, the Zurich policy explicitly stated that their war and civil unrest exclusion did not apply to "cyberterrorism."[266] The policy defined cyberterrorism separately as:

> [T]he use of information technology to execute attacks or threats against Your Network Security by any person or group, whether acting alone, or on behalf of, or in connection with, any individual, organization, or government, with the intention to:
>
> 1. cause harm;
> 2. intimidate any person or entity; or
> 3. cause destruction or harm to critical infrastructure or data, in furtherance of financial, social, ideological, religious, or political objectives.[267]

In a 2020 analysis of fifty-six cyber-insurance policies, Daniel Woods and Jessica Weinkle suggested that this emerging trend for cyber-insurance to affirmatively cover cyberterrorism had "weakened" the war exclusions in such policies.[268] But it was not clear from those broad definitions which category an attack like NotPetya would fall under, so the inclusion of cyberterrorism in their coverage did little to resolve the ambiguities and uncertainty faced by policyholders.

The rewriting of insurance policy exclusions is typical of the aftermath of significant legal controversies over denied claims tied to war. For example, Sun Life broadened its life insurance exception to apply to "war, whether declared or not" after Pearl Harbor,[269] and Aetna excluded hijackings following the explosion of Pan Am Flight 093.[270] Clearly, insurers need to do a better job of describing more clearly which computer-based threats are excluded from their coverage, but rephrasing the insurance exclusions that apply to cyber risks will be no small feat for insurers as the

---

[266] *Id.*

[267] *Id.* at 8.

[268] Daniel W. Woods & Jessica Weinkle, *Insurance Definitions of Cyber War,* 45 GENEVA PAPERS ON RISK & INS. 639, 639 (2020).

[269] Cladys Ching Pang v. Sun Life Assurance Co. of Can., 37 Haw. 208, 208, 211 (1945).

[270] Pan Am. World Airways, Inc. v. Aetna Cas. & Sur. Co., 368 F. Supp 1098, 1120 (S.D.N.Y. 1973), *aff'd*, 505 F.2d 989 (2d Cir. 1974).

attempts to differentiate between cyber war and cyberterrorism already indicate. Defining clearer exclusions for cyberattacks will be challenging both because of the broad range of threats carriers have to consider, and because at the same time, they are trying to exclude certain threats. Many insurers are also aggressively developing and marketing cyber-insurance policies designed to cover other, closely related online threats.

One of the striking differences between the definitions of warlike actions and cyber terrorism in these cyber-insurance policies is that while the former relies primarily on attribution and being able to reliably identify whether or not a nation state, governmental authority, or military force is the perpetrator of an attack, the latter focuses instead on the impacts of the incident in question. Classifying cyberattacks according to the kind of damage they do to data or critical infrastructure has several advantages over trying to categorize them based on their perpetrators and broader political context. First, attribution remains a challenging and slow process for many cyberattacks, but the impacts of those incidents are often much clearer and less controversial in their immediate aftermath. So using those impacts as a means of determining whether a cyberattack is covered under an insurance policy has the potential to avoid disputes over attribution and instead focus on the less contentious fall-out of those attacks. Second, this approach could allow for the disaggregation of different victims impacted by the same malware or attack vector. Instead of considering NotPetya as a piece of malware, to be itself a warlike act because it was created by a particular entity, the code's impacts on different victims and targets could be evaluated separately, each in their own respective context. This would help address the challenge of narrowly targeting cyberattacks and the subsequent wide range of geographically diverse collateral damage that can result from the release of malware. Moreover, while this approach would certainly not solve the threat of correlated risks, it might reframe the risk correlation challenges that insurers face in modeling and covering cyber risks. By allowing the disentangling of different victims affected by the same piece of malware, or other attack vector, insurers might be able to reconsider how they can use the different threats that their policyholders face to allow for more diversification of their risk pools. For instance, this might allow for the risks that critical infrastructure operators face to be treated differently from those faced by other firms—even if all of those policyholders could be affected by the same piece of malicious code. It will still be the case that a single piece of malware can cause widespread and varied damages to many victims across different sectors and locations, but perhaps for insurance purposes, it would make more sense to consider which of those types of damages are

covered or not, rather than arguing over which types of attacks are or are not excluded from a policy.

Over time, war exclusions in insurance policies have been shaped by a series of historical events to encompass an increasingly broad range of activities carried out by a variety of different actors. As concerns that these exclusions may be overly broad (when it comes to cyberattacks) force insurers to start crafting explicit inclusions for cyberterrorism activity, it may be time to consider whether the historical emphasis of these exclusions on being able to definitively identify the perpetrator and motive of such attacks is ill-suited to the nature and breadth of cyberattacks. Instead, there may be more value in predicating such exclusions of large-scale cyberattacks that present the possibility of significantly correlated risks on their particular victims, impacts, and scale—characteristics that are both more easily verified and allow for more granular distinctions in the cyber domain.