5

"INSURRECTION, REBELLION, REVOLUTION, RIOT": NOTPETYA, PROPERTY INSURANCE, AND WAR EXCLUSIONS

In June 2017, the multinational food company Mondelez International was hit by the NotPetya virus. NotPetya exploited a vulnerability in the Microsoft Windows operating system to encrypt the contents of infected computers' hard drives and demanded a ransom payment of roughly $300 worth of Bitcoin before it would turn the contents of the computers back over to their owners. NotPetya infiltrated more than eighty companies worldwide during the summer of 2017, including Mondelez, which had to shut down 1,700 servers and 24,000 laptops due to NotPetya infections. In the aftermath of the incident, Mondelez filed a claim with its insurer, Zurich American Insurance, 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." 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. Mondelez filed a $100 million lawsuit against Zurich in October 2018 and the case (unresolved at the time of writing) serves as a reminder of how cyber risks—and, by extension, the types of costs that companies look to their insurers to help cover—have changed since the early days of data breach liability insurance policies.[1]

Early cyberinsurance policies focused on coverage for breaches of personal data, both because those were the incidents about which insurers had the most information, thanks to breach notification laws, and because they were the incidents that businesses—especially retailers—were primarily concerned would cost them money, again because of the mandatory notification in most states. However, as the landscape of online threats broadened, businesses in all sectors began to face a new set of costly and serious risks, ranging from ransomware to cloud service outages to economic espionage.

As the threat environment continued to evolve, businesses also began realizing the limitations of their existing CGL and commercial crime insurance policies and began clamoring for more coverage of threats beyond straightforward data breaches. Since 2015, a whole host of specialized cyberinsurance offerings have emerged to meet this demand, from personal cyberinsurance for high-net-worth individuals to online extortion insurance, coverage for business interruptions due to third-party vendor outages, and even policies that cover renting temporary equipment and services to withstand denial-of-service attacks. Embedded in these new, specialized cyberinsurance policies, however, is a set of fairly boilerplate exceptions, many of which are drawn from other areas of insurance, including CGL and property insurance. While these exceptions may be more routine or immediately understandable when applied to other types of risk, they often present unique problems and complications when it comes to dealing with cyber risks, both because of the nature of these risks and the patchwork nature of cyberinsurance coverage.

The "warlike action" exclusion in Mondelez's property coverage raises difficult questions about what constitutes war (or "warlike" activity) in the online domain. Since the lines distinguishing 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 no longer uncommon and excluding them from coverage could place a significant burden on policyholders. Moreover, the lengthy and sometimes contentious process of determining 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.

PROPERTY INSURANCE AND OPEN-PERIL COVERAGE

Modern property insurance coverage derives from two of the oldest forms of insurance, maritime and fire insurance. Forms of insurance for both marine expeditions as well as fire damage date back centuries and William Reynolds Vance describes the emergence of both in his 1904 *Handbook of the Law of Insurance*, tracing the start of early mutual insurance contracts for ships and their cargo back to the early thirteenth century in the maritime

states of Italy. According to Vance, Italian merchants introduced the practice in England and prominent British insurer Lloyd's got its start in these contracts arranged among maritime merchants in the late seventeenth century. Edward Lloyd owned a London establishment called Lloyd's Coffee House where merchants would gather and arrange their insurance contracts, with individuals who wanted to insure particular voyages writing their names or initials beneath descriptions of the expedition written on slips of paper. It was through this process that insurers came to be known as "underwriters."[2]

The seventeenth century also witnessed the beginning of the business of fire insurance, according to Vance, who cites the Great Fire of London of 1666 as the motivation for many British insurance brokers to begin issuing fire coverage, followed closely by the establishment of the first fire insurance company, Sun Fire Office, in 1710.[3] Insurance policies covering fire damage were less well received in England than those for maritime expeditions because of a concern that fire insurance would cause more incidents of arson. Indeed, this appeared to be the case for a period during the mid-nineteenth century when fire insurance grew rapidly in popularity, accompanied by a significant increase in the overall number of fires, the number of fires per household and per capita, and the percentage of fires in England determined to be "of suspicious origin," which rose from 34.5 percent of fires in 1852 to 52.5 percent of fires in 1866.[4] In the United States, however, fire insurance met with much greater success following the formation in 1752 of the first US fire insurance company, the Philadelphia Contributionship for Insuring Houses from Loss by Fire, for which Benjamin Franklin served as one of the directors.[5]

While both early marine and fire insurance policies dealt with protections for loss of or damage to property, they developed according to very different models. John Gorman points out that "in the early days of insurance, the greatest single hazard to property on land was fire, whereas the hazards to property being transported by sea were inexhaustibly many."[6] Therefore, fire insurance was tied to a particular type of risk—fire damage—whereas marine insurance was typically written or designed to cover "all the perils of the sea." The latter model is sometimes referred to as "all risks" or "open peril" coverage, as opposed to "specified peril" or "named peril" insurance, such as fire policies, that specify precisely what type of risk they cover. The distinction is an important one for cyberinsurance coverage because of how difficult it can

be to pin down specific cyber risks for this type of coverage—even a relatively straightforward risk like "computer fraud" is open to a variety of different interpretations and variations—and how wary many insurers are of taking an all risks approach to covering such a complicated and constantly changing set of threats. The development of modern property insurance in the twentieth century centered largely on the development of all risk or open peril commercial and homeowner policies that appealed to insurance customers because they offered broad coverage against direct losses to their property.[7]

Open peril property insurance grants policyholders protections for all "direct physical loss to property" except for certain types of losses that are specifically excluded. As Kenneth Abraham points out, "this approach places great pressure on the exclusions and limitations to coverage. If a particular form of direct physical loss to property is not excluded, it is covered."[8] This is also the case with CGL policies, but the exclusions in CGL insurance and property insurance policies follow two converse principles. Abraham explains, "In property insurance there is no coverage unless the peril causing damage comes from the outside-in, so to speak. In contrast, in CGL insurance there is no coverage unless the damage for which the insured is held liable comes from the inside-out."[9] This distinction helps explain why Sony was denied coverage for its 2011 data breach under a CGL policy—the damage came from outside the company, hence Justice Oing's insistence that what really mattered was that outside hackers had perpetrated the breach, not whether Sony had been negligent. It also hints at the reasons why property insurance might be a more attractive tool than CGL for policyholders seeking coverage for cyber-related damages perpetrated by outside attackers. Property insurance wouldn't help with coverage of third-party liability costs, of course, but especially as computer systems become increasingly connected to various forms of physical property, the first-party costs of cyberattacks were becoming increasingly significant, especially since first-party insurance could include coverage for notification costs and business interruption, which were significant components of many cybersecurity incidents.

Even before the growth in cyber-physical systems, some insurance customers were already looking to their property insurance to cover certain types of computer-related costs. In the late 1990s, many large companies were scrambling to update their computer systems in order to avoid any Y2K-related failures when the two-digit year field for the date reset to "00"

on January 1, 2000. For the most part, these efforts were successful at preventing significant damage or interruptions but the maintenance and updating work required was extensive and expensive. Several organizations later filed claims to recoup portions of those costs under their property insurance "sue and labor" provisions. Sue and labor clauses typically provide coverage to policyholders who take steps to prevent imminent losses or damages that, had they occurred, would have been covered by those same property insurance policies.[10] Many of those Y2K claims were denied, prompting a series of lawsuits in 2000 brought by companies including Kmart, The Gap, Mandalay Resort Group, and Nike.[11]

These suits were largely unsuccessful; several courts ruled that the losses these companies had averted by updating their computer systems would not have been covered under their property insurance policies in the first place, and therefore the sue and labor provisions did not apply to the mitigation costs. For instance, in a 2004 ruling, the Third Circuit Court of Appeals found that telecommunications firm GTE could not claim coverage for remediating its computers systems to address Y2K glitches. GTE's property insurance through Allendale Mutual Insurance Co. included a standard sue and labor clause that covered situations where the policyholder faced "actual or imminent loss or damage" to their property from a risk that the policy covered. Under those circumstances, GTE would be permitted to "sue, labor, and travel for, in, and about the defense, the safeguard, and the recovery of the property" and Allendale would "contribute to the expenses so incurred according to the rate and quantity of the sum herein insured."[12] In other words, if GTE could show that the damage that would have resulted from not fixing the Y2K problem would have been covered under their property insurance then they might also be able to use that policy to cover the costs of preemptively mitigating that damage.

Although the Y2K glitch would have been unlikely to cause significant physical property damage, GTE's decision to file a claim with its property insurer stemmed from a common provision in its policy that included coverage for "loss resulting from necessary interruption of business conducted by the Insured and caused by loss, damage, or destruction by any of the perils covered herein." Those perils included not just physical losses but also "any destruction, distortion or corruption of any computer data, coding, program or software except as hereinafter excluded."[13] This type of property insurance coverage for business interruption losses would be especially

important for later cases, including the Mondelez one, in which cybersecurity incidents like ransomware or denial-of-service attacks prevented businesses from conducting their normal operations, even if they did not result in any outright theft or physical damage.

GTE's policy, like all open peril insurance, also included several exclusions. The Third Circuit ultimately ruled that two of those barred the potential Y2K damages from being covered under the policy and thereby barred the mitigation work from being covered under the sue and labor clause as well. The two exclusions in GTE's property insurance that the Third Circuit focused on were the defective design and inherent vice exclusions. The former precludes coverage for "the cost of making good defective design or specifications" and the Third Circuit, agreeing with a previous district court ruling, determined that the Y2K problem was one of defective design and therefore excluded from coverage under the property policy. "The essence of the Y2K problem is that the two-digit date design precludes the system from functioning properly on or after January 1, 2000. The problem in this case was not that a program or system malfunctioned, or some external threat caused damage to GTE's systems," the court ruled. "Rather, the system performed in exactly the manner it was designed to operate—the problem is that the system as designed and specified did not permit recognition of dates in the 21st century."[14]

Additionally, the Third Circuit found that even if the Y2K bug had not been a matter of defective design, any damage it caused would still have been excluded from coverage under GTE's property insurance because of the "inherent vice" exclusion which applied to "any existing defects, diseases, decay or the inherent nature of the commodity which will cause it to deteriorate with a lapse of time." The Third Circuit cited another Y2K property insurance lawsuit, brought by the Port of Seattle against its insurer, Lexington Insurance Co., and decided two years earlier in 2002, also in favor of the insurers. In that case, Judge Susan R. Agid of the Court of Appeals of Washington had determined that "but for the two-digit date field code programmed into the Port's software, the arrival of January 1, 2000, would not result in loss. Thus, the Port's Y2K problem is an excluded inherent vice because the date field is an internal quality that brought about its own problem."[15] The Third Circuit agreed and similarly disqualified GTE's claim that Y2K-related damages would have been covered under their property insurance policy.

The Y2K cases also coincided with the insurance industry beginning to craft specific exclusions aimed at cyber losses, perhaps in part because of the attention Y2K had brought to the potential for digital problems to cause significant losses. In 2001, Lloyd's Underwriters' Non-Marine Association (NMA) developed two exclusions, Electronic Data Endorsements A and B (also referred to as NMA 2914 and NMA 2915), that excluded coverage for the "loss, damage, destruction, distortion, erasure, corruption or alteration of electronic data," though they did allow for coverage of fires or explosions caused by computer malfunctions.[16] Those exclusions were widely adopted by property insurers in the early 2000s, spurred in part by rumors that reinsurers were planning to include NMA 2914 or 2915 in their reinsurance policies beginning in 2002.[17] Then, in 2003, the insurance industry developed the Institute Cyber Attack Exclusion Clause, also known as CL380, which excluded losses "arising from the use or operation, as a means for inflicting harm, of any computer, computer system, computer code, computer virus or process or any other electronic system." The CL380 coverage exemption clauses also became popular with property insurers, enabling them to deny coverage for malicious cybersecurity incidents.[18] The development and adoption of these early cyber-focused exclusions in property insurance policies spoke to carriers' heightened awareness about cyber risk in the aftermath of Y2K and the resulting claims disputes—despite the fact that insurers were triumphant in most of those disputes because courts generally held that policyholders had created the Y2K software problems themselves, internally.

Ten years later, when Justice Oing ruled in the Sony data breach case, he would disqualify Sony's claims under its CGL policy for exactly the opposite reason: the breach had been caused by external factors, rather than by Sony bringing about its own problem. This reflects Abraham's point about the converse nature of property and CGL insurance exclusions such that the former covers only damage that "comes from the outside-in" and the latter only applies to liability resulting from damage that "comes from the inside-out." In the case of NotPetya, however, the damage to Mondelez, and many other firms, clearly originated from the outside—later reports attributed the malware to the Russian government, but even before victims understood who was behind the incidents, there was no question that some outside third party had initiated the widespread ransomware attacks. So Zurich could not rely on the defective design or inherent vice exclusions

wielded by insurers to such great effect following Y2K. Instead, to avoid covering the most expensive cyberattack in history, Zurich would have to look to one of the many other exclusions in the Mondelez property policy.

"WAR IN THE ONLY SENSE THAT MEN KNOW AND UNDERSTAND IT": WAR EXCLUSIONS AND PEARL HARBOR

The exclusion Zurich pointed to in Mondelez's property insurance covered losses or damage directly or indirectly caused by "hostile or warlike action in time of peace or war." The practice of excluding war risks from open peril insurance policies dated back more than one hundred years before NotPetya. Originally, in the eighteenth and nineteenth centuries, 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. However, in 1898, Lloyd's added a "free of capture and seizure" (FC&S) clause to its general marine cargo clause that excluded coverage for any losses caused by war. As FC&S 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. 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 80 percent of the war risks insurers underwrote. 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. 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 evolved from their roots in marine insurance to become a common feature of 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. 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. 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, where their son had purchased a $1,000 life insurance policy prior to his death and named them as beneficiaries. Idaho Mutual denied the claim because Rosenau's policy included an exclusion for "death, disability or other loss sustained while in military, naval, or air service of any country at war."[19]

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 the Rosenaus, ordering Idaho Mutual to pay them the full $1000 due under their son's policy. The insurer appealed this decision to the Idaho Supreme Court, arguing that the United States was already at war when Howard Rosenau died at Pearl Harbor, and his death was therefore excluded from coverage. To support this argument, Idaho Mutual cited the preamble of the resolution that 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." The preamble of that document stated, "the Imperial Government of Japan has committed unprovoked acts of war." It concluded, "The state of war between the United States and the Imperial Government of Japan, which has been thrust upon the United States is hereby formally declared." These references to the Pearl Harbor attack as an "unprovoked act of war" and a preexisting "state of war" between the United States and Japan that was merely codified, not initiated, by Congress on December 8, meant that the Pearl Harbor attack occurred in a "country at war," Idaho Mutual argued.[20]

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. If the court accepted the insurer's interpretation of what it meant to be "at war" then that "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 hostilities in some force along the border

between Manchuria and Russian Siberia," the Rosenaus' lawyers wrote in response to Idaho Mutual's appeal. 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 led to actual wars that were declared as such by the nations involved. "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," the Rosenaus pointed out. "It was possible, no matter how improbable, that the Pearl Harbor attack could have been atoned for and adjusted without 'war' necessarily ensuing."

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

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," the Idaho Supreme Court determined. 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."

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. "Where 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*," Justice James F. Ailshie wrote in his dissent. 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." 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, according to him, "Our 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."

While the Rosenaus were ultimately successful in forcing their son's insurer to pay out his policy in 1944, other beneficiaries met with more mixed results. In 1942, two years prior to the final ruling in the Rosenau case, for instance, the Supreme Court of Massachusetts had ruled against Marcella Stankus, who was seeking a life insurance payout from New York Life Insurance Company following the death of Anthony Stankus in 1941. Anthony, like Howard Rosenau, was a Navy seaman, second class. Unlike Rosenau, though, he did not die at Pearl Harbor—he died two months earlier, on October 30, 1941, when his ship, the USS *Reuben James* was sunk by a torpedo in the Atlantic Ocean. Like Rosenau, Stankus died in possession of a life insurance policy with a war exclusion. The exclusion in Stankus's policy was worded slightly more broadly than the one in Rosenau's to rule out coverage for death resulting "directly or indirectly from war or any act incident thereto."[21] 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.

An early judgment by a lower court had agreed with that argument, holding that the insurer must pay out the full claim to Marcella, but when New York Life Insurance appealed that decision, the Supreme Judicial Court of Massachusetts sided with them, reversing the initial decision. Justice James Joseph Ronan authored the 1942 opinion, writing that "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."[22] Two years later, in his dissent in the Rosenau case, 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*. 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."[23] In his dissent, Ailshie 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. This line of reasoning would be relevant for NotPetya as well, since the ongoing conflict that the malware was designed for was between Russia and Ukraine, but the damage inflicted by it spread well beyond the borders of those two countries.

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 decision similar to that of the Idaho court, ruling in favor of Gladys Ching Pang, who was suing Sun Life Assurance Company of Canada for refusing to pay out the life insurance policy of her husband, Tuck Lee Pang, a Honolulu Fire Department employee who had died at Pearl Harbor. "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," the Hawaii Supreme Court concluded, ruling 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.[24]

Then, 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 the *Stankus* case by reversing a judgment for the beneficiaries of the life insurance policy belonging to Captain Mervyn S. Bennion, a naval officer from Utah who died at Pearl Harbor on the battleship *West*

Virginia. Bennion's life insurance policy, also issued by New York Life Insurance, 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.[25]

The difference between the outcomes in favor of the insurers in the *Stankus* and *Bennion* cases 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 Idaho and Hawaii courts in *Rosenau* and *Pang* were in favor of a very narrow, legalistic interpretation of war. 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. The Tenth Circuit insisted that "mankind . . . does not stand on ceremony or wait for technical niceties" in its "definitive search" to understand what war is.[26] In a similar vein, the Massachusetts court argued that "the words of an insurance policy . . . must be given their usual and ordinary meaning." That "ordinary meaning," the court held, was determined by "ordinary people" and what they would consider to be war. Ronan explained: "The 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."[27] This "ordinary person" test presents significant challenges when applied to emerging notions of cyberwar, where there is little consensus or common 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* relies 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. Ronan cited a September 11, 1941, address by President Roosevelt in which he declared, "From now on, if German or Italian vessels of war enter the waters the protection of which is necessary for American defense, they do so at their own peril," as well as the passage of the Lend-Lease Act in March 1941 as indicators that the United States was

already effectively engaging in war-related activities at the time of Stankus's death. Ronan wrote:

> 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 conveying 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.[28]

It's striking that the president's statements carried so much weight with the Massachusetts court 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 court in the *Rosenau* case, dealing with an incident that occurred much closer to the official declaration of war in the United States. This uncertainty around the weight of public statements about the warlike nature of certain events also has important implications for cybersecurity incidents, particularly since terms like "cyberwar" are thrown around freely for political purposes with relatively little consistency or clarity about what they actually mean.

The very different rulings in the *Stankus* and *Bennion* cases as compared to the *Rosenau* and *Pang* disputes also make clear just how important the specific language of the actual exclusion written into an insurance policy can be. In the *Rosenau* ruling, for instance, the majority justified its decision to diverge from the rationale used to decide the *Stankus* case by stating that the war-related provisions in Stankus's life insurance coverage were "quite different" from those included in Rosenau's policy. Unlike the Stankus and Bennion policies, which excluded deaths that "resulted from war or any act incident thereto," the Rosenau policy specifically excluded injuries "sustained while in military, naval, or air service of any country at war." The Idaho court focused particularly on the phrase "at war," arguing that it "very clearly" meant the exclusion applied only during a time when war had been legally declared. 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 RMS *Lusitania*, when it was sunk by a German submarine. In that case—which the beneficiaries of Vanderbilt's life insurance lost against his insurer, Travelers—the war exclusion had ruled out coverage for deaths "resulting, directly or indirectly, wholly or partly, from war or riot." The absence of that crucial reference to a "time of war" differentiated the Vanderbilt policy from the Rosenau policy, the Idaho Supreme Court decided, giving Travelers more leeway to interpret the sinking of the *Lusitania* as an excluded act than Idaho Mutual had to interpret Pearl Harbor as occurring "in time of war."

In other words, the majority in the Rosenau ruling did not hold that Pearl Harbor was any less an act of war than the torpedoing of the *Lusitania* or the USS *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. Pang's life insurance policy issued by the company had excluded death "resulting from riot, insurrection, or war," but shortly after Pearl Harbor the company modified that exclusion in new policies, inserting, after the word "war," the words "whether declared or not."[29]

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 was not unique to life insurance, it spread into other insurance products, too, including property insurance. For instance, the policy Mondelez had purchased from Zurich before 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."[30] 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. 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. The New York court cited an even older maritime law case, decided in 1800, in which the US Supreme Court had ruled that "every contention by force between two nations in external matters under authority of their respective governments is not only war, but public war."[31] Going by that logic, the New York Supreme Court 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.[32]

Twenty-six years later, the Tenth Circuit would use a similar rationale in deciding the *Bennion* case and determining that Pearl Harbor was an act of war, asserting that "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."[33]

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. The ransomware attacks were not violent, they did not look 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 by many to be Russia—a sovereign government. However, most of the victims, including Mondelez, were private entities, so NotPetya was not exactly a "contention by force between two nations." This was yet another way in which cyberattacks complicated traditional interpretations of war and war exclusions—the entanglement of public and private actors under circumstances that insurers and earlier insurance disputes had not anticipated and for which insurers had not devised clear rules.

"A MOST UNUSUAL AND EXPLICIT CONTRACT": TERRORISM AND OVERLAPPING COVERAGE

Pearl Harbor and the sinking of the *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" 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. A series of more recent insurance disputes dealing with circumstances further removed from war than the *Lusitania* or Pearl Harbor sheds some light on how war exclusions might apply to situations like NotPetya, as well as the role of these exclusions in property insurance policies, like the one Mondelez had purchased from Zurich. These cases reveal how much remains uncertain and unclear in the interpretation of insurance policy war exclusions, particularly when it comes to distinguishing between acts of war and acts of terrorism.

On September 6, 1970, Pan American Flight 093 was hijacked by two passengers, forty-five minutes after the Boeing 747 had departed from Amsterdam, heading to New York. 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). After the hijackers threatened to blow up the plane in midair, Lebanese officials permitted the flight to land in Beirut on the condition that it refuel and then leave. 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. Egyptian officials permitted the plane to land after the hijackers lit the fuses of the explosives while the plane was still in the air. 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. The explosives detonated on schedule and the plane was destroyed. Pan Am filed a claim with its insurers for the value of the aircraft, totaling $24,288,759.[34]

Pan Am had purchased comprehensive insurance coverage from several different insurers. From Aetna Casualty and Surety Co., 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." Despite its name, that insurance came with a long list of exclusions, including any losses or damage resulting from:

1. capture, seizure, arrest, restraint or detention or the consequences thereof or of any attempt threat, or any taking of the property insured or damage to or destruction thereof by any Government or governmental authority or agent (whether secret or otherwise) or by any military, naval or usurped power, whether any of the foregoing be done by way of requisition or otherwise and whether in time of peace or war and whether lawful or unlawful . . . [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"].[35]

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. That coverage had an upper limit of $14,226,290.47 in coverage and covered the three clauses of excluded risks in the all-risk policy, verbatim. 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 first two clauses of the all-risk insurance exclusions. This coverage Pan Am obtained from the Secretary of Commerce who is authorized under the Federal Aviation Act of 1958 to issue insurance for risks that are excluded from commercial policies under "free of capture and seizure" clauses, like the first two clauses in Pan Am's all-risk policies exclusions. Because the US government was authorized only 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 all-risk insurers to make an additional premium payment of $29,935 in order to delete the third clause of its exclusion that had previously ruled out coverage for "strikes, riots, [and] civil commotion" and cover damage caused by those risks up to $10,062,393.

At the time of the hijacking, Pan Am therefore had a complicated patchwork of insurance coverage, and the question of which of its many insurers was responsible for covering the damage to the airplane depended on which

of the three clauses of the exclusion the hijacking fell under. If the hijacking was deemed to be a clause 1 peril ("capture, seizure . . . or any taking . . . by any military . . . or usurped power") or a clause 2 peril ("war . . . civil war, revolution, rebellion, insurrection or warlike operations"), then Aetna and the other all-risk insurers would be off the hook for it and coverage would be paid by Lloyd's ($14,226,290.47) and the US government ($9,763,709.53), totaling $23,990,000. On the other hand, if the hijacking was deemed to be a clause 3 peril ("riots, civil commotion"), then Pan Am would be owed $10,062,393 from Aetna as well as an additional $14,226,290.47 from Lloyd's, totaling $24,288,683.47. Finally, if the hijacking was determined not to fall into any of the excluded categories of risks described in the three clauses, then Aetna and the other all-risk insurers would be responsible for the entire $24,288,759 claim for the destroyed plane.[36] This arrangement of dividing up different types of large-scale risks into a set of consistent categories that can then each be covered by the appropriate entities, whether private-sector carriers or governments, offers certain lessons for cyberinsurance, as well. If insurers and policymakers were able to agree on what cyberwar was, then it might be possible for each to offer certain types of complimentary coverage that would enable policyholders to be confident that whatever a court determined about the nature of a particular incident, they would still be covered.

Unsurprisingly, all of the insurers claimed that the Pan Am 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 clause 1 and 2 exclusions—the ones it had no responsibility to cover—because it was perpetrated by a "military . . . or usurped power" and was an example of "revolution, rebellion, insurrection or warlike operations." Lloyd's and the US government argued that the hijacking did not fall under any of the exception clauses, all of which were covered by their war risk policy, and was therefore entirely the responsibility of the all-risk insurers. Pan Am itself took this position as well, arguing that the hijacking was not an excluded risk, hence their decision to sue Aetna. Pan Am further argued that, if the hijacking was an excluded risk, then it fell under the clause 3 exclusion as a "riot" or "civil commotion." 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.[37]

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 lengthy decision that discussed the political circumstances surrounding the Middle East and the PFLP at some length. 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. 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 . . . [and] gives Israel Fantom airoplanes which attack our camps and burn our village." Aetna argued that the "seizure and destruction of the aircraft were announced by the group as a blow and as retaliation against the United States," and concluded that "these facts alone would be sufficient to place the loss under the broadly drawn war risk language." Frankel rejected these arguments for relying on an overbroad definition of war. Aetna's justification for why the hijacking of the Pan Am plane qualified for the war risk exclusion "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," Frankel pointed out.[38] Nor did he allow that the larger Arab-Israeli conflict was to blame for the hijacking or could be said to have "proximately caused" the incident.

Several courts ruling 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 them to be considered acts of computer fraud. Similarly, Frankel felt there was too much distance—both literal and metaphorical—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. "It 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 'Conflict,' acts of 'war' for insurance purposes," Frankel wrote in his ruling.[39] And Aetna had not, in Frankel's view, authored a sufficiently explicit (or unusual) contract for this purpose. In fact, the judge noted that, 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." 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.[40]

In 1974, the Second Circuit Court of Appeals upheld Frankel's ruling, agreeing with him 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." 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 was therefore still covered under the exceptions listed in clause 1. But the Second Circuit decided that "in order to constitute a military or usurped power the power must be at least that of a de facto government" and the PFLP did not meet that bar in their view. 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 "the hijackers did not wear insignia. They did not openly carry arms. Their acts had criminal rather than military overtones. They were the agents of a radical political group, rather than a sovereign government." It was not an "insurrection" because "the PFLP did not intend to overthrow King Hussein when it hijacked the Pan American 747." It was not a "civil commotion" because "for there to be a civil commotion, the agents causing the disorder must gather together and cause a disturbance and tumult." It was not a "riot" because "the hijacking was accomplished by only two persons."[41]

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. In this regard, the court suggested, the history of property insurance and its roots in early marine policies had not served the insurers well. The Second Circuit dismissed the language of the Pan Am policy exclusions as being based on "ancient marine insurance terms," which, in the eyes of the Second Circuit, "simply do not describe a violent and senseless intercontinental hijacking carried out by an isolated band of political terrorists."[42]

"THE SPECIAL MEANING OF WAR": THE LEGACY OF *PAN AM*

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 opened in Beirut, Lebanon. In October 1975, conflict broke out in the neighborhood in West Beirut where the hotel was located between the Muslim Nasserist political party, the Mourabitoun, and the Christian right-wing party called the Phalange. 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.

On "Black Saturday," December 6, 1975, the fighting in Beirut escalated significantly and the Holiday Inn became a focal point for the combatants. 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. 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."[43]

Holiday Inn had insured its foreign properties through Aetna under an all-risk policy similar to the one that covered Pan Am's fleet; it provided coverage for "all risks . . . of direct physical loss or damage . . . from any external cause except as hereinafter provided." 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 with any political organization." In fact, Holiday Inn had agreed to higher premiums so that Aetna would include civil commotion coverage for their Beirut property. But the Holiday Inn policy still excluded any

losses or damage caused "directly or indirectly, proximately or remotely" by "war, 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." 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 was therefore excluded from Holiday Inn's coverage. Holiday Inn—like Pan Am before it—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.[44]

District judge Charles S. Haight Jr., who decided the Holiday Inn case in 1983 in favor of the hotel chain, relied heavily on the *Pan Am* precedent in his ruling. While Aetna had called various journalists to testify that the events in Beirut were widely regarded as a civil war, Haight rejected that testimony in favor of the assertion made by the Second Circuit in its *Pan Am* ruling that, "the specific purpose of overthrowing the constituted government and seizing its powers is a necessary element of both 'insurrection' and 'civil war.'" 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." 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." Instead, Haight ruled:

> 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.[45]

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. One of the most fascinating elements of the cases that crop up around these war exclusions is this phenomenon of US judges trying to sort out unbelievably complicated geopolitical conflicts, like the one in Beirut, that almost no one fully understood. The process of disputing these denied claims compels the legal system to sort out the most chaotic and uncontrolled stories—terrorist attacks, cyberattacks, civil unrest easing into civil war—and classify them within the tight confines of the language in insurance policies.

"Journalists and politicians invariably referred to these events in Lebanon as a 'civil war.' They do so today," Haight wrote toward the end of his ruling. 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." 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" quite different from how they might be used and understood by the general public. Unlike the courts that insisted, following Pearl Harbor, that any event that looked to an ordinary person like war should be considered as such for insurance purposes, 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, an approach in line with interpreting ambiguities in the coverage in favor of the policyholder, rather than the insurer. In *Stankus*, the Massachusetts Supreme Court had advocated for interpreting war under its "ordinary meaning," but Haight had no interest in the ordinary meaning of all-risk policy exclusions; he cared only about their insurance meaning.

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 and was even extended to other insurance contracts besides all-risk property policies. In July 2019, when the Ninth Circuit Court of Appeals reversed a ruling in favor of Atlantic Specialty Insurance Company, an entire section of the opinion authored by Judge A. Wallace Tashima was titled "The Special Meaning of 'War' in the Insurance Context." That case was brought by Universal Cable Productions, 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. Universal filed a claim with Atlantic under its television production insurance policy to cover the costs of interrupting and moving production, but Atlantic denied the claim, citing the four war exclusions in Universal's policy, which excluded coverage for losses caused by (1) war (including "undeclared or civil war"); (2) "warlike action by a military force"; (3) insurrection, rebellion, and revolution; and (4) "any weapon of war including atomic fission or radioactive force, whether in time of peace or war."[46]

A district court in California concluded in 2017 that Atlantic was correct in its assessment, and that the Hamas rockets fell under the first two exclusion categories of war and warlike action because "such a conflict easily would be considered a 'war' by a layperson." 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"—a provision presumably designed to help the insured rather than the insurers. The Ninth Circuit reversed the district court 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" those terms "by usage." 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." Since Hamas was not, in the court'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." 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. Tashima noted in the ruling that Hamas launched unguided missiles that were "likely used to injure and kill civilians because of their indiscriminate nature." Therefore, "Hamas' conduct consisted of intentional violence against civilians—conduct which is far closer to acts of terror than 'warlike action by a military force,'" Tashima concluded.

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 target civilians. Attribution of cyberattacks can be a slow and tricky endeavor, but at least in the case of NotPetya that process seemed to point unequivocally to the Russian government as the responsible party. 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" than an attack launched by a nonsovereign group like Hamas, Mourabitoun, or the PFLP.

On the other hand, while the perpetrator of NotPetya may have been a government, 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 intended targets with close ties to the ongoing Russia-Ukraine conflict. 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." Perhaps most important, for all the extensive damage NotPetya caused, it was not a violent attack. Unlike almost every other incident that has raised legal disputes on the meaning of war exclusions in insurance—from the sinking of the *Lusitania* and 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. To call a piece of computer code, no matter how destructive, an act of war when it resulted in no physical destruction or loss of lives would be to go against most people's common conceptions of what war looks like—and it would go against the special insurance meaning of war that had evolved in prior cases. 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 on CNN, but said explicitly, "I don't think it was an act of war."[47] 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, it fundamentally shut down computers and deleted data (much like the Sony Pictures breach) rather than causing broader physical damage, suggesting it still retained many more elements of an act of cyber sabotage than a violent

or warlike act. The key exceptions to this are the critical infrastructure targets of NotPetya, including the Ukrainian power grid, which did result in some clear kinetic consequences, 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. This, then, raises an interesting question of whether NotPetya was a single attack or whether each infiltration by the virus of an individual company or computer network should be seen as a separate attack—in which case the attack on Mondelez would seem even less in line with any definition of war.

MONDELEZ, NOTPETYA, AND CYBERWAR

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. 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." Mondelez promptly filed a claim with Zurich, following the attack, and provided its insurer with documentation of the malware and its impacts. On June 1, 2018, Mondelez received a letter from Zurich denying the claim on the grounds that NotPetya was excluded from its 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.[48]

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 life insurance dispute about Pearl Harbor. 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, 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 Pan Am, Holiday Inn, and Universal insurance policies, and 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 declaration. In the more recent property insurance disputes about war exceptions involving 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. 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. However, as in the *Pan Am*, *Holiday Inn*, and *Universal* cases, NotPetya primarily affected civilian targets 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. And unlike all of these conflicts, of course, NotPetya caused no direct physical damage to the policyholder's property. That didn't 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, 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. That process of attribution lasted months and took place during the nearly yearlong period between Mondelez's initial filing of an insurance claim and Zurich's denial of that claim. Beginning immediately after the NotPetya attacks in June 2017, Ukrainian officials and cybersecurity researchers cast blame for the attack on Russia. 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."[49] 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." Later that month, US cybersecurity company FireEye made a similar claim, with its head of global cyber intelligence, John Watters, telling the *Financial Times*, "we are reasonably confident" Russia was responsible for NotPetya, based on analysis of the targets, code, and malware infection vectors. "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."[50]

On February 14, 2018, the UK National Cyber Security Centre published a statement saying the Russian military was "almost certainly responsible" for NotPetya. 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, as did White House press secretary, Sarah Huckabee Sanders. Sanders's brief statement read, in its entirety:

> 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.[51]

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."[52] A

spokesman for the Russian government, Dmitry Peskov, denied the coordinated allegations and denounced them as "Russophobic."[53]

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's possible for a cyberattack attribution to be. The evidence pointing to Russia includes similarities between the NotPetya code and previous strains of malware attributed to Russia. 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 encrypt the hard drives of computers it infected. Instead, it overwrote the master boot records of those computers, making it nearly impossible for the files to be restored. 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 it required victims to send confirmation of their payments to a particular fixed email address. 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.[54]

These 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. This lack of financial motivation ruled out traditional cybercrime organizations and pointed to a state actor, either acting on its own or in coordination with outside agents (in which case the incident might seem less warlike). The attackers' 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. 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.[55] This focus on Ukraine aligned with earlier Russian cyberattacks that targeted 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."[56]

This political context—and even the language used to describe it—is relevant to Zurich's argument that NotPetya was a "warlike action." In July 2019, eight months after Mondelez filed its lawsuit against Zurich, the Ninth Circuit issued its ruling in the *Universal* case stating 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."[57] 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. 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." 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." But just because Zurich's interpretation of the war exclusion was unprecedented didn't 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)." In framing its argument this way, Mondelez implied that malware, at least when it is directed at a private company that operates no critical infrastructure, cannot constitute "hostile or warlike action" rather than that anything about the specific nature of NotPetya or the damage it incurred should be considered unwarlike.[58]

However, Mondelez's contention that "malicious code," or cyberattacks more generally, could not be considered warlike was at odds with the growing trend of recognition by nations and international organizations that

cyberattacks were rapidly becoming an integral part of warfare and that "incursions into computers" had the potential to cause serious damage, even physical damage. 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 and trigger a military response.[59] At the time, Stoltenberg did not point to any specific examples of known cyberattacks that had reached that level, but 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.

On March 29, 2017, just a few months before NotPetya hit Mondelez, an adviser for the Center for Strategic and International Studies, 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, it was "an example of precisely the type of cyber operation that could be seen as warfare."[60] 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's not hard to imagine Zurich building its case on statements like these. 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: "The release of NotPetya was an act of cyberwar by almost any definition."[61]

It is difficult to predict exactly how much weight such statements will carry in court. 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. 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 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 "journalists and politicians invariably referred to these events in Lebanon as a 'civil war'" on the grounds that it was irrelevant to determining whether the

conflict was a civil war in the "insurance meaning" of the words.[62] It seems entirely plausible that a court could similarly dismiss references to NotPetya as an act of cyberwar as irrelevant to the question of whether the cyberattack qualified as warlike in an insurance context.

One insurance broker, 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. "For a cyber-attack to reach the level of warlike activity, its consequences must go beyond economic losses, even large ones," McCabe wrote. Furthermore, he pointed out, "the 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."[63] As the representative of an insurance broker—an organization that helped customers purchase insurance policies—McCabe clearly had an interest in representing the interests of its clients 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: "if 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."[64]

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 interpreted in favor of coverage."[65] The *Pan Am*, *Holiday Inn*, and *Universal* rulings in favor of the policyholders rather than their insurers all supported this argument—that absent specific language excluding a certain scenario, courts were generally inclined to interpret the exclusions fairly narrowly. On the other hand, in a certain light, NotPetya could be viewed as fitting even that narrow definition because, unlike the Pan Am, Holiday Inn, and Universal incidents, 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." Similarly, the *Holiday Inn* ruling rested in part on the fact that "there was no 'war' in Lebanon between sovereign or quasi-sovereign states." Neither of those rationales quite fits 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." 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," so too a court could conceivably determine that it was a stretch to deem "warlike" the inflicting of damage on the civilian property of a multinational food company headquartered in Chicago, Illinois, far from Russia and Ukraine. Of all of these cases, it's hard not to view NotPetya as far and away the least warlike. After all, the Pan Am, Holiday Inn, and Universal incidents all involved the obvious, physical alteration of property and risk to human life in ways that NotPetya absolutely, unambiguously did not.

NO CLAW BACKS

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. 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. On July 18, 2018, Zurich sent Mondelez an email "formally rescind[ing]" its previous coverage denial and promising to resume work

on the claim. Then, in another email sent less than a week later on July 24, Zurich offered Mondelez a $10 million partial payment toward the company's insurance claim, which the insurer's head of property claims later promised would be "unconditional" and "not subject to a 'claw back' provision." However, that payment never materialized—nor did Zurich ever appear to resume work on the claim.[66]

Mondelez, in its complaint against Zurich, was 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. In particular, Mondelez hypothesized in the suit, Zurich feared the possibility of Mondelez taking legal action, as it would, indeed, ultimately go on to do. 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. If that was in fact the intention of those emails, then they seem to have worked, since Mondelez waited until October 2018 to file its lawsuit, more than four months after its initial claim was denied by Zurich. Mondelez later claimed that it "refrained to its detriment from instituting immediate litigation challenging the June 1, 2018 denial letter" because of the "explicit representations and promises from Zurich" made in the July 2018 emails from the insurer.[67]

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. Mondelez goes so far as to claim in its 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." 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 White House 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.[68]

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 of NotPetya inflicted on hundreds of companies affected 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. 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. 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 cyberinsurance providers such as Allianz and AIG—for $1.3 billion under its property insurance policies.[69] Merck's arguments for why the war exclusions did not apply to NotPetya closely mirrored Mondelez's and primarily centered on the claim that those exclusions were never intended to address cybersecurity incidents nor were they tailored to that purpose. "The 'war' and 'terrorism' exclusions do not, on their face, apply to losses caused by network interruption events such as NotPetya. . . . They 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," Merck argued in its lawsuit.[70]

These arguments hint at some of the ways NotPetya may reshape the cyber exclusions in property policies. But the incident had perhaps even more significant impacts on the exclusions written into stand-alone cyber policies. However, to construe policies that had been specifically marketed as protecting against cyber losses so that they excluded large and damaging cyberattacks was more problematic for insurers. Understandably, they were concerned about reassuring their customers that war exclusions would not prevent them from being able to exercise such policies. Some insurers even told policyholders and brokers they would not enforce war exclusions for cyber-related claims because they didn't want to "scare off customers."[71] 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. They note that, "unlike in traditional insurance settings, it is often difficult or impossible for cyber insurers to identify in coverage exclusions the causal mechanisms of potentially catastrophic cyber risks without eviscerating coverage for ordinary cyberattacks that policyholders demand."[72]

In order to reassure policyholders that stand-alone cyber policies would still be useful in the wake of NotPetya claim denials, insurers began to explicitly include coverage for "cyberterrorism" in stand-alone cyberinsurance policies, without ever quite clarifying how cyberterrorism differed from warlike acts. For instance, Zurich's stand-alone cyberinsurance 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.[73]

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 its war and civil unrest exclusion did not apply to "cyberterrorism." The policy defined cyberterrorism separately as:

> the 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.[74]

In a 2020 analysis of fifty-six cyberinsurance policies, Daniel Woods and Jessica Weinkle suggest that this emerging trend for cyberinsurance to affirmatively cover cyberterrorism had "weakened" the war exclusions in such policies.[75] 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—Sun Life

broadened its life insurance exception to apply to "war, whether declared or not" after Pearl Harbor, Aetna excluded hijackings following the explosion of Pan Am flight 093. 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 attempts to differentiate between cyberwar 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 of them are also aggressively developing and marketing cyberinsurance policies designed to cover other, closely related online threats. There is also still tremendous disagreement and uncertainty about what cyberterrorism actually looks like and what types of incidents would fall into that category, who the perpetrators of those attacks will be, and what kinds of damage they will cause.

One of the striking differences between the definitions of warlike actions and cyber terrorism in these cyberinsurance policies is that while the former relies primarily on attribution and being able to reliably identify whether 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 its 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 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.

This is a section of doi:10.7551/mitpress/13665.001.0001

Cyberinsurance Policy

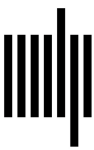
Rethinking Risk in an Age of Ransomware, Computer Fraud, Data Breaches, and Cyberattacks

By: Josephine Wolff

Citation:

Cyberinsurance Policy: Rethinking Risk in an Age of Ransomware, Computer Fraud, Data Breaches, and Cyberattacks
By: Josephine Wolff
DOI: 10.7551/mitpress/13665.001.0001
ISBN (electronic): 9780262370752
Publisher: The MIT Press
Published: 2022

The open access edition of this book was made possible by generous funding and support from MIT Press Direct to Open



The MIT Press

The MIT Press would like to thank the anonymous peer reviewers who provided comments on drafts of this book. The generous work of academic experts is essential for establishing the authority and quality of our publications. We acknowledge with gratitude the contributions of these otherwise uncredited readers.

This book was set in Bembo by Westchester Publishing Services.

Library of Congress Cataloging-in-Publication Data

Names: Wolff, Josephine, author.
Title: Cyberinsurance policy : rethinking risk in an age of ransomware, computer fraud, data breaches, and cyberattacks / Josephine Wolff.
Description: Cambridge, Massachusetts : The MIT Press, [2022] | Series: Information policy series | Includes bibliographical references and index.
Identifiers: LCCN 2021045988 | ISBN 9780262544184 (paperback)
Subjects: LCSH: Computer insurance. | Computer security—Management. | Cyberspace—Security measures—Management. | Computer crimes—Prevention. | Risk management.
Classification: LCC HG9963.5 .W65 2022 | DDC 658.4/78—dc23/eng/20220114
LC record available at https://lccn.loc.gov/2021045988